N° d'ordre : 616/IRS/TCO Année universitaire : 2019 / 2020

UNIVERSITÉ D'ANTANANARIVO

INSTITUT D'ENSEIGNEMENT SUPERIEUR ANTSIRABE VAKINANKARATRA (IES-AV)

MENTION TELECOMMUNICATION

MEMOIRE

en vue de l'obtention

du diplôme de :

Grade : MASTER

Titre : INGENIEUR

Domaine : Science de l'Ingénieur
Mention : Télécommunication

Parcours : Radiocommunications

Par : RABEMANANTSOA Mihaja Narindra

Titre : ETUDES ET MISE EN PLACE DE SUPERVISION RESEAUX ET SYSTEMES

Soutenu le 03 Septembre 2021 à la salle de réunion Vatofotsy Antsirabe-I devant la commission d'examen composé par :

Président de Jury	***:***	M. ANDRIANAIVONDRIAKA Nirina Alain, Docteur en Télécommunication
Examinateurs	***:***	M. RAKOTONIRINA Hariniony Bienvenu, Docteur en Télécommunication
		M. RAKOTONDRAMANANA Radiarisainana Sitraka, Docteur en Télécommunication
		M. RATIANARIVO Paul Ezekel, Docteur en Systèmes et Dispositifs Electroniques
Directeur de mémoire	***:***	M. ANDRIAMIADANOMENJANAHARY Harivelo Chandellina Camille, Docteur en Sciences Cognitives et Applications

TENY FISAORANA

Ho an' Andriamanitra irery ihany ny voninahitra noho izao andro nomeny ahy izao ka nahafahako manao izao fanolorana ny vokam-pikarohana atolotro izao.

Fisaorana lehibe no atolotro ho :

- Professeur RAVELOMANANA Mamy Raoul, filohan'ny anjerimanotolo Antananarivo.
- Professeur RAJAONARISON Eddie Franck, talehan'ny IES-AV.
- Andriamatoa RANDRIANANDRASANA Marie Emile, « Maître de conférences », filohan'ny sampana « Télécommunication » eto amin'ny IES-AV.
- Andriamatoa ANDRIAMIADANOMENJANAHARY Harivelo Chandellina Camille, « Docteur en Sciences Cognitives et Applications », tale ny fanohana-kevitra, na dia teo aza ny andraikitra maro izay nosahaniny dia teo fona izy nandany fotoana, toro-hevitra ary nitondra fanatsarana izao fanohana-kevitra izao.

Fisaorana lehibe ihany koa ho an'ireo fikambanan'ny mpitsara izay hanome ireo heviny amin'izao boky izao sy ny fanatrehana izany :

- Andriamatoa ANDRIANAIVONDRIAKA Nirina Alain, « Docteur en Télécommunication »
- Andriamatoa RATIANARIVO Paul Ezekel, « Docteur en Systèmes et Dispositifs Electroniques »
- Andriamatoa RAKOTONDRAMANANA Radiarisainana Sitraka, « Docteur en Télécommunication »
- Andriamatoa RAKOTONIRINA Hariniony Bienvenu, « Docteur en Télécommunication ».

Mankasitraka ireo mpampianatra, ary ny mpiaramiasa ao amin'ny « Institut d'Enseignement Supérieur Antsirabe Vakinankaratra » izay niara-nisalahy tamiko, ary indrindra ireo mpampianatra ao amin'ny « mention Télécommunication » izay, nitoto nahafotsy sy nahandro nahamasaka, raha tsy nisy azy ireo dia tsy tomombana ireo fahalalana izay noratoviko nandritra izay fotoana nampianaran'izy ireo izay.

Fisaorana mitafotafo no atolotro ho an'ireo Ray aman-dReniko satria izy ireo no masoandro amambolana, vovonana iadiany loha, nanohana ahy ara-bolasy ara moraly tamin'izao fianarako izao, kiady sy voninahitra, satria ny hazo hono no vanon-ko lakana dia ny tany naniriany no tsara.

REMERCIEMENTS

Gloire au Seigneur de m'avoir permis de vivre ce jour de présentation de mon mémoire de fin d'étude en ingénieur.

J'annonce mes sincères remerciements à :

- Professeur RAVELOMANANA Mamy Raoul, Président de l'Université d'Antananarive.
- Professeur RAJAONARISON Eddie Franck, Directeur de l'Institut d'Enseignement Supérieur Antsirabe Vakinankaratra.
- Monsieur RANDRIANANDRASANA Marie Emile, Maître de conférences, Chef de la mention Télécommunication au sein de l'IES-AV.
- Monsieur ANDRIAMIADANOMENJANAHARY Harivelo Chandellina Camille, Docteur en Sciences Cognitives et Applications, mon directeur de mémoire, malgré ses lourdes tâches il a toujours pu partager son temps ses conseils et ses critiques au cours de la préparation de cette ouvrage. Ma gratitude lui est toujours destiner.

Mes remerciements vont aussi aux membres du Jury qui ont bien voulu émettre leurs opinions dans la valorisation et l'évaluation de cet ouvrage en tant qu'examinateurs :

- Monsieur ANDRIANAIVONDRIAKA Nirina Alain, Docteur en Télécommunication
- Monsieur. RATIANARIVO Paul Ezekel, Docteur en Systèmes et Dispositifs Electroniques
- Monsieur RAKOTONDRAMANANA Radiarisainana Sitraka, Docteur en Télécommunication
- M. RAKOTONIRINA Hariniony Bienvenu, Docteur en Télécommunication.

Mes vifs remerciements s'adressent également à tous les enseignants et personnels de l'Institut d'Enseignement Supérieur Antsirabe Vakinankaratra au complet et ceux de la mention Télécommunication en particulier car, sans leurs appuis ma connaissance n'aurait pas pu aboutir vers cette présentation de mon mémoire de master.

Je souhaite également remercier les personnes les plus importantes de ma vie, mes parents, leurs soutiens durant toutes ses années d'étude me sont plus chers. Si aujourd'hui j'ai pu bénéficier de mes études c'est encore de leurs travaux et de leurs bien vaillances. Cependant, je ne pourrais oublier ceux qui m'ont aidé à l'aboutissement de ce livre.

TABLE DES MATIERES

NOTATIONS ET ABREVIATIONS

1. Majuscules latines

$X(t)$	Nombre moyenne de client
T	Durée moyenne de service
$P_0(t)$	Probabilité transitoire
$P_0(\infty)$	Régime transitoire par rapport à la probabilité transitoire
I_e	Lapse de temps d'exécution
I_r	Ensemble des intervalles dans un état de fonctionnement
I_{bi}	Ensemble d'intervalle d'état bloqué avec un réveille ou en marche direct
I_{bd}	Ensemble des intervalles des états bloqués en réveillent direct
$O(n)$	Complexité globale

2. Minuscules latines

C_b^2	Coefficient de variation
t	Temps de trajet
$z(t)$	Processus de diffusion approximation
u	Durée inter-arrivée moyenne

3. Minuscules grecques

λ	Taux d'arrivé
π	Valeur de phase (3,14…)

4. Majuscules grecques

Δ	Variation

5. Notations spéciales

$\boldsymbol{\Phi(z)}$	Densité de probabilité

6. Abréviations

API	Application Programming Interface
ARP	Address Resolution Protocol
ARPANet	Advanced Research Projects Agency Network
ATA	Advanced Technology Attachment
CDN	Content Delivery Network
CDS	Cisco Discovery Protocol
CLI	Command-Line Interface
CPU	Central Processing Unit
DAS	Direct Attached Storage
DDP	Datagram Delivery Protocol
DNS	Domain Name Service
DOS	Denial Of Service
DSM	Disque Station Manager
FAI	Fournisseur d'Accès à Internet
FBI	Federal Bureau of Investigation
FTP	File Transfer Protocol
GNS3	Graphical Network Simulator
GUI	Graphical User Interface
HP	Hewlett-Packard
HTML	HyperText Markup Language

IAAS	Infrastructure As A Service
IDS	Intrusion Detection Systeme
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IT	Information Technology
IPX	Internet Packet eXchange
iSCSI	Internet Small Computer Systems Interface
LAN	Local Area Network
LXC	LinuX Containers
MIB	Management Information Base
MRTG	Multi Router Traffic Grapher
NAS	Network Area Storage
NASA	National Aeronautics and Space Administration
NAT	Network Address Translation
NFS	Network File System
NTFS	New Technology File System
OS	Operating System
PAAS	Platform As A Service
PC	Personal Computer

PHP	Preprocessor HyPertext
PNG	Portable Network Graphics
PRTG	Paessler Router Traffic Grapher
RFC	Request For Comments
RRD	Round-Robin Database
SAAS	Software As A Service
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSH	Secure SHell
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UML	Unified Modeling Language
VM	Virtual Machine
VNE	Virtual Network Editor
WAN	Wide Area Network
WIFI	Wireless Fidelity
WOL	Wake On LAN
WWW	World Wide Web

LISTES DES TABLEAUX ET DES FIGURES

1. Liste des tableaux

2. Liste des figures

INTRODUCTION GENERALE

Le monde de l'informatique ne cesse de croitre en termes de performance et de qualité de service. Les entreprises cherchent des réseaux et systèmes qui leurs permettent de faire des économies. Les sociétés demandent également des produits simples en termes de déploiement, donc elles souhaitent un environnement sans encombrement, qui ne demande pas trop de place.

La performance du système d'information d'une entreprise est d'une importance capitale pour son efficacité et son bon fonctionnement. La recherche de cette performance entraine de plus en plus l'utilisation d'un système informatique pour la gestion quotidienne des informations.

Des modes de services sur internet sont en vents sur le marché de la technologie moderne. De nos jours, les services donnés sont liés à internet, donc il faut quand même un investissement à long termes. Les ingénieurs étudient la faisabilité du besoin de l'entreprise, étudient les matériels nécessaires, évaluent si des services externes sont obligatoires ou pas. Ils analysent les gains et les pertes à long termes. Quel type d'implémentation un réseau local va-t-il avoir besoin pour une supervision à distance ? Quel genre de technologie va pouvoir offrir à un administrateur cette opportunité ?

Dans ce travail, des recherches ont été faites par rapport aux différentes technologies de pointes au niveau de la mise en place des réseaux informatiques, des moyens de surveillance du réseau et système. Le service d'hébergement réseau est l'un des services disponible via internet, bien d'autre se vende et retrouve des clients particuliers. C'est pour cela que dans cette étude on parle de Cloud et de ses services. On y parle également de la supervision informatique des réseaux et systèmes, par des logiciels qui sont de nos jours plus qu'incontournable.

Nous avons quatre chapitres qui mènent vers le déploiement d'une supervision réseau quelconque.

Dans le premier chapitre, il y l'étude préalable et l'état de l'art d'un environnement cloud où les échanges et les services d'information à distance est en voie d'expansion importante. L'étude de ses plateformes aidera à trouver quel genre de technique est favorable pour une entreprise.

Le second chapitre sera, la solution et conception de notre propre environnement de travail. L'existence des plateformes de monitoring de réseau et de système est très efficace en termes d'analyse de performance du réseau lui-même.

Le troisième chapitre parle de la réalisation et mise en place de la supervision réseaux. Plusieurs plateformes de déploiement de réseau et système ont été installés afin d'établir un environnement stable pour réussir l'étude.

Le dernier chapitre montre la simulation du projet est essentiellement la représentation, l'interprétation, et la perspective d'avenir de notre supervision réseau personnalisée. S'en suit alors des implémentations complémentaires de la surveillance d'un réseau et système local. Vue l'avancée et la modernité qu'offrent les appareils Android, on n'a pas pu s'en passé de cette technologie. La réalisation se porte sur une mise en place d'un réseau local quelconque et d'assurer la supervision de celui-ci par un des logiciels de monitoring qu'on trouve plus pratique. Pour commencer, voyons la première partie du développement sur l'étude des avancées technologiques.

CHAPITRE 1
ETUDE PREALABLE ET ETAT DE L'ART DES NOUVELLES TECHNOLOGIES DE COMMUNICATION

1.1 Introduction

Dans un monde qui suit le développement technologique on ne peut s'en passer des innovations qui s'optimisent régulièrement. Plusieurs technologies de pointes se vendent sur le marché électronique chaque jour, avec des versions stables que ceux encours de test par des communautés open source. Des versions gratuites sont également échangées afin de permettre aux internautes ou des petits intellectuels à promouvoir les produits.

Il faut savoir quand même que des produits sont déjà stables et plus commercialisés et offrent plusieurs opportunités à tous types d'utilisateurs. Dans cette partie, il existe différent technologie de pointe qui a favorisé la communication et échange d'information à distance.

1.2 Cloud

L'image du Cloud est utilisée de façon métaphorique pour désigner internet. Cette technologie permet aux entreprises d'acheter des ressources informatiques sous la forme de service, de la même manière que l'on consomme de l'électricité, au lieu d'avoir à construire et entretenir des infrastructures informatiques en interne. Cette comparaison date de l'époque à laquelle les infrastructures gigantesques des fermes de serveurs internet se présentent sous la forme d'un grand nuage blanc, en acceptant les connexions et distribuant des informations tout en flottant [1.01].

Il existe plusieurs types de service qui différentie les fournisseurs de cloud.

- IAAS (Infrastructure As A Service) : Seule l'infrastructure matérielle est externalisée.
- PAAS (Platform As A Service) : L'externalisation concerne l'infrastructure matérielle, les données et les applications.
- SAAS (Software As A Service) : Le tout-compris qui inclut l'externalisation complète, la mise en fonctionnement et la maintenance. [1.02] Il s'agit de la formule la plus courante.

En sachant les services et les dispositions qu'offrent cloud dans le monde de l'avancement technologique. La méfiance et le doute se pose toujours dans chaque utilisateur.

Quelle technologie du monde moderne est favorable pour le bon fonctionnement de l'entreprise et qui assure un bon service de long terme ?

1.2.1 Guide des entreprises à utiliser cloud

Le Cloud Computing d'entreprise est guidé par la réduction des coûts, mais également par les changements du monde extérieur, au-delà du monde de l'entreprise dans notre société hyper-connectée. L'avènement de Consumer IT ou du Web 2.0, des réseaux sociaux et de l'Internet des Objets transforment la façon de vivre, d'apprendre, de collaborer, de travailler, de consommer et même de jouer. Ces changements dans la société transforment également la façon de concevoir et de gestion dans les entreprise, ils incluent également une chaîne de valeur à tout un chacun.

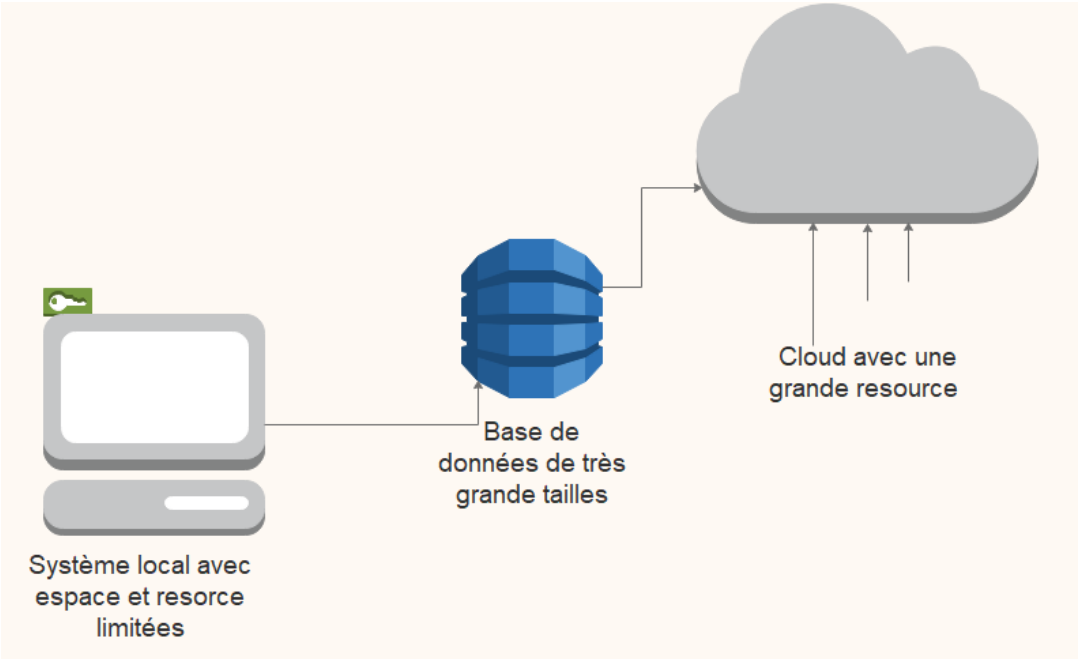


Figure 1.01: *Transfert de données locales vers cloud*

1.2.2 Avantages et inconvénients du cloud dans une entreprise

Autant qu'outils de travail, de communication et d'échange d'information, cloud représente des forces de nécessité et des faiblesses qui lui rend moins intéressant par moment.

1.2.2.1 Avantages du cloud au sein de l'entreprise

Cette technologie offre plusieurs avantages et des bénéfices pour les utilisateurs professionnels et les utilisateurs finaux.

Les trois principaux avantages sont :

- L'approvisionnement en libre-service ; l'approvisionnement en libre-service permet aux utilisateurs finaux d'accéder à n'importe quelle ressource informatique à la demande.

- L’élasticité de service ; L’élasticité offre l’opportunité d’augmenter ou de réduire la consommation de ressources en fonction des besoins de l’entreprise.
- Le paiement à l’utilisation **;** c’est-à-dire que les utilisateurs ne paient que l’espace dont ils ont besoin ou à l’utilisation, l’utilisateur est autorisé par les firmes à ne payer que pour les ressources consommées.

Il existe encore d’autre avantage qui ne laisse pas les entreprises et les grands consommateurs indifférents comme ;

a. Coûts

Les coûts des « Data Centers » et des services informatiques peuvent être réduits et établis de manière proportionnelle à l’utilisation**.** Selon la quantité d’usage, les coûts seront plus ou moins élevés grâce à l’élasticité rapide.

b. Sécurité et la garantie aux risques

Les dépenses et les prises de risques pour l’innovation peuvent être considérablement réduites grâce au « Cloud Computing ». Ainsi, les entreprises peuvent prendre des paris plus risqués et tester davantage de nouvelles idées. Les nouveaux projets peuvent être soutenus directement s’ils prennent de l’envergure, ou abandonnés s’ils échouent**.** La stabilité et l’élasticité offre aux entreprises des possibilités inédites pour essayer de nouvelles idées d’activités et pour les développer si elles s’avèrent pertinentes.

c. Ouverture au développement uniforme au monde de la technologie

Aujourd’hui, les chaînes de valeur des entreprises sont composées d’environ 20 entreprises. Le « Cloud Computing » permet à une entreprise de collaborer d’une nouvelle manière avec ses partenaires commerciaux. Or, la collaboration est la clé vers l’obtention d’avantages compétitifs au sein de la chaîne de valeur.

En développant des espaces de travail partagés au sein des Communautés Clouds, les employés d’entreprises multiples peuvent travailler ensemble au sein d’un réseau d’entreprise virtuel comme s’ils travaillaient pour une seule et même compagnie. Ils participent tous au sein du même système de création de valeur, et partagent leurs ressources de communication, d’information et d’informatique.

1.2.2.2 Inconvénients du cloud au sein de l'entreprise

Pour de nombreuses personnes, le stockage local utilisé pendant les dernières décennies demeure aujourd'hui supérieur au Cloud Computing. Ces personnes considèrent qu'un disque dur permet de garder les données et les programmes physiquement proches, autorisant un accès rapide et simplifié pour les utilisateurs de l'ordinateur ou du réseau local.

Une illustration se présente, en 2013, l'ancien roboticien de la NASA ou « National Aeronautics and Space Administration » Randall Monroe a tenté de prédire, quand la bande passante d'internet surpasserait celle de FedEx. Pour cause, peu importe la vitesse d'une connexion internet, il reste moins cher d'envoyer des centaines de giga-octets de données via les avions et les camions de FedEx que par internet. Après réflexion, sa prédiction porte sur l'année 2040.

En lisant cette conclusion, Cory Doctorow a perçu une critique implicite du Cloud Computing de la part de Monroe. Selon lui, la vitesse et le coût du stockage local sont moins élevés qu'une connexion en réseau contrôlée par une entreprise de télécommunications.

En voyant cela, il est possible que l'évolution du stockage des données avec cloud pourrait s'avérer être à un terme défini dans un future plus ou moins proche. Cependant, plus d'inconvénient se présente dans le marché, mais les entreprises sont quand même tentées faute de besoin plus vaste. Ainsi plusieurs défaillances sont laissées à régler dans le futur.

a. Confiance au producteur de service

C'est le principal reproche émis à l'égard du Cloud. Les télécoms, les entreprises de médias et les FAI (ou Fournisseur d'Access Internet) contrôlent l'accès. Faire entièrement confiance au Cloud signifie également croire en un accès continu aux données sans aucun problème sur le long terme. Un tel confort est envisageable, mais son coût est élevé. De plus, ce prix continuera d'augmenter à mesure que les fournisseurs de Cloud trouvent un moyen de faire payer plus cher en mesurant par exemple l'utilisation du service. Le tarif augmente proportionnellement à la bande passante utilisée.

En dehors de ce problème de confiance, de nombreux autres arguments s'opposent au Cloud Computing. Le cofondateur d'Apple, Steve Wozniak, a ainsi critiqué le Cloud en 2012 en présageant de nombreux problèmes de grande envergure dans les cinq années à venir. On peut par exemple redouter des crashs. Durant l'été 2012, Amazon a rencontré ce type de problème. En tant

que fournisseur d'entreprises comme Netflix ou Pinterest, l'entreprise américaine a ainsi provoqué la mise hors service des plateformes de ces clients. En 2014, Dropbox, Gmail, Basecamp, Adobe, Evernote, iCloud et Microsoft ont rencontré des problèmes similaires. En 2015, ce fut le tour de Apple, Verizon, Microsoft, Google et Microsoft. Ces désagréments ne durent généralement que quelques heures, mais représentent une perte d'argent colossale pour les entreprises affectées.

b. Problème de propriété intellectuelle

Par ailleurs, Wozniak a exprimé ses inquiétudes concernant la propriété intellectuelle. Il est en effet difficile de déterminer à qui appartiennent les données stockées sur internet. On peut prendre pour exemple les nombreuses controverses survenues au sujet des changements de conditions d'utilisation de sites dérivés du Cloud comme Facebook ou Instagram. Ces réseaux sociaux créent la polémique en s'octroyant des droits sur les photos stockées sur leurs plateformes. Il y a également une différence entre les données mises en ligne et les données créées directement au sein du Cloud. Un fournisseur pourrait aisément revendiquer la propriété de ces dernières. La propriété est donc un facteur à prendre en compte.

Aucune autorité centrale ne gouverne l'usage du Cloud pour le stockage et les services. L'Institute of Electrical and Electronics Engineers (IEEE) tente de devenir cet organe régulateur. En 2011, il a créé l'IEEE Cloud Computing Initiative, visant à établir des standards pour l'utilisation, particulièrement dans le domaine des entreprises. Pour l'heure, les règles sont encore floues et les problèmes se règlent au cas par cas.

1.3 Backup cloud

Cloud se divise en plusieurs types de service selon le besoin de l'entreprise et le mode de consommation de ressource qui a été vu au-dessus. Il peut alors offrir la récupération et le sauvegarde des données à tout moment. Il existe plusieurs plateformes de développement pour cela. Il y a de nombreuse technique de sauvegarde de données ou d'utilisation de ressource.

En informatique, la sauvegarde est l'opération de copie préventive de données sur un support indépendant. Elle a pour but de mettre en sécurité des informations et de pallier toute éventualité de panne matérielle, d'infection par un logiciel malveillant, et de suppression volontaire ou fortuite. L'utilité de la sauvegarde est de pouvoir restaurer le plus rapidement possible un système après une défaillance ou un incident.

Il est facile et commun de réaliser une sauvegarde partielle de ses données : en copiant régulièrement ses documents privés, photos, vidéos, sur un disque dur externe.

Toutefois, il s'agit rarement d'une méthode de sauvegarde sûre, car les données originales et leur copie demeurent stockée au même endroit. Si en cas d'erreur matérielle sur un des disques, on pourra récupérer les données sur l'autre, l'ordinateur et le disque dur restent soumis aux mêmes risques extérieurs (inondation, incendie...).

1.3.1 Généralité sur la sauvegarde

Dans un milieu professionnel, la sauvegarde est généralement plus globale, et vise à préserver une copie de l'ensemble des données des systèmes en réseau, à partir du serveur. Elle est un impératif pour limiter les pertes économiques en cas de dommages informatiques, et elle fait gagné en productivité en proposant notamment la récupération de versions précédentes des documents. La sauvegarde est un domaine très important pour les entreprises qui possèdent des milliers de données. Plusieurs entreprises se reposent sur la capacité de gestion leurs bases de données.

1.3.1.1 Critères de sauvegarde

Quelle que soit la stratégie de sauvegarde souhaitée, il existe plusieurs critères à prendre en compte lors de sa conception :

- la capacité de stockage nécessaire ;
- la fiabilité du support ;
- la vitesse de transfert des données ;
- la facilité à restaurer les données ;
- le besoin de récupérer les différentes versions des documents.

Cependant il existe une option de sauvegarde qui pourra rendre le travail plus facile et plus sécurisé dans un autre point de vue.

1.3.1.2 Option de la sauvegarde en ligne

De nos jours, on observe aussi bien pour les particuliers et pour les entreprises une tendance à la sauvegarde « en ligne ». En hébergeant les copies des fichiers sur un serveur en ligne, on remet la responsabilité de la redondance des données et de la surveillance du matériel, sur les épaules du prestataire de services.

Généralement, le coût de ces prestations est très abordable, et dispose de plusieurs avantages :

- Pouvoir accéder facilement aux données depuis n'importe quel périphérique connecté à Internet,
- Répondre à la règle de séparation physique du stockage des données, et donc minimiser le risque de perte en passant par un prestataire spécialisé dans le domaine.

1.3.2 Définitions à mettre en avant

Il existe des définitions qui pourraient mettre les gens dans une confusion lors ce qu'une discussion est mise sur la table. Ses deux mots pourraient mettre en désordre l'idée finale lors d'un échange d'information alors aussitôt fixer la différence.

1.3.2.1 Archive

Un emplacement plus sure et plus sécurisé à fin de stocker des données ou autre documents à utiliser plus tard ou dans un moment précis. Cet emplacement est de grande taille ou selon le besoin.

1.3.2.2 Backup

Semblable à un archive, cependant l'espace est utilisée pour faire une copie conforme à un document ou fichier que l'entreprise possède. Dans un court ou long terme le backup permettra à récupérer un fichier ou autre document intacte si jamais ce dont elle avait utilisé est infecté ou perdu.

1.3.3 Docker

Le docker est un logiciel flexible et offre plusieurs fonctionnalités dont les techniques de manipulation donnent des ouvertures à plusieurs autres possibilités.

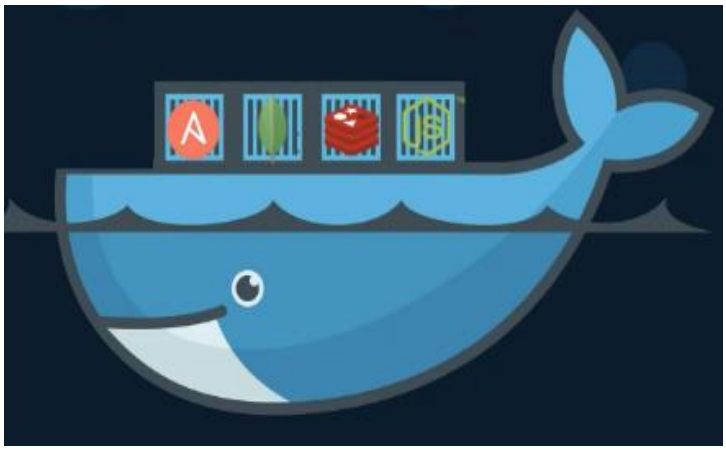


Figure 1.02 : *Image représentant docker*

Le terme « Docker » désigne plusieurs choses :

- Le projet d'une communauté Open Source,
- Les outils issus de ce projet Open Source,
- L'entreprise Docker Inc. qui constitue le principal soutien de ce projet, ainsi que,

Les outils que l'entreprise prend officiellement en charge. Docker est donc l'ensemble des technologies et une entreprise qui partagent le même nom, cela peut prêter à confusion [1.03]. Surtout que l'on ne peut quand même les séparés.

1.3.3.1 Conteneur

C'est une virtualisation des cloisonnements au niveau de l'OS, c'est-à-dire qu'en partageant le même noyau, le conteneur fait fonctionner des environnements linux indépendant les uns des autres dans plusieurs partie qui se trouve dans un même noyau. Cette partie est le conteneur lui-même.

1.3.3.2 Mode de fonctionnement

Le conteneur virtualise l'environnement d'exécution tell les processeurs, la mémoire vive ou le système de fichier et ne virtualise pas la machine. Il s'exécute principalement dans deux fonctionnalités linux LXC : LinuX Conteneur.

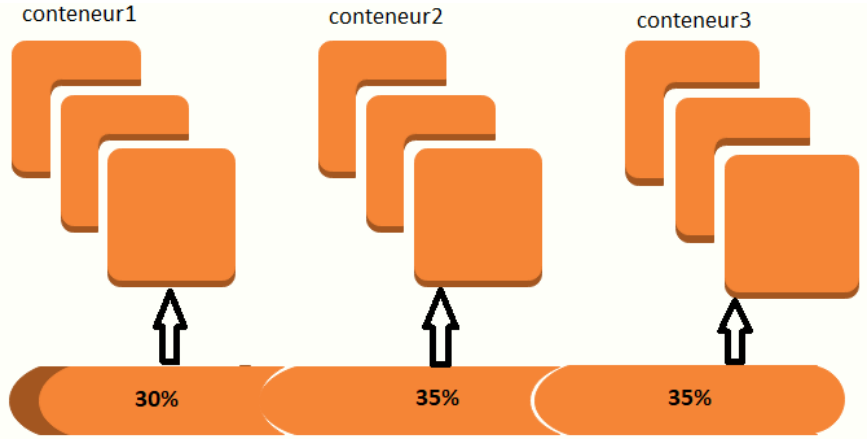


Figure 1.03 : *Distribution de ressource par conteneur*

La technologie Docker utilise le noyau Linux et des fonctions de ce noyau, telles que les groupes de contrôle cgroups et les espaces de noms, pour séparer les processus afin qu'ils puissent s'exécuter de façon indépendante. Cette indépendance reflète l'objectif des conteneurs : exécuter plusieurs processus et applications séparément les uns des autres afin d'optimiser l'utilisation de

votre infrastructure tout en bénéficiant du même niveau de sécurité que celui des systèmes distincts.

Les deux principales fonctionnalités de linux LXC sont :

- La fonctionnalité des groupes, qui permet de limiter et d'isoler l'utilisateur des ressources.
- La fonctionnalité de cloisonnement des espaces de nommage.

1.3.3.3 Caractéristiques du conteneur

Il se caractérise par la couche intermédiaire du contrôleur. Le contrôleur gère un ensemble de fonctionnalité pour les conteneurs.

- L'interaction des conteneurs avec l'OS,
- La sécurité par la gestion de privilège et de ressource,
- La duplication et la suppression du conteneur,
- L'accessibilité des conteneurs à travers les API et CLI,
- La migration ou la portabilité des conteneurs,
- La possibilité de simuler différent de celui de l'OS hôte.

Docker est alors une technologie de virtualisation par conteneur reposant sur la LXC de linux, il permet de créer des conteneurs qui vont uniquement contenir des applications avec leur dépendance. Ces conteneurs permet d'embarquer des applications dans l'OS hôte mais de manière virtuellement isolé.

Le docker engin fait tourner le conteneur et joue le rôle de contrôleur. Docker Engine donne accès au noyau du système d'exploitation hôte et est capable de créer, de démarrer et d'arrêter des conteneurs.

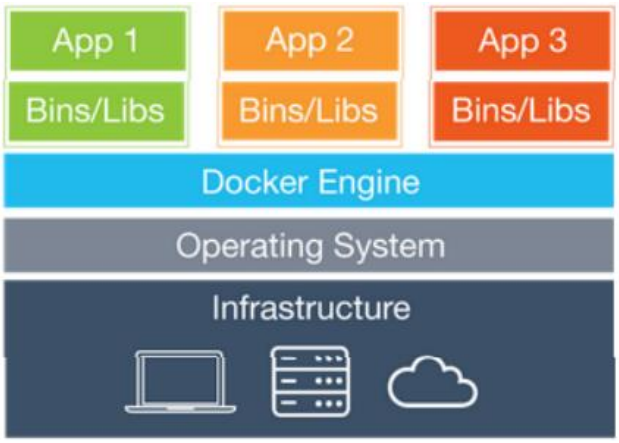


Figure 1.04 : *Architecture d'un conteneur Docker*

Étant donné que Docker utilise le noyau du système d'exploitation hôte, une image Docker est beaucoup plus petite qu'une machine virtuelle.
Les conteneurs Docker peuvent fonctionner sur n'importe quel ordinateur sur lequel Docker Engine a été installé.

1.4 Scénarios de mise en place de bon fonctionnement de réseau et système

En cherchant des outils et des techniques pour la bonne gestion du réseau et système de communication informatique, des difficultés se présentent en termes de choix.

1.4.1 Premier scénario

Il existe plusieurs infrastructures physiques qui suivent des normes bien avancées, elles sont livrées avec des configurations déjà dans les normes avec des notifications bien compréhensibles même pour des personnes qui ne sont pas dans le domaine.

Plusieurs types de système de stockage connecté directement aux serveurs/machines se vendent en unité dans le marché de la technologie telle :

- NAS ou « Network Area Station »
- DAS ou « Direct Attached Storage »
- SAN ou « Storage Area Network »

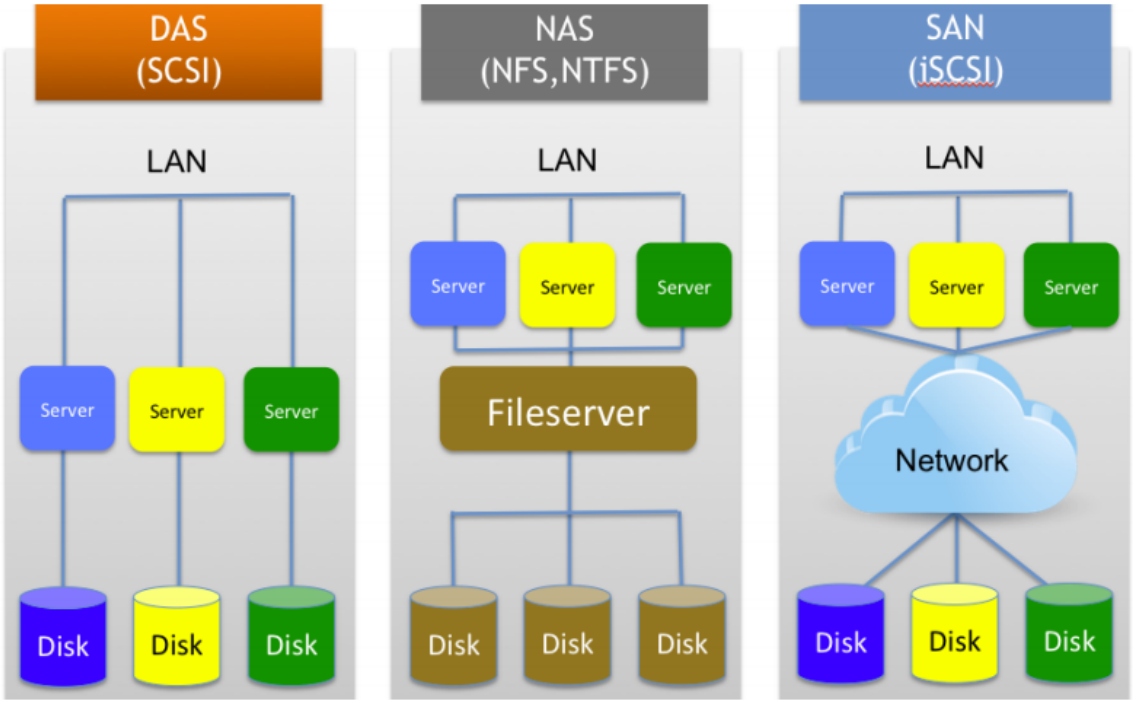


Figure 1.05 : *Dispositions du système de stockage par rapport aux serveurs*

Comme ce qui se présente dans la figure ci-dessus, ces systèmes de stockages se distinguent par des systèmes d'interface tels SCSI ou « Small Computer System Interface » pour DAS et iSCSI ou « Internet Small Computer Systems Interface » pour SAN. Tant dis que NAS exploite les fichiers NFS ou « Network File System » et NTFS ou « New Technology File System ».
Le NAS sera l'objet d'étude dans cette partie.

1.4.1.1 NAS

Le N.A.S ou « Network Area Storage » est un serveur de stockage en réseaux. En effet, c'est un boitier dans laquelle un disque dur va être insérer et ensuite il va être connecté à ce boitier au réseau local au niveau du routeur de l'entreprise. [1.04]
Tous les appareils qui vont se connecter au même réseau que NAS vont pouvoir utiliser, modifier et télécharger tous les fichiers qui s'y trouvent.

C'est un appareil révolutionnaire dont des configurations évolutives sont possible, avec les nouvelles technologies software, synology, les producteurs de NAS favorisent plusieurs implémentations et services livrés avec le matériel. Des plateformes y sont préconfigurés, il faut juste que le client l'active lui-même selon ses besoins.

Figure 1.06 : *Représentation matérielle d'un NAS*

a. Configurations sur NAS

Comme tout serveur existant, il est possible de mettre en place toute configuration qui convient à l'entreprise sur le NAS. Cela revient à l'administrateur d'y permettre, d'empêcher ou d'y limiter

l'accès. Au lieu d'avoir un disque dur externe qui peut se connecter uniquement à un seul appareil, il est faisable d'avoir un NAS qui se trouve dans un endroit et toutes les personnes connectées aux mêmes réseaux vont pouvoir accédées à ses données.

Il se pourrait également que l'administrateur y configurer docker qui est bien connu comme ce qui est noté auparavant une virtualisation plus légère. Donc aves des hébergements illimités grâce aux conteneurs du docker aux différents usages. Cependant il faut bien savoir gérer l'espace du disque.

Il se pourrait par exemple que des entreprises vont faire tourner des logiciels de « smart-com » donc des systèmes domotique branchés directement sur le NAS, pour éviter de payer un prestataire externe.

Il faut remarquer quand même que NAS est un produit de distribution linux. Grace à cela, des ingénieurs vont pouvoir développer ces capacités en adaptant aux besoins de l'entreprise.

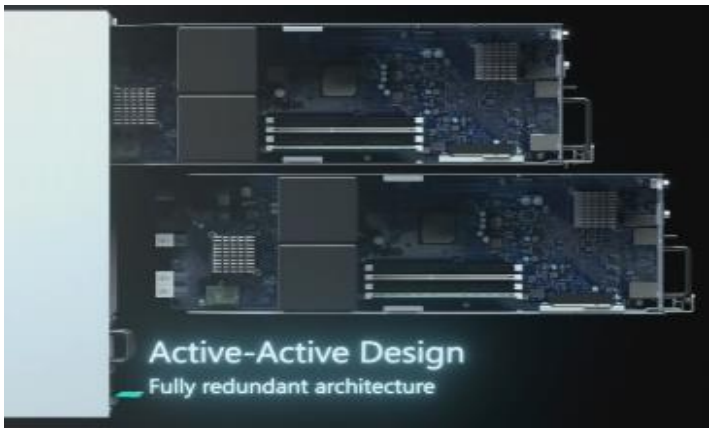


Figure 1.07 : *Mode d'activation d'un redondant sur le NAS afin de sauvegarder le NAS lui-même.*

Figure 1.08 : *Place de configuration de sécurité afin de limiter l'espionnage.*

b. Avantages

NAS est très intéressants pour les entreprises qui souhaitent utiliser beaucoup de fichier et qui souhaitent collaborer avec différents employés.

On peut stocker n'importe quel fichier dans un NAS, il existe plusieurs applications qui facilitent l'usage de NAS qui sont gratuits.

Par exemple, l'utilisateur possède un pc sous Windows, il existe une application qui s'appelle active backup, qui va lui permettre de sauvegarder en entier son pc.

Pour ce faire il télécharge une application sur le Windows source est d'activer cette application lors de la connexion avec le NAS et le NAS lui-même va créer un fichier de sauvegarde en heure bien précise.

Il existe des fonctionnements sous DSM « Disque Station Manager » pour linux. DSM est l'OS de NAS qui est un produit synology donc très développé en termes de produit software, qui sera très facile à utiliser pour les utilisateurs.

NAS va pouvoir remplacer le service de cloud, car il va pouvoir servir de cloud privé à l'entreprise ou à une famille dans le besoin, dont le stockage se trouvera au bureau ou à la maison.

En termes de sécurité et de confidentialité, NAS est très fiable par rapport aux autres services de cloud traditionnel car l'administrateur du réseau est la seule entité qui entre en contact avec les données qui s'y trouve.

Il existe des modes de sécurisation dont le producteur du produit propose aux utilisateurs de NAS afin que les hackers ne puissent s'y connecter.

Fini la facturation de l'emplacement des bases des données privées dans les cloud traditionnel, L'entreprise peut faire de l'économie sur les termes de service qu'offre les autres services de cloud. Et il pourra également faire une économie d'avenir plus sure vers une autre technologie de pointe plus futuriste.

c. Inconvénients

Le NAS est sans disque dur, et donc il faut acheter un disque dur selon le besoin de la société. Cependant il faut choisir des disques durs qui sont compatibles à NAS.

En plaçant le NAS près du routeur, les utilisateurs vont pouvoir s'y connectés en temps voulus, cependant la connexion va dépendre entièrement du niveau de la connexion dont l'entreprise dispose. Car si l'utilisateur se trouve hors du réseau local il y a un service de redirection qui se nomme « Quick Connect » dans NAS.

Si l'accès externe est ouvert sur le NAS alors il y a de forte chance qu'un malveillant puisse pirater le NAS.
En termes d'implémentation il faut quand même une personne bien certifiée pour pouvoir profiter du service. Cela dit qu'un ingénieur favorise le paramétrage de NAS au sein de l'entreprise.

Et termes de sécurité de l'appareil NAS lui-même, il est important de favoriser l'emplacement du hardware et de mettre en place une seconde sauvegarde du NAS à l'aide d'un autre NAS pour améliorer sa sécurité en cas d'inondation ou d'incendie [1.05].

Avoir son propre matériel de communication et d'échange de document est important pour une entreprise, surtout quand la base de données contient des informations confidentielles.

1.4.2 Second scénario

Les différentes techniques de manipulation des protocoles de sécurisation informatiques et des bases de données sont également des scénarios qui mènent au bonne fonctionnement et conduit à la protection de nos documents vitaux.

1.4.2.1 SNMP

Des ordinateurs aux serveurs, en passant par les commutateurs, routeurs, imprimantes et autres périphériques, un réseau réunit des appareils très différents. Plus le nombre de participants est important, plus l'effort nécessaire à l'administrateur et les difficultés rencontrées dans la gestion du réseau sont considérables. C'est la raison pour laquelle utiliser des outils de gestion est impératif lorsqu'il s'agit de garantir la fonctionnalité et la sécurité de tous les systèmes sur la durée. L'un des protocoles auquel de nombreuses solutions logicielles ont recours est le Simple Network Management Protocol (SNMP), aujourd'hui considéré comme l'un des principaux protocoles standard. Il est supporté par la quasi-totalité des terminaux. [1.06]

L'SNMP est dit Simple Network Management Protocol, il est constitué de trois éléments bien plus importants :

- Les objets de gestion,
- les agents et
- le système de gestion du réseau.

Ce protocole est un ensemble d'élément de communication standard en réseau TCP/IP. La supervision SNMP est très utilisé pour tous utilisateurs qui est responsable des serveurs et des

équipements de réseau tells les hôtes, routeurs, switches et autres. Il permet à l'administrateur de garder à l'écoute des réseaux et de l'utilisation de largeur de bands. L'implémentation permet à l'utilisateur également de traquer les erreurs importantes comme les temps de fonctionnements de appareils et les niveaux du trafiques.

a. Fonctionnement du SNMP

La gestion de réseau via SNMP est basée sur un modèle agents/manager. Le poste de gestion central est ici le système depuis lequel l'administrateur surveille et gère les différents participants au réseau. Pour ce faire, un logiciel de gestion permettant l'interrogation SNMP de données ainsi que l'initiation de certaines actions est installé.

Les agents, qui sont également des applications, viennent en contrepartie des différents composants réseau. Ils collectent les données pertinentes sur l'hôte cible et les transmettent au poste de gestion. Ils sont par ailleurs en mesure de procéder personnellement à des réglages et de déclencher certaines actions. Les applications agents de ce type sont déjà implémentées par défaut dans la plupart des systèmes Windows et Linux courants, sous la forme par exemple du Daemon SNMP (uniquement sous Linux).

Le protocole SNMP fixe sept types de messages possibles pour la communication entre le manager et l'agent :

- Requête GET : les requêtes GET sont les messages standards permettant de consulter un ensemble de données défini sur l'appareil souhaité dans le réseau.
- Requête GETNEXT : ce format de message est utilisé pour interroger les ensembles de données consécutifs, par ex. dans le cas de tableaux.
- Requête GETBULK : l'application de gestion peut envoyer une requête GETBULK (à partir de la version SNMPv2) afin d'interroger un nombre défini d'ensembles de données avec une seule et même requête. Une requête GETBULK correspond à plusieurs requêtes GETNEXT consécutives.
- Requête SET : les requêtes SET permettent au manager de modifier un ou plusieurs ensemble(s) de données de l'appareil souhaité dans le réseau ou de déclencher certaines actions. Un exemple de scénario type nécessitant plusieurs modifications simultanément : la configuration d'une adresse IP exigeant l'indication simultanée d'un masque de sous-réseau.

- Réponse GET : si le manager a demandé un ou plusieurs ensemble(s) de données, ou initié des modifications ou des actions, l'agent répond en envoyant des réponses GET. Ces paquets de réponses contiennent soit les données demandées ou une confirmation des modifications apportées, soit un message d'erreur lorsque les requêtes n'ont pas reçu de réponses convenables.
- Trap SNMP : les traps SNMP sont des messages envoyés par les agents sans instructions de la part du poste de gestion. Cela se produit lorsqu'un événement imprévu déterminé est survenu. Les traps peuvent communiquer de deux façons différentes sur le type d'événement survenu : la première possibilité, préservant les ressources, consiste à joindre un numéro d'identification unique. Le manager peut se référer à la base de données informative (MIB) déjà évoquée pour en connaître la signification. Avec la seconde possibilité, les traps SNMP fournissent des informations sur l'événement, mais contiennent également les données correspondantes sans avoir à afficher un numéro d'identification spécifique.
- Requête INFORM : les requêtes INFORM assurent généralement la même fonction que les traps SNMP. Contrairement à ces dernières, les paquets INFORM se démarquent toutefois par l'envoi d'un accusé de réception par le manager. Par conséquent, l'agent peut renvoyer le message si celui-ci n'a pas atteint le manager à la première tentative.

Comme il a été déjà évoqué, le SNMP impose l'utilisation du protocole de transport sans connexion UDP pour la transmission des paquets de messages énumérés. Ceci permet de garantir une surveillance du réseau qui préserve particulièrement les ressources. Pour l'envoi des différentes requêtes GET aux agents (ainsi que pour les réponses correspondantes), le SNMP utilise le port UDP 161, tandis que les traps SNMP sont envoyés automatiquement à travers le port UDP 162.

b. Différents types de version en SNMP

Initialement, le SNMP ne permettait pas aux gestionnaires de communiquer entre eux et aux agents d'envoyer des messages avec accusé de réception. D'autre part, de nombreuses applications n'étaient que partiellement supportées au début du protocole malgré l'ambition d'être un standard ouvert. C'est pourquoi les correctifs du protocole apparus au cours des années suivantes ont principalement visé à intégrer des mécanismes correspondants dans le SNMP.

Une autre aspiration essentielle du groupe de travail IETF responsable du protocole a été, dès le début, d'accroître la sécurité du processus de gestion. Il est possible d'observer ce résultat dans la troisième version. Cette étape d'optimisation du protocole SNMP ainsi que d'autres étapes sont présentées de façon un peu plus détaillée dans la description suivante des différentes versions SNMPv1, SNMPv2 et SNMPv3.

- **SNMPv1**

En tant que première version du protocole de gestion de réseau, la version SNMPv1 pose les bases du modèle gestionnaires/agents et les bases de la communication entre le poste de gestion et les différents agents. Le SNMP y est décrit comme un protocole simple agissant au niveau de l'application et pouvant s'appuyer sur l'UDP (User Datagram Protocol) et l'Internet Protocol (IP), mais aussi sur des protocoles réseau comparables tels que le DDP AppleTalks (Datagram Delivery Protocol) ou Internet Packet Exchange (IPX). Le seul mécanisme de sécurité intégré est alors l'échange d'un nom de communauté envoyé avec les requêtes correspondantes.

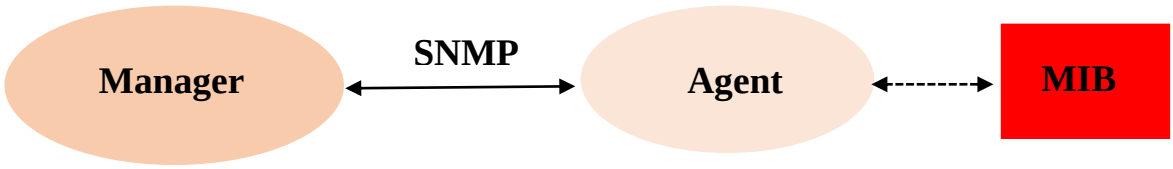


Figure 1.09 : *Architecture snmpv1*

- **SNMPv2**

L'un des problèmes majeurs de la première version du protocole SNMP réside dans le fait que le nom de communauté assure la sécurité n'est transmis qu'en texte clair. C'est la raison pour laquelle les développeurs se sont rapidement penchés sur une nouvelle variante appelée Secure SNMP, dans laquelle cette chaîne serait transmise sous une forme cryptée. Toutefois, cette version n'a jamais été publiée, car elle a été directement remplacée par la version SNMPv2. D'autres améliorations ont été apportées à la version initiale du protocole : un traitement des erreurs optimisé, la possibilité d'une communication de manager à manager ainsi que des commandes SET plus performantes.

Le principal avantage comparé à la version SNMPv1 réside toutefois dans l'implémentation des nouveaux types de messages GETBULK (pour l'interrogation de plusieurs données dans une même requête) et INFORM (pour les accusés de réception des réponses des agents).

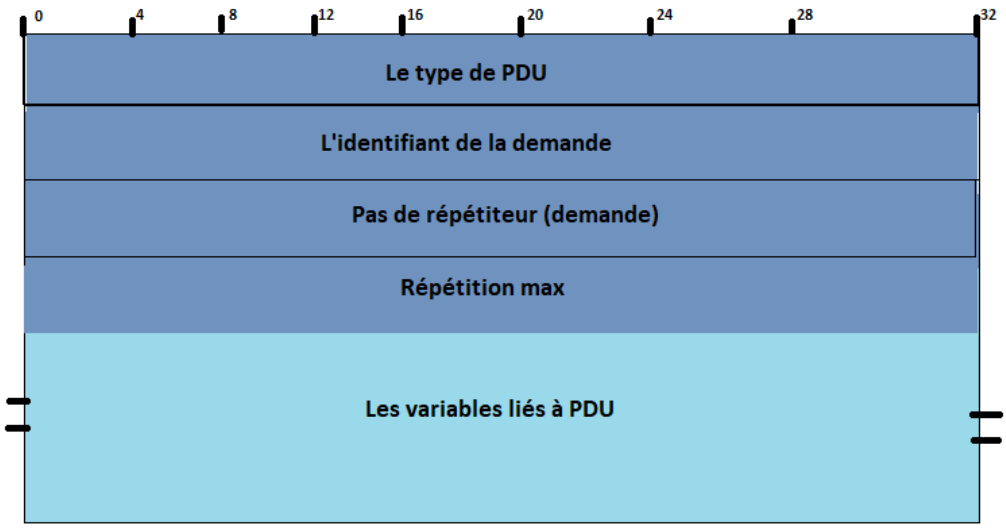


Figure 1.10 : *SNMP Version 2 sous forme GetBulkRequest-PDU*

- **SNMPv3**

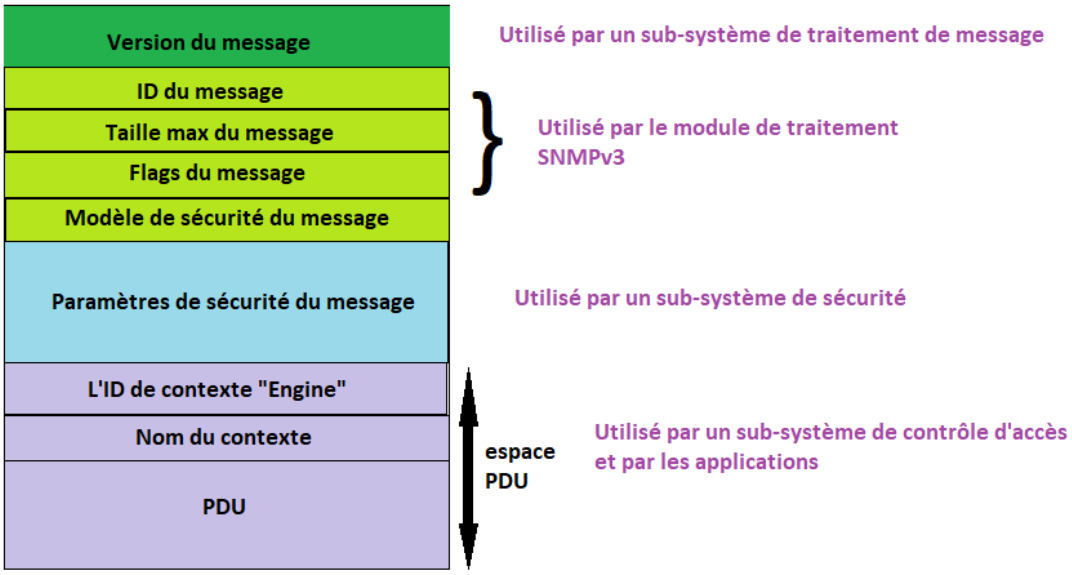


Figure 1.11 : *Structure de message sous SNMPv3*

Après la première étape, de moindre ampleur, franchie avec la deuxième version du protocole, l'IETF ou « Internet Engineering Task Force » s'est pleinement consacrée à la sécurité dans la

version SNMPv3 et a remplacé le nom de communauté par un nom d'utilisateur et un mot de passe. D'autre part, et contrairement aux versions antérieures, la troisième version du protocole inclut des fonctionnalités permettant de crypter la transmission des paquets SNMP.

1.4.2.2 Autres types de protocoles de surveillances réseaux

Les protocoles de surveillance des réseaux et systèmes sont les sources de développement de la sécurité informatique depuis jusqu'à nos jours.

a. ICMP

Les périphériques réseau, tels que les routeurs et les serveurs, utilisent l'Internet Control Message Protocol pour envoyer des informations sur les opérations IP et pour générer des messages d'erreur en cas de défaillance des périphériques.

b. Cisco Discovery Protocol

Le Cisco Discovery Protocol facilite la gestion des périphériques Cisco en découvrant ces périphériques, en déterminant leur configuration et en permettant aux systèmes qui utilisent différents protocoles de couche réseau de se connaître.

1.5 Etude d'évaluation de performance de réseau

Dans un domaine où les paquets d'information sont les principales sources de travail, il faut savoir quel type de donnée est mis en réseau et savoir comment se transporte les files de donnée dans le trafic.

Des actions de gestion des ressources doivent être prises pour adapter l'utilisation des ressources au trafic offert. C'est la modélisation dynamique de trafic de données.
Le principe général de la théorie différentielle du trafic est de dériver la forme exacte de l'équation différentielle associée à l'espérance mathématique du trafic de chaque flux dans chaque ressource du réseau. Cette équation différentielle fait intervenir des probabilités transitoires du modèle Markovien dont l'expression analytique n'est en général pas connue.

Pour estimer ces probabilités transitoires on introduit des approximations basées sur des relations implicites entre les probabilités d'états et le trafic moyen. Le comportement du réseau peut alors être déterminé, en régime transitoire et en régime stationnaire, par intégration numérique de ces équations différentielles autonomes [1.07].

Deux tâches sont nécessaires dans la réalisation d'une étude d'évaluation de performance de réseau ; la modélisation des réseaux à commutation de paquets et la mise en place de procédé de graphe.

1.5.1 Modélisation des réseaux à commutation de paquets

Une recherche a établi tout un ensemble de modèles différentiels pour des systèmes élémentaires Markoviens et non Markoviens permettant de représenter les organes d'un réseau à commutation de paquets : files M/M/1, M/G/1 [1.08, 1.09, 1.10, 1.11, 1.12, 1.13, 1.14, 1.15].

Par définition, une file d'attente M/M/1 est une file d'attente dont le processus des arrivées est un processus de Poisson d'intensité λ, et que les temps de service sont i. i. d. de loi commune la loi exponentielle de paramètre μ.
Une partie de ces travaux a été publiée dans [1.16].
Exemples ;

- Par constatation des résultats ci-dessous l'approximation obtenue pour une file M/G/1 [3.15]. Par définition, un modèle de file d'attente M/G/1 est un système de file d'attente dans lequel les clients arrivent suivant un processus de Poisson d'intensité $\lambda > 0$. Les temps de service successifs sont des variables aléatoires i. i. d, indépendantes du processus des arrivées. On note T la durée moyenne de service, $C_b^2 \neq 1$ son coefficient de variation et on suppose que $\lambda T < 1$, où λ est le taux d'arrivée. Soit $X(t)$ le nombre moyen de clients et $\dot{X}(t)$ sa dérivée par rapport au temps et ρ est un variable au régime transitoire. $\rho = \lambda/\mu$.

Le point de départ est l'équation différentielle suivante

$$\dot{X}(t) = \lambda - \frac{1}{T}[1 - P_0(t)] \qquad (1.01)$$

Cette équation fait intervenir la probabilité transitoire $P_0(t)$ qui est inconnue. En prolongeant au régime transitoire les relations stationnaires $P_0(\infty) = 1 - \rho$ et $X(\infty) = \rho + \frac{\lambda^2 \overline{x^2}}{2(1-\rho)}$, on obtient l'approximation suivante.

$$\dot{X}(t) \approx \lambda - \frac{1}{T}\frac{-2\big(1 + X(t)\big) + \sqrt{4(1 + X(t))^2 + 8X(t)(C_b^2 - 1)}}{2(C_b^2 - 1)} \qquad (1.02)$$

Un des intérêts de ces modèles différentiels est qu'ils permettent de déterminer la réponse transitoire du système à des phénomènes dynamiques tels que par exemple des variations de trafic.

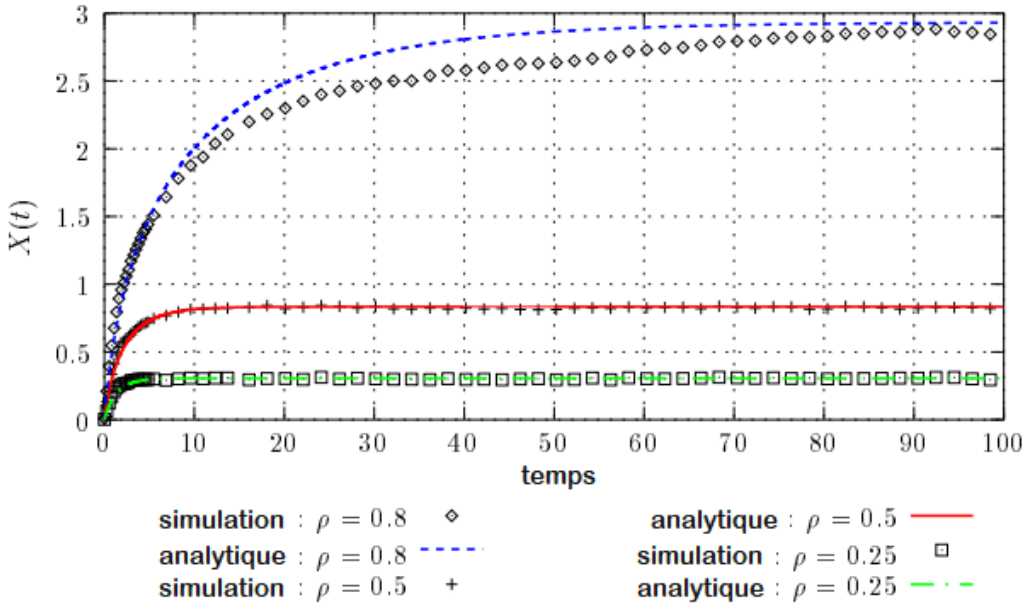


Figure 1.12 : *Approximation différentielle d'une file M/G/1 avec loi de service uniforme ou distribution uniforme*

La théorie du trafic différentiel a de plus l'avantage de fournir des approximations du transitoire d'un coût calculatoire bien plus faible que celles obtenues avec des processus de diffusion, et qui se comporte correctement quel que soit le taux d'utilisation. [1.17].

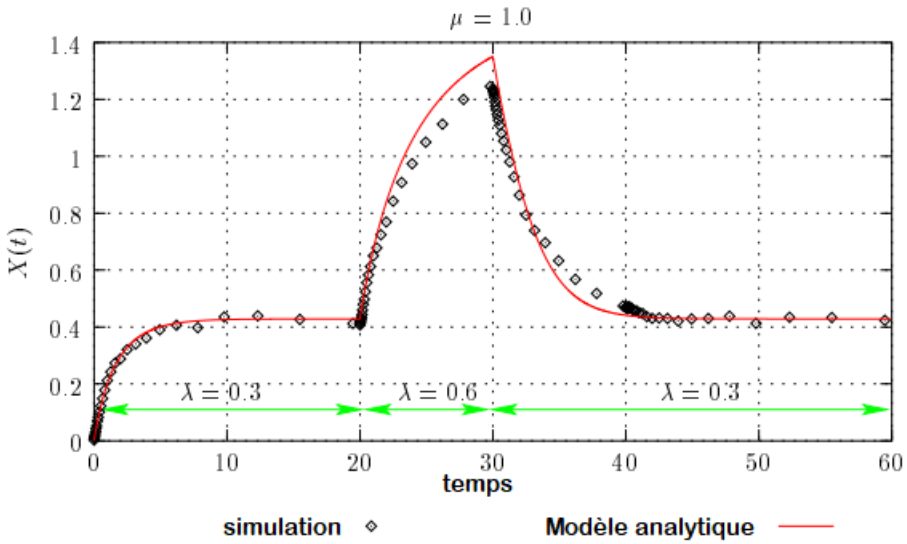


Figure 1.13 : *Réponse transitoire d'une file M/M/1 à des variations de trafic*

- Recherche de la densité de probabilité à z(t). Soit z(t) le processus de diffusion approximant le nombre de clients dans une file d'attente ayant des durées inter-arrivées de moyenne μ_a et de coefficient de variation au carré c_a^2 , et des durées de service de moyenne μ_b et de coefficient de variation au carré c_b^2.

La densité de probabilité associée à z(t) sachant que, $z(0) = z_0$ est donnée par [1.18].

$$p(z,t;z_0,0) = (\partial/\partial x)\left\{\Phi\left(\frac{z-z_0-\beta t}{\sqrt{\alpha t}}\right) - exp\left(\frac{2\beta z}{\alpha}\right)\Phi\left(-\frac{z+z_0+\beta t}{\sqrt{\alpha t}}\right)\right\} \qquad (1.03)$$

Où $p(z,t;z_0,0)$: Densité Gaussienne,

$\Phi(z) = \int_{-\infty}^{z} \frac{1}{\sqrt{2\pi}} exp\left(-\frac{1}{2}u^2\right) du$: Densité de processus de diffusion,

$\alpha = \frac{c_a^2}{\mu_a} + \frac{c_b^2}{\mu_b}$: coefficient de variation par rapport au temps,

$\beta = \frac{1}{\mu_a} - \frac{1}{\mu_b}$: constante par rapport au temps,

L'approximation diffusion, utilisée en fort trafic, a néanmoins deux avantages importants : elle est plus précise quand l'état initial, $x_0 \neq 0$, et elle offre une approximation de la distribution de probabilités (et non seulement de sa moyenne).

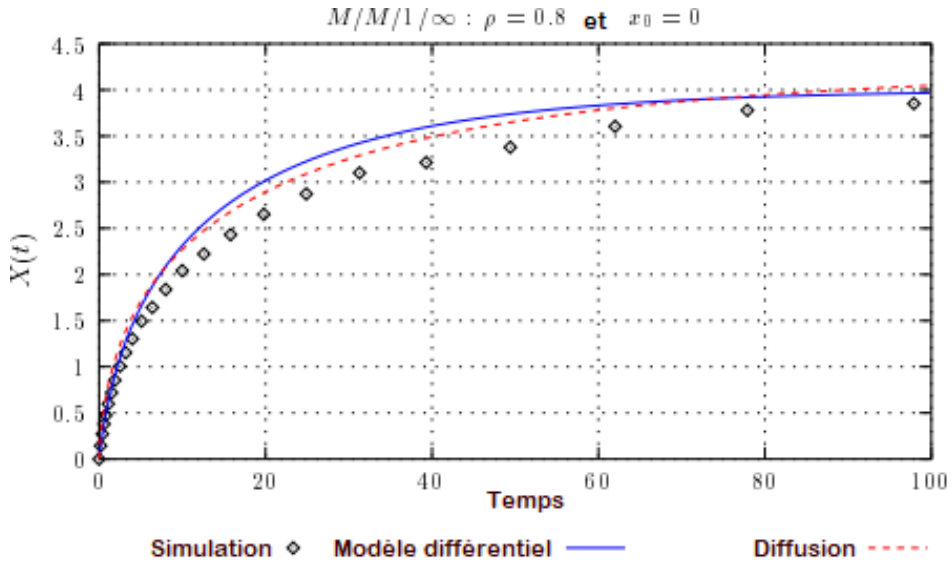


Figure 1.14 : *Réponses transitoires d'une file M/M/1 obtenues avec le modèle différentiel, l'approximation diffusion et avec des simulations événementielles quand $x_0 = 0$.*

Signalons enfin que des approximations différentielles peuvent être développées pour évaluer le comportement transitoire des réseaux de Jackson ou de Gordon-Newell.

Ainsi, dans le cas d'un réseau ouvert de Jackson, l'équation différentielle gouvernant le nombre de clients au nœud i peut être approximée par

$$\dot{X}_i(t) \approx \lambda_i + \sum_{j=1}^{n} r_{j,i}\,\mu_j \left(\frac{X_j(t)}{1+X_j(t)}\right) - \mu_i(1 - r_{i,j}) \left(\frac{X_i(t)}{1+X_i(t)}\right) \quad (1.04)$$

Où λ_i est le taux d'arrivée au nœud i depuis l'extérieur et

$r_{i,j}$ est la probabilité qu'un client sortant du nœud i aille vers le nœud j.

L'approximation ci-dessus converge vers la solution stationnaire exacte et les résultats numériques présentés dans [1.19] indiquent qu'elle est très précise en régime transitoire.

Tout cela à était le résultat d'une étude bien ciblé dans le cadre de réseaux de communication à une échelle plus petite que moyenne afin de mettre en évidence les trafics qui s'y trouve.

1.5.2 Mise en place de procédé de graphe

Dans la figure 3.15 présente l'interaction basique entre les tâches observées en traçant différents types de programme. Les graphes d'exécutions complexes sont la combinaison de ses sous-graphes.

- La ligne droite horizontale présente l'état en marche tant disque la ligne en pointillée l'état d'exécution bloquée.
- La ligne verticale représente des signaux en réveils.

Il existe alors trois tâches d'exécution, tâche A, tâche B et tâche C. Ceux avec X ne font pas parties des graphes. Le chemin critique est défini comme la séquence d'un segment d'exécution, qui va permettre de réduire le temps d'achèvement de l'exécution [1.20].

En précisant les valeurs, l'objectif, et la représentation voulue dans cette étude, il faut mettre en place des algorithmes de graphe afin de représenter les trafics dans le site internet de supervision, les réseaux de communication interne ou externe qui sont liés au réseau local.

a. Approximation d'une voix critique

Maintenant parlons de la possibilité de produire des chemins d'approximation critique des évènements qui se passent dans le noyau et que ses chemins sont valable. Pour cela, il faudra considérer le côté horizontal comme intervalle accordé au temps et il faut utiliser l'intervalle

arithmétique pour comparer ses éléments composants. La négligence du vide et les intervalles d'interruption, le lapse de temps d'exécution est défini comme élément des intervalles [1.21].

$$I_e = I_r \cup I_{bi} \cup I_{bd} \tag{1.05}$$

Où . $I_e =$ Lapse de temps d'exécution,

.$I_r =$ Ensemble des intervalles dans un état de fonctionnement,

.$I_{bi} =$ Intervalle de l'état bloqué avec un réveille ou mise en marche indirect et

.$I_{bd} =$ Intervalle des états bloqués en réveille direct.

On définit l'approximation de chemin critique comme élément d'exécution où I_{bd} est un récursive de substitution par l'intervalle plus en chevauchement de l'exécution où il existe une émission de signal de mise en réveille.

La procédure se termine quand $I_{bd} \neq 0$.

Il existe également trois éléments d'intervalles pour analyser la différence entre le chemin critique I_{exact} et son approximation I_{approx} :

- $I_{good} = I_{exact} \cap I_{approx}$ sont les correctes intervalles identifier par l'approximation.
- $I_{incorrect} = I_{approx} \setminus I_{exact}$ sont les intervalles inclus dans l'approximation mais pas affectés par le temps d'achèvement.
- $I_{missing} = I_{exact} \setminus I_{approx}$ sont des intervalles absents depuis l'approximation.

Notons que la variation $I_{incorrect} \Delta I_{missing} = \emptyset$, parce que chaque intervalle dans $I_{incorrect}$ un complément dans $I_{missing}$. Cependant l'erreur relative est $\sum I_{incorrect} / \sum I_{exact}$.

Différentes tâches sont analysées dans les graphes suivants.

- Graph (a)

Montre le cas où la tâche A réveil la tâche B et puis, le traitement de la tâche A est complète. Ce diagramme représente le comportement de l'instance entre un producteur et consommateur dans le marché. Le graphe peut être observé comme l'union de deux chemins de traitement. Si la ligne de liaison (B0, B1) est réduite par une petite quantité Є, le temps d'attente sera réduit et la tâche A sera complète plus rapidement.

Cependant, réduire la ligne de liaison (A1, A2) causera l'attente de (A2, A3) d'augmenter, et ne produira aucun « speed-up ».

- Graphe (b)

C’est un exemple de répétition, est peut être vue comme la concaténation ou enchaînement du graphe (a). Le chemin critique est simplement la concaténation du sous-graphe chemin critique.

- Graphe (c)

C’est de type programme parallèle où des tâches multiples sont engendrées en une seule fois. Si la ligne de liaison (B0, B1) est réduit, alors le temps d’attente (A3-A4) sera réduit, puis l’attende entre la ligne (A5, A6) sera augmenté, et le temps d’achèvement n’avancera pas. Cependant, la ligne (C0, C1) est influencée par le temps d’arrêt. Il peut s’affirmer que la ligne (A1, A2) mettant en marche la tâche C est dans le chemin critique. Cela reflète le fait que la dernière liaison à finir dans le groupe limite le « speed-up » achevable.

Les deux derniers cas (e) et (f) peuvent apparaître si la trace est mutilée pour le temps de fenêtre dans une des parties qui nous intéresse. Autrement, ils ont une implication significative dans le rétablissement du chemin critique.

- Graphe (e)

C’est un exemple de traitement asynchrone. La tâche A réveil la tâche B, mais n’attend jamais un résultat de sa part. Dans ce cas, aucun blocage n’apparaît et il y a affirmation que la tâche B n’est jamais dans un chemin critique pour la tâche A.

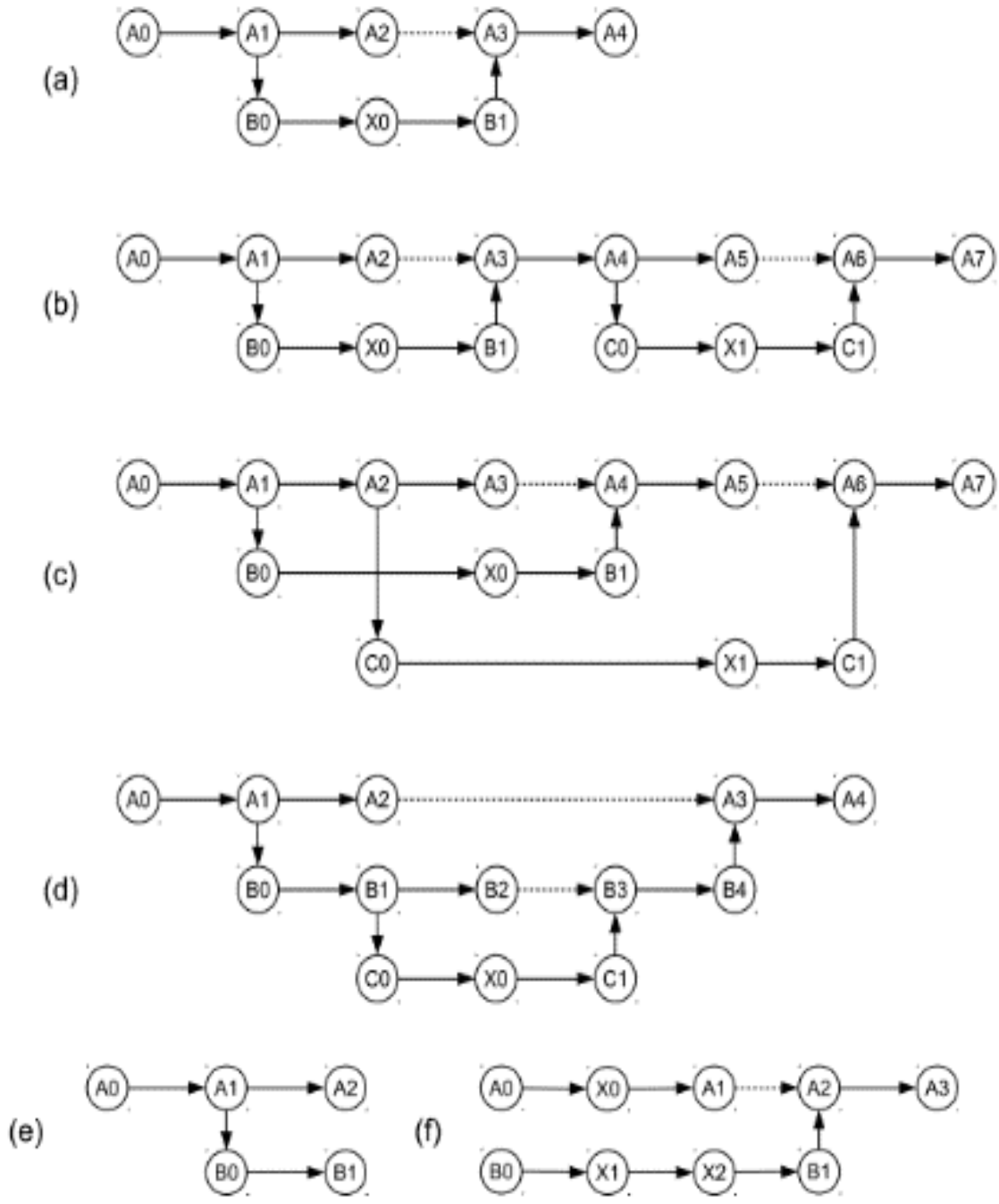
- Graphe (f),

La tâche A attend la tâche B, mais il n’y a pas de signal de priorisation de la part de la tâche A à B comme dans les cas précédents. Cela pourrait poser une barrière dans une calcule intérieure, mais aussi une contention de fermeture dans une ressource de partage. Dans ce cas de barrière, la ligne (B0, B1) affecte le temps d’arrêt, et pourrait présenter aucun défaut spécifique.

Parlons également de la capacité de l’approximation à récupérer l’ensemble des tâches qui contribuent à la voie critique.

Il y a relèvement de la différence entre les lignes horizontales du chemin critique et l’approximation pour les graphiques de base de la figure 3.15.

Dans le tableau suivant se trouve les différents chemins parcourues par les graphes ou sous graphes. Les graphes sont en effet des suites de valeurs et de déplacement que les tâches empreintes durant son exécution. Les valeurs exactes sont des tâches définies correctes par les valeurs d’approximation critiques.



Flèche horizontale, exécution de tâche en marche.

Flèche verticale, temps de réveil d'une autre tâche.

Flèche à pointillée, exécution de tâche dépendamment de l'exécution précédente, tâche bloquée.

Figure 1.15 : *Graphes d'exécution basique*

Tableau 1.01 : *Chemins critiques des graphes d'exécution basique*

Sous Graphe	Exact	Approximation	Incorrect	Absent
(a)	A0, A1, B0, B1, A3, A4	A0, A2, X0, B1, A3, A4	(A1, A2)	(B0, X0)
(b)	A0, A1, B0, B1, A3, A4, C0, C 1, A6, A7	A0, A2, X0, B1, A3, A4, A5, X1, C1, A6, A7	(A1, A2), (A4, A5)	(B0, X0), (C0, X1)
(c)	A0, A2, C0, C1, A6, A7	A0, A3, X0, B1, A4, A5, X1, C1, A6, A7	(A2, A3), (A4, A5)	(X0, B1), (C0, X1)
(d)	A0, A1, B0, B1, C0, C1, B3, B4, A3, A4	A0, A2, B1, B2, X0, C1, B3, B4, A3, A4	(A1, A2), (B1, B2)	(B0, B1), (C0, X0)
(e)	A0, A2	A0, A2	∅	∅
(f)	A0, X0, X1, B1, A2, A3	A0, A1, X2, B1, A2, A3	(X0, A1)	(X1, X2)

Des calculs de différences ont été faits entre les lignes horizontales des chemins critiques et des chemins d'approximation pour les graphes basic de la figure 1.15.

- Dans le graphique (a) ;

La différence est liée au bord (A1, A2) représentant l'exécution effectuée après la signalisation de la sous-tâche et avant le blocage. Il représente la partie asynchrone de l'exécution. Même les programmes avec une conception synchrone présentent un certain niveau de comportement asynchrone, parce qu'il y a toujours des instructions exécuter après le réveil et avant de bloquer. Malheureusement, il n'y a pas de limite supérieure au niveau asynchrone d'une tâche. En continuant avec le graphique (a), si le bord (A1, A2) augmente parce que la tâche A participe au calcul, l'erreur relative de l'approximation augmentera, jusqu'au point où le blocage disparaît, la Graphique (e) sera obtenu à la place, et il n'y a pas d'erreur.

Les deux tâches sont correctement identifiées autant que contribution pour le chemin critique.

- Dans le graphique (c) ;

Le bord (X0, B) de la tâche B est mal identifier par l'approximation. Mais en attendant que la tâche C s'exécute avant la tâche B, il n'y aura pas de blocage qui attend la tâche B, l'erreur pourra réduire et la tâche B ne pourra faire partie de l'approximation. Par conséquent, l'attente d'ordre d'exécution provoque un effet pour l'approximation.

Quand plusieurs résultats sont attendus, c'est généralement une bonne approche de programmation d'utiliser un appel de système en attendant n'importe quelle ressource d'être prêt à l'usage (prenons par exemple, select() and wait()) que d'attendre qu'un évènement spécifique se produise (tel que read() and waitpid()).

Le diagramme du graphe (c) est alors plus pratique à l'usage. Dans tous les cas la dernière tâche à faire est correctement identifier et cette connaissance est bien plus important les analyses de performances.

- Pour le cas imbriqué dans le graphique (d) ;

Les trois tâches contribuant à la trajectoire critique sont correctement identifiées par l'approximation à condition que la fenêtre de blocage soit suffisamment grande. L'erreur est concentrée sur la première moitié du graphique, tandis que la dernière partie est plutôt des erreurs libres et souples.

- Pour le graph (f) ;

Le cas de la barrière est similaire au raisonnement fait pour graphique (a). L'approximation est une mesure du déséquilibre w.r.t. la tâche donnée. Nous considérons maintenant le cas de la contention de verrouillage sous deux hypothèses, à savoir que la durée critique de la section τ_{cs} est courte, et que la durée de blocage est uniformément répartie entre $0 < \tau_b < \tau_{cs}$.

Ensuite, nous pouvons affirmer que l'erreur moyenne de l'approximation est $\tau_{cs}/2$. L'erreur relative globale sera proportionnelle à la probabilité de contention de verrouillage et est généralement une situation rare pour la plupart des programmes. Nous concluons que, selon ces hypothèses, l'erreur de l'approximation liée à la contention de verrouillage est faible.

Nous concluons que l'approximation présentée produira de bons résultats pour la plupart des programmes en synchrone, que la dernière tâche d'un groupe est correctement identifiée, et que l'erreur liée à la contention de verrouillage devrait être faible pour la plupart des programmes.

L'interprétation de l'approximation dans le cas d'applications asynchrones ou parallèles doit tenir compte des aspects spécifiques de la méthode.

b. Méthode d'approximation

La méthode dans la figure 3.10 fonctionne en itérant à partir d'un sommet de départ. Si un bord de blocage est rencontré, le bord entrant représentant le réveil est suivi vers l'arrière. L'intervalle de blocage est comptabilisé dans la sous-tâche. Si la sous-tâche elle-même bloquée, alors ce processus est appliqué de manière récursive. L'itération sur la tâche principale se poursuit lorsque l'intervalle de blocage est complètement calculé.

Tableau 1.02 : *Etats d'évènement dans le noyau (1)*

Temps	Evènements	CPU	Champ (états)
10	Temps d'arrêt	0	{prev_tid = 1234, prev_state = 1}
20	Temps de réveille	1	{tid = 1234}
30	Temps d'arrêt	1	{prev_tid = 5678}
40	Temps d'arrêt	0	{next_tid = 1234}

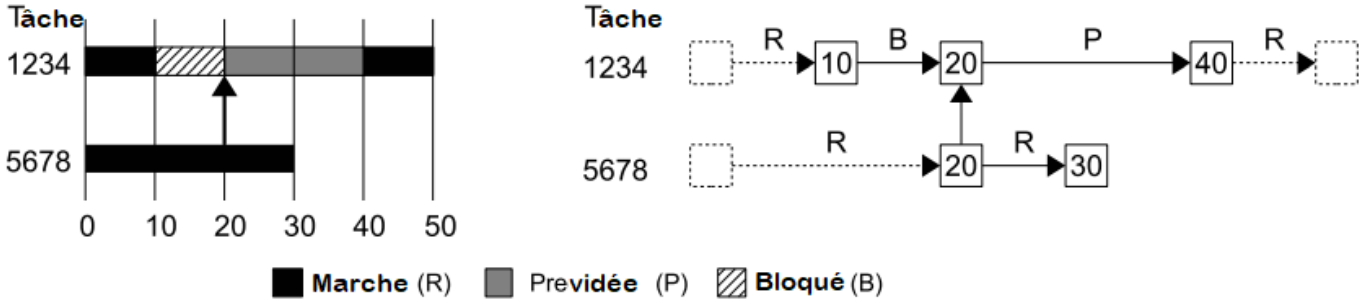


Figure 1.16 : *Exemple d'évènement de réveille depuis une sous-tache*

Tableau 1.03 : *Etat d'évènement dans le noyau (2)*

Temps	Evènements	CPU	Champ (états)
10	Temps d'arrêt	0	{prev_tid = 1234, prev_state = 1}
20	Temps d'entré expirer	1	{}
30	Temps de réveille	1	{tid = 1234}
40	Temps de sorti expirer	1	{}
50	Temps d'arrêt	0	{next_tid = 1234}

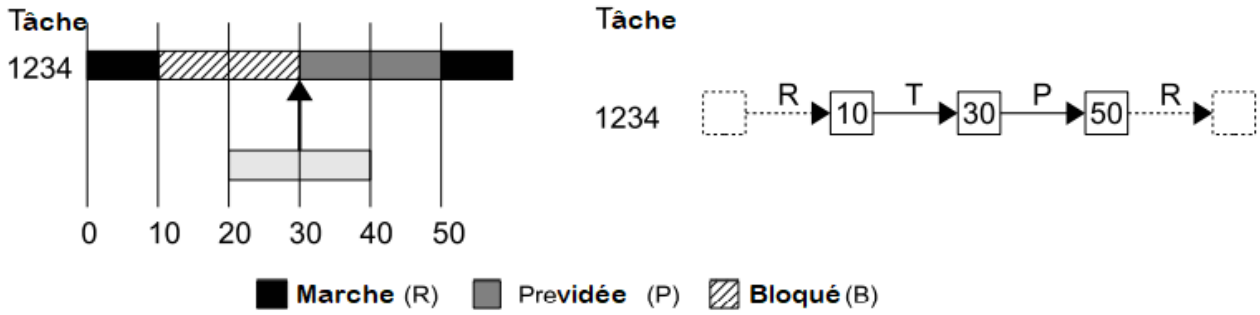


Figure 1.17 : *Exemple d'évènement de réveille durant une interruption de temps données*

Les temps d'exécution des tâches sont de 0 à 50, des évènements sont produits durant le temps de transition l'état de CPU ou « Central Processing Unit » se trouve toujours entre [0, 1], les tâches sont exécutées de manière de chiffrement tel : 1234 et 5678.

Dans les figures, les couleurs noires représentes le temps de réveille et d'exécution de tâche, entre temps, des blocages (en raillés) d'exécution se produit afin de mettre en place des préoccupations d'autres évènement qui se passent dans le CPU qui est en couleur plus claire, pour terminer avec le temps arrêt.

La complexité à construire et la taille résultante du graphique d'exécution sont proportionnelles aux nombres d'événements dans la trace.

1.6 Conclusion

Cloud va pouvoir offrir plus de ressource, de flexibilité et la sécurité aux transferts de données de plus la sauvegarde de données. Il assure qu'il n'y a pas de gaspillage de ressource. L'administrateur peut alors favoriser la distribution de ressource selon le besoin de chaque département. Les demandes vont favoriser la mise en place des sécurités de données et des transferts via internet.

Avec la technologie Docker, il est possible de traiter les conteneurs comme des machines virtuelles très légères et modulaires. En outre, ces conteneurs offrent une grande flexibilité : les utilisateurs créent, déploient, copient et déplacent d'un environnement à un autre, ce qui permet d'optimiser les applications pour le cloud.

Les fichiers et les ressources des données sont manipulables et traçables selon les études qui ont étaient établis auparavant. Les chemins choisis par le programmeur valorisent l'état des fichiers et des données. L'étude des chemins favorise la sécurité et les échanges entre différents infrastructure du réseau et du système. De nouvelle méthode permet de retrouver les relations d'attente entre les tâches et les périphériques d'un ordinateur local. Il a été établi que le chemin

critique exact d'une application nécessite des évènements qui ne sont pas visibles depuis le système d'exploitation.

Il ne reste que l’étude des déploiements des technologies qui sont favorable et donnent plus d’avantage à l’entreprise ou à un utilisateur quelconque. Dans la deuxième partie se trouve la solution et la conception d’une supervision personnalisée selon les entreprises ou l’administrateur.

CHAPITRE 2
SOLUTION ET CONCEPTION DE MISE EN PLACE D'UNE SUPERVISION RESEAUX

2.1 Introduction

Le monitoring informatique également nommé supervision informatique est la surveillance permanente d'un système dans un but préventif. Le monitoring englobe une surveillance de plusieurs aspects de ce système informatique : le fonctionnement général, le débit, la sécurité, l'utilisation des ressources, le contrôle des flux…. [2.01].

La supervision réseau correspond à l'ensemble des actions à mettre en œuvre pour surveiller l'activité de tout un environnement réseau. Visant à permettre aux administrateurs système de travailler mieux, plus rapidement et plus efficacement, elle se concentre sur des aspects comme la consommation de bande passante et la disponibilité des périphériques réseau.

Le périmètre de surveillance englobe les systèmes locaux et distants d'un environnement informatique, comme les bases de données, applications, instances cloud, serveurs, et infrastructures réseau. La supervision réseau permet aux administrateurs de vérifier que leurs réseaux fonctionnent sans anicroche, efficacement, et sans rencontrer d'erreurs [2.02].

Dans ce chapitre, il y a l'étude des plateformes de monitoring, des mises en place de graphe de performance de tâche et des choix de politique de supervision.

2.1.1 Utilisation du monitoring

Le monitoring informatique permet de connaître l'état de santé global du système. De ce fait, lorsqu'il existe un besoin par exemple d'effectuer une sauvegarde, il faut s'assurer de la disponibilité d'un espace de stockage suffisant sur le disque dur. Il existe également différents types de vue d'ensemble qui favorise la supervision dans le monitoring.

2.1.1.1 Avoir une image fiable du système informatique

Pour réaliser cette image il y a procession à des :

- mesures de performances (ex : temps de réponse par exemple)
- mesures de disponibilité (ex des composants hardware et software d'un réseau)
- mesures d'intégrité (ex : l'état des processus sur une machine)
- mesures de changement.

2.1.1.2 Monitoring pour lutter contre les attaques

Le monitoring informatique est l'élément indispensable pour protéger un système contre les cybercriminels. Malheureusement les pare-feu et anti-virus ne suffisent pas à bloquer toutes les attaques.

En sachant, combien il est important de réagir rapidement en cas d'attaque malveillante afin de limiter la casse que pourrait subir l'entreprise et surtout la perte de données cruciales.

Grace au monitoring informatique, les équipes d'experts en infogérance sont capables d'agir rapidement et d'éliminer la menace avant qu'elle ne sévisse.

De par son fonctionnement le monitoring informatique permet de détecter les intrusions et les comportements inhabituels.

2.1.1.3 Monitoring informatique pour éviter les pannes

Le monitoring informatique permet aussi d'anticiper les défaillances et donc d'éviter les pannes en étant alerté des dysfonctionnements avant que le problème ne survienne.

L'objectif est de déterminer avec détails les activités du système et de définir des seuils de tolérance à ne pas franchir. Il est ainsi plus simple d'éviter un plantage du système par exemple.

Le monitoring informatique permet également d'en savoir plus sur les effets des changements opérés sur système informatique lui-même car il y a des mesures détaillées des variations liées aux changements.

2.1.1.4 Bande passante : un indicateur de sécurité

La surveillance de l'utilisation de la bande passante permet de déjouer bon nombre d'attaques. En effet, les outils de surveillance du trafic facilitent la comparaison entre les comportements normaux et ceux suspects en termes de trafic.

En général, les virus et les logiciels malveillants consomment une quantité importante de bande passante. Ainsi, la surveillance de la consommation de cette bande passante peut donc également s'avérer très utile pour identifier les anomalies de sécurité.

2.1.1.5 Technique d'évaluation pour le système informatique

Analyser les données, les flux, identifier la source du problème, prendre les mesures qui s'imposent. Le monitoring informatique permet d'établir une image claire et précise de du système

informatique. Ainsi, grâce aux constats on peut adapter au mieux le système informatique à une structure personnalisé et donc avoir une meilleure gestion de la sécurité et obtenir des coûts plus adaptés aux réseaux et systèmes.

2.1.1.6 Monitoring et le pack d'infogérance

La surveillance du réseau est un élément majeur pour la sécurité d'un système informatique. Le monitoring permet de s'assurer que l'ensemble du système est protégé et opérationnel en toute circonstance.

Ainsi, un bon pack d'infogérance doit obligatoirement intégrer pour une bonne prestation de monitoring.

2.1.2 Avantages et inconvénients de la supervision réseau

En sachant que le monitoring est un logiciel comme tout autre, il existe cependant des avantages et des inconvénients dont il ne faut pas négliger.

2.1.2.1 Avantages

Des avantages se présentent étant les points forts du monitoring d'un réseau.

a. Identifier les goulots d'étranglement et éliminer les perturbations qui en découlent

Les applications et les périphériques qui consomment une quantité excessive de bande passante peuvent parfois paralyser tout un réseau. C'est la raison pour laquelle tout administrateur doit impérativement connaitre précisément l'ampleur du trafic qui transite par les réseaux dont il est responsable. En supervisant le trafic et la bande passante, il faut garder en permanence un œil sur les capacités du réseau pour éviter les perturbations causées par les goulots d'étranglement et les phénomènes de saturation. Cela contribuera à garantir la continuité des activités au sein de l'entreprise ou de l'organisation.

b. Optimiser les performances et en finir avec les interruptions de service

Pour que ses processus de travail fonctionnent comme il se doit, toute entreprise doit pouvoir comptée sur la disponibilité constante de ses bases de données. Si un serveur web ou un serveur de messagerie plante, l'organisation en ressentira aussitôt les effets et sera contrainte de débloquer des ressources précieuses pour remédier au problème. Il est donc essentiel de garder en permanence un œil sur les aspects les plus stratégiques de la base de données, comme les délais de requête, de connexion et de réponse. Fort d'un outil complet de supervision réseau, l'entreprise

sera en mesure de surveiller tous les serveurs 24h/24, 7j/7 et de faire en sorte qu'ils soient toujours sur le pied de guerre.

c. Garantir le bon fonctionnement des périphériques et applications

Beaucoup d'applications conditionnent directement la bonne marche d'une entreprise, d'où la nécessité de superviser son réseau pour détecter d'éventuels problèmes et erreurs avant qu'ils se matérialisent. Sinon, il y a risque de voir ces grains de sable gripper la machine et perturber fortement le fonctionnement de l'entreprise.

Si besoin il faut s'aspirer à aider les collègues à maximiser leur productivité, il faut donc assurer que l'ensemble des périphériques et des applications du réseau local et du réseau WAN fonctionnent sans chocs.

2.1.2.2 Inconvénient de la supervision d'un réseau

Les plateformes de supervision représentent surtout des incompatibilités au sein de certains appareils, faute de bugs ou des défauts plus spécifiques.

Des complications peuvent se présenter au niveau de la manipulation donc on a besoin surtout d'une formation afin de faire connaissance avec le produit de notre étude. Présentations des architectures et des failles de réseaux connectées à internet

Internet est une grande architecture et réseau qui présente des dangers et des failles de sécurités très important. Le monde possède un accès illimité à internet donc peut faire toute une attaque dans un temps illimité.

2.1.3 Failles existantes dans le monde internet

Présentant une illustration d'étude étrangère en Amérique sur l'espionnage internet.

En entreprise, c'est le réseau local qui est connecté à Internet. Il est donc indispensable de contrôler les communications entre le réseau interne et l'extérieur. De plus une formation du personnel est indispensable (règles de sécurité, déontologie, attention aux participations aux forums qui sont archivées ...).

Les problèmes de sécurité qu'on peut rencontrer sur un réseau d'entreprise ou sur l'Internet relèvent d'abord de la responsabilité des victimes avant d'être imputables aux hackers. Une menace qui a sensiblement augmenté au cours de ces dernières années, nous indique la dernière étude du Computer Security Institute, un institut professionnel de San Francisco qui réalise chaque année un sondage auprès des entreprises en collaboration avec le FBI.

Dans cette étude, plus de 40 % des sociétés interrogées ont déclaré que des intrus s'étaient introduits dans leurs systèmes depuis l'Internet, 38 % des sociétés ont détecté des attaques de type déni de service, et 94 % ont été infectées par un virus en 2000.

D'autre part, la sécurité peut dépendre d'autres entreprises dont la capacité d'attaque et souvent négligées, il y a jugement à tort. Alors que le gouvernement et les forces de l'ordre cherchent à interpeller les intrus, les sociétés ne se préoccupent trop souvent que de relancer leurs réseaux après une attaque [2.03].

Ce pendant cette étude était faite vers le début du vingtième siècle de nos jour au vingt-unième siècle, certaine entreprise voudrais savoir d'où viennent les attaques et comment poursuivre les malfaisants.

Après des années d'évolution d'infrastructure « hardware » et « software », de l'année 2000 ici l'année de cette petite analyse au-dessus et l'année 2020 de nos jours, beaucoup de technologie de défense et d'attaque ont vu le jour.

2.1.3.1 Types d'attaques

Plusieurs attaques se présentent dans le marché du monde hacker et du monde de sécurité informatique.

a. IP spoofing

Usurpation d'adresse IP ou Internet Protocol, il y intrus mais envoi une requête provient d'une machine autorisée. Une bonne configuration du routeur d'entrée permet d'éviter qu'une machine extérieure puisse se faire passer pour une machine interne.

b. DNS spoofing

Le DNS Spoofing est une cyberattaque visant le DNS qui consiste à rediriger les internautes à leur insu vers des sites frauduleux cherchant à voler les informations récoltées. Pousse un serveur de DNS à accepter l'intrus. Solution : séparer le DNS du LAN de celui de l'espace public [2.04].

c. Flooding

C'est simplement le fait d'inonder une machine ciblée dans le but de bloquer ou gêner son fonctionnement. L'action de flooding peut être effectuée de diverses manières. Mais généralement en raid massif de connexions non terminées.

d. Smurf

C'est un ping flooding un peu particulier. C'est une attaque axée réseaux, faisant partie de la grande famille des Refus De Service (DOS : Denial Of Service). Si le routeur permet cela, il va transmettre le broadcast à tous les ordinateurs du réseau, qui vont répondre à l'ordinateur cible. La cible recevra donc un maximum de réponses au ping, saturant totalement sa bande passante [2.05].

e. Web bug

Un mail publicitaire est envoyé en HTML, même si l'apparence est normale, avec une image transparente gif d'un pixel par un lien du type :

<img src="http://www.serveur.xx/image.gif ?email=utilisateur@adresse">.

Si le courrier est ouvert pendant la connexion, la requête de téléchargement de l'image vient confirmer la lecture du message et la validité de votre adresse. Conseil : ne pas valider l'ouverture automatique du format HTML ou ne pas ouvrir ses courriers en ligne. Un utilitaire de détection de « web bug » BUGNOSIS est disponible sur www.bugnosis.org.

f. Hoax

Un « hoax » est une rumeur que l'on transmet par mail. Ces rumeurs colportent souvent des problèmes de sécurité soit disant découverts par des services officiels ou célèbres… Elles peuvent causer un véritable préjudice à certaines sociétés et de toute façon encombrent le réseau.

Avant de retransmettre un tel message il est prudent de vérifier son authenticité. www.hoaxbuster.com (site français) recense la plupart des messages bidon.

2.1.3.2 Hacker et cracker

Il existe une communauté, une culture partagée, de programmeurs expérimentés et de spécialistes des réseaux, dont l'histoire remonte aux premiers mini-ordinateurs multiutilisateurs, il y a quelques dizaines d'années, et aux premières expériences de l'ARPAnet.

Les membres de cette culture ont créé le mot « hacker ». Ces informaticiens sont généralement discrets, anti-autoritaristes et motivés par la curiosité. Il y a un autre groupe de personnes qui s'autoproclament des « hackers ». Ces gens (principalement des adolescents de sexe masculin) prennent leur pied en s'introduisant à distance dans les systèmes informatiques et en piratant les systèmes téléphoniques, généralement à l'aide d'outils écrit par d'autres et trouvés sur Internet. Ils publient sur alt.2600.

Les vrais hackers appellent ces gens des « crackers » et ne veulent rien avoir à faire avec eux. Les vrais hackers pensent que les crackers sont des gens paresseux, irresponsables et pas très brillants.

2.1.4 Différents types d'architectures

Avant toute chose, même si l'intrus parvient à franchir les barrières de protection (coupe-feu, système d'authentification, etc.), il est encore possible de l'arrêter avant qu'il n'attaque. Placés sur le réseau de l'entreprise, les outils de détection d'intrusion décèlent tout comportement anormal ou trafic suspect. Malgré la mise en place de solutions d'authentification, chargées de filtrer et de contrôler les accès au réseau, il arrive que des intrus y pénètrent.

C'est même le caractère propre des pirates de contourner les serveurs d'authentification, coupe-feu et autres barrières de protection des systèmes. Une fois entrés, plus rien ne les empêche de saboter, de voler et d'endommager les applications. Interviennent alors les systèmes de détection d'intrusion.

En auscultant en permanence le trafic, ils repèrent le hacker et alertent aussitôt l'administrateur. Protégeant l'entreprise des attaques externes, ces systèmes sont également capables de détecter le pirate interne qui représente encore entre 70 à 80% des actes de malveillance auxquels sont confrontées les sociétés.

2.1.4.1 Deux catégories d'outils supervision réseau sur le marché :

- La première : Analyser le trafic réseau,
- La seconde : Etudier le comportement des utilisateurs au niveau d'un système ou d'une application.

Dans tous les cas, des ressources humaines devront être affectées à la supervision des systèmes de détection d'intrusion pour gérer les alertes, mais aussi pour détecter ce que les outils n'auront peut-être pas vu. Coûteuses, ces ressources freineraient aujourd'hui les entreprises dans l'adoption de ces solutions.

Il existe deux types d'architecture dans la disposition des matériels locaux en connexion avec les infrastructures externe.

a. Architecture classique

Une architecture classique est que toute disponibilité de configuration et de protection se trouve dans un même routeur.

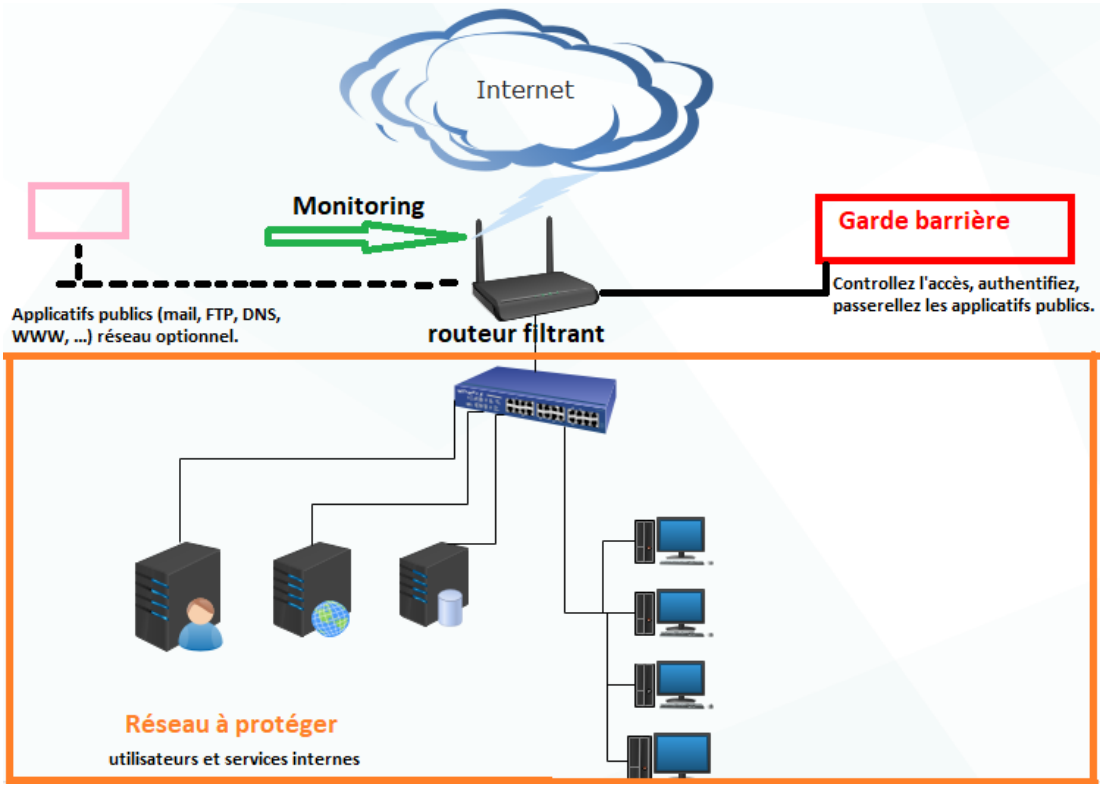


Figure 2.01 : *Représentation classique d'un réseau de communication avec Internet*

b. Architecture concentrée

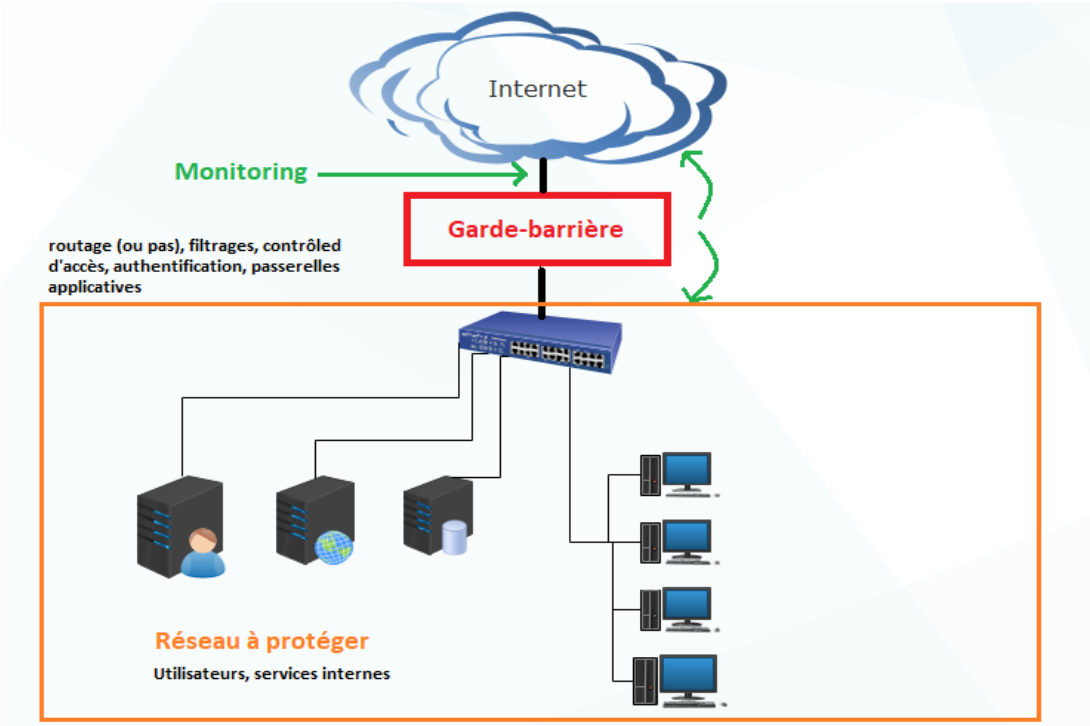


Figure 2.02 : *Architecture concentrée de réseaux connectés à Internet*

Dans une architecture concentrée, il existe une machine dédiée au routage entre LAN et Internet. Le trafic est analysé au niveau des datagrammes IP (adresse, utilisateur, contenu...).

Un datagramme non autorisé sera simplement détruit, l'IP sachant gérer la perte d'information. Une translation d'adresse pourra éventuellement être effectuée pour plus de sécurité (protocole NAT Network Address Translation RFC 1631+2663).

Cependant, un « firewall » est inefficace contre les attaques ou les bévues situées du coté intérieur et qui représentent 70% des problèmes de sécurité.

2.2 Différents types de logiciel de supervision réseaux

En favorisant et en choisissant le monitoring comme solution à l'étude mise en place pour minimiser l'attaque et l'intrusion au sein d'un réseau d'entreprise.

Il existe cependant plusieurs outils et plateforme de supervision dont l'utilisation sera favorable la sécurité et bonne évaluation du système et du réseau.

2.2.1 Nagios

Il faut savoir que NMAP est très important en termes de sécurité dans Nagios. NMAP est un outil d'exploration réseau et scanneur de ports/sécurité dont la syntaxe est la suivante : NMAP [types de scans ...] [options] {spécifications des cibles}. NMAP existe aussi en mode graphique sous le nom « Zenmap GUI ».
NMAP permet d'éviter certaines attaques et aussi de connaître quels services qui tournent sur une machine. Une installation faite un peu trop vite peut laisser des services en écoute (donc des ports ouverts sans que cela ne soit nécessaire) et donc vulnérables à une attaque. Il est un logiciel très complet et très évolutif, et il est une référence dans le domaine du scanning.
Cependant, NMAP a été conçu pour rapidement scanner de grands réseaux, mais il fonctionne aussi très bien sur une cible unique.

NMAP innove en utilisant des paquets IP bruts (raw packets) pour déterminer :

- quels sont les hôtes actifs sur le réseau,
- quels services (y compris le nom de l'application et la version) ces hôtes offrent,
- quels systèmes d'exploitation (et leurs versions) ils utilisent,
- quels types de dispositifs de filtrage/pare-feux sont utilisés, ainsi que des douzaines d'autres caractéristiques [2.06].

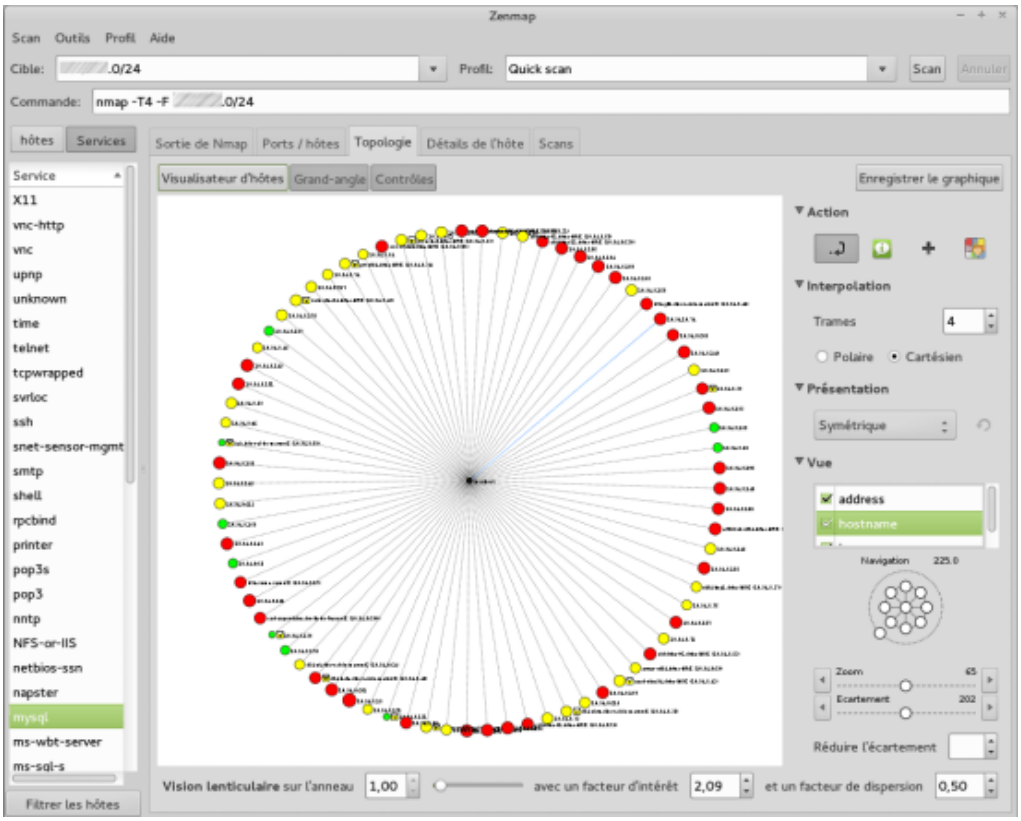


Figure 2.03 : *Représentation visuelle d'une topologie de réseau avec Zenmap GUI*

Nmap est généralement utilisé pour les audits de sécurité mais de nombreux gestionnaires des systèmes et de réseau l'apprécient pour des tâches de routine comme les inventaires de réseau, la gestion des mises à jour planifiées ou la surveillance des hôtes et des services actifs.

2.2.1.1 Présentations

Figure 2.04 : *Représentation des services à superviser*

Son interface reprend un découpage classique :

- « Home » accueil : Page d'accueil avec Le « Tactical Overview » de Nagios permettant un coup d'œil rapide aux problèmes survenus et accès aux statistiques des performances du moteur et de ses composants.
- « Monitoring » ou supervisé : Possède plusieurs vues, mais reprend la grande idée de l'arbre des groupes d'équipements.
- « Views » ou vues : Permet d'accéder à tous les graphiques avec un menu arborescent. Accès à une cartographie du réseau en applet Java.
- « Reporting » ou rapport : Un tableau de présentation ressemblant à celui de Zabbix en ajoutant une frise chronologique de la disponibilité de l'équipement.
- Administration : La possibilité de la configuration des accès utilisateurs.

2.2.1.2 Formulaires de liaison

- Module d'auto-détection des ressources présentes sur le réseau (via NMAP).
- Création de graphes au sein des modules :
- Mécanismes de patrons/modèles.
- Module unique, donc moins de ressources systèmes consommées, sans outil externe.
- Test de validité des configurations de Nagios avant mise en production.

2.2.1.3 Avantages

- La robustesse et la renommée de Nagios ;
- L’interface Nagios est beaucoup plus sympathique, permettant de tout configurer, de garder un œil sur tout le réseau en permanence ;
- Les utilisateurs de Nagios ne seront pas perdus pour autant, l'interface reprenant avantageusement certaines vues Nagios ;
- La solution complète dans Nagios permet le rapport, la gestion de panne et d'alarmes, gestion utilisateurs, ainsi que la cartographie du réseau ;
- L’entreprise Nagios pousse le développement ;
- Le logiciel peut être décoléré (mise en veille par rapport au serveur Nagios) du serveur Nagios et tourner tout seul sur un autre serveur.

Les avantages de Nagios se situent surtout dans l’ouverture de développement du logiciel grâce à des équipes dans le monde qui offrent leurs contributions sur la plateforme open source.

2.2.1.4 Inconvénient

L'interface peut paraître complexe car il existe beaucoup d'options, c'est-à-dire des aspects visuels de configuration possible nécessitant une petite formation.

2.2.2 Centreon

Centreon est un produit dérivé de Nagios, présente plusieurs aspects qui mettent en priorité la possibilité de développement du produit à de nombreux utilisateurs.

Centreon, basé sur Nagios, se présente comme une évolution de celui-ci pour tout d'abord son interface mais aussi ses fonctionnalités.

Créé en 2003 par des français souhaitant améliorer Nagios et son interface très austère, Centreon (anciennement Oréon) a été repris par une nouvelle entreprise nommée Merethis. Centreon reprend donc les avantages du moteur de Nagios et permet ainsi d'être entièrement compatible avec des solutions existantes.

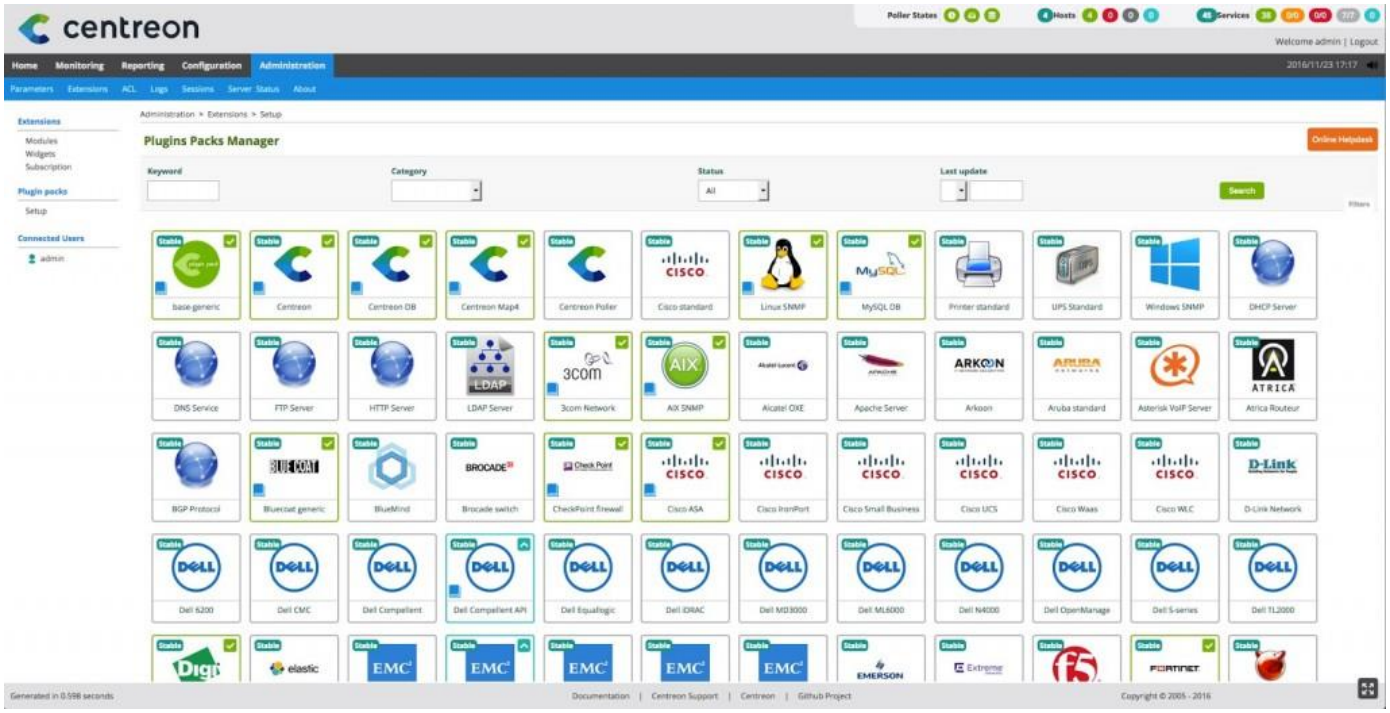


Figure 2.05 : *Représentation des matériels disponibles dans le menu plugins*

2.2.2.1 Présentation de Centreon

- Surcouche applicative au-dessus de Nagios.
- Intégration d'une interface multi-utilisateurs complète et intuitive.
- Ajout de nouvelles possibilités de supervision.
- Utilisation du langage PHP pour réaliser le client Web.

- Projet français basé sur la licence GPL v2.
- Large communauté d'utilisateurs.
- Création d'une activité de services par les fondateurs du projet.

2.2.2.2 Fonctionnalités de Centreon

- Interface de configuration des différents éléments de Nagios :
- Hôtes, services, contacts, alertes, etc.
- Formulaires complets et intuitifs.
- Gestion graphique des fichiers de configuration et des plugins. Nagios.cfg et resource.cfg
- Politique de gestions des profils utilisateurs (droits, langues, accès aux ressources).
- Stockage des informations de configuration dans des fichiers textes et une base de données [2.07].

2.2.2.3 Inconvénients rencontrés par Centreon

- Le développement qui n'est pas encore en phase avec celui de Nagios : parfois rencontre des problèmes de compatibilité ;
- L'implémentation est un peu plus lourde que du Nagios pur. Génération des graphes à partir de RRD ou Round-Robin Database

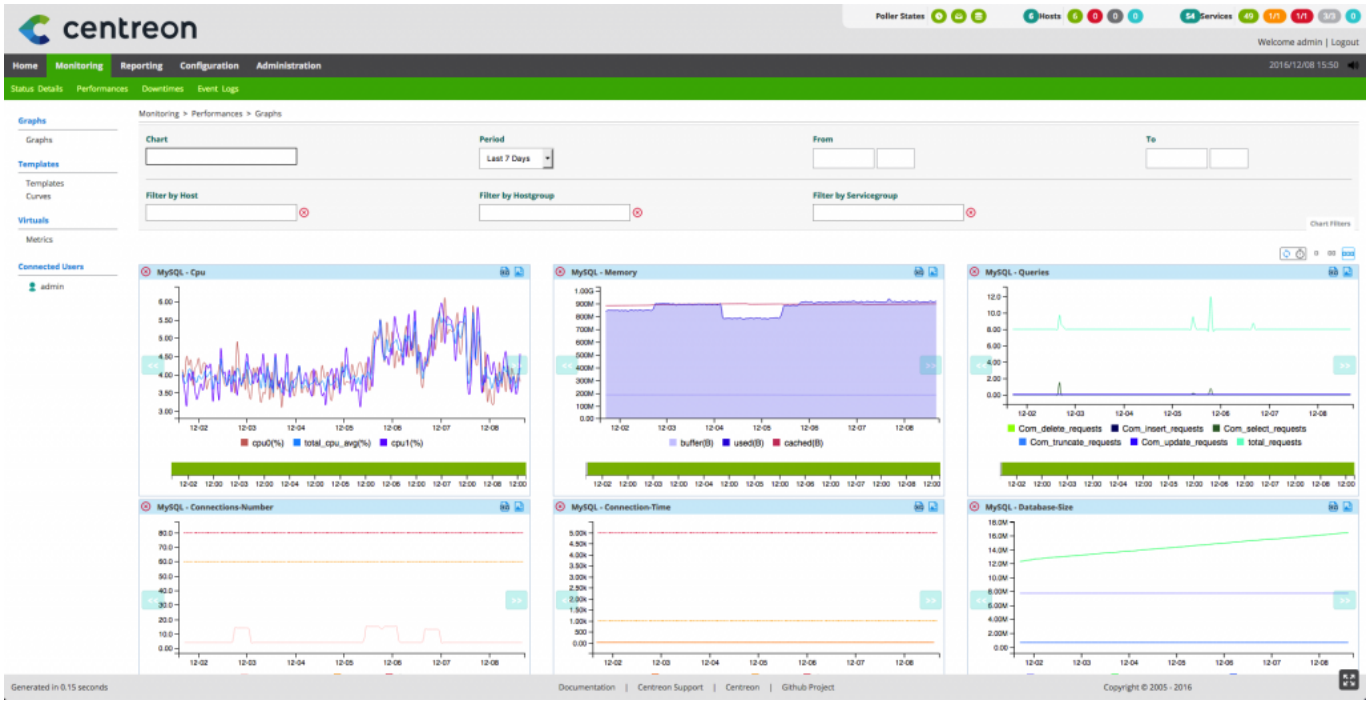


Figure 2.06 : *Représentation graphique de plage de performance et de fonctionnement avec Centreon.*

La supervision graphique des données est ce qui permet d'avoir un historique. Alors il existe la possibilité de comparer des graphes.

Centreon génère également les fichiers de configuration de Nagios (c'est-à-dire :/etc/nagios) à partir des informations saisies dans l'interface Web.

A cela, Centreon offre un « toolkit » proposant des fonctionnalités avancées comme :

- Traceroute,
- NMAP,
- WOL,
- Reboot,
- Ping, etc…

Ce sont des configurations dont les utilisateurs vont mettre en place aux machines qu'il va surveiller. Les utilisateurs ont une facilité de choix de monitoring par rapport à Centreon.

2.2.3 MRTG (Multiple Router Traffic Grapher)

MRTG est un logiciel dédié à la supervision réseau. Il permet d'obtenir toute une série de statistiques (visualisation de charge sur un réseau, utilisation de bande passante...) concernant un appareil informatique (tels que routeurs, serveurs, ou PC) sous forme de représentations graphiques.

2.2.3.1 Présentations

Il va pour cela cherché des informations directement sur les interfaces des machines du réseau via le protocole SNMP (Simple Network Management Protocol) est un protocole facilitant l'administration de systèmes à distance [2.08].

Outil connu des grandes entreprises, entièrement configurable et gratuit, MRTG (Multi Router Traffic Grapher) est un « Freeware » constitué de scripts en langage Perl, distribué librement sur le Web. Il présente les résultats de ses recherches sur des pages Web classiques, ce qui facilite nettement l'accès à un utilisateur quelconque, quelle que soit la machine utilisée.

MRTG est un outil réalisé en Perl et en C dans le but de surveiller la charge des liens réseaux. Il génère des pages html contenant des images au format PNG qui représentent graphiquement l'état en temps réel de la ressource surveillée.

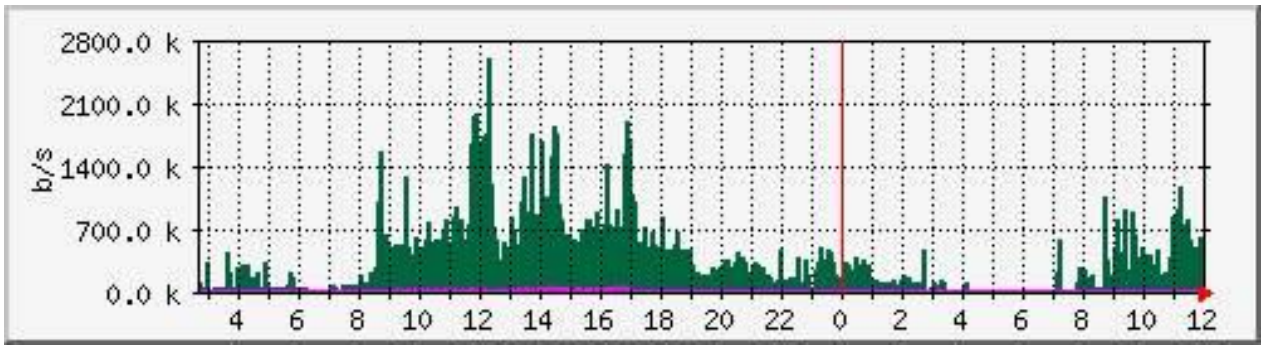


Figure 2.07 : *Représentation graphique de trafic vers les serveurs par MRTG*

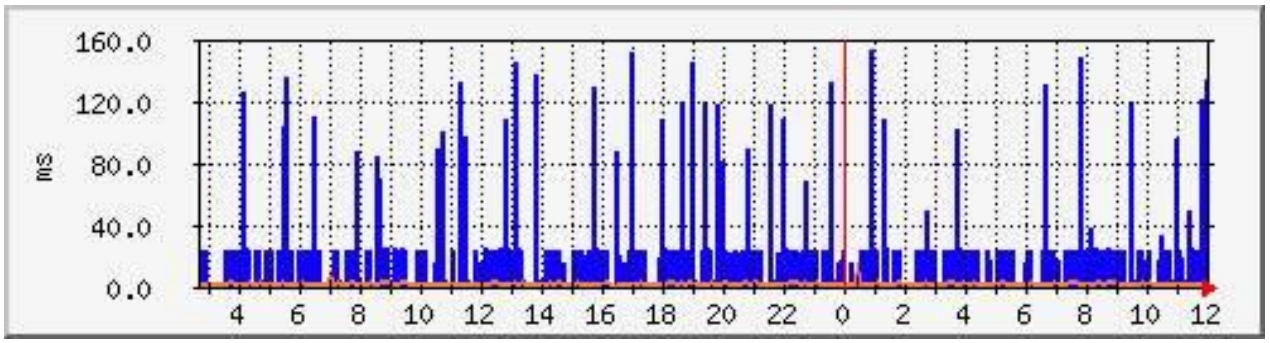


Figure 2.08 : *Représentation graphique du trafic vers les clients par MRTG*

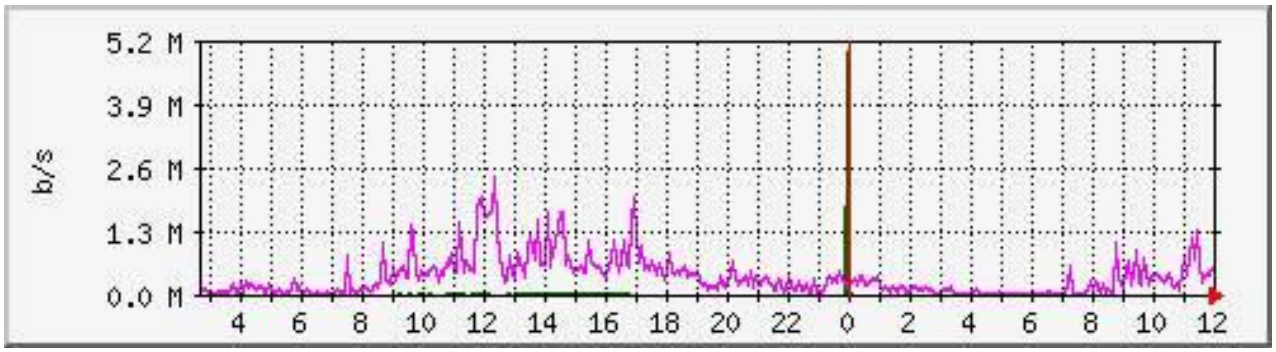


Figure 2.09 : *Représentation graphique de connexion TCP*

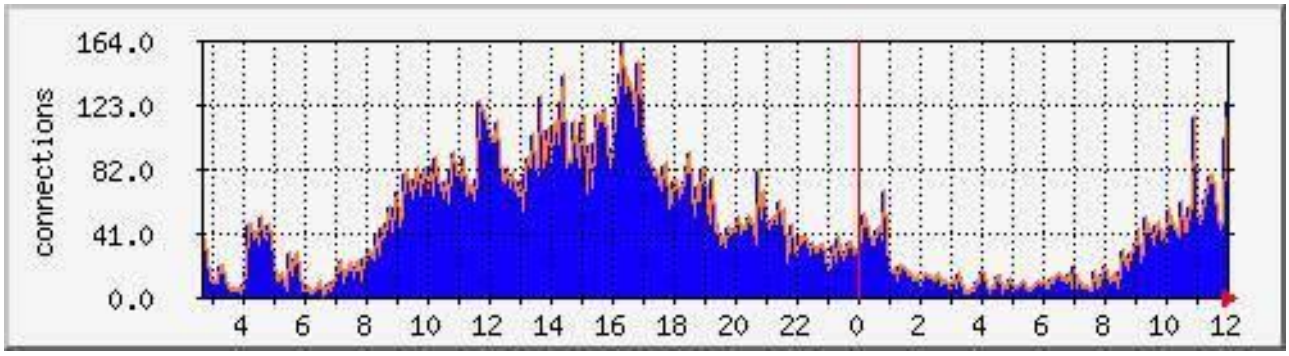


Figure 2.10 : *Représentation graphique de trafics sortant et entrant du serveur*

2.2.3.2 Principe de fonctionnement avec MRTG

Un script Perl recherche les données via le protocole SNMP et envoi celles-ci à un programme. Ce programme est spécifié à une tâche et ce qui va les stocker et générer les graphiques. A la base l'auteur avait dans le but de surveiller le trafic passant par des routeurs, mais MRTG se basant sur SNMP, les possibilités se sont étendues à toute variable. Encore mieux, il est aussi possible créer un script qui surveillera n'importe quel type de donnée non disponible dans SNMP. L'utilisateur possède ainsi un système de surveillance déjà conséquent qui permet sur une même page de surveiller un réseau et de garder les traces des anciennes données.

2.2.3.3 Avantages

MRTG possède de nombreux avantages :

- MRTG est un logiciel gratuit, développé par une communauté de développeurs passionnés.
- MRTG est un outil multi plateforme (Linux, Unix, Windows), car il utilise un script perl.
- MRTG étant basé sur le protocole SNMP, il n'est pas limité au simple contrôle du trafic mais on peut contrôler n'importe quelle variable SNMP que l'on a choisie car MRTG réalise une commande SNMPGET. De plus on peut même employer un programme externe pour recueillir les données qui doivent être contrôlées via MRTG. Enfin on peut contrôler plus de 50 liens réseaux à partir d'une machine UNIX ou LINUX.
- MRTG possède une configuration qui se fait par l'intermédiaire d'un fichier de configuration unique, ce qui permet un control total de ses fonctionnalités.

2.2.3.4 Inconvénients

- Passe trop de temps à créer des pages HTML (mal adapté à des grands sites) ;
- Trop orienté SNMP ;
- Graphiques à deux courbes ;
- Pas de gestion des données non fournies.

D'autre logiciel offre des services similaires en spécifiant leurs techniques et configuration nécessaire.

2.3 Conception de monitoring personnalisé propre à une entreprise quelconque

Le mot anglais « uptime », que l'on peut traduire par disponibilité ou temps de service, est utilisé en informatique pour définir la période de temps durant laquelle un système informatique est en fonction et disponible. Appliquée à un réseau, la notion d'uptime se définit en termes de

disponibilité et de fiabilité des serveurs et des appareils, ou par domaine et disponibilité des sites web. La plupart du temps, elle est affichée sous forme de pourcentage. Une disponibilité de 90 % sur l'ensemble d'une journée signifie que le **sys**tème a été fonctionnel et disponible pendant exactement 1296 minutes (soit 21,6 heures) ce jour-là [2.09].

2.3.1 Conception en UML ou « Unified Modeling Language »

L'UML est un langage de modélisation unifié, qui varie selon le besoin d'un concepteur. Dans cette étude il sera utilisé pour l'étude de cas par rapport à un système de supervision réseau.

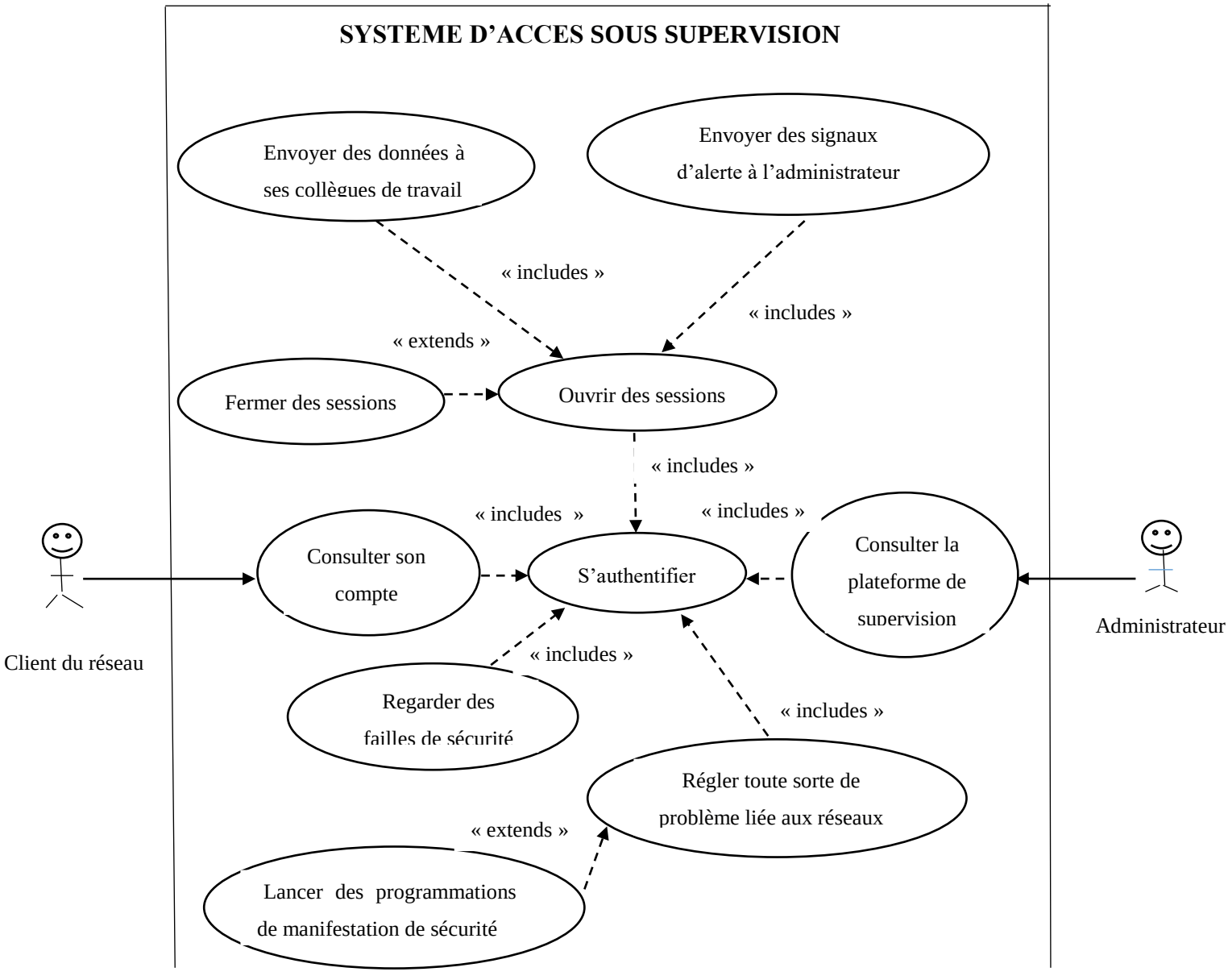


Figure 2.12 : *Diagramme de cas d'utilisation*

En UML, on établit des diagrammes de cas d'utilisation pour répondre à la question, à quoi va servir le logiciel ?

2.3.2 Monitoring sous PRTG

Il existe plusieurs plateformes de surveillance sous PRTG depuis son développement. Les plateformes sous Windows, Mac, Linux sont plus connues, mais il existe cependant une plateforme sous Android.

2.3.2.1 Etude de la plateforme PRTG

PRTG est une des plateformes conçus et mise dans le marché pour sa stabilité.

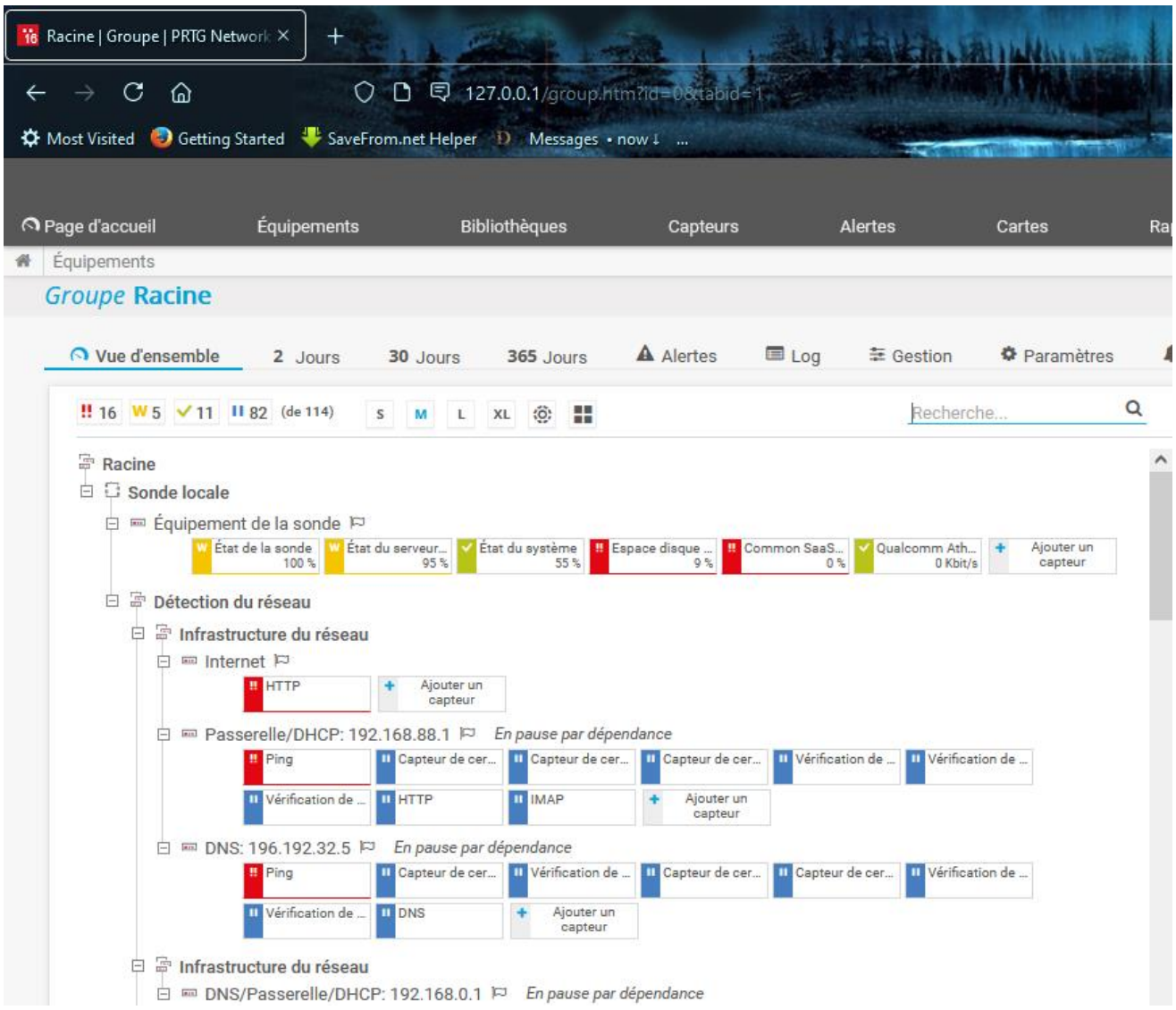


Figure 2.13 : *Plateforme de supervision sous PRTG*

a. Offre sans engagement

La version de base de PRTG est gratuite et intègre 100 capteurs utilisables à vie. Durant les 30 premiers jours, il existe également de la version complète du logiciel et d'un nombre illimité de capteurs, de sorte à se familiariser au fonctionnement de PRTG.

b. Outil unique pour les besoin de surveillance

PRTG dispose plusieurs outils de surveillance complète et centralisé qui couvre tous les besoins de surveillance. PRTG est facile à configurer et économe en bande passante.

c. Outil qui identifie automatiquement la cause des pannes

Grâce à PRTG, la possibilité de visualiser d'un coup d'œil l'ensemble de l'infrastructure informatique est disponible et bien mise en évidence. Le logiciel permet de suivre en tout temps la disponibilité des services et leurs éventuelles interruptions, mais aussi de déterminer la cause des dysfonctionnements.

d. Système d'alerte réactif

Le système de notification personnalisable de PRTG alerte l'utilisateur immédiatement en cas de problème, si bien qu'il est possible de le résoudre avant que la situation n'empire. Plutôt que d'attendre que l'incendie se déclare pour l'éteindre, il y a également une mesure préventive son départ.

e. Rapports exhaustifs

PRTG dispose d'un système de rapport (reporting) exhaustif incluant des statistiques, des graphiques, et bien plus encore. Il y a aussi possibilité de créer des rapports personnalisés et faire en sorte qu'ils soient automatiquement transmis à aux supérieurs hiérarchiques. Ces rapports permettront aussi de voir comment et à quels postes l'entreprise peut économiser des ressources.

f. Compatibilité parfaite

Le large éventail de capteurs de surveillance : des sondes préconfigurées qu'embarque PRTG lui permet de garantir une compatibilité parfaite avec la quasi-totalité des fabricants d'appareils, parmi lesquels Cisco, Dell, Oracle ou bien HP.

2.3.2.2 Avantages de la PRTG

PRTG est une plateforme de supervision réseau et système adapté à tous appareils de communication liée entre eux, présentant plusieurs avantages.

a. Disponibilités des serveurs

Avec PRTG, il y a possibilité de vérifier le temps de fonctionnement de tous les serveurs. Qu'il s'agisse de CDN, d'un serveur FTP, d'un serveur de messagerie, d'un serveur DNS, d'un serveur web comme IIS, d'un serveur SQL ou de serveurs virtuels comme VMware ou Hyper-V, PRTG consigne absolument tout.

Charge CPU, mémoire, bande passante et bien d'autres paramètres des performances de des serveurs sont surveillés par défaut.

b. Disponibilité des appareils

Avec PRTG peut vérifier si des appareils fonctionne ou pas, qu'il s'agisse d'un ordinateur de bureau, d'un routeur, d'un commutateur ou de tout autre composant réseau.

c. Disponibilité des sites web

Bien souvent, la disponibilité du site web d'une entreprise joue un rôle majeur dans les performances de ses ventes. Et pour cause : chaque seconde où le site est inaccessible est autant de temps pendant lequel les clients sont dans l'incapacité de consulter les produits ou de passer commande. Grâce à PRTG, la surveillance est non seulement la disponibilité, la rapidité et les performances de des bases de données, mais aussi le contenu du site web.

2.3.2.3 Simplicité au niveau de l'utilisation plateforme PRTG

Beaucoup d'entreprise se repose sur l'utilisation de ce produit grâce aux facilités de manipulation, d'étude et de mise en place de la plateforme.

a. Gain de temps

Avec PRTG, il n'y a qu'un seul et même outil de supervision pour tout le hardware de l'entreprise. Grâce au tableau de bord et aux applications, il est possible de voir d'un coup d'œil et vérifier que tout est en ordre sur l'ensemble du réseau, à tout moment et depuis n'importe quel endroit.

b. Vecteur d'économie

80 % des utilisateurs ont réalisé des économies importantes, sinon considérables, dans le domaine de la gestion réseau. L'expérience montre que le coût des licences a été rentabilisé en seulement quelques semaines.

Remarquons : Les «capteurs» sont les éléments de supervision de base de PRTG. Un capteur surveille généralement une valeur mesurée dans un réseau, par exemple le trafic d'un port de commutateur, la charge du processeur d'un serveur, l'espace libre d'un lecteur de disque. Il y a en moyenne de 5 à 10 capteurs par appareil ou d'un capteur par port au commutateur.

2.3.2.4 Implémentation de la surveillance PRTG dans Android

PRTG possède une plateforme Android propre à lui. Cependant, la possibilité que l'entreprise peut s'offrir une plateforme personnalisée pour la surveillance spécifique d'un système ou d'un réseau bien défini va faciliter les tâches aux chefs de maintenance ou chefs de service de l'entreprise.

Tableau 2.01: *Représentation d'une architecture Android*

Couche applicative	Alarme, Navigateur, Calculatrice, Calendrier, Caméra, Horloge, Contacts, Téléphone, Courriel, Accueil, Messagerie instantanée, Visionneuse de contenu multimédia, Album photo, SMS/MMS, Appel vocal
Cadriciel Android	Fournisseurs de contenu (ou Content Providers), Gestionnaires (ou Managers), Système de vues
Bibliothèques logicielles natives	Engin d'exécution Android
Bibliothèque logicielle élémentaire, MVD/ART	Gestionnaire audio, Freetype, Libc, Cadriciel média, OpenGL/ES, SQLite, SSL, Gestionnaire de surface, WebKit
CAM	Audio, Bluetooth, Caméra, Gestion Numérique des Droits (Digital Rights Management, GND), Stockage externe, Graphiques, Entrées, Média, Capteurs, TV
Noyau Linux	Pilotes de périphériques, gestionnaire d'alimentation.

a. Application Android

De nos jours, l'utilisation des appareils Android est une évolution technologique dont il faut prendre en compte l'importance. Les entreprises mettent en dispositions des appareilles de communication pour tous ou des personnels bien définies. Plusieurs produits Android circulent dans le monde de la technologie. D'autant plus des applications gratuites ou payantes s'échange

dans différents sites web. Les entreprises ne peuvent risquer la vulnérabilité de leurs infrastructures par ses produits.
L'entreprise peut donc favoriser ses propres applications sur commande ou produire leurs propres applications par leurs propres informaticiens ou programmeurs.
Android est construit en suivant une structure en couche telle que représentée au tableau 2.01 [2.10], et est construit sur la base d'un noyau Linux.
Ce type d'architecture permet d'abstraire les actions élémentaires (accès mémoire, gestion de l'alimentation, etc.) pour les développeurs d'applications et d'isoler les composantes les unes des autres pour des questions de sécurité.

- Couche applicative

La couche Android déployées sur un appareil. Le SE Android expose un kit de développement logiciel (Software Development Kit, SDK) en Java permettant la création d'applications capables d'interagir avec le système via l'Application Programming Interface (API) d'Android.
Le SDK et l'API sont mis à jour régulièrement par Google tant pour corriger des problèmes de sécurité que pour l'ajout de nouvelles fonctionnalités. Pour qu'une application s'exécute sur un appareil Android, celui-ci doit avoir une version du SE suffisamment à jour pour supporter les fonctionnalités de la version de l'API visée. Pour cette raison, un développeur peut volontairement choisir de créer une application visant une version de l'API antérieure à la dernière disponible.
De cette façon, l'application peut être utilisable sur des appareils plus anciens. Une fois installées sur un appareil, les applications utilisent le cadriciel (ou framework) d'Android pour communiquer avec les différentes composantes du SE.

- Cadriciel Android :

Cette couche est responsable d'offrir aux applications les services applicatifs qu'elles nécessitent pour accomplir leurs tâches. Les différentes abstractions offertes par cette couche sont ensuite redirigées vers les couches subséquentes pour le traitement [2.11].

- Engin d'exécution Android

Cette couche est responsable de l'exécution des applications en tant que telles. En plus de contenir le nécessaire à l'exécution des applications Android, cette couche est responsable de la conversion du bytecode Dalvik en instructions-machines exécutables par le processeur de la plateforme. Jusqu'à la version 4.4.4, cette conversion est réalisée par la compilation à la volée (Just-In-Time

Compilation, JIT) par un interpréteur contenu dans la machine virtuelle Dalvik (Dalvik Virtual Machine, MVD). L'interpréteur est conçu pour conserver en mémoire vive le code compilé des sections de bytecode les plus fréquemment parcourues pendant l'exécution de l'application. Cela permet de minimiser l'impact sur la performance de la compilation à la volée, tel que décrit par Cheng et Buzbee [2.12].

Depuis la version 5.0 d'Android, Android Runtime (ART) remplace la MVD officiellement. Ce nouvel environnement d'exécution délaisse la compilation à la volée et utilise plutôt la compilation anticipée (Ahead-Of-Time Compilation, AOT). Tel qu'il est expliqué par Ghuloum et al. [2.13], ce changement de paradigme améliore les performances et réduit la consommation énergétique. Ces optimisations se font au coût d'un temps d'installation plus long et de plus d'espace de stockage utilisé par installation.

- Bibliothèques logicielles natives :

Il arrive que certaines parties d'une application nécessitent d'être optimisé afin de répondre aux besoins de performances d'une utilisation donnée. Le rendu 3D, la cryptographie ou encore la lecture de contenu multimédia en sont de bons exemples. Dans ces cas, des bibliothèques logicielles natives (C/C++) offrent aux applications Android la capacité d'exécuter du code natif afin d'optimiser la vitesse d'exécution de segments de code coûteux en temps de traitement ou requérant un contrôle plus fin de ses structures de données internes.

- Couche d'abstraction matérielle

Étant un SE ouvert, Android permet aux fabricants de choisir les composantes qu'ils désirent intégrer à leurs appareils. La couche d'abstraction matérielle (Hardware Abstraction Layer, CAM) offre une interface universelle permettant d'interagir avec les périphériques sans se soucier des particularités d'implémentations de chaque fabricant. Ces particularités sont déléguées aux pilotes de périphérique. L'implémentation de ces derniers est typiquement la responsabilité des manufacturiers d'appareils Android puisqu'ils adaptent le SE lors de la conception de ces dispositifs [2.14].

- Noyau Linux

Le SE Android est construit sur la base d'un noyau modifié de Linux [2.15]. Ce noyau orchestre les fonctionnalités élémentaires d'Android telles que la gestion des fils d'exécutions, des périphériques, de l'alimentation, de la mémoire vive et du contrôle des accès et privilèges. Ce

noyau est compilé à partir d'une mouture appelée Bionic [2.16] découlant de glibc et de BSD. L'une des caractéristiques principales de Bionic est qu'il a été optimisé pour les processeurs à faible fréquence d'horloge, ce qui était, à l'origine, le cas des processeurs des premiers appareils Android, tel que décrit par Devos [2.17].

Cette composante d'Android est la plus critique puisqu'une erreur ou une corruption à ce niveau est susceptible de compromettre l'entièreté de l'appareil. De ce fait, il s'agit de l'une des cibles d'attaques les plus prisées pour l'exploitation d'Android [2.18].

En sachant, les différentes couches existantes dans un système d'exploitation Android, la possibilité d'en tirer la faisabilité de l'application personnalisée pour une entreprise quelconque est réalisable.

b. Conception d'application Android

L'objectif de la conception est de ramener l'interface du PRTG local dans une application nommée supervisionLOCAL sur les appareils Android d'un ou plusieurs chefs de service en réseau ou système, afin que son intervention soit rapide et défini.

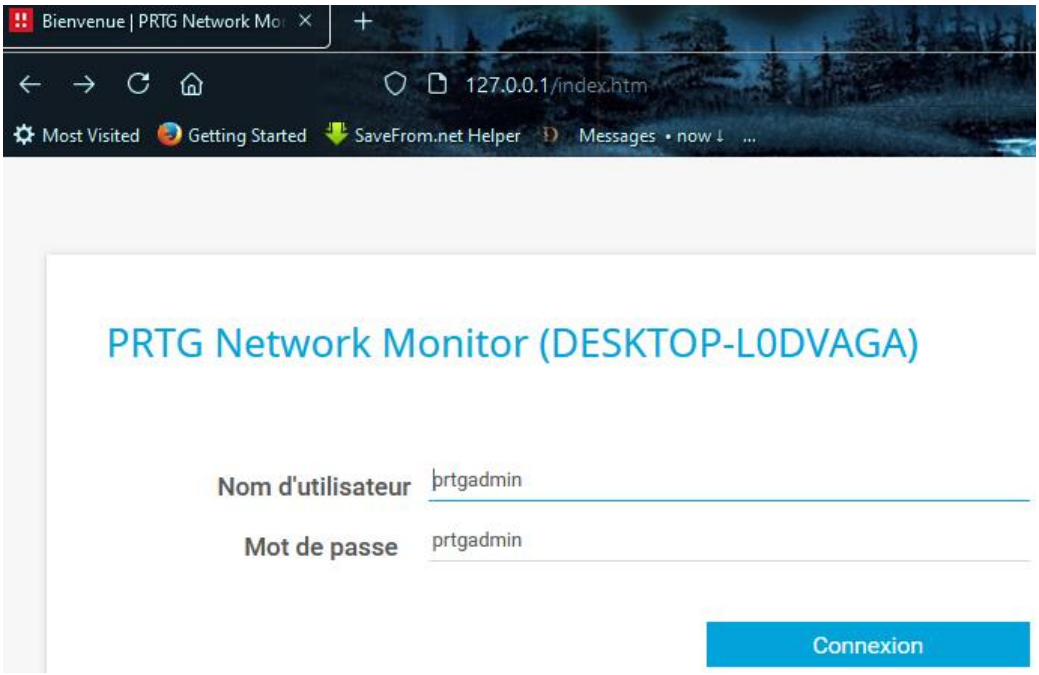


Figure 2.14 : *Représentation du site web avec PRTG*

Figure 2.15 : *Programmer un site web local dans une application Android*

Mettre en place une liaison entre le site du réseau local de surveillance avec une application Android personnalisé est le projet final de notre étude afin d'aider les utilisateurs à avoir une vision globale de son environnement de travail.

2.3.3 Concevoir des « sniffers » de réseaux avec python

Python est un langage de programmation pour le développement de systèmes très avancée et flexible. Il permet au développeur ou administrateur de réseau de mettre en place un environnement personnalisé selon le besoin du réseau d'entreprise.

Figure 2.16 : *Logo de Python*

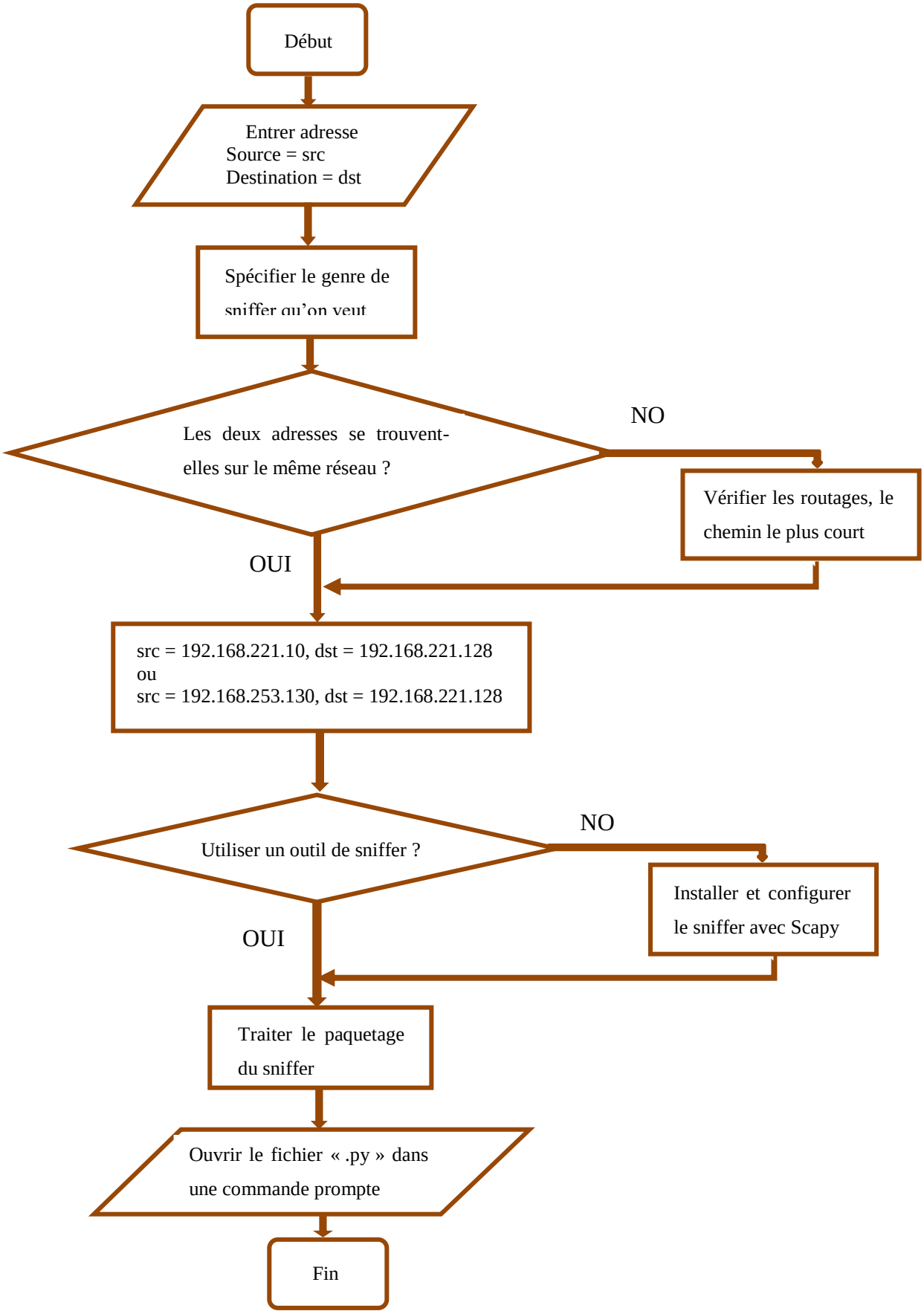


Figure 2.17 : *Algorithme de sniffer avec Python*

2.3.3.1 Intégration de Scapy

Scapy est l'outil de manipulation de réseau qu'offre python. Plusieurs techniques de supervision de réseaux y sont programmables. Ainsi que des tests de manifestation de l'extérieur qui sont des types d'attaques aux réseaux.

Scapy est un programme de manipulation de paquet informatique assez robuste. Il peut facilement accomplir plusieurs tâches classiques telles que scanné le réseau, tracé les routages de paquets. Il peut remplacer : « hping, arpspoof, arpsk, tcpdump » et bien plus de logiciel d'espionnage réseau de nos jours.

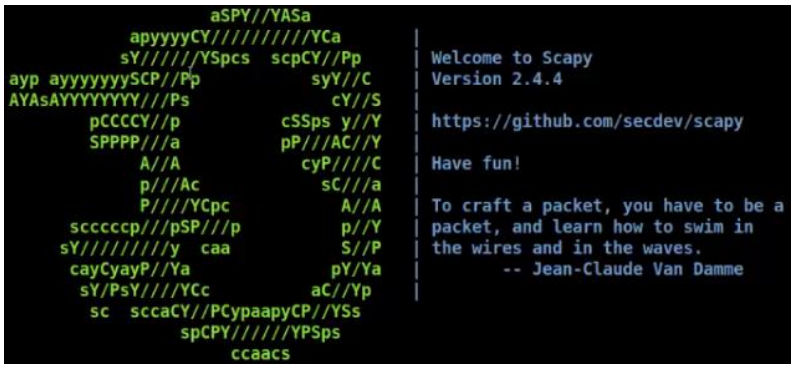


Figure 2.18 : *Iinstallation réussite avec Scapy*

2.4 Conclusion

Les études qui sont faites dans cette recherche montrent une réponse évidente du fait que la supervision des infrastructures des réseaux et du système est très importante au sein d'une entreprise. Grâce à l'avancée technologique que monde découvre et innove chaque année, la télécommunication et les échanges électroniques s'améliore pour être à la portée de tous utilisateurs. Amélioré le quotidien des responsables dans les entreprises les autorise, à offrir un environnement de responsabilité à tout employé. Android est un des appareils technologique qui est plus à la portée de l'entreprise. De ce fait, inclure le port des appareils Android au sein d'une société améliorera les échanges d'informations dans l'entreprise et favorise l'intervention des agents de travails.

CHAPITRE 3
REALISATION D'UNE SUPERVISION RESEAUX

3.1 Introduction

La mission d'un ingénieur-réseau commence dès la phase de conception d'un réseau nouveau. Il participe au choix des logiciels et des matériels, il est responsable de l'installation du réseau. L'ingénieur système-réseau allie des compétences dans deux domaines : l'informatique et les télécommunications. Il identifie et résout les problèmes des utilisateurs. Par ailleurs, il est aussi responsable de la sécurité sur le réseau. C'est lui qui assure la confidentialité des données qui y transitent.

L'ingénieur système-réseau est capable d'identifier et d'anticiper les besoins en informatique de l'entreprise. Pour cela il travaille avec les gestionnaires de réseau qui l'informent sur les baisses de performances et les dysfonctionnements éventuels.

L'ingénieur système-réseau a une connaissance pointue des différents matériels existants sur le marché et des dernières avancées technologiques. Il doit être curieux, avoir une grande capacité d'adaptation. Cet ingénieur travaille en majeur partie dans des entreprises de moins de cinq cents salariés, au-delà, les fonctions système et réseau sont souvent distinctes.

3.1.1 Réseau à mettre en place

La réalisation se fait dans un environnement PC physique avec Windows10. Dans ce PC des machines virtuelles sont installées dans VMware Workstation Pro [3.01]. La machine physique et les machines virtuelles sont des serveurs mises en liaison réseau par le logiciel GNS3.

3.1.1.1 Architecture du réseau

Le réseau est une mise en place de trois différents types de serveurs. Deux serveurs monitoring et un serveur de données.

L'architecture figure 3.01 offre des résultats d'étude différents. Les trois serveurs se trouvent dans la même plage d'adresse afin qu'ils se retrouvent facilement, car les échanges de données y seront nécessaire. Cependant lors de la configuration des machines clients l'administrateur va pouvoir configurer chaque client selon le service qui lui convient.

Les configurations d'équipements d'un même réseau contiennent un grand nombre de paramètres redondants. Citons, entre autres, les paramètres d'authentification, ceux relatifs aux interfaces interconnectées, une grande partie des paramètres relatifs aux protocoles de routage.

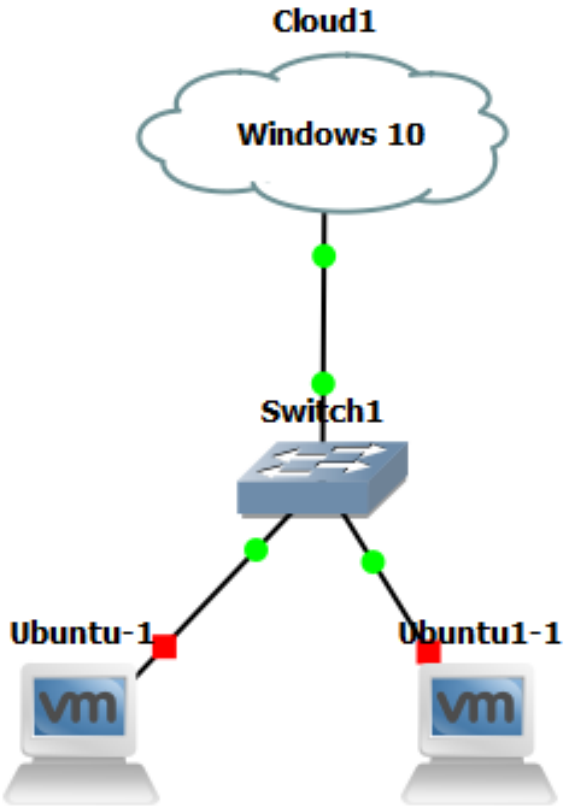


Figure 3.01 : *Architecture du réseau avec GNS3*

L'architecture topologie en étoile est une structure qui relie par câble chaque station à un serveur central chargé de les gérer et de les contrôler. Bien que cette configuration soit simple, elle engendre des coûts de câblage élevés en plus d'une limitation de la puissance du nœud central (limite relative aux débits à assurer).

3.1.1.2 Méthode souhaitée par la supervision : IDS « Intusion Detection Système »

Comme l'étude précédente montre, les attaques que peux subir le system varient selon la faille (Réseau ou Programmation), de ce fait la détection d'intrusion peut se faire à plusieurs niveaux de classification du système. Il existe Cinq niveau d'étude mise en place par le système IDS, chaque niveau se divise en quelque branche d'étude lui-même.

a. Approche de détection :

Les IDS peuvent être répertoriés dans deux grandes approches de détection. Une approche basée sur les scénarios, elle utilise des bases de signatures d'attaque pour la recherche d'intrusion. La deuxième approche est basée sur le comportement du système vis-à-vis des intrusions. Notant que cet aspect est lié au module d'analyse de l'IDS [3.02].

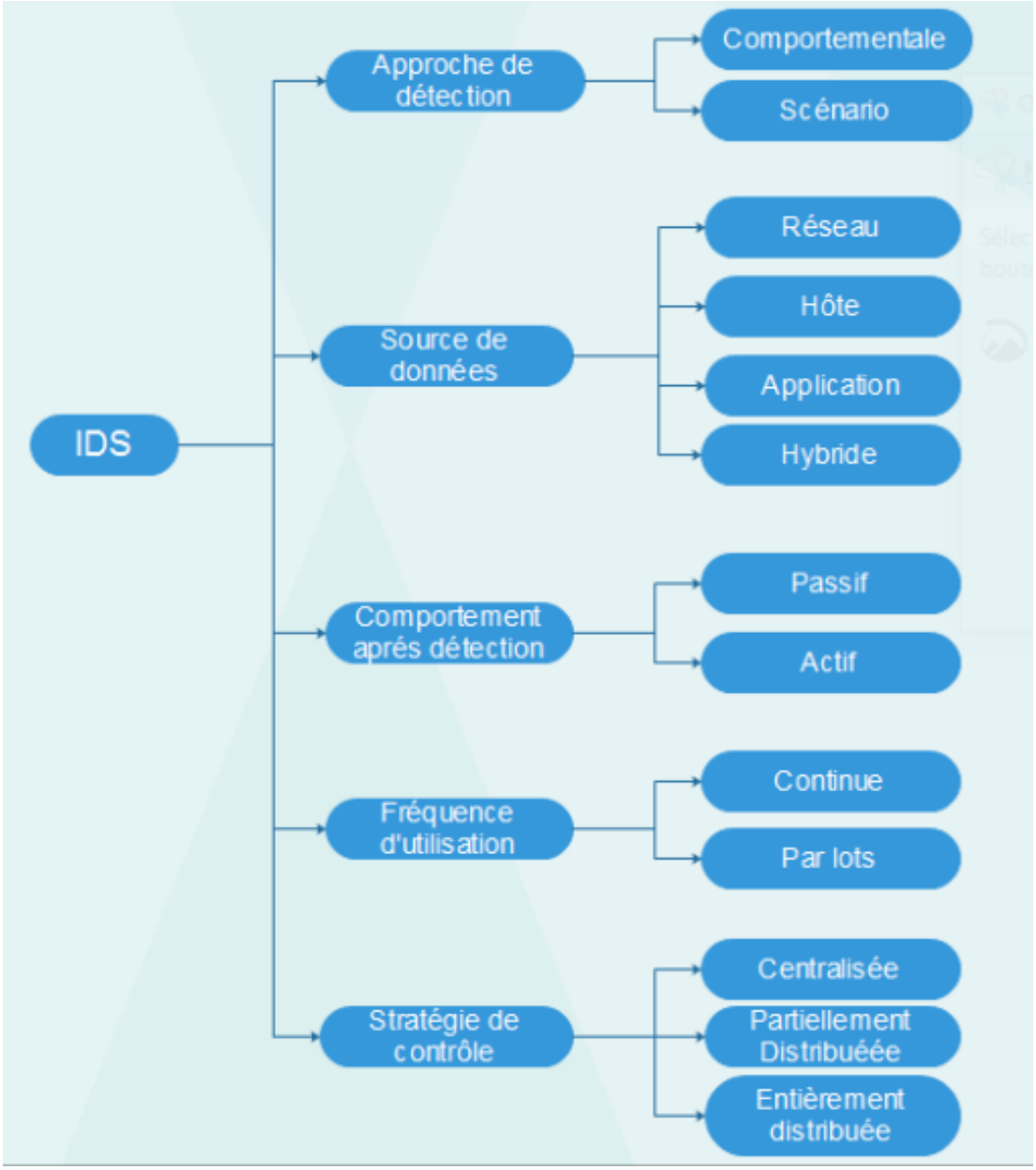


Figure 3.02 : *Classification des systèmes de détection d'intrusion*

b. Source de données :

Les données utilisées dans l'IDS jouent un rôle très important dans le mécanisme de détection d'intrusions. C'est l'interface entre l'IDS et le système surveillé. Les données traitées peuvent provenir d'un trafic réseau ou bien des fichiers locaux du système d'exploitation, comme ça peut provenir des fichiers traités par uns application. Il y a aussi des IDS qui utilisent plusieurs sources de données, c'est une forme hybride. Dans l'architecture d'un IDS, cet aspect est directement lié au module de capture ou bien à la source de données [3.02].

c. Comportement après détection :
Si l'IDS détecte une attaque, deux comportements peuvent être adoptés, une réponse passive ou active. Cet aspect est souvent lié au module de réponse de l'IDS [3.02].

d. Fréquence d'utilisation :

Cet aspect dépend du mode du fonctionnement du module d'analyse de l'IDS. Deux modes d'analyse peuvent être assurés par un IDS : continu ou bien par lots [3.02].

e. Stratégie de contrôle :
Elle décrit les méthodes de gestion des modules composant l'IDS, ainsi que les modes de contrôle appliqués aux entrées et aux sorties de l'IDS. Trois stratégies peuvent être appliquées aux IDS : centralisée, partiellement distribuée ou bien entièrement distribuée [3.02].

3.1.2 Owncloud

L'accès aux services informatiques d'un Cloud privé n'est pas public, mais uniquement réservé à certains utilisateurs ou à une entité prédéfinie. Pour cela, et contrairement au Cloud public, le fournisseur correspondant apporte des ressources dédiées. L'accès se fait via Internet ou bien via un réseau privé.

Les services d'un Cloud privé sont habituellement spécialement conçus pour répondre aux besoins des entreprises. Ces dernières ont le choix entre héberger directement l'infrastructure du Cloud privé sur le site même de l'entreprise ou bien dans le centre de données d'un fournisseur de services, assurant ainsi un niveau de sécurité bien supérieur. Les différents composants et services sont adaptés à chaque entreprise : ordinateurs, stockage et exploitation du réseau peuvent en effet être adaptés individuellement.

De ce fait, Owncloud est une des plateformes qui existe dans le domaine cloud privé qui nécessite qu'un administrateur le gère.

3.1.2.1 Installation d'Owncloud

Les prérequis mémoire pour exécuter un serveur Owncloud sont très variables et dépendent du nombre d'utilisateurs et de fichiers, et du volume d'activité. Owncloud a besoin au minimum de 128 Mo RAM et il est recommandé d'utiliser au moins 512 Mo [3.03].

Figure 3.03 : *Installation d'Owncloud sur Ubuntu 14.04 LTS*

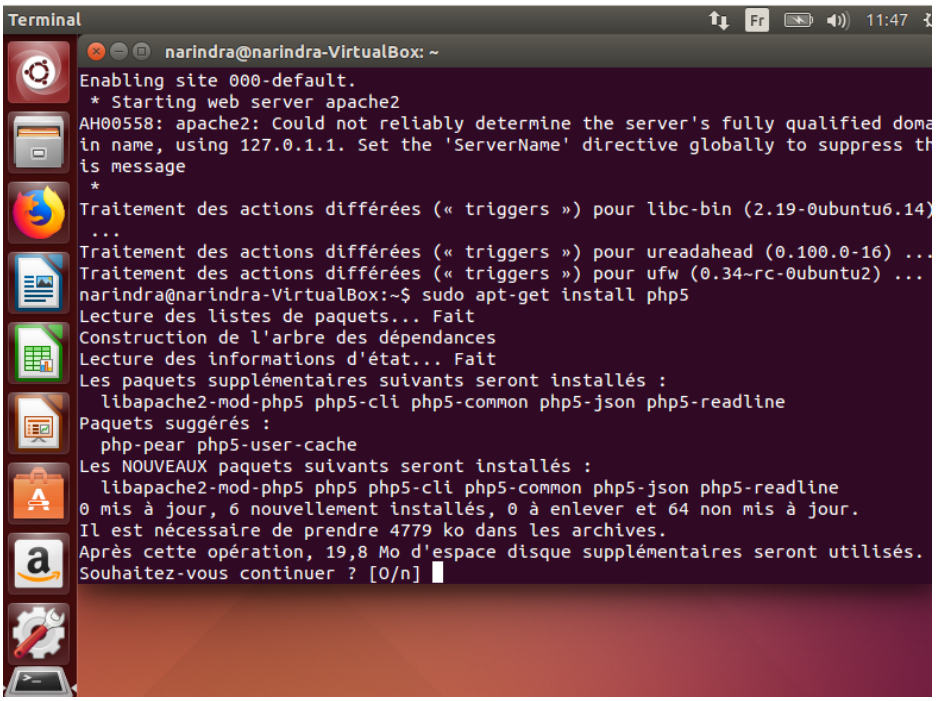


Figure 3.04 : *Installation des serveurs web, base de données et php5*

Pour de meilleures performances, stabilité, support et intégralité des fonctionnalités, il est conseillé d'utiliser les plateformes [3.04]:

- Système d'exploitation Ubuntu 14.04 LTS,
- Base de données traitée avec MySQL,

- Serveur web avec Apache version 2,
- « RunTime » PHP avec PHP version 5.

3.1.2.2 Environnement Owncloud

La recherche d'un environnement de serveur adapté à son projet peut parfois être semée d'embûches. La notion actuelle la plus récurrente est celle de l'hébergement cloud avec infogérance. Cette solution est caractérisée par sa flexibilité face au besoin en ressources des clients qui peuvent fluctuer en temps réel et par son offre complète qui comprend l'installation mais également la mise à jour.

Plusieurs techniques d'installation sont conseillées afin de garantir la sécurité de l'environnement de travail surtout en termes de partage de document avec un serveur de fichier tel dans cette implémentation [3.05].

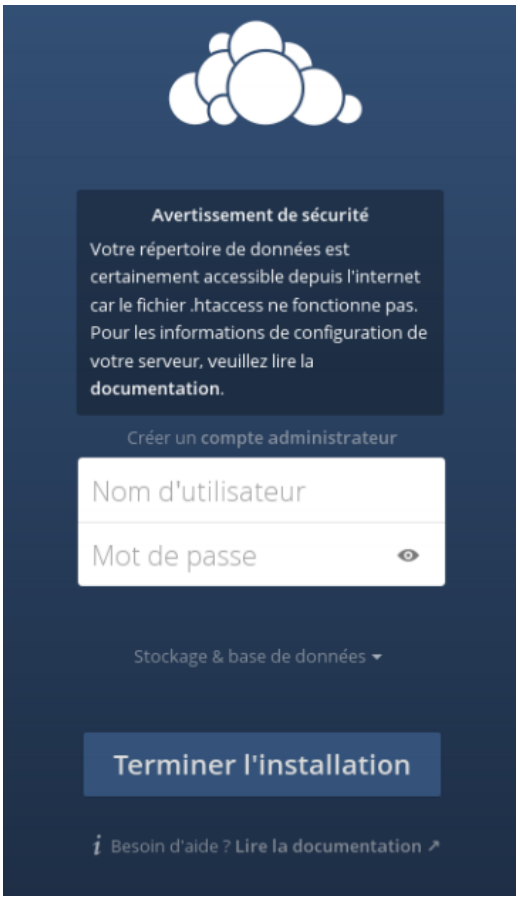


Figure 3.05 : *Installation complet, finalisation*

Quand les prérequis d'Owncloud sont remplis et que les fichiers d'Owncloud sont installés, la dernière étape est terminer l'installation en lançant l'assistant d'installation.

Cela se passe en trois étapes :

- Pointer le navigateur Web sur l'adresse http://localhost/owncloud ;
- Saisir le nom d'administrateur et le mot de passe désiré ;
- Cliquer sur Terminer l'installation pour la finalisation de montage de Owncloud et pour assurer le lancement des paquets qu'il fallait télécharger.

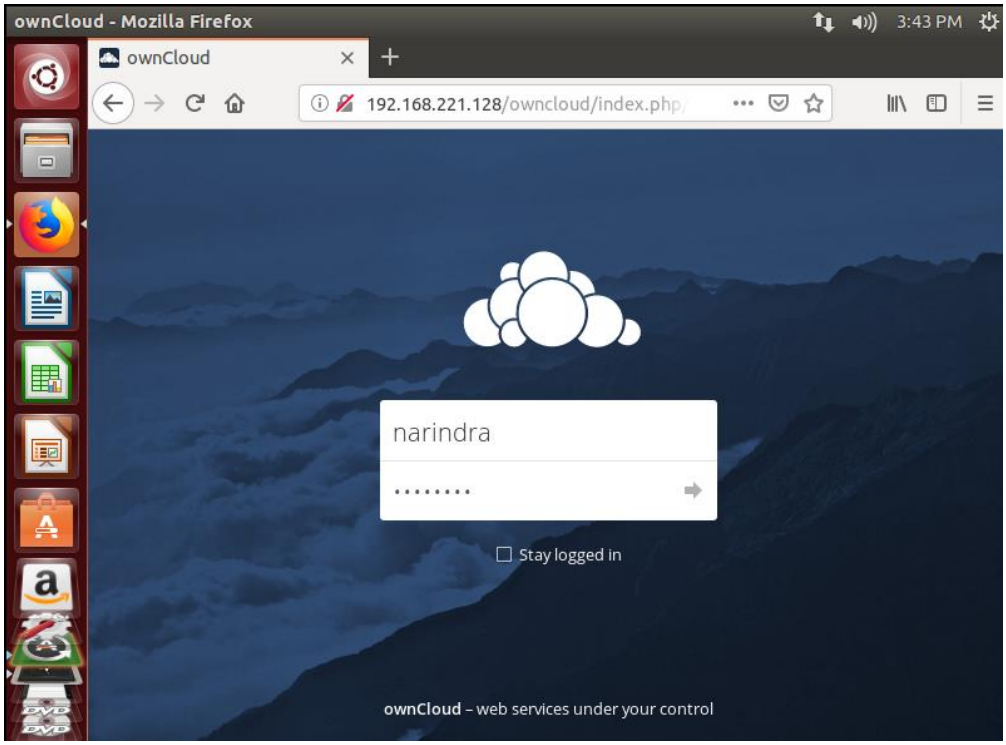


Figure 3.06 : *Login dans Owncloud*

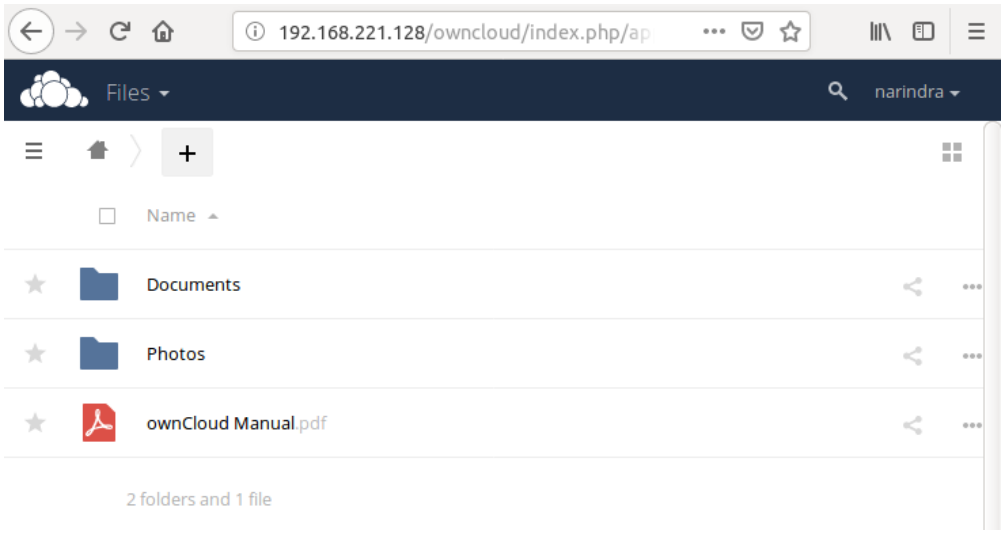


Figure 3.07 : *Page d'accueil avec Owncloud du point de vue client*

Les administrateurs peuvent régler les utilisateurs clients Owncloud pour qu'il se lance dès que leurs ordinateurs démarrent, et qu'ils fassent la synchronisation dès que les utilisateurs ont accès à internet, cela permet d'éviter les mauvaises surprises (aller dans « Paramètres » dans l'interface du client Owncloud sur l'ordinateur).

L'accès aux fichiers dépend en entier des configurations de permission de groupe ou de privilège que l'administrateur offre à chaque utilisateur client au sein de l'entreprise, lorsqu'il se connecte dans le réseau local.

3.1.3 GNS3

GNS3 est un simulateur réseau assez poussé qui permet de mettre en place des infrastructures réseau de façon réaliste, mais totalement virtuelle. Dans cette mise en place il faut savoir comment intégrer les machines virtuelles sous VMware Workstation Pro dans le logiciel GNS3, cela peut être particulièrement pratique pour [3.08] :

- Simuler une mise en production à moindres frais,
- Reproduire un environnement de production pour simuler une migration, une attaque ou une panne,
- Tester, vérifier ou faire éprouver une configuration ou une architecture aussi bien système que réseau.

3.1.3.1 Préparer les cartes réseau

Dans le but d'avoir une mise en place simple, il faut commencer par identifier les cartes réseau virtuelles (il y celles que VMware a créé sur le poste pour lier les VMs la machine réelle, puis au réseau) que l'administrateur va utiliser. Il faut donc se rendre dans le gestionnaire de carte réseau du PC physique.

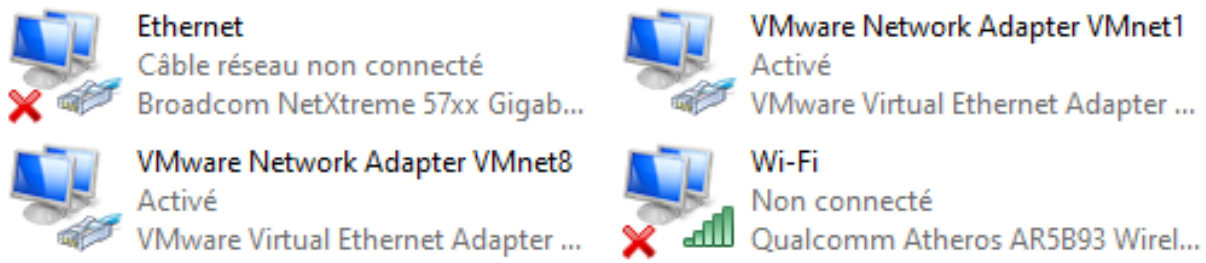


Figure 3.08 : *Cartes réseau par défaut de VMware Workstation*

```
Carte Ethernet VMware Network Adapter VMnet1 :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::65e4:dc5b:807f:79f9%20
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.253.1
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . :

Carte Ethernet VMware Network Adapter VMnet8 :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::34f3:5dc0:8251:5232%19
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.221.1
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . :
```

Figure 3.09 : *Adresses IP configurés sur les cartes réseaux VMware*

Dans la machine physique il est simple de configurer les cartes réseaux selon le besoin des adresses IPv4. Donc faire correspondre les machines virtuelles à mettre en liaison selon l'un des « Adapter VMnet ».

3.1.3.2 Configurer VMware Workstation pour GNS3

Il faudra passer en suite à la configuration côté Workstation qui est aussi plus simple que dans la machine physique. On commence par aller dans "Édit", puis dans "Virtual Network Editor" et enfin on sélectionnera "NAT" qui est donc associé à "VMnet8".

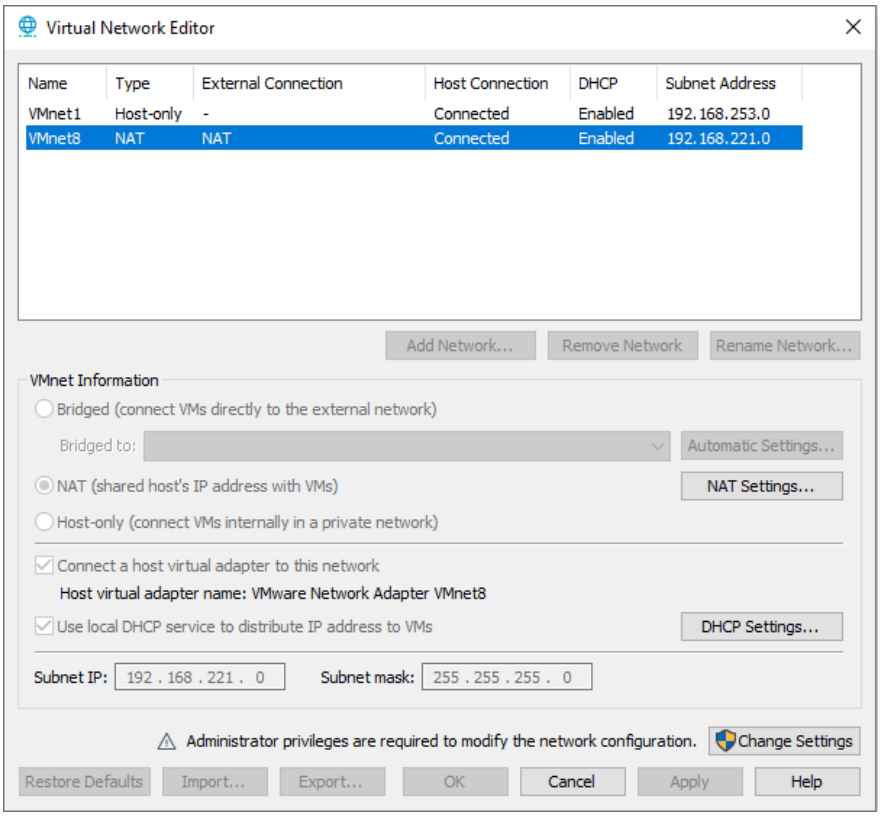


Figure 3.10 : *Accès à la configuration réseau de VMware Workstation*

3.1.3.3 Configuration GNS3

Ensuite passer à la partie configuration sur GNS3, il s'agit de la dernière étape avant d'avoir une intégration fonctionnelle de VMware Workstation dans GNS3. Il faut pour cela penser à démarrer GNS3 en tant qu'Administrateur pour pouvoir accéder aux cartes réseau du système, après avoir ouvert le schéma réseau, il faut ajouter à celui-ci un "nuage" :

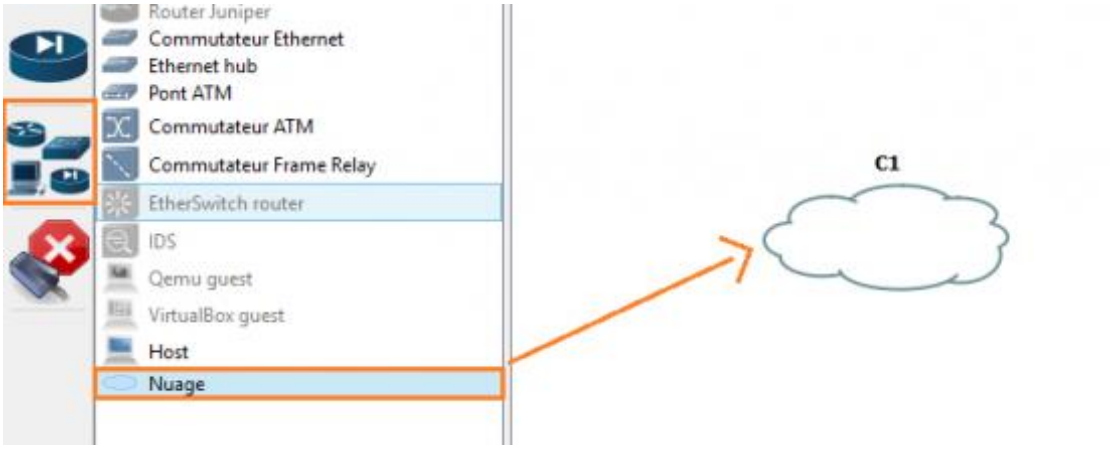


Figure 3.11 : *Intégration d'un Cloud dans le réseau GNS3 pour connecter les VM Workstation*

Selon la figure auparavant, un réseau de serveur a été établi afin de mettre en œuvre un monitoring de ce réseau et d'assurer la liaison et l'échange de données dans ce même réseau. La liaison entre les machines virtuelles et de la machine physique est assuré par un switch et un serveur DHCP parmi les machine dans GNS3. Il faut donc s'assurer de la configuration de celui-ci afin d'établir une bonne connexion.

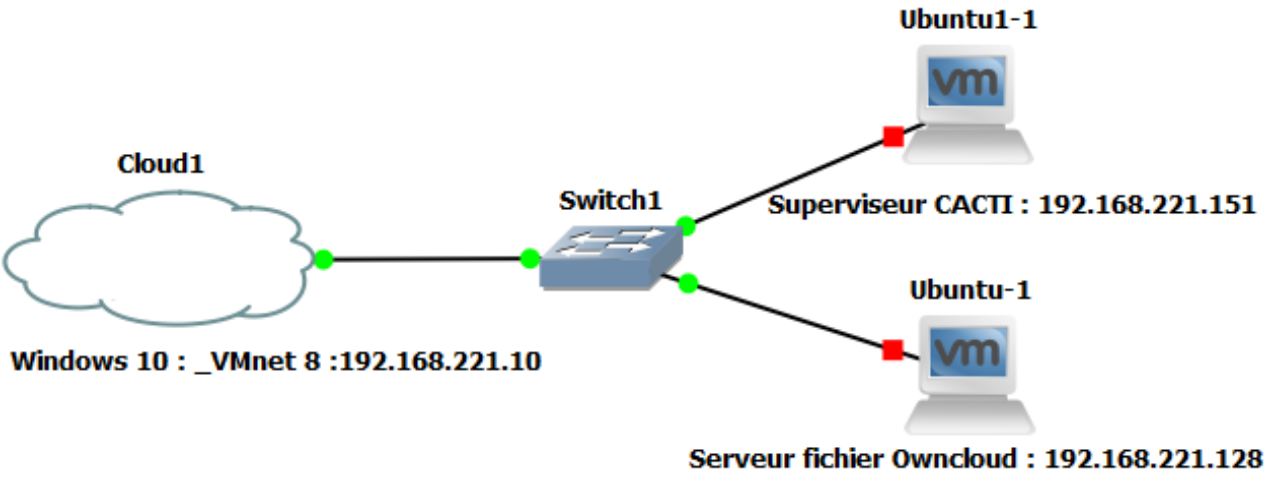


Figure 3.12 : *Architecture du réseau à mettre en place avec GNS3*

3.1.4 Wireshark

Wireshark, un outil d'analyse du réseau anciennement connu sous le nom d'Ethereal, capture les paquets en temps réel et les affiche dans un format lisible par l'homme. Wireshark inclut des filtres, un codage couleur et d'autres fonctionnalités qui permettent de creuser profondément dans le trafic réseau et d'inspecter les paquets individuels [3.09].

Wireshark inspecte le trafic réseau d'un programme suspect, analyser le flux de trafic sur le réseau ou résoudre des problèmes liés à le réseau.

2114 154.723045	34.107.221.82	192.168.43.38	HTTP	365 HTTP/1.1 302 Found (text
2115 154.723732	192.168.43.38	34.107.221.82	TCP	54 50712 → 80 [ACK] Seq=302
2116 154.725853	192.168.43.38	34.107.221.82	TCP	54 50712 → 80 [ACK] Seq=302
2117 154.726916	192.168.43.38	34.107.221.82	TCP	54 50712 → 80 [RST, ACK] Seq
2118 155.531685	192.168.43.38	196.192.32.5	ICMP	74 Echo (ping) request id=0
2119 155.531685	192.168.43.38	192.168.88.29	ICMP	74 Echo (ping) request id=0
2120 156.535246	192.168.43.38	192.168.0.107	ICMP	74 Echo (ping) request id=0
2121 157.538673	192.168.43.38	196.192.32.5	ICMP	74 Echo (ping) request id=0
2122 157.806680	192.168.43.38	34.107.221.82	TCP	66 50713 → 80 [SYN] Seq=0 Wi
2123 157.902629	34.107.221.82	192.168.43.38	TCP	66 80 → 50713 [SYN, ACK] Seq
2124 157.902815	192.168.43.38	34.107.221.82	TCP	54 50713 → 80 [ACK] Seq=1 Ac
2125 157.904661	192.168.43.38	34.107.221.82	HTTP	355 GET /canonical.html HTTP/
2126 157.952289	34.107.221.82	192.168.43.38	HTTP	365 HTTP/1.1 302 Found (text
2127 157.952759	192.168.43.38	34.107.221.82	TCP	54 50713 → 80 [ACK] Seq=302
2128 157.953907	192.168.43.38	34.107.221.82	TCP	54 50713 → 80 [ACK] Seq=302
2129 157.954856	192.168.43.38	34.107.221.82	TCP	54 50713 → 80 [RST, ACK] Seq
2130 158.519258	192.168.43.38	192.168.0.107	ICMP	74 Echo (ping) request id=0

Figure 3.13 : *Présentation de flux de trafic par Wireshark*

3.1.4.1 Plateforme de Wireshark

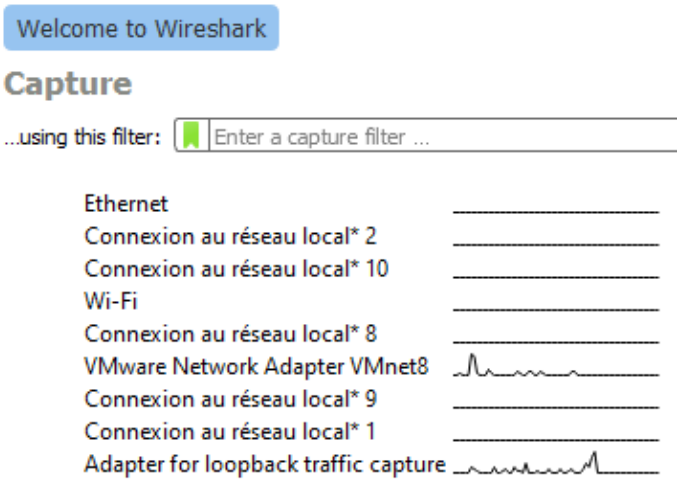


Figure 3.14 : *Différents types de capture valable sur Wireshark*

Après avoir téléchargé et installé Wireshark, il est lancé par un double-cliquer sur le nom de l'interface réseau (network interface) sous Capture pour commencer à capturer les paquets sur cette interface. Par exemple, si l'utilisateur souhaite capturer du trafic sur son réseau sans fil, cliquez sur l'interface sans fil (Wi-Fi). Il est possible de configurer les fonctionnalités avancées en cliquant sur Capture> Options.

Dès l'appui sur le nom de l'interface, les paquets commencent à apparaître en temps réel. Wireshark capture chaque paquet envoyé vers ou depuis le système.

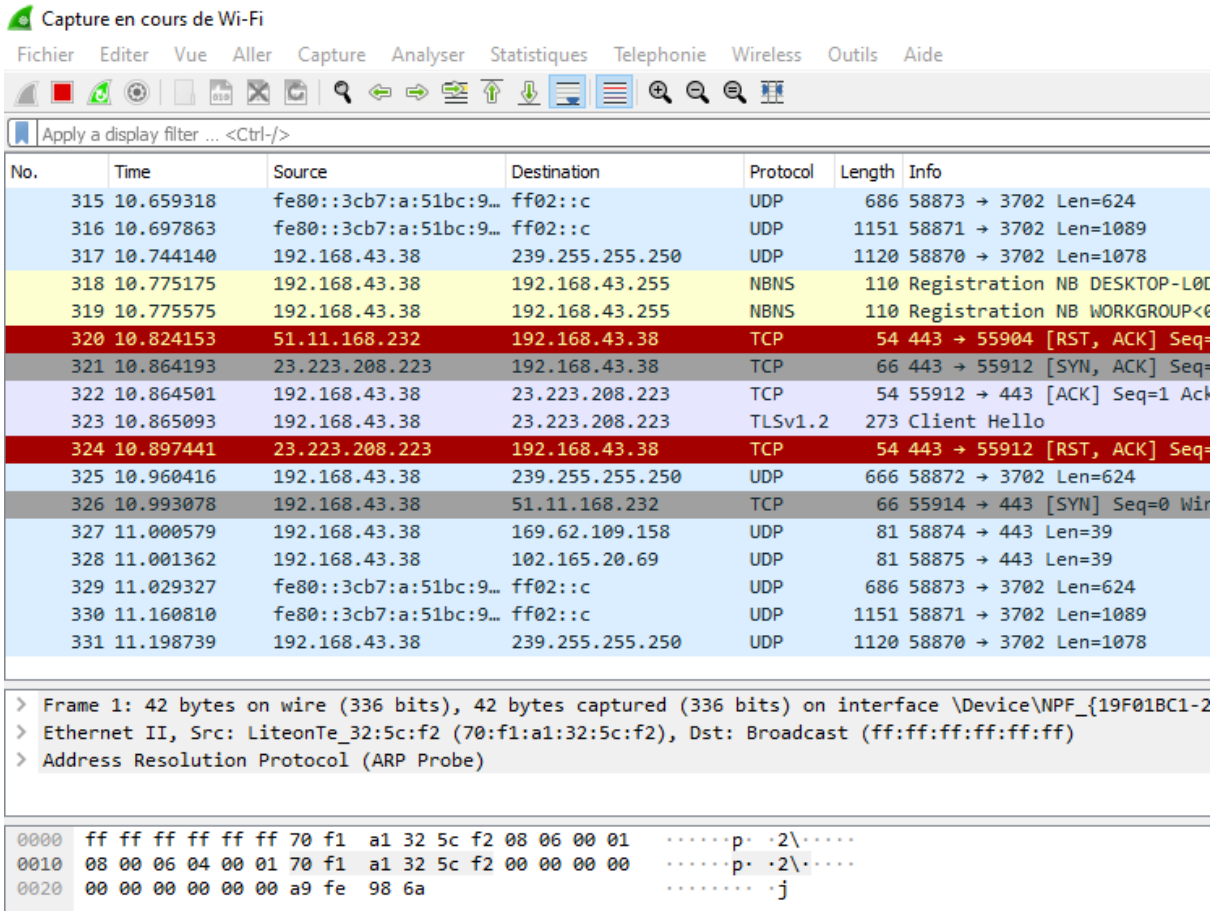


Figure 3.15 : *Mode de capture depuis le trafic Wifi*

Si le mode « promiscuous » n'a pas été activé par l'utilisateur, il sera activer par défaut, tous les autres paquets du réseau sont également affichés au lieu de seulement les paquets adressés à la carte réseau.

Pour vérifier si le mode « promiscuous » est quand même activé ou pas, cliquez sur Capture> Options et vérifiez que la case à cocher activer le mode « promiscuous » sur toutes les interfaces c'est à dire « Enable promiscuous mode on all interfaces » est activée au bas de cette fenêtre.

3.1.4.2 Codes de couleurs

L'utilisateur doit probablement voir les paquets mis en évidence dans une variété de couleurs différentes. Wireshark utilise des couleurs pour aider à identifier les types de trafic en un coup d'œil. Par défaut, violet clair est le trafic TCP, bleu clair est le trafic UDP et noir identifie les paquets avec des erreurs, par exemple, ils pourraient avoir été livrés dans le désordre.

Pour voir exactement ce que signifient les codes de couleur, cliquez sur Affichage> Règles de coloration (View > Coloring Rules). Il est possible également d'y personnaliser et modifier les règles de coloration si nécessaire.

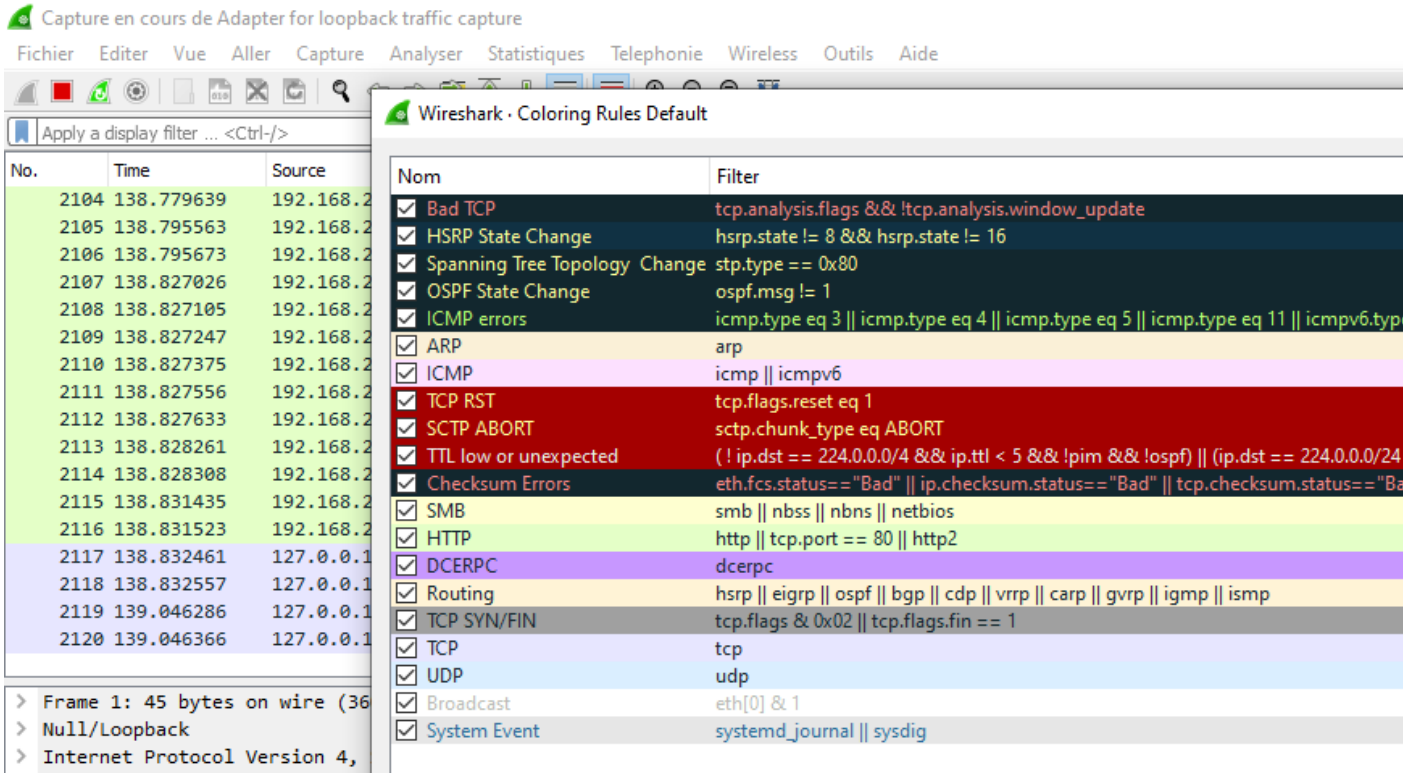


Figure 3.16 : *Choix de présentation en couleur des trafics dont nous voulons spécifier*

3.1.5.3 Exemples de captures

S'il n'y a rien d'intéressant à inspecter sur le réseau, le wiki de Wireshark a défendu le réseau. Le wiki contient une page d'exemples de fichiers de capture dont il est possible de charger et inspecter. Cliquez sur Fichier> Ouvrir (File > Open) dans Wireshark et recherchez le fichier téléchargé. Il est faisable également de sauvegarder les captures dans Wireshark et les ouvrir plus tard. Cliquez sur Fichier> Enregistrer (File > Save) pour enregistrer les paquets capturés.

3.1.4.3 Filtrage des paquets

S'il est important d'inspecter quelque chose de spécifique, comme le trafic qu'un programme envoie en téléphonant à la maison, cela permet de fermer toutes les autres applications utilisant le réseau afin que l'utilisateur puisse restreindre le trafic. Cependant, il est probable d'avoir une grande quantité de paquets à passer au crible. C'est là que les filtres de Wireshark entrent en jeu.

La manière la plus simple d'appliquer un filtre consiste à le saisir dans la zone de filtre en haut de la fenêtre et à cliquer sur Appliquer Apply (ou sur Entrée). Par exemple, tapez « dns » et les paquets DNS seront les seules en vue. Lorsqu'un utilisateur commence à taper, Wireshark l'aidera à compléter automatiquement le filtre.

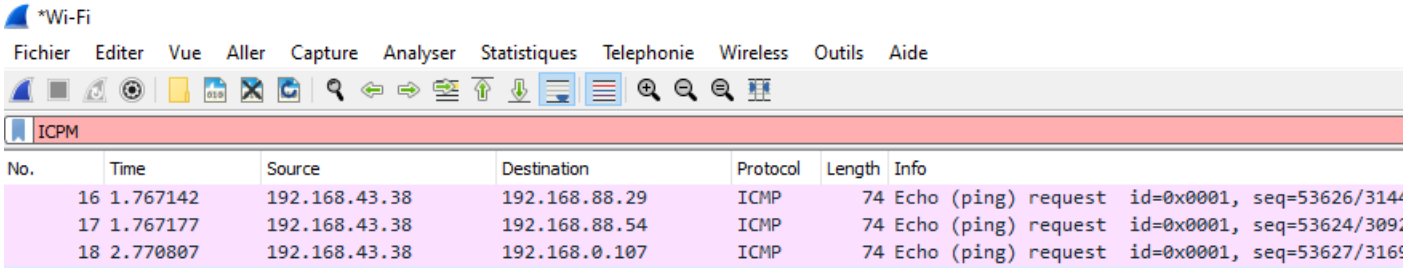


Figure 3.17 : *Exemple de filtrage de paquet par Wireshark*

En appuyant également sur Analyser> Afficher les filtres (Analyze > Display Filters) pour choisir un filtre parmi les filtres par défaut inclus dans Wireshark. De là, il est possible d'y ajouter des filtres personnalisés et les enregistrer pour y accéder facilement à l'avenir.

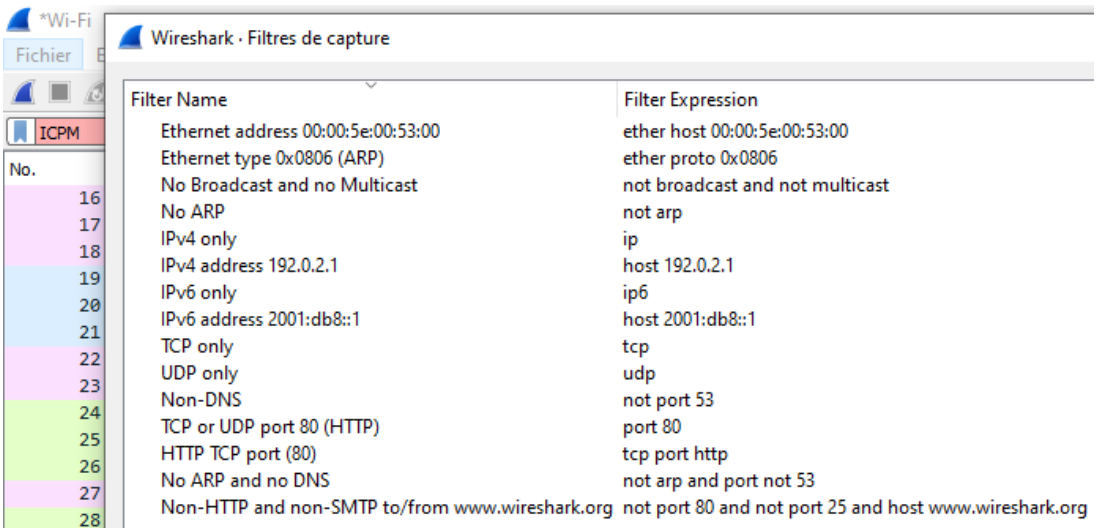


Figure 3.18 : *Personnalisation de Filtre par Wireshark*

Une autre chose intéressante que Wireshark offre, en cliquant avec le bouton droit sur un paquet et de sélectionner Suivre> Flux TCP (Follow > TCP Stream). L'utilisateur verra la conversation TCP complète entre le client et le serveur. Il est possible de cliquer sur d'autres protocoles dans le menu Suivre (Follow) pour voir les conversations complètes pour d'autres protocoles, le cas échéant.

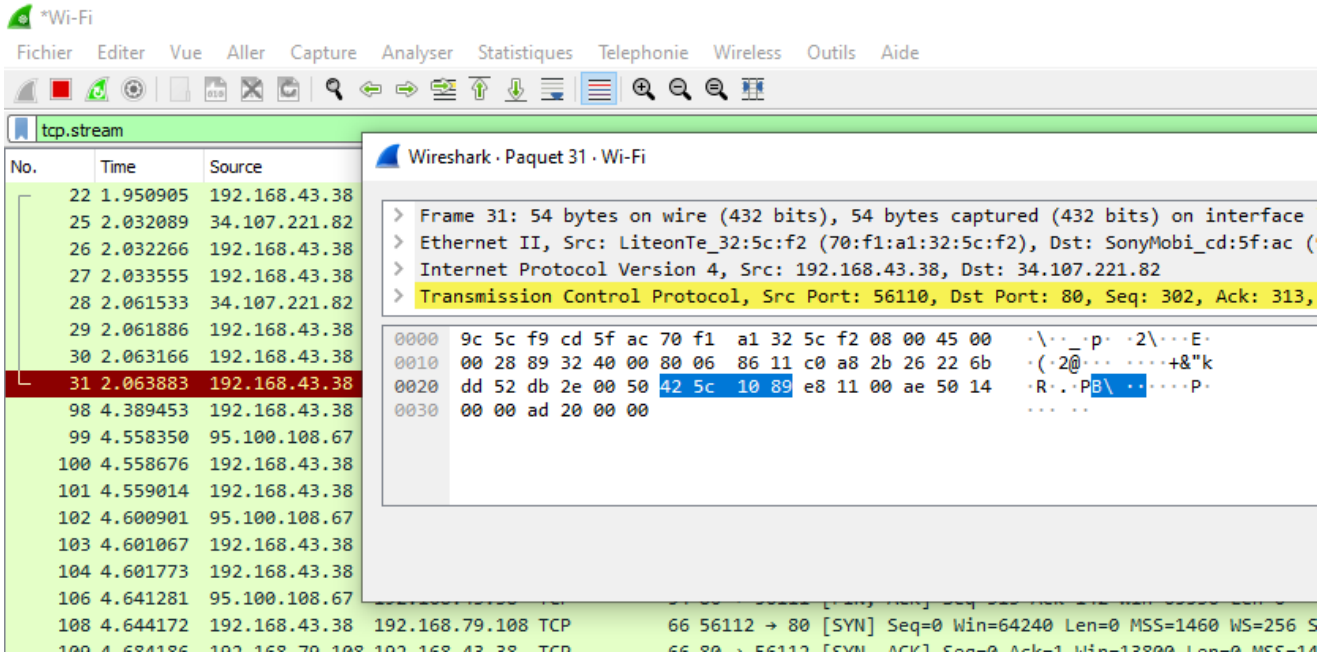


Figure 3.19 : *Conversation TCP complète entre le client et le serveur*

Wireshark est un outil extrêmement puissant, et la réalisation de la mise en place du réseau dans GNS3 va se montrer grâce à son utilisation. Pour vérifier que les transferts et la liaison sont établis, Wireshark est l'outil indispensable.

3.1.5 PRTG

Par la suite de ce qui a été vue auparavant, PRTG sera utiliser autant que principale, outil de supervision dans cette réalisation. La machine physique Window10 héberge le logiciel, et l'interface web « localhost » lui appartient [3.10].

3.1.5.1 Environnement PRTG

Il offre plusieurs vues sur l'état générale de la communication entre la machine hôte et les serveurs qui y sont liés. Il montre également plusieurs paramètres et possible configuration pour des meilleures expériences dans l'étude des réseaux et du système.

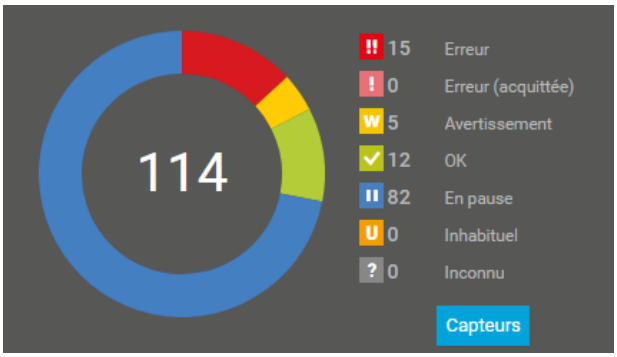


Figure 3.20 : *Représentation en diagramme de tous les capteurs par PRTG*

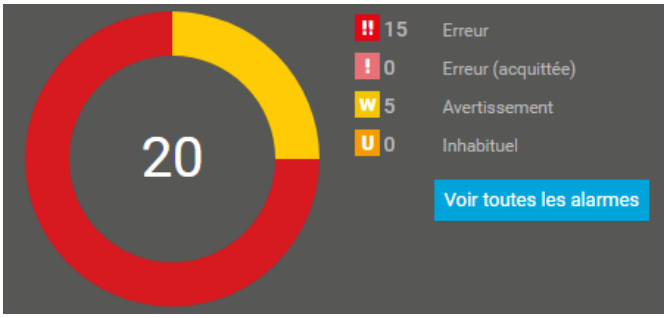


Figure 3.21 : *Représentation en diagramme de toutes alarmes actives par PRTG*

Les deux diagrammes figures 3.24 et 3.25 montrent la capacité de capture d'état du système par PRTG, cependant des compléments en termes de capteur sont possibles par plugin. En effet, chaque utilisateur possède des objectifs plus précisent dans l'accomplissement.

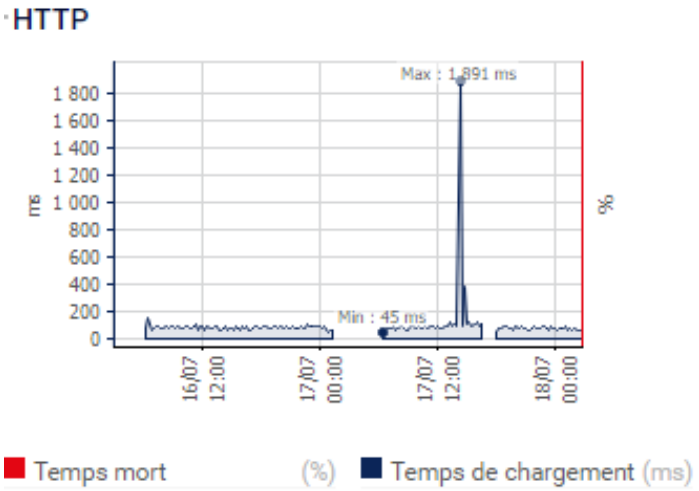


Figure 3.22 : *Représentation graphique du taux de transfert par le protocole HTTP dans PRTG*

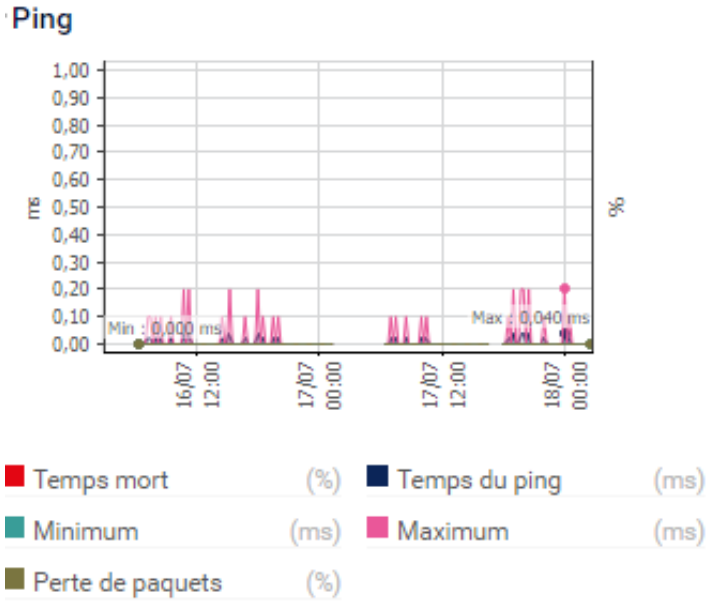


Figure 3.23 : *Représentation graphique du taux de rencontre entre la machine physique avec les autres serveurs par rapport au temps*

PRTG donne une évaluation complète de l'état d'échange durant tout le temps de commission de la machine hôte avec l'extérieur.

3.1.5.2 Configuration sur PRTG

Si l'utilisateur veut ajouter des machines à surveiller, il n'y a pas plus pratique et facile que sur PRTG. Le plus important est de mettre en place le réseau ou connaitre l'adresse de la machine à surveillé. En connaissant l'adresse IP de la machine, l'administrateur du réseau va pouvoir mettre en place des techniques de monitoring qui lui convient.

L'administrateur va créer :

- Un « Device » dans PRTG, ce Device portera l'IP de la machine à surveiller. Elle sera configurée de par son nom, icone, genre de gestion d'écoute, de l'héritage par le choix de la version de SNMP qui inclut le type d'authentification, type de cryptage de donnée.
- Des écoutes seront configurées en suite pour le Device. L'administrateur va choisir qu'es ce qu'il veut surveiller dans la machine, ou choisir le système dont il veut cibler, ou observé le genre de technologie exploité par la machine sous surveillance.
- Des capteurs seront alors placer sur le Device pour ne rien manquer de l'activité de la machine cible sous protection.

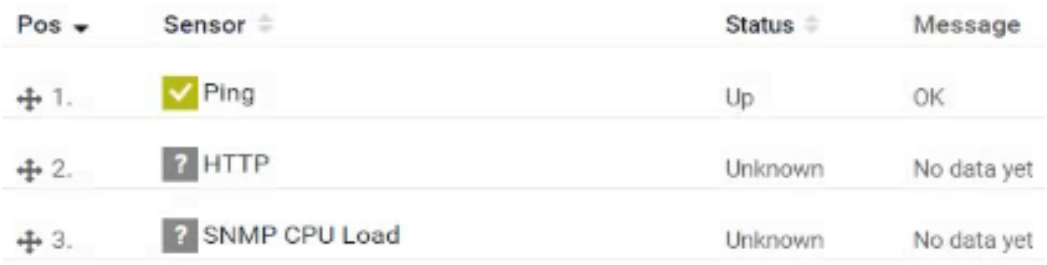


Figure 3.24 : *Installation d'écoute sur une machine à mettre sous surveillance*

3.1.6 Android Studio

Android est une surcouche au-dessus d'un système Linux. C'est une technologie incontournable, il est à la portée de tout le monde mais varie selon sa version. C'est un ensemble de couche de bibliothèque JAVA et d'application.

Android Studio est installé dans un système d'exploitation Windows10 dans cette réalisation, le système est de 64bits.

3.1.6.1 Installation d'Android studio sur Windows10

L'installation d'Android Studio se fait en deux étapes [3.11]:

- Le téléchargement de l'installer sous Windows10 de JDK ou « Java Development Kit » se fait sur le site propre à Oracle, sur https://oracle.com/java/technologies/javase-jdk14-downloads.html/ ce site inclut la mise à jour du License. JDK est l'environnement de développement pour créer des applications et des composants utilisant le langage de programmation java.

  Lors de son installation, l'utilisateur crée son chemin dans l'emplacement des variables d'environnement sous Windows. Et crée un nouveau variable du système.
- Installation Android Studio est mieux faite en ligne après son téléchargement dans https://developer.android.com/studio/ car des paquets pourraient manquer.

3.1.6.2 Création d'application pour smartphone Android

Android Studio offre plusieurs possibilités de développer des applications selon le besoin des développeurs. Dans cette partie, l'application sera utilisée sur un appareil téléphonique sous Android.

Figure 3.25 : *Logiciel plateforme Android Studio*

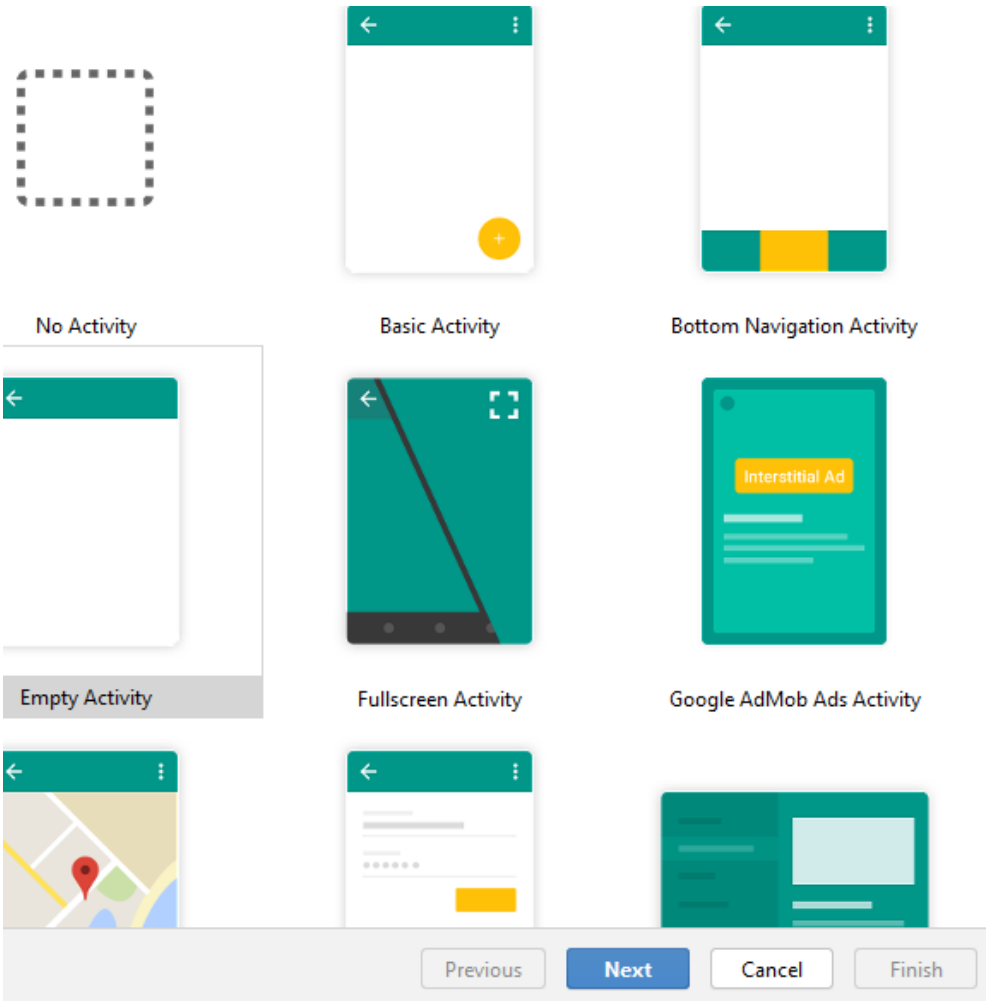


Figure 3.26 : *Différents types d'interface téléphonique qu'offre Android Studio*

3.1.6.3 Programmation sous Android Studio

Android Studio possède une plateforme flexible en termes de code et de souplesse de produit.

- Le langage JAVA est le langage de programmation utilisé dans le cadre de ce projet Android est le Java, très répandu dans les développements informatiques actuels. Ce langage offre un ensemble de librairies qui facilitent le développement et dispose d'une documentation bien fournie.
- XML, pour la réalisation des interfaces graphiques de l'application il faut utiliser le langage XML. Le XML est un langage informatique qui sert essentiellement à stocker/transférer des données de type texte structurées en champs arborescents. Ce langage est qualifié d'extensible car il permet à l'utilisateur de définir des marqueurs (balises) qui facilitent le parcours au sein du fichier et donc la lecture de l'information. Ce langage est couramment utilisé et son apprentissage est libre.

Toutes les programmations qui sont faites sur Android Studio vont permettre à l'utilisateur de l'application d'avoir une vue d'ensemble du monitoring sur PRTG. Ainsi il peut avoir accès à la surveillance du système et au réseau local de son environnement de travail.

activity_main.xml | MainActivity.java | AndroidManifest.xml | BuildConfig.java

```
1  package com.example.supervisionprtg;
2
3  import ...
10
11 public class MainActivity extends AppCompatActivity {
12
13     WebView web;
14
15     @Override
16     protected void onCreate(Bundle savedInstanceState) {
17         super.onCreate(savedInstanceState);
18         setContentView(R.layout.activity_main);
19         web=findViewById(R.id.webView);
20         WebSettings WebSettings = web.getSettings();
21         WebSettings.setJavaScriptEnabled(true);
22         web.setWebViewClient(new Callback ());
23         web.loadUrl("127.0.0.1/index.htm");
24     }
25
26     private class Callback extends WebViewClient {
27
28         @Override
29         public boolean shouldOverrideKeyEvent(WebView view, KeyEvent event) { return false; }
32     }
33 }
```

Figure 3.27 : *Codage de l'interface Webview sous fichier java*

Figure 3.28 : *Codage du l'interface du Webview dans le fichier XML*

3.1.7 Python

L'outil de programmation de « sniffing » du réseau, il donne les informations nécessaires à l'administrateur lors d'une attaque ou malveillance dans le système. Le « sniffing » des paquets permet de détailler le réseau de sa supervision et des analyses de l'utilisation des largeurs de bandes. Cela demande aux utilisateurs des connaissances de réseau et de ses modes de fonctionnements pour pouvoir mettre en évidence les données supervisées [3.12].

Python va exécuter deux types de surveillance de réseaux et systèmes ;

- Par programmation de fichier « nomfichier.py », programmable sur tout type d'éditeur de texte.
- Par Scapy, un outil manipulable selon le besoin de l'administrateur.

Dans la figure ci-dessous Figure 3.34, l'administrateur a construit un paquet similaire à ceux envoyés par l'utilitaire bien connu « ping ». Ce dernier ajoute par défaut une charge utile de 56 octets (qui peut contenir des informations d'horodatage, notamment sous GNU/Linux).

superviseur réseau.py

```
#!/usr/bin/env python3

import os as _os
import sys as _sys
import time as _time
import socket as _socket
from struct import Struct as _Struct
from ipaddress import IPv4Address as _IPv4Address

_fast_time = _time.time
_write_err = _sys.stdout.write
tcp_header_unpack = _Struct('!2H2LB').unpack_from
udp_header_unpack = _Struct('!4H').unpack_from
class RawPacket:

 def __init__(self, data):
 self.timestamp = _fast_time()
 self.protocol = 0
 self._name = self.__class__.__name__
 self._dlen = len(data)
 # parsing ethernet header here because it is more efficient
 self.dst_mac = data[:6].hex()
 self.src_mac = data[6:12].hex()
 self._data = data[14:]
 # NOTE: this is very slow to have to print and should only be used for testing or
learning. Generally you wouldnt need
 # to print a string representation of the class instance anyways.
 def __str__(self):
 return '\n'.join([
```

Figure 3.29 : *Programmation supervision réseau par Python*

```
>>> sniff(count= 1, iface="eth0", prn=lambda x: x.summary())
Ether / IP / TCP 192.168.221.128:ssh > 192.168.221.10:23564 PA / Raw
<Sniffed: TCP:1 UDP:0 ICMP:0 Other:0>
>>> sniff(count= 1, iface="eth0", prn=lambda x: x.show())
###[ Ethernet ]###
  dst= 00:50:56:c0:00:08
  src= 00:0c:29:ae:aa:77
  type= 0x800
###[ IP ]###
     version= 4L
     ihl= 5L
     tos= 0x10
     len= 76
     id= 39993
     flags= DF
     frag= 0L
     ttl= 64
     proto= tcp
     chksum= 0x6286
     src= 192.168.221.128
     dst= 192.168.221.10
     \options\
###[ TCP ]###
        sport= ssh
        dport= 23564
        seq= 4004360689L
        ack= 1409974193
        dataofs= 5L
        reserved= 0L
        flags= PA
```

Figure 3.30 : *Construction de paquet par Scapy*

3.2 Conclusion

Plusieurs mises en place ont été faites afin de favoriser la réalisation de l'étude de l'implémentation d'une surveillance réseaux et systèmes locale sur un appareil Android.

Les logiciels de réseau choisis sont favorable afin d'avoir un environnement de travail plus simple à surveiller. Trois logiciels de monitoring sont implémentés pour bénéficier de résultats différents, donc l'administrateur a une marge de comparaison de performance entre Wireshark, CACTI et PRTG. GNS3 est réaliste en termes d'espace de simulation de réseau grâce aux configurations Cisco qui y aient intégrées.

Un serveur de fichier de donnée est toujours important dans n'importe quelle entreprise. Il est encore plus favorable d'avoir accès à ses données via une application en smartphone personnalisée appartenant à l'entreprise lui-même.

CHAPITRE 4
SIMULATION DU LANCEMENT DE LA SUPERVISION RESEAUX

4.1 Introduction

Dans cette simulation il y a les représentations de la fonctionnalité du projet de recherche établi dans cette étude. Elle présente tous les modes d'utilisation de l'application mobile nommée « supervisionPRTG ».

Le logiciel PRTG est avant tout un logiciel d'administration de réseau, PRTG surveille toutes sortes de serveurs, y compris sur les réseaux distribués [4.02]. Il faut savoir que gérer un réseau de taille quelconque est un travail qui mélange l'accomplissement et le retard par rapport à d'autre IT. Un fort partenariat entre Paessler et Baramundi nous permet de gérer et de superviser l'infrastructure d'un réseau facilement. Ensemble ils ont créé un IT performant sécurisé et fiable où nous avons tout sous contrôle.

Cette application va offrir à l'utilisateur une ouverture de l'emplacement la supervision du réseau dont il est responsable, via son appareil Android. A tout moment où l'administrateur reçoit des messages d'alerte ou notification de la part des utilisateurs du réseau, il va pouvoir travailler à distance de son bureau ou consulter à distance l'état de la communication dans le réseau dont il s'en charge.

S'ensuit le lancement des programmes développés avec le langage Python. Il est important de savoir que ce langage est très avancé dans le domaine de la supervision réseau, il donne plus d'information que ce qu'un administrateur devrait savoir concernant le réseau informatique dont il s'occupe.

Plusieurs programmes ont été alors développés afin de lancer la surveillance dont on veut se concentrer. De ce fait les traitements vont se faire en peu de temps que de lancer un grand programme.

4.2 Simulation de l'application

Voyons comment va se représenter l'application Android supervisionPRTG en état de marche pour la supervision de réseau dont on a mis en place précédemment [4.01].

Dans la figure ci-dessous, nous avons une présentation du site web local avec PRTG. La figure 4.01 représente les différents types d'élément mise en supervision sous la plateforme. La plateforme est très expressive de ce que nous avons comme état de fonctionnement des réseaux.

Car dès que nous entrant sur le site web, nous savons immédiatement tout ce qui ne va pas bien dans les réseaux, ainsi nous allons pouvoir prendre des décisions immédiates selon le besoin et l'état prioritaire de la situation en elle-même.

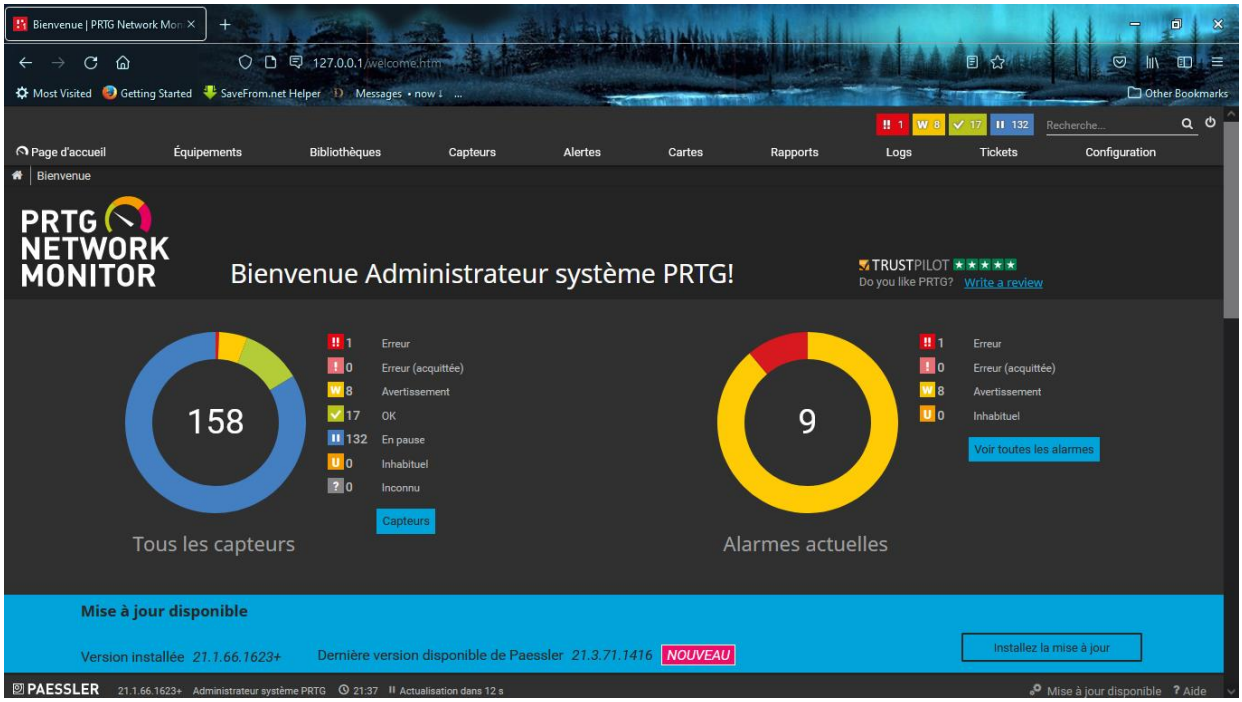


Figure 4.01 : *Présentation la plateforme PRTG sur le site web local*

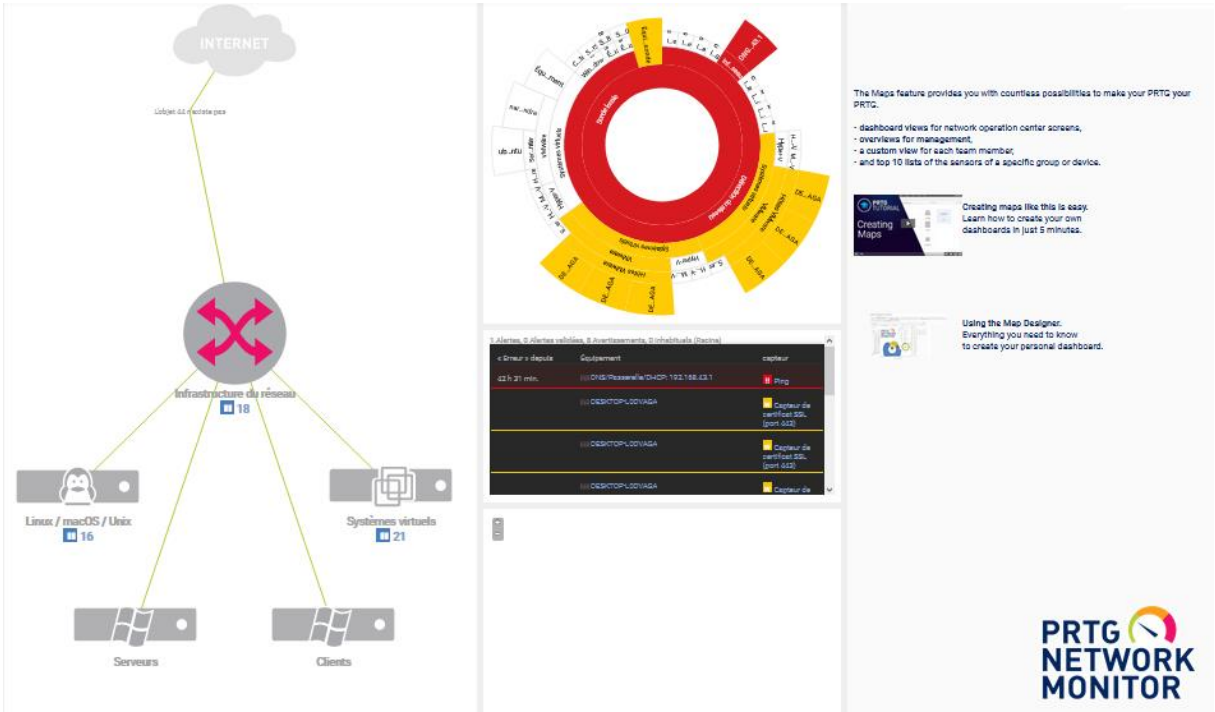


Figure 4.02 : *Les types de supervisions disponibles sur PRTG*

Dans la figure 4.02 ci-dessus nous avons une nouvelle forme de la plateforme de PRTG. Cette nouvelle présentation est déjà une nouvelle facilitation de notre travail. En effet, dans cette figure on voit comment le réseau est configuré et comment les appareils sont disposés dans l'entreprise, et même si la disposition sont de très long distance, la vue de tout cela est possible. Une image en perspective de la disposition des matériels est alors discernée.

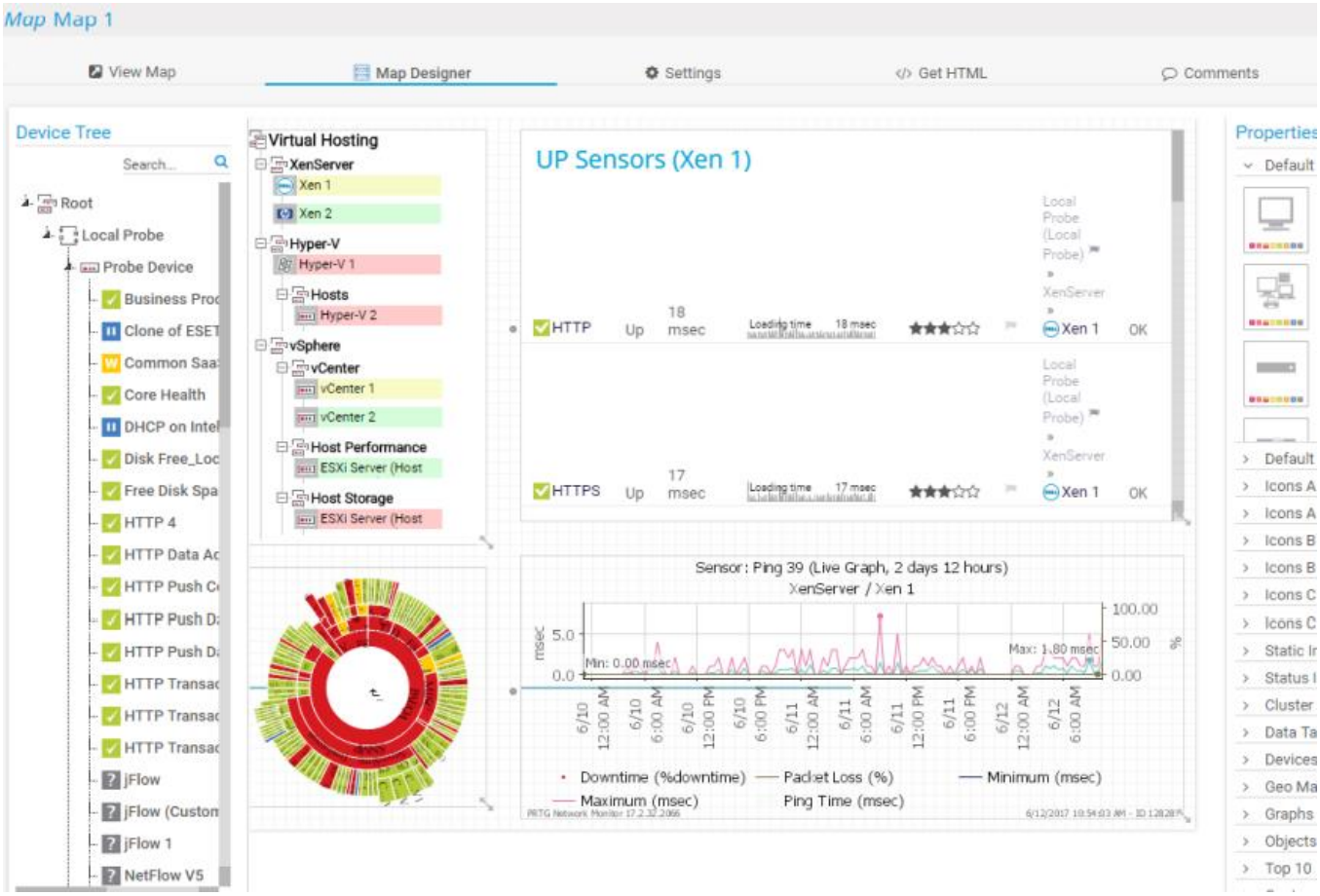


Figure 4.03 : *Présentation d'une carte pour un aperçu individuel de réseau sous supervision avec PRTG*

Il est important de noter qu'avec PRTG l'essentiel est d'avoir un capteur pour chaque élément à superviser, car c'est la nature même du travail à faire.

Pour le reste si nécessaire, il suffit de pinger un matériel quelconque et être en connexion avec ce matériel, alors la plus grande partie du travail est faite. Reste à faire et non le moindre c'est d'établir les commande à distance, pour que le matériel répond ou que au moins notre action fait effet aux autres appareils connectés. L'outil de supervision purement software qu'on a dans l'étude montre déjà l'ampleur de l'installation des capteurs et leurs travails. Le nombre de capteur dépendra des outils et des besoins de l'utilisateur.

Nous avons mis en place des simulations d'interconnexion entre une machine de travail avec un appareil mobile, un smartphone, et établit des contrôles à distance entre les deux afin de mettre en pratique le contrôle et supervision à tout moment et avec tout appareil à disposition grâce à PRTG.

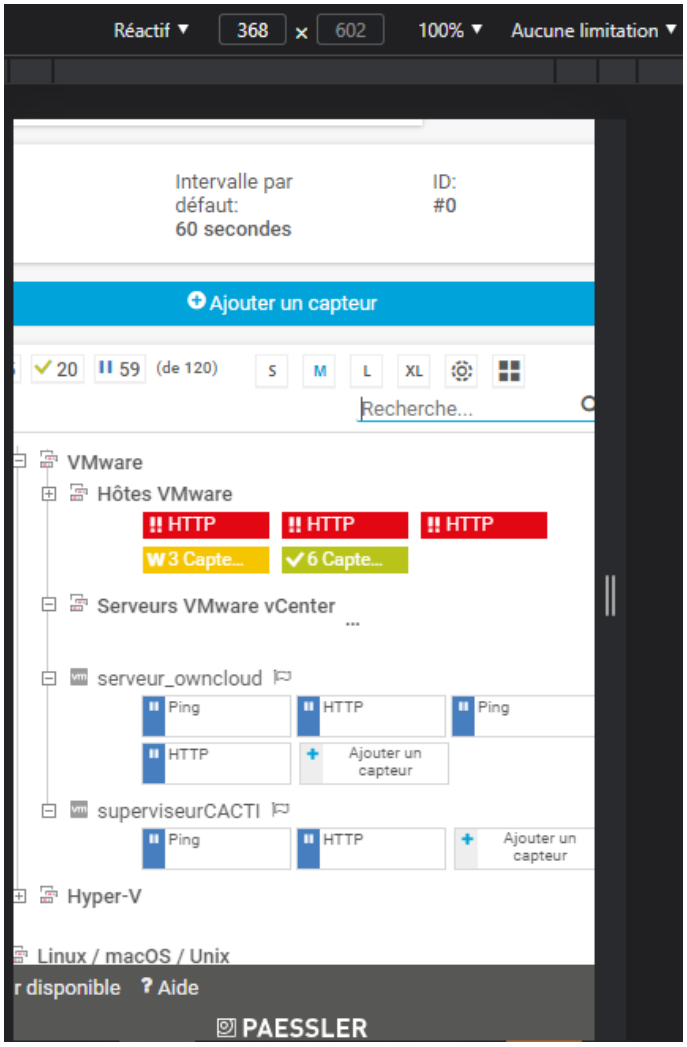


Figure 4.04 : *Présentation en état réactif du site web*

Il est important de savoir qu'un site web pourrait ne pas être réactif ou « responsive » pour être traduit en une application Android. Dans le travail, on va mettre en connexion nos appareils à un seul routeur, ou pour aller plus loin, créer un nom de domaine de travail sur un routeur quelconque. Maintenant il existe un domaine local qui appartiendra à la simulation, et ainsi réglé les appareils connectés à la machine principale pour s'assurer des stricts sécurités possible.

Maintenant la machine et PRTG reconnait les adresse IP et domaine dont ils vont partager les données. On va préparer Android Studio pour la simulation.

4.2.1 Présentation de l'interface de l'application

```
logcat
2021-08-03 07:16:32.026 673-673/? W/memtrack@1.0-se: type=1400 audit(0.0:551443): avc: denied { search } for name="proc"
 dev="debugfs" ino=14143 scontext=u:r:hal_memtrack_default:s0 tcontext=u:object_r:qti_debugfs:s0 tclass=dir permissive=0
 ppid=1 pcomm="init" pgid=1 pgcomm="init"
2021-08-03 07:16:32.096 673-673/? I/chatty: uid=1000(system) memtrack@1.0-se identical 2 lines
2021-08-03 07:16:32.096 673-673/? W/memtrack@1.0-se: type=1400 audit(0.0:551446): avc: denied { search } for name="proc"
 dev="debugfs" ino=14143 scontext=u:r:hal_memtrack_default:s0 tcontext=u:object_r:qti_debugfs:s0 tclass=dir permissive=0
 ppid=1 pcomm="init" pgid=1 pgcomm="init"
2021-08-03 07:16:35.981 2279-2377/? I/QCNEJ/CndHalConnector: -> SND notifyWifiStatusChanged(RatInfo{type=1, subType=101,
 state=CONNECTED, v4=IfaceAddrPair{iface=wlan0, addr=192.168.0.114}, v6=IfaceAddrPair{iface=, addr=}, timestamp=2021-08-03
 09:16:35.981, isAndroidValidated=true, netHandle=1726593288926, slotIdx=0} WifiInfo{freq=TWO_GHz, state=3, ssid=MEDIATHEQUE
  2, bssid=98:da:c4:ad:48:52, dns=[192.168.0.1, 0.0.0.0, 0.0.0.0, 0.0.0.0, ]})
2021-08-03 07:16:38.876 2169-2169/? W/lowpool[439]: type=1400 audit(0.0:551447): avc: denied { search } for name="proc"
 dev="debugfs" ino=14143 scontext=u:r:priv_app:s0:c512,c768 tcontext=u:object_r:qti_debugfs:s0 tclass=dir permissive=0
 ppid=1033 pcomm="main" pgid=2169 pgcomm="gle.android.gms"
2021-08-03 07:16:39.000 2279-2377/? I/QCNEJ/CndHalConnector: -> SND notifyWifiStatusChanged(RatInfo{type=1, subType=101,
 state=CONNECTED, v4=IfaceAddrPair{iface=wlan0, addr=192.168.0.114}, v6=IfaceAddrPair{iface=, addr=}, timestamp=2021-08-03
 09:16:39.0, isAndroidValidated=true, netHandle=1726593288926, slotIdx=0} WifiInfo{freq=TWO_GHz, state=3, ssid=MEDIATHEQUE
 2, bssid=98:da:c4:ad:48:52, dns=[192.168.0.1, 0.0.0.0, 0.0.0.0, 0.0.0.0, ]})
```

Figure 4.05 : *Représentation de la compilation du codage dans le logiciel Android studio*

Pour que la simulation se compile correctement et éviter l'insécurité de l'interconnexion, PRTG a déjà spécifié une configuration, dans l'administration log, cette spécification des adresses IP confirme quel appareil va pouvoir continuellement faire des commandes à distance aux infrastructures du réseau [4.02].

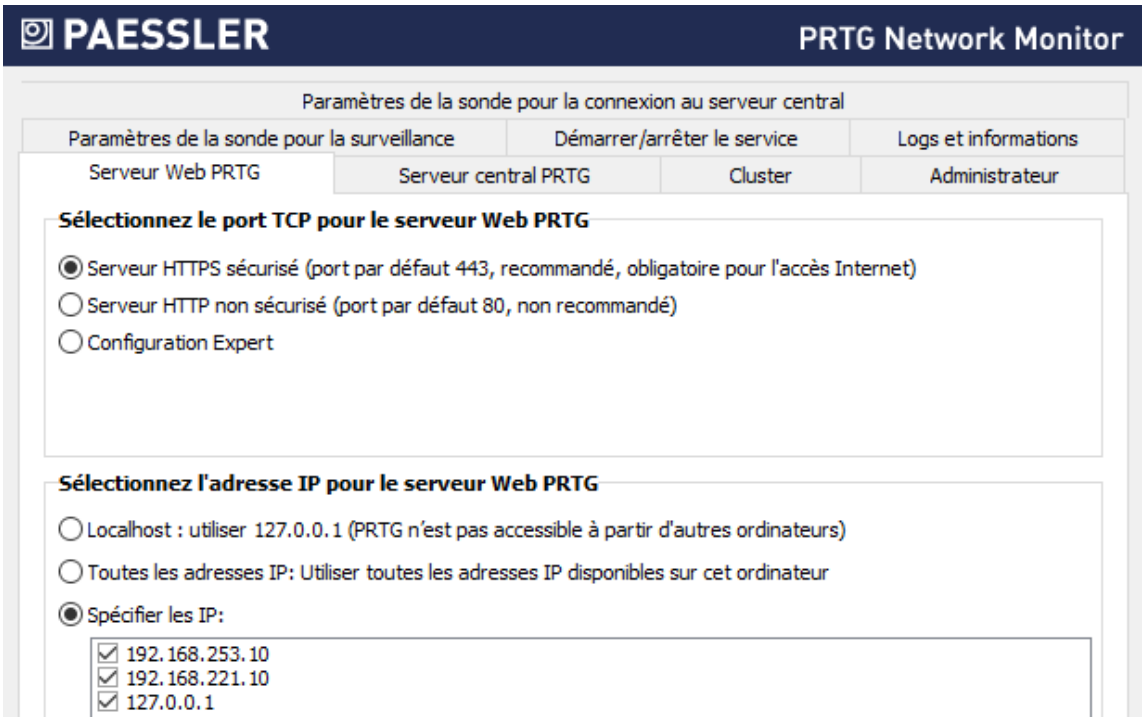


Figure 4.06 : *Représentation côté administratif des adresses IP avec PRTG dans la machine serveur*

Après que les différentes configurations sur Android Studio et PRTG soient faites, il existe maintenant une application née sur le smartphone qu'on a appelé « supervisionPRTG », qui permet de superviser un parc informatique à tout moment et de réagir par la suite si nécessaire.

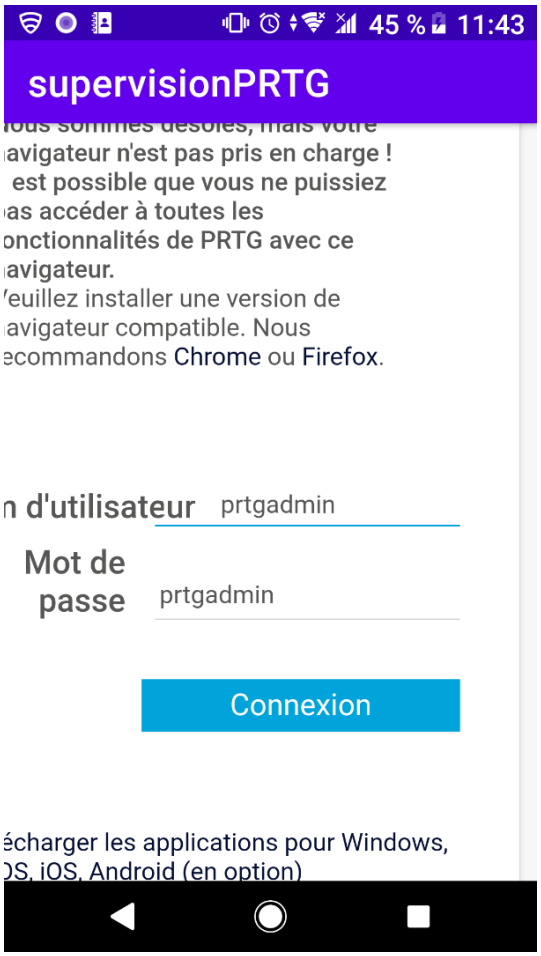


Figure 4.07 : *Image donnant accès à la supervision locale*

La configuration et la présentation de l'application et comme sur la plateforme de travail que l'administrateur y travail, seule différence est la taille de l'écran et l'aptitude à s'y adapter. Figure 4.07 représente le login sur la plateforme, est la confirmation de la sécurisation sur la plateforme. C'est-à-dire qu'on est sur le domaine DNS demandé. Il est important de noter que la version de l'Android sur le smartphone pourrait affecter bien évidement la réalisation du projet et la capacité du système qui s'y trouve.

Selon l'ampleur du projet à superviser la sécurité va de l'avant est l'exécution de chaque action est l'essentiel. Cependant s'il s'agit de mettre un œil sur un parc informatique, surveiller son environnement de travail ou sa maison. Chaque utilisateur ayant le besoin spécifique d'utiliser cette application trouvera une satisfaction.

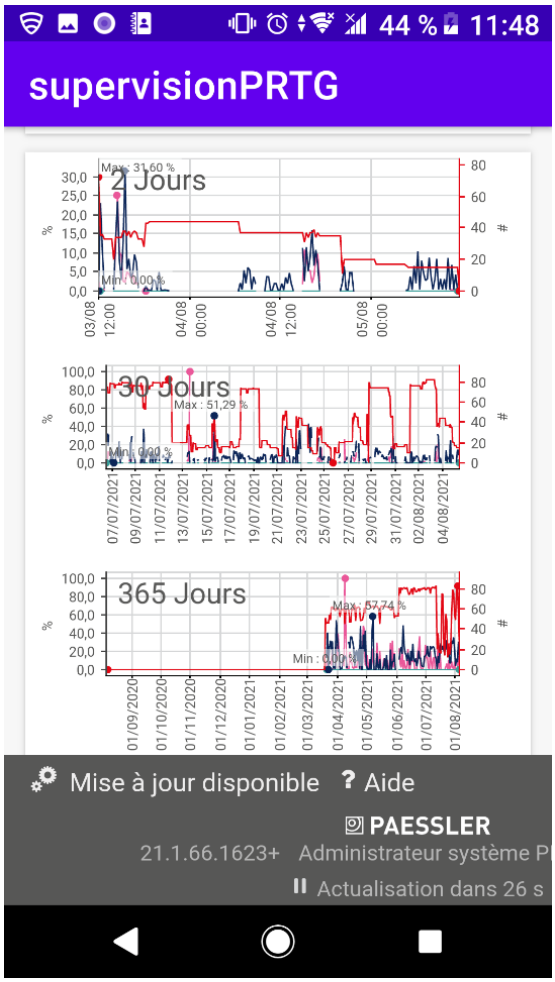


Figure 4.08 : *Supervision graphique en temps réel des activités sur le réseau local sur un smartphone*

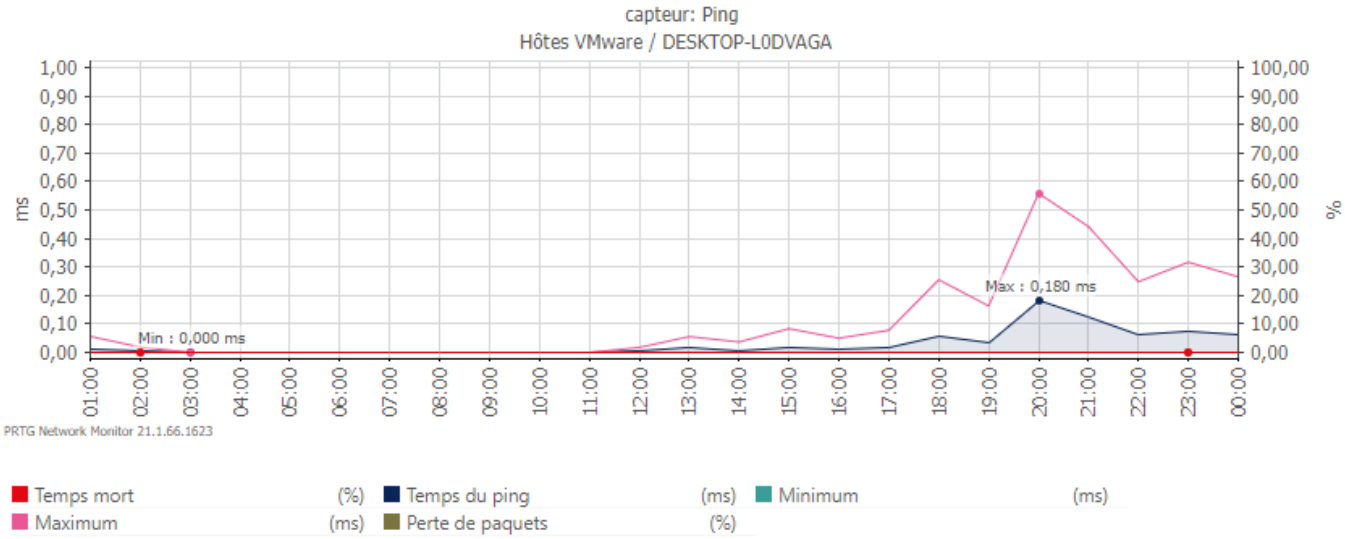


Figure 4.09 : *Données graphique venant d'un capteur sur un ordinateur*

Figure 4.08 et figure 4.09 représentent les données en graphique des activités d'un matériel sous capteur en surveillance. Dans un ordinateur elles seraient présentées comme dans la figure 4.09.

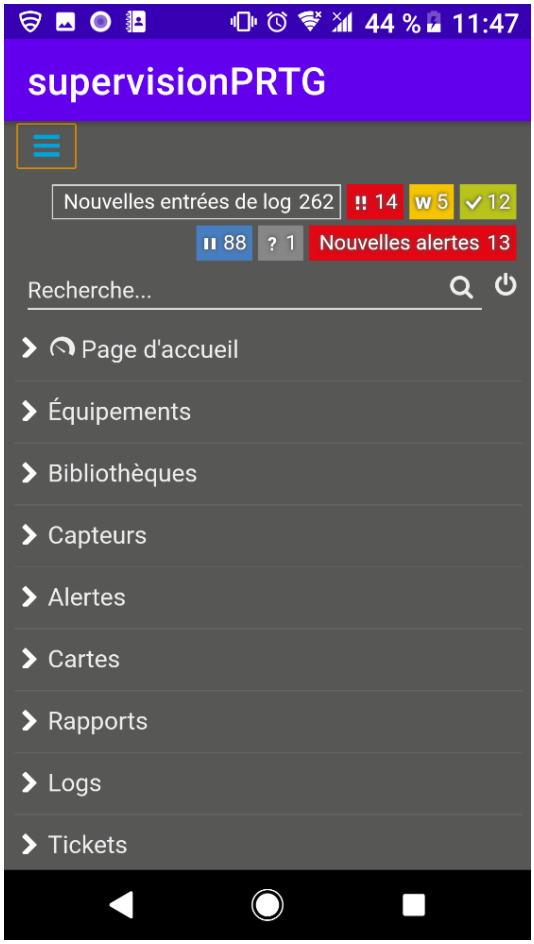


Figure 4.10 : *Possibilité de configuration de la supervision du réseau*

La figure 4.10 représente le Dashboard au complet de la plateforme, elle permet une ouverture directe des activités souhaitées par l'utilisateur et offre des services encore plus large.

4.2.2 Interprétation du résultat

L'application offre une ouverture flexible telle sur un PC ou MAC. L'interface de l'application est la même que celle de l'interface sur le Windows dont on a mis en place précédemment. La communication de l'appareil Android et de l'emplacement du logiciel de supervision doit se faire sur un même domaine DNS pour éviter le « net :: ERROR_CONNECTION_TIMEOUT » [4.03] [4.04]. Ce qui est un cas plus courant lors de la connexion à Internet.

Vu la flexibilité de l'interface, il est perceptible que le site web de PRTG est bien responsive, pour pouvoir offrir à un appareil Android une telle accessibilité [4.05].

4.2.3 Perspective de l'implémentation de l'application

En vue de la simulation et des études dont on a effectué, les appareils Android sont les outils du développement technologique du futur. Les applications Android sont les logiciels qui vont mener et faciliter la communication entre appareil électronique et humaine.

Le développement des logiciels avec des fichiers « .XML » va favoriser un peu plus le monde du travail en réseau, toutes infrastructures en réseau vont pouvoir bénéficier du développement technologique. Et le travail des maintenances, chefs de production, administrations vont être accessible via son appareil Android.

Le futur de la supervision de réseau et système via appareil Android s'annonce plus intéressant et plus grand dans un projet du futur et même du présent par l'avancé des smartphones et des technologies.

4.3 Simulation des paquets sniffés par python

On a choisi un langage qui est très représentatif de ce que l'on pourrait attendre lorsque le but final est de pouvoir mettre un œil sur le réseau sous toutes les couches informatiques possible.

En programmant des fichiers d'attaque voici les résultats par la supervision de réseau [4.06] [4.07]. Pour faciliter le travail, on a utilisé des commandes à distance avec « ssh ou Secure Shell » sur Windows 10 le PC physique. En utilisant windows10, nous allons pouvoir lancer également des « sniffing » sur Scapy de Python.

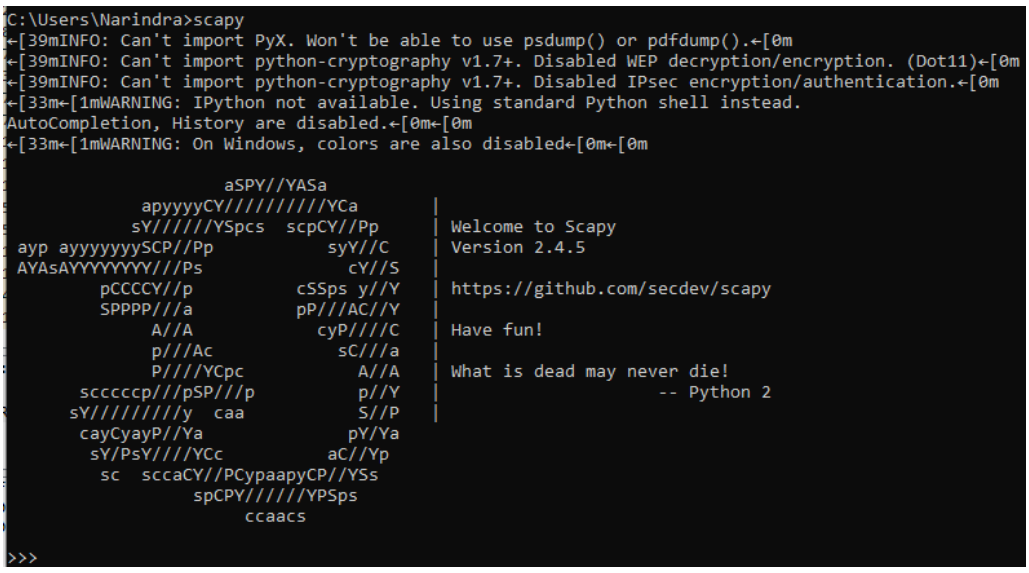


Figure 4.11 : *Présentation de Scapy sur windows10*

4.3.1 Présentations

La simulation va se divisées en deux parties, l'une représente l'interconnexion entre les réseaux par une attaque ARP ou « Address Resolution Protocol », l'autre une simulation d'écoute par commande python.

4.3.1.1 Simulation d'une attaque ARP et visionnage sous Wireshark

Dans les trois figures ci-dessous se trouvent une programmation sous python ;

Le fichier « intrusioNet.py » est une suite de code configurée préalablement selon le besoin de l'administrateur, qui consiste à lancer une attaque inoffensive afin de vérifier la liaison et la communication dans le réseau.

*intrusioNet.py ×

```
from scapy.all import *


pack=ARP()

pack.pdst="192.168.221.10"

pack.hwsrc="FF:FF:FF:FF:FF:FF"

pack.psrc="192.168.221.44"
pack.hwdst="FF:FF:FF:FF:FF:FF"

pack.inter=RandNum(10, 40)
pack.loop=1

pack.show()

i=0
while i< 1000:
      send(packet)
      i=i+1
```

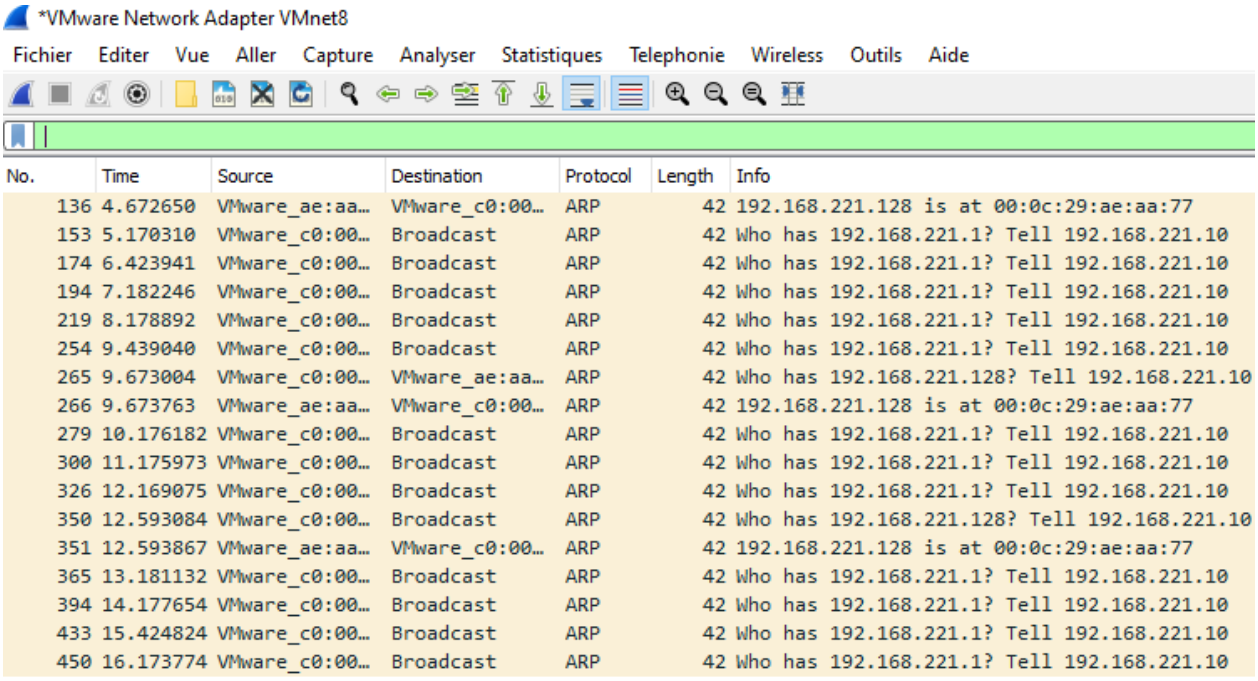
Figure 4.12 : *Programmation simplifiée d'un ARP*

Dans la figure 4.13, le lancement d'ARP vers la machine cible « 192.168.221.10 » est activé, le fichier a été intégré avec une fausse adresse. Cela pour infiltrer dans le réseau « 192.168.221.44 » et l'accompagner d'une adresse MAC «FF:FF:FF:FF:FF:FF ».

S'en suit dans la figure 4.13, la mise en évidence de ce qui a été créée, on voit alors qu'il existe une attaque ARP sous le logiciel Wireshark. Dans la figure 4.15, on a regardé dans la machine cible s'il y a des adresses anormales, ce qui a évidemment été mise en certitude, ce qui a été écrite, a été constaté [4.08]. Bien que le fichier n'est pas de grande taille l'essentiel et sa mise en évidence, il est important pour chaque administrateur d'avoir son propre outil de traque plus simplifier.

```
root@ubuntu:/home/narindra# sudo python Desktop/intrusioNet.py
###[ ARP ]###
  hwtype    = 0x1
  ptype     = 0x800
  hwlen     = 6
  plen      = 4
  op        = who-has
  hwsrc     = FF:FF:FF:FF:FF:FF
  psrc      = 192.168.221.44
  hwdst     = FF:FF:FF:FF:FF:FF
  pdst      = 192.168.221.10
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
```

Figure 4.13 : *Lancement d'une intrusion ARP avec python*



No.	Time	Source	Destination	Protocol	Length	Info
136	4.672650	VMware_ae:aa…	VMware_c0:00…	ARP	42	192.168.221.128 is at 00:0c:29:ae:aa:77
153	5.170310	VMware_c0:00…	Broadcast	ARP	42	Who has 192.168.221.1? Tell 192.168.221.10
174	6.423941	VMware_c0:00…	Broadcast	ARP	42	Who has 192.168.221.1? Tell 192.168.221.10
194	7.182246	VMware_c0:00…	Broadcast	ARP	42	Who has 192.168.221.1? Tell 192.168.221.10
219	8.178892	VMware_c0:00…	Broadcast	ARP	42	Who has 192.168.221.1? Tell 192.168.221.10
254	9.439040	VMware_c0:00…	Broadcast	ARP	42	Who has 192.168.221.1? Tell 192.168.221.10
265	9.673004	VMware_c0:00…	VMware_ae:aa…	ARP	42	Who has 192.168.221.128? Tell 192.168.221.10
266	9.673763	VMware_ae:aa…	VMware_c0:00…	ARP	42	192.168.221.128 is at 00:0c:29:ae:aa:77
279	10.176182	VMware_c0:00…	Broadcast	ARP	42	Who has 192.168.221.1? Tell 192.168.221.10
300	11.175973	VMware_c0:00…	Broadcast	ARP	42	Who has 192.168.221.1? Tell 192.168.221.10
326	12.169075	VMware_c0:00…	Broadcast	ARP	42	Who has 192.168.221.1? Tell 192.168.221.10
350	12.593084	VMware_c0:00…	Broadcast	ARP	42	Who has 192.168.221.128? Tell 192.168.221.10
351	12.593867	VMware_ae:aa…	VMware_c0:00…	ARP	42	192.168.221.128 is at 00:0c:29:ae:aa:77
365	13.181132	VMware_c0:00…	Broadcast	ARP	42	Who has 192.168.221.1? Tell 192.168.221.10
394	14.177654	VMware_c0:00…	Broadcast	ARP	42	Who has 192.168.221.1? Tell 192.168.221.10
433	15.424824	VMware_c0:00…	Broadcast	ARP	42	Who has 192.168.221.1? Tell 192.168.221.10
450	16.173774	VMware_c0:00…	Broadcast	ARP	42	Who has 192.168.221.1? Tell 192.168.221.10

Figure 4.14 : *Manifestation de l'intrusion vue par Wireshark*

```
C:\Users\Narindra>arp -a

Interface : 192.168.221.10 --- 0x14
  Adresse Internet      Adresse physique      Type
  192.168.221.40        ff-ff-ff-ff-ff-ff     dynamique
  192.168.221.44        ff-ff-ff-ff-ff-ff     dynamique
  192.168.221.128       00-0c-29-ae-aa-77     dynamique
```

Figure 4.15 : *Intégration des adresses « fake » dans l'interface réseau de la machine attaquée*

Dans la figure 4.13, figure 4.14 et figure 4.15 existent ce que l'on pourrait appeler un envoi avec accusé de réception de paquet. La machine virtuelle qui a lancé le paquet d'information a laissé sa trace sur la machine physique cible, et cela par le biais de Wireshark, on a pu le mettre en évidence comme paquet bien reçu.

4.3.1.2 Lancement d'une programmation sous python pour la supervision du réseau local

Plusieurs commandes ou codes par python permettent au administrateur d'aller plus loin dans le besoin de sniffer son propre réseau, pour des tests ou pour menace de malveillance.

Dans ce premier « sniffing » la figure 4.16, on lance un sniffing sans avoir spécifié la demande, il résulte des centaines de paquets, à savoir 327 paquets TCP, 689 paquets d'UDP et d'autre encore.

Dans la deuxième requête, on spécifie le nombre à cinq paquets à sniffer, et il en résulte ; quatre paquets UDP et un paquet quelconque, sans qu'on y entre en détail.

Dans la quatrième ligne de commande, il y a la requête en détail des paquets sniffés. Par l'invocation du variable a, et en associant a par la fonction « summary » : « a.summary( ) ».

Dans la cinquième requête de sniffing, il y a demande d'un seul paquet venant de l'interface eth0 par la fonction lambda en fonction du variable x, x:x.summary ( ).

```
>>> sniff()


^C<Sniffed: TCP:327 UDP:689 ICMP:18 Other:111>
>>> sniff(count=5)
<Sniffed: TCP:0 UDP:4 ICMP:0 Other:1>
>>> a=_
>>> a.summary()
Ether / IP / UDP 192.168.221.10:netbios_ns > 192.168.221.255:netbios_ns / NBNSQu
eryRequest
Ether / IP / UDP 192.168.221.10:mdns > 224.0.0.251:mdns / Raw
Ether / IPv6 / UDP fe80::34f3:5dc0:8251:5232:mdns > ff02::fb:mdns / Raw
Ether / IP / UDP 192.168.221.10:netbios_ns > 192.168.221.255:netbios_ns / NBNSQu
eryRequest
Ether / ARP who has 192.168.221.1 says 192.168.221.10 / Padding
>>> sniff(count=1, iface="eth0", prn=lambda x:x.summary())
Ether / ARP who has 192.168.221.128 says 192.168.221.10 / Padding
<Sniffed: TCP:0 UDP:0 ICMP:0 Other:1>
>>> packet=sr1(IP(dst="192.168.253.130")/TCP(dport=80))
Begin emission:
.Finished to send 1 packets.
*
Received 2 packets, got 1 answers, remaining 0 packets
```

Figure 4.16 : *Lancement des « sniff » possible sur Scapy de Python*

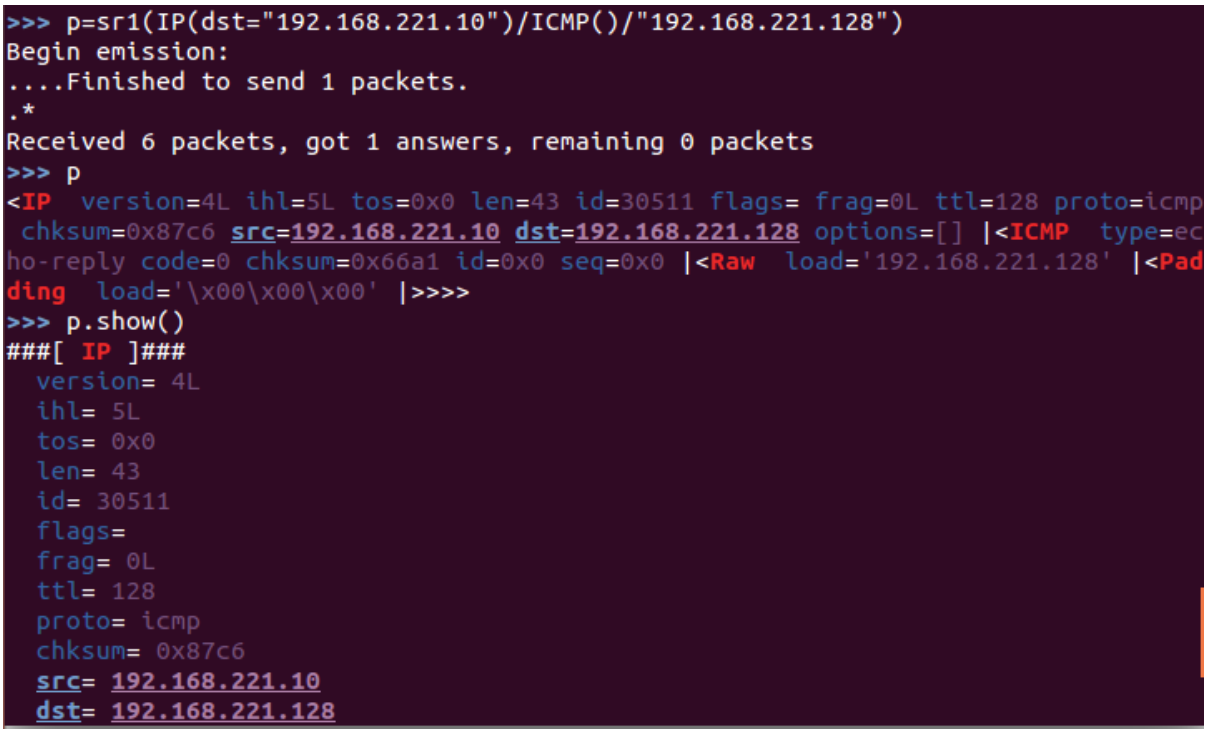


Figure 4.17 : *Lancement de paquet envoyer et recevoir sur un réseau*

Dans la figure 4.17, une fonction p a été lancée d'une source à un destinataire pour sniffer les paquets et connaitre l'aboutissement de la requête en précisant l'adresse IP source et destinataire, cela va de même dans la requête de la figure 4.18, pour sniffer des ports spécifiques.

Figure 4.18 : *Types de commande pour superviser les activités sur des ports précis*

Les trois figures : 4.16, 4.17, 4.18 ci-dessus montrent les capacités d'observations de réseau à distance, surtout quand un administrateur sait quel genre de fonction ou de manipulation il a

besoin pour favoriser ses recherches. [4.09] Dans la figure 4.18 plus précisément, il y a l'illustration d'écoute sur les ports en envoyant et recevant des paquets ou des signalements d'interconnexion.

4.3.2 Interprétation du résultat

Python est un langage de programmation complet, favorise la personnalisation de chaque technique d'infiltration sur un réseau de communication informatique. En sachant cela, Python est un langage fondamental sur la création de mode de sécurité et de monitoring de réseau. Grâce à ses capacités et flexibilités, il est capable d'assurer la performance d'un réseau, ainsi que testé la vulnérabilité qui peut s'établir. Python détient la troisième place du langage le plus utilisé dans le monde de développement et programmation informatique, après Java et JavaScript [4.10] [4.11] [4.12] [4.13].

4.3.3 Perspective de la supervision réseau par python

Python est un langage compréhensible, flexible et intégrable pout toute programmation. Plusieurs types de logiciels offrent la supervision de réseau, pourtant beaucoup d'entre eux choisissent d'intégrer des fichiers pythons. De ce fait et d'autres raisons de maniabilités, Python est encore un langage nécessaire et très capable pour réaliser multiple projet d'avenir en réseau et système.

4.4 Conclusion

L'application Android est bien en marche, elle offre toute les activités dont le logiciel PRTG offre lui-même. Cependant, la sécurité et le bon fonctionnement autant qu'administrateur doit se faire à partir du serveur principal qui contient le logiciel PRTG, car le logiciel possède une application d'administrateur à l'intérieur. Cette application d'administration offre à l'administrateur le choix d'administrer quel appareil va pouvoir consulter à distance le logiciel grâce à son adresse MAC ou « Medium Access Control » ou l'IP préconfiguré. Les applications Android offrent une facilité de travail. Facilite le transport et sécurité physique des appareils. Peut import l'endroit où il faut accomplir une mission, les appareils Android sont plus transportable et facile à manipuler.

Python est l'outil de programmation de supervision de réseau complet dont les programmeurs et administrateurs informatique utilisent pour mener à bien leurs travails.

CONCLUSION GENERALE

Des études et analyses de performance de logiciel ont été réalisées pour lesquelles ses produits sont favorables dans un environnement préalable. Il est nécessaire de comprendre le mode de fonctionnement de ses logiciels, pour établir le besoin à son utilisation.

Les systèmes cloud sont des produits de technologie de pointe le plus performant et le plus utilisé de nos jours. La complexité de ces systèmes provient des faits qu'ils sont exécutés de manière distributive sur des architectures à multiples cœurs. De ce fait, les services offertes sont d'une garanti sans égales. Ces grandes tailles permettent aux cloud des services hétérogènes, qui impliquent différentes technologies de pointes de ses librairies et environnements de programmation.

Docker est un environnement de personnalisation de fonctionnement, il offre plusieurs options de paramètre interne qui vise d'alléger l'exécution de tâche dans une entreprise. En sachant que des dizaines de services sont lancés chaque jour dans un réseau et système de communication et d'échange informatique, il est difficile de mettre de l'ordre ou de régulariser certain fonctionnement dans des logiciels. Docker est un logiciel de solution de rangement des logiciels grâce aux emplacements qui s'y trouve, ce sont les conteneurs.

Des serveurs de monitoring de communication et d'échange de données sont implémentés dans les réseaux et systèmes des entreprises de grande ou de petite taille. Il est possible d'en utiliser de différent type au sein d'une entreprise. Il est important de savoir comment se présent les fichiers échangés ou l'état des tâches durant les heures de pointes, et même en avoir des notifications de temps à autre hors du zone de travail.

Administrer un site de réseaux et systèmes informatique est un travail qui a besoin d'être bien évaluer et analyser pour pouvoir offrir une bonne communication entre tous les utilisateurs. La sécurité logique et physique dépend entièrement d'une bonne architecture de réseau. Des protocoles de sécurité telle SNMP sont configurés au niveau de chaque appareil afin de filtrer toute action malveillante.

La réalisation et la simulation d'un système de supervision réseaux est un succès pour l'avancée de la sécurité et de la performance au niveau de la communication et d'échange informatique.

Les applications et appareils Android sont les produits de l'innovation de nos jours produits par Java. Sachant que chaque utilisateur de smartphone utilise plus d'une dizaine d'application Android par jour, les développeurs de Java conquis le monde de la technologie du futur. Chaque utilisateur de smartphone peut rester connecté de jour comme de nuit pour ne rien raté du monde extérieur. Et si cela est profitable pour un simple utilisateur de consommation, tel un client d'un magasin en ligne. Les grandes entreprises à Madagascar pourraient développer une application Android. Pour des chefs de production ou des chefs de maintenance, la détection de panne est souvent source de ralentissement de production. Si un développeur d'application Android facilite leurs travails en minimisant le temps de découverte de la source des failles, alors la productivité ne pourrait que s'améliorer.

Pour terminer, le monde de la technologie ne cessera d'innover, de nombreuses découvertes et d'amélioration augmente de jour en jour grâce à l'avancé de la communication sans fil et internet. En parlant de l'avancée de la télécommunication, le 5G favorisera l'internet des objets et la performance de la communication en temps réel. Viendra aussi l'internet quantique, le mode de communication du futur.

ANNEXES

Annexe 1 : FICHIER XML

A1.1 Codage fichier PRTG « table.xml »

```
<prtg>
     <prtg-version>21.1.66.1623+</prtg-version>
     <options>
          <usertimezone>
          </usertimezone>
          <userdatesettings>
          </userdatesettings>
          <graphs>
          </graphs>
          <sensortypes>
          </sensortypes>
          <usedtags>
          </usedtags>
          <tasks>
          </tasks>
      </options>
              <sensortree>
                 <nodes>
                    <group id="0">
                         <name>Racine</name>
                         <id>0</id>
                         <url>/group.htm?id=0</url>
                         <tags/>
                         <priority>3</priority>
                         <fixed>1</fixed>
                         <hascomment>0</hascomment>
                          <status_raw>3</status_raw>
                          <active>true</active>
                   <probenode id="1">
                   </probenode>
                 </group>
              </nodes>
           </sensortree>
</prtg>
```

A1.2 Codage PRTG nœuds « table.xml »

```
<nodes>
       <group id="0">
       <name>Racine</name>
       <id>0</id>
       <url>/group.htm?id=0</url>
       <tags/>
       <priority>3</priority>
       <fixed>1</fixed>
       <hascomment>0</hascomment>
       <status_raw>3</status_raw>
       <active>true</active>
       <probenode id="1">
             <name>Sonde locale (Sonde locale)</name>
             <id>1</id>
             <url>/probenode.htm?id=1</url>
```

```
            <tags/>
        <priority>3</priority>
        <fixed>1</fixed>
        <hascomment>0</hascomment>
        <status_raw>3</status_raw>
        <active>true</active>
              <device id="40">
              <summary> 0,3,2,1,0,0,0,0</summary>
              <name>Équipement de la sonde</name>
              <deviceicon>A_Server_1.png</deviceicon>
              <id>40</id>
              <url>/device.htm?id=40</url>
              <tags/>
       <priority>5</priority>
       <fixed>1</fixed>
      <hascomment>0</hascomment>
      <host>127.0.0.1</host>
      <status_raw>3</status_raw>
      <active>true</active>
               <sensor id="1003">
               </sensor>
               </device>
               <group id="50">
               <name>Détection du réseau</name>
               <id>50</id>
               <url>/group.htm?id=50</url>
               <tags/>
              <priority>3</priority>
              <fixed>0</fixed>
              <hascomment>0</hascomment>
              <status_raw>3</status_raw>
              <active>true</active>
              <group id="53">
               </group>
           </probenode>
        </group>
</nodes>
```

A1.3 Codage application supervisionPRTG « activity_main.xml »

```
<?xml                      version="1.0"                      encoding="utf-8"?>
<LinearLayout        xmlns:android="http://schemas.android.com/apk/res/android"
    xmlns:tools="http://schemas.android.com/tools"
    android:layout_width="match_parent"
    android:layout_height="match_parent"
    android:orientation="vertical"
    tools:context=".MainActivity">
    <WebView
        android:id="@+id/webView"
        android:layout_width="match_parent"
        android:layout_height="match_parent">
```

```
        <androidx.recyclerview.widget.RecyclerView
            android:layout_width="match_parent"
            android:layout_height="match_parent"
            android:layout_x="314dp"
            android:layout_y="49dp"                                    />
    </WebView>
</LinearLayout>
```

A1.4 Codage application supervisionPRTG « AndroidManifest.xml »

```
<?xml                    version="1.0"                    encoding="utf-8"?>
<manifest            xmlns:android="http://schemas.android.com/apk/res/android"
    package="com.example.supervisionprtg">
    <uses-permission              android:name="android.permission.INTERNET"/>
    <uses-permission             android:name="android.permission.SET_ALARM"/>
    <uses-permission   android:name="android.permission.ACCESS_NETWORK_STATE"/>
    <application
        android:networkSecurityConfig="@xml/network_security_config"
        android:allowBackup="true"
        android:icon="@mipmap/ic_launcher"
        android:label="@string/app_name"
        android:roundIcon="@mipmap/ic_launcher_round"
        android:supportsRtl="true"
        android:theme="@style/Theme.SupervisionPRTG">
        <activity                                  android:name=".MainActivity">
            <intent-filter>
                <action      android:name="android.intent.action.MAIN"      />
                <category   android:name="android.intent.category.LAUNCHER"   />
            </intent-filter>
        </activity>
    </application>
</manifest>
```

Annexe 2 : CODAGE D'ETUDE DE GRAPHE

A2.1 Construction de graphe d'exécution de tâche

```
Input: trace T
Output: execution graph G
1: T ASK ← {initial tasks} .
2: CP U ← ∅
3: CT X ← ∅
4: for all task t ∈ T ASK do .
5:     if t.state is running then
6:       CP U[t.cpu] ← t
7:     end if
8:     Create initial vertex of task t with timestamp t.begin
9: end for
10: for all event e ∈ T do .
11:    if e.type is sched_switch then
12:       link_horizontal(e.prev_tid, e.ts, running)
13:       link_horizontal(e.next_tid, e.ts, preempted)
14:       CP U[e.cpu] ← e.next_tid
15:    else if e.type is sched_wakeup or
16:       sched_wakeup_new then
17:       interrupt ← Peek CT X[e.cpu]
18:    if interrupt is not null then
19:        link_horizontal(e.tid, t.ts,
20:        labelof(interrupt))
21:    else
22:        v1 ← link_horizontal(e.tid, e.ts, blocked)
23:        v2 ← link_horizontal(CP U[e.cpu], e.ts,
24:             running)
25:             link_vertical(v1, vimages2)
26:   end if
27:   else if e.type is interrupt entry then
28:        Push e to CT X[e.cpu]
29:   else if e.type is interrupt exit then
30:        Pop from CT X[e.cpu]
31:   end if
32: end for
33:   function link_horizontal(task, ts, l) .
34:   tail ← last vertex of task from G
35:   Create vertex v with timestamp ts
36:   Create edge tail[right] → v[lef t] with label l
37: return v
38: end function
39: function link_vertical(from, to, l)
40:   Create edge from[up] → to[down] with label l
41: end function
```

A2.2 Codage graphique d'approximation de chemin critique

```
Input: execution graph G, task T, vs, ve
Output: path P
1: v ← vs
2: while v is not ve do .
3:   E ← v.right
4:   append process(E) to P
5:   v ← E.to
6: end while
7: function process(edge)
```

```
8:      if edge.label is blocking and
9:          edge.to has incoming vertical edge then
10:       return resolve(edge)
11:     else
12:       return E
13:     end if
14: end function
15: function resolve(edge)
16:     TMP ← ∅
17:     v ← edge.to.down.from .
18:     while v.ts > edge.from.ts do .
19:       E ← v.lef t
20:       prepend process(E) to TMP
21:       v ← E.from
22:     end while
23:     return TMP
24: end function
```

REFERENCES

[1.01] https://www.lebigdata.fr/definition-cloud-computing/ avril 2021

[1.02] https://www.futura-sciences.com/tech/definitions/informatique-cloud-computing-11573/2021

[1.03] https://www.redhat.com/fr/topics/containers/what-is-docker /2021

[1.04] https://www.synology.com/fr-fr/support/nas_selector /2021

[1.05] Documentaire sur une les nouvelles technologies du monde france2 /2019. Madrzejewski Alexia.

[1.06] https://www.manageengine.com/network-monitoring/what-is-snmp.html/2021

[1.07] C. Bruni, P. D'Andrea, U. Mocci, and C. Scoglio. Optimal capacity management of virtual paths in an ATM network. In IEEE Globecom 94 Proceedings, 1994.

[1.08] J. Abate and W. Whitt. Transient behavior of the M/M/1 queue: starting at the origin. Queueing Systems, 2, 1987.

[1.09] D. Kelton. Transient exponential-erlang queues and steady-state simulation. Commu nications of the ACM, 28(7), 1985.

[1.10] W. D. Kelton and A. M. Law. The transient behavior of the m/m/s queue, with implications for the steady-state simulations. Operations Research, 33(2), 1985.

[1.11] I. J. Lee and E. Roth. A heuristic for the transient expected queue length of markovian queueing systems. Operations Research Letters, 14(1), 1993.

[1.12] D. S. Lee and S. Q. Li. Transient analysis of a switched poisson arrival queue under overload control. Performance Evaluation, 17(1), 1993

[1.13] R. Murray and W. D. Kelton. The transient behavior of the m/ek/2 queue and steady state simulation. Comput. Operat. Res., 15, 1988.

[1.14] A. R. Odoni and E. Roth. An empirical investigation of the transient behavior of

stationary queueing systems. Operation Research, 31, 1983.

[1.15] L. Saaty. Time-dependent solution of the many-server poisson queue. Operations Research, 8, 1960.

[1.16] J. M. Garcia, D. Gauchard, O. Brun, P. Bacquet, J. Sexton, and E. Lawness. Modélisation différentielle et simulation hybride distribuée. Calculateurs Parallèles, Réseaux et Systèmes Répartis, 2002.

[1.17] Kobayashi. Application of the diffusion approximation to queueing networks ii:No nequilibrium distributions and applications to computer modeling. Jour. of the Ass. for Comp. Machinery, 21(3), 1974.

[1.18] C. L. Wang. On the transient delays of m/g/1 queues. J. Appl. Prob., 36(3), 1999.

[1.19] J. Abate and W. Whitt. Transient behavior of the M/M/1 queue: starting at the origin. Queueing Systems, 2, 1987.

[1.20] Broberg, L. Lundberg et H. Grahn, “Performance optimization using extended critical path analysis in multithreaded programs on multiprocessors”, Journal of Parallel and Distributed Computing, t. 61, no 1, p. 115–136, 2001.

[1.21] P. Fournier et M. Dagenais, “Analyzing blocking to debug performance problems on multi-core systems”, ACM SIGOPS Operating Systems Review, t. 44, no 2, p. 77– 87, 2010.

[2.01] https://mdsi.re/a-quoi-sert-le-monitoring-informatique/ /2021

[2.02] https://www.fr.paessler.com/what-is-network-monitoring /2021

[2.03] https://moodle.utc.fr/pluginfile.php/16777/mod_resource/content/0/SupportIntroSecu/co/CoursSecurite_8.html

[2.04] https://www.nameshield.com/ressources/lexique/spoofing/./2021

[2.05] https://www.securiteinfo.com/attaques/hacking/smurf.shtml/2021

[2.06] https://www.nagios.org /. Environment et platform NAGIOS. 2021

[2.07] https://www.centreon.com /, Environnement et Plateforme CENTREON/2021.

[2.08] https://www.technologuepro.com/reseaux/Analyse-de-protocoles/analyse-de-trafic-reseau-via-outil-MRTG.html

[2.09] C. Bruni, P. D'Andrea, U. Mocci, and C. Scoglio. Optimal capacity management of virtual paths in an ATM network. In IEEE Globecom 94 Proceedings, 1994.

[2.10] 2.4.1.1.1.1 Google Inc : Security, 2015. URL https://source.android.com/devices/tech/security/index.html

[2.11] Shiju P. John : Android Architecture, 2015. URL http://www.eazytutz.com/android/android-architecture/

[2.12] Ben Cheng et Bill Buzbee : A JIT Compiler for Android's Dalvik VM. In Google IO developer conference, page 32, San Francisco, CA, 2010. URL http://www.android-app-developer.co.uk/android-app-development-docs/ android-jit-compiler-androids-dalvik-vm.pdf.

[2.13] Anwar Ghuloum, Brian Carlstrom et Ian Rogers : Google I/O 2014 - The ART runtime, 2014. URL https://www.youtube.com/watch?v=EBlTzQsUoOw.

[2.14] Google Inc : Android Interfaces and Architecture, 2015. URL https://source.android.com/devices/.

[2.15] Google Inc : Application Fundamentals, 2015. URL http://developer.android.com/guide/components/fundamentals.html.

[2.16] Google Inc : platform/bionic.git - Git at Google, 2015. URL https://android.googlesource.com/platform/bionic.git.

[2.17] Mathieu Devos : Bionic vs Glibc Report. Rapport technique, Universiteit Gent, Gent, 2014. URL http://irati.eu/wp-content/uploads/2012/07/bionic{_}report.pdf.

[2.18] Google Inc : Application Security, 2015. URL https://www.google.com/about/appsecurity/android-rewards/.

[3.01] VMware Workstation Pro, étude de la faisabilité de la mise en place d'un réseau.

[3.02] Z. ABDELHALIM. Recherche et détection des patterns d'attaques dans les réseaux IP à haut débit. Thèse de doctorat. Université d'Evry Val d'Essonne. Janvier 2011.

[3.03] https://primabord.eduscol.education.fr/qu-est-ce-que-l-informatique-dans-lesnuages-ou-le-cloud-computing. Plateforme Owncloud, la dépendance de la RAM de la machine.

[3.04] Les prés configurations avec les installations des outils de travail avec la plateforme Owncloud. https://primabord.eduscol.education.fr/qu-est-ce-que-l-informatique-dans-lesnuages-ou-le-cloud-computing.

[3.05] https://primabord.eduscol.education.fr/qu-est-ce-que-l-informatique-dans-lesnuages-ou-le-cloud-computing. La sécurité du stockage et de la base des données par Owncloud.

[3.06] L'environnement de CACTI dans Ubuntu 14.04 LTS

[3.07] Des configurations préinstallées dans CACTI pour assurer l'accès à la plateforme

[3.08] Graphical Network Simulator By Mike Fuszner. Les différentes capacités qu'offrent GNS3, pour bénéficier d'un environnement de réseau stable.

[3.09] Les différents filtres et contrôles de supervision sur un réseau par Wireshark. https://www.wireshark.org/docs/ wsug_html_chunked/.

[3.10] Environnement d'implémentation de supervision avec PRTG. https://www.fr.paessler.com/what-is-network-monitoring.

[3.11] Installation et mise en place de plateforme de développement d'application avec Android Studio. https://devstory.net/12665/android-fonction.

[3.12] https://www.researchgate.net/publication/342261101_programming, Paessler AG, 2013, auteur : Roshan Poudel, Londre Metropolitan University.

[4.01] Marche de faisabilité d'intégration d'API avec PRTG. https://www.fr.paessler.com/what-is-network-monitoring.

[4.02] https://www.tutorialgateway.org/Tutoriel démonstration with Kimberley Trommler, tech field day extra at CISCO Live Europe Paessler. 2017

[4.03] Lancement de l'application sur les appareils: machine physique source et téléphone Android via câble USB. https://devstory.net/12665/android-fonction.

[4.04] Des erreurs de permission de la connexion, réglable autant qu'administrateur de PRTG. https://www.fr.paessler.com/what-is-network-monitoring.

[4.05] Catherine Boileau, François Gagnon, https://Atomrace.com/coder_securiser

[4.06] Reolandt Cyril https://connect.ed-diamond.com/GNU-Linux-Magazine/GLMFHS-090/ Scapy, le couteau siusse Python pour réseau.

[4.07] https://raw.githubuserscontent.com/DOWRITTV/py3-tutorial-source.Python Packet Sniffer_NO Scapy_Network.

[4.08] Walkthrough: Python - Microsoft https://docs.microsoft.com/en-us/advertising/guides/

[4.09] https://www.researchgate.net/publication/ par Roshan Poudél : (PDF) Writing an Quick Packet Sniffer with Python & Scapy

[4.10] https://scapy.readthedocs.io/en/latest/advanced_usage.html. Advanced usage — Scapy 2.4.5. documentation.

[4.11] https://amalgjose.com/2020/05/17/python-program-to-check-the-internet/ Published by Amal G Jose, © 2021 AMAL G JOSE

[4.12] https://www.binarytides.com/python-packet-sniffer-code-linux/, Code a network Packet Sniffer in Python for Linux. Copyright © 2021 · BinaryTides

[4.13] https://docs.python.org/3/library/os.html/. Miscellaneous operating system interfaces — Python 3.9.6 document. 8/28/2021.

FICHE DE RENSEIGNEMENTS

Nom : RABEMANANTSOA

Prénoms : Mihaja Narindra

Adresse de l'auteur : 0910G100 Mahafaly Vatofotsy

Téléphone : 032 41 179 43

E-mail : NARINDRA14RABEMANANTSOA@gmail.com

Titre du mémoire : ETUDES ET MISE EN PLACE DE SUPERVISION RESEAUX ET SYSTEMES

Nombre de pages : **111**

Nombre de tableaux : **04**

Nombre de figures : **83**

Directeur de mémoire : M. ANDRIAMIADANOMENJANAHARY Harivelo Chandellina Camille, Docteur en Sciences Cognitives et Applications.

Téléphone : 034 14 001 33

Mail : chandellina.camille@gmail.com

FAMINTINANA

« Cloud » no tekinolojia vaovaon'ny fifandraisan-davitra sy ny kajy mirindra. Ny « Docker » dia iray amin'ireo orinasa lehibe mampanofa « Cloud ». « Monitoring » no fomba iray fanaraha-maso ny toeram-pifandraisana iray, izay ampiasaina maneran-tany. Ny PRTG dia iray amin'ireo tekinika aminy fanaraha-maso, izay vokatra avy amin'ny « Cloud ». Ny « ssh » dia tekinika afahana mampiasa fitaovana ara-kajy mirindra alavitra, izay ampiasain'ny tompon'andraikitra. Android dia sampana ara-kajy mirindra natao hoan'ny telefonina. Ny « Python » kosa dia lojika afaka amokarana fomba fanaraha-maso ny « parc informatique » iray. Koa ato amin'ity boky ity dia famoronana lojika ahafahana manara-maso ny fitaovam-pifandraisana no natao manokana.

Teny misongadina : Android, Cloud, Docker, Monitoring, PRTG, Python.

RESUME

Cloud est l'outil informatique dont, chaque utilisateur loue le mode de service qui lui convient. Docker est une des grands fournisseurs de ce service. Le monitoring est une technique et technologie de supervision réseaux et système plus exploité dans le monde de l'informatique. PRTG est une des services de cloud. Grace à la commande ssh, tout administrateur peut accéder à son poste de travail, peu importe où il est. Android est une branche informatique exploitant les appareils mobiles, associé à la PRTG il offre une supervision réseau à toute heure. Python est un logiciel qui offre une programmation flexible et intégrable à tout plateforme, permet de programmer une supervision réseau.

Mots clés : Android, Cloud, Docker, Monitoring, PRTG, Python.

ABSTRACT

Cloud is the main technology witch bring the easy way when working with network and system. Most companies don't buy but rent service and network by cloud. Docker is a big company which provide Cloud. Monitoring the network and system is one way to manage the interconnection inside a local network, the administrator could take control all about the devices and sensor possible by using ssh or a website. PRTG is a logical which gives a monitoring to networks and system. Android is a platform for mobile devices and administrator could combines PRTG and Android for more access and monitoring to a network. Python is a program which offer many possibility for sniffing network.

Keywords : Android, Cloud, Docker, Monitoring, PRTG, Python.