Ordre...../F.S.S.A/UAMOB/2019

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE AKLI MOAND OULHADJE-BOUIRA

Faculté des Sciences et des Sciences Appliquées
Département : **Génie Electrique**

Mémoire de fin d'étude

Présenté par :

BOUAOUD Katia
ARABI Selma

En vue de l'obtention du diplôme de **Master 02** en **:**

Filière : **Télécommunication**
Option : **Systèmes des Télécommunications**

Thème

La mise en place d'une solution de monitoring et suivi des systèmes informatiques et resaux

Devant le jury composé de :

BENZAOUI Amir	MCA	UAMOB	Président
MEDJEDOUB Smail	MAA	UAMOB	Encadreur
SAOUD Bilal	MCA	UAMOB	Encadreur
KASMI Rida	MCA	UAMOB	Examinateur
DJALID Asma	MCB	UAMOB	Examinateur

Année Universitaire 2018/2019

Remerciement

Tout d’abord, Nous tenons à remercier « Allah », le clément et le miséricordieux de nous avoir donné la force et le courage de mener à bien ce modeste travail.

Il n'est jamais facile pour un étudiant de trouver un stage, c'est pourquoi on remercie l'entreprise **SONTRACH** de nous avoir accueillie durant ces 5 mois.

On tient à remercier tout particulièrement Monsieur **A. BOUAOUA** En tant que maître de stage dans l’entreprise, SONTRACH qui Nous a beaucoup appris et a partagé ses connaissances de manière très pédagogique dans domaine du Système réseaux et informatique, On le remercie aussi pour sa disponibilité et la qualité de son encadrement dans entreprise (Sonatrach) durant tout La durée de stage. Merci également à toute l'équipe de l'entreprise, car chacun d'entre eux a su trouver un peu de temps pour nous aider dans notre mission.

Faire notre stage de dernière année dans votre entreprise a été un plaisir, nous avant pu apprendre beaucoup grâce à vous, et surtout nous étions conforté dans notre projet professionnel , ce qui est un aboutissement de notre cursus universitaire.

Nous tenons exprimer nos vifs remerciements à nous encadreurs Monsieur **S. Medjedoub** et Monsieur **B. Saoud** pour le temps consacré à nous écouter, et à nous orienter, et pour les conseils qu’ils ont sus nous prodiguer durant l’évolution de notre projet.

Nous voulons aussi remercier tous les professeurs qui ont contribué à notre formation. Que tous les membres du jury trouvent ici l’expression de nous profonds respects pour avoir pris la peine d’examiner notre mémoire.

Enfin, nous remerciements vont également à toutes les personnes qui ont, de près ou de loin, apporté leurs aides et encouragements.

Dédicaces

Je dédie ce travail qui n'aura jamais pu voir le jour sans le soutien indéfectible et sans limite de **mes chers parents** qui ne cessent de me donner avec amour le nécessaire pour que je puisse arriver à ce que je suis aujourd'hui. Que dieux vous protège et que la réussite soit toujours à ma portée pour que je puisse vous combler de bonheur.

Je dédie aussi ce travail à :

Mon cher frère **Boualem Amine,**

Ma chère sœur **Wissame** et son Mari **Amine**

A ma petite nièce **TAMARA**

Ma chère sœur **Imane** et son fiancé **Slimane**

Son oublié mon oncle **Hamid**

Mes deux grand Mères

Tous mes cousins et cousines.

Tous mes amis ET Surtout Amira, Roumissa, Ahmed

ET aussi ma chère binôme Katia que je respect

À tous ceux qui m'estiment.

Selma ARABI

Dédicace

Je dédie ce modeste travail :

A Mes très **chère Parents** que dieu les protège

En témoignage de ma profonde affection Qu'ils sachent que ce travail est

En partie le fruit de leur soutien, leur sacrifies et tous leur effort qu'ils ont

Fraient pour mon éducation ainsi que ma formation.

Leur fierté à mon égard aujourd'hui est pour moi la meilleure des

Récompenses.

Mes deux grandes mères

A mes deux cher frères **Slimane** et **Yanis**

A toute ma famille.

Son oublié mes petites cousine **Maroua**, **Maissa**, **Lina** et mon cousin **Fouad**

A mes chers amis : **Cherif**, **Meriem**, **Hayet**, **Rabah**, **Soula**,

Selma ma cher binôme avec qui j'ai passé de très bons moments.

A toute la promotion de Master2 2018/2019.

Et a tous mes collègues

Bouaoud Katia

Résumé

Aujourd'hui les systèmes informatiques et réseaux sont très utilisés dans les entreprises. Ces réseaux devenus très importants en terme de nombre des équipements et en terme de services qu'ils offrent. La société SONATRACH possède aussi un réseau WAN de taille important (équipements et services). La gestion de ce réseau est devenue très difficile avec le temps. Dans notre projet nous avons proposé d'utilisé un logiciel de supervision afin d'automatiser la gestion, diagnostique et le contrôle de réseau informatique de la société SONATRACH. Nous avons montré l'efficacité du logiciel de monitoring OBSERVIUM à base de protocole SNMP avec plusieurs tests.

Mots-clés: Monitoring, Linux (Centos7), Réseau informatique, Machine virtuelle, SNMP, OBSERVIUM

Abstract

Today software systems and computer networks are widely used in companies. These networks have becomes very important in term of devices number and in term of services that can provide. SONATRACH company also has a large WAN network (devices and services). The management of this network became very difficult over time. In our project, we have proposed to use a supervision software in order to automate the management, diagnosis and control of SONATRACH's computer network. We have showen the powerful of OBSERVIUM monitoring software, which is based SNMP protocol, with several tests.

[Keywords: Monitoring, Linux (Centos7), Computer network, Virtual machine, SNMP, OBSERVIUM]

Sommaire

Chapitre III : Monitoring

Chapitre IV : Mise en place de la solution de supervision

Table des figures

Table DES ABREVATION

- ACLs : Access Control List
- AD : Active Directory
- CIFS: Common Internet File System
- DAS: Direct Attached Storage
- DHCP : Dynamic Host Configuration Protocol
- DMZ : Demilitarized Zone
- DNS : Domain Name System
- FC : Fibre Chenal
- FSF : Free Software
- IAP : Institue Algérien de Pétrole
- ICMP : Internet Control Message Protocol
- IETF: Internet Engineering Task Force
- IHM : interface Homme-Machine
- IP : Internet Protocol
- LAN : Local Area Network
- MIB : Management Information Base
- MPLS : Multi-Protocol Label Switching
- NAS : Network Attached Storage
- NAT : Network address translation
- NFS : Network File Système
- OID : Object Identifier
- OS : Operating System
- PHP : Hyper Texte Preprocessor
- RRDtool : Rond-Robin Data base

- SaaS: Software As A Service
- SAN : Storage Area Network
- SCSI: Small Computer System Interface
- SMB: Server Message Block
- SNMP : Simple Network Management Protocol
- SQL : Structured Query Language.
- TCP: Transmission Control Protocol
- UDP : User Datagram Protocol
- VM : Virtuelles Machines
- WAN : Wide Area Network
- WMI : Windows Management Instrumentation
- XML : Extensible Markup Language

Introduction générale

Actuellement, les systèmes informatiques dans les entreprises deviennent de plus en plus importants mais aussi complexes. Le besoin de maintenance et de gestion de ces systèmes est rapidement devenu une priorité, d'autant plus qu'une panne au niveau de ce système pourrait parfois avoir des conséquences catastrophiques (1).

C'est pourquoi les administrateurs systèmes/réseaux font appel à des logiciels de surveillance et de supervision. Ces logiciels vérifient l'état du système ainsi que des machines connectées et permettent à l'administrateur d'avoir une vue d'ensemble en temps réel de l'ensemble du parc informatique sous sa responsabilité. Il peut être aussi informé (par email, par SMS) en cas de problème. Grâce à un tel système, les délais d'interventions sont fortement réduits, sans que les utilisateurs du système en question soient affectés ou se rendent compte des problèmes survenus (2).

Dans les systèmes informatiques d'entreprise de nombreuses composantes sont donc à surveiller : l'utilisation de la bande passante, les routeurs, les serveurs, les postes de travail, le bon cheminement de l'information entre les machines, la consommation processeur, la consommation de mémoire RAM, ou encore le niveau de stockage du ou des disques durs présents dans cette machine. Etc. Dans ce mémoire nous allons présenter des outils qui nous permettent de contrôler les équipements d'un réseau informatiques localement ou à distant. Nous avons choisi l'outil OBSERVIUM, nous avons étudié cet outil. Les étapes d'installation et d'utilisation de l'outil OBSERVIUM ont été illustrées dans notre mémoire. Un exemple de test et d'évaluation de l'outil OBSERVIUM a été effectué réellement sur le réseau de la société SONATRACH.

Le présent mémoire est structuré en quatre chapitres.

Dans le premier chapitre intitulé «Présentation de l'organisme d'accueil» nous décrivons l'entreprise d'accueil et le cadre du projet et ses objectifs. Tout d'abord nous présentons l'organisme d'accueil et les différentes tâches effectués par la société.

Le second chapitre intitulé « Généralités sur les système informatique » on décrive les déférents composants de système informatique d'entreprise

Le troisième chapitre sera intitulé « le monitoring » présente un rappel du principe de supervision avant de passer à l'étude comparative d'un certain nombre d'outils de supervision existants et le choix de l'outil à mettre en place.

Le dernier chapitre « Mise en place de la solution de supervision» Au sein de ce dernier chapitre, nous allons présenter l'environnement de travail ainsi que les outils logiciels que nous avons utilisés pour la réalisation de notre projet. Et quelques tests et enfin quelques captures écrans des interfaces de l'outil utilisé, à savoir, OBSERVIUM

I.1. Introduction

Nous présentons dans ce chapitre la société d'accueil SONATRACH ainsi que l'Institut algérien du pétrole IAP, lieu de notre stage, y compris le Département Informatique et Systèmes de Gestion.

I.2. SONATRACH

SONATRACH, Société Nationale pour la Recherche, la Production, le Transport, la Transformation, et la Commercialisation des Hydrocarbure, c'est une entreprise publique algérienne créée le 31 décembre 1963 [3].

Acteur majeur de l'industrie pétrolière, surnommée la major africaine, SONATRACH est classée la première entreprise en Afrique, toutes activités confondues.

SONATRACH s'organise autour de 04 grandes activités :

- Activité Exploration-Production.
- Activité Liquéfaction, Raffinage et Pétrochimie.
- Activité Transport par Canalisation.
- Activité Commercialisation.

Chaque activité est constituée de plusieurs divisions. Nous nous intéressons Seulement à l'activité Exploration-Production qui se divise en 05 :

- Division Exploration.
- Division Forage.
- Division Production.
- Division Associations.
- Division PED. (Petroleum Engineering Development)

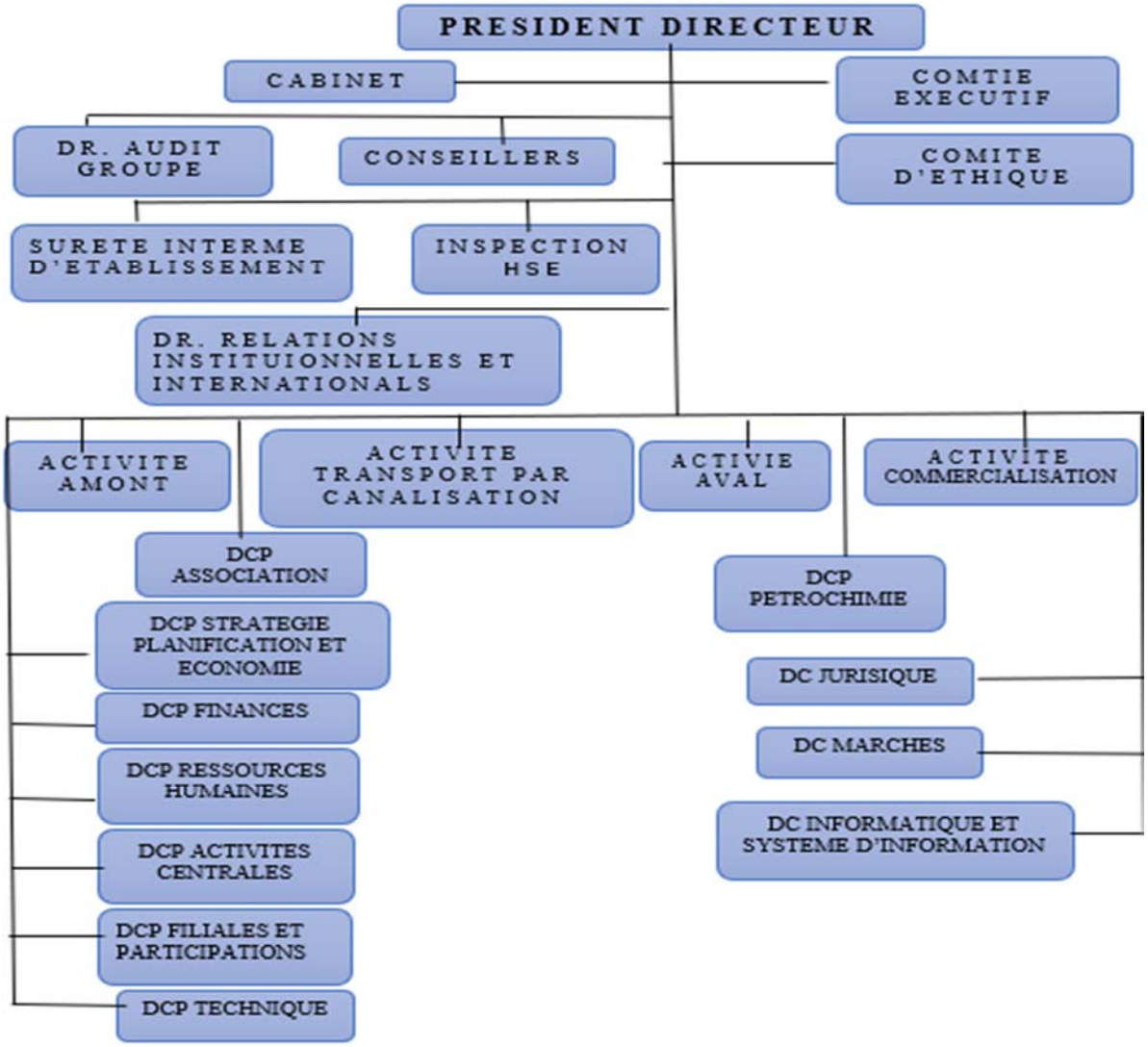


Figure I-1 : l'organisation de la société Sonatrach [3].

I.3. Cadre du projet

Dans le cadre de l'obtention d'un diplôme du mastère en systèmes de télécommunications a Faculté de science et technologie de Bouira, ils nous ont demandé d'élaborer un rapport suite à un stage de six mois. C'est dans ce cadre et pour l'année universitaire 2018/2019 que nous avons effectué le présent projet au sein de l'IAP qui porte sur la mise en place d'une solution de monitoring et suivi des systèmes informatiques et réseaux.

I.4. Travail demandé

Recherche, Implémentation et configuration d'une solution Open Source qui vise à superviser à distance les différents serveurs de la société avec gestion des alertes dans un environnement Multi plateformes.

I.5. Plan du travail [3].

Le but principal du projet est de pouvoir établir, choisir ou installer une station de surveillance des serveurs qui remplissent les conditions suivantes :

- ✓ Comprendre le réseau et les systèmes installés au niveau de la société
- ✓ Comprendre les protocoles de communication des réseaux informatique (TCP/IP)
- ✓ Recherche documentaire sur les solutions existantes en termes du monitoring des réseaux et systèmes
- ✓ Etude comparative entre les différentes solutions trouvées (avantages/inconvénient) de chaque solution
- ✓ Choisir la meilleure solution pour le compte de notre société
- ✓ Comprendre le fonctionnement de la solution choisie au détail près (protocoles de communication avec les systèmes et équipement réseau)
- ✓ Mise en place de la solution (installation et configuration)
- ✓ Tests de la solution :

Suivi des systèmes et équipement réseau via la solution installée

Envoi des alertes à l'administrateur réseau/systèmes en cas d'anomalie

Génère des rapports

I.6. L 'Institut algérien du pétrole (IAP)

L'Institut algérien du pétrole (IAP), est une grande école algérienne spécialisée dans les métiers de l'industrie du pétrole et des hydrocarbures en général. Son siège est à Boumerdes.

Les activités de l'enseignement sont données sur 4 sites : Boumerdes , Arzew, Skikda et Hassi Messaoud.

Il a pour objet la prise en charge des besoins du secteur de l'énergie, en matière de formation de spécialisation, de perfectionnement, de recyclage et de recherche appliquée, toutes disciplines confondues. L'institut assure des formations opérationnelles de niveau international en adéquation avec les besoins du secteur de l'énergie. [3]

➢ Bref Historique

Novembre 1965 : Création de l'IAP EPA

Juillet 1999 : Intégration à Sonagraphe (rattachement au PDG),

Janvier 2004: Groupement d'Intérêt Commun

Septembre 2006 : Société par Actions, IAP Spa

Septembre 2011 : Création du projet IAP-CU et transfert des activités de l'IAP Spa

Novembre 2011 : Direction Centrale de Sonagraphe, IAP CU

Janvier 2012 : Dissolution de l'IAP Spa

Juillet 2012 : Dissolution de Naftogaz Spa et transfert de ses activités à l'IAP-CU

Novembre 2012 : l'IAP est devenu une direction de la Direction Exécutive Ressources Humaines de Sonatrach.

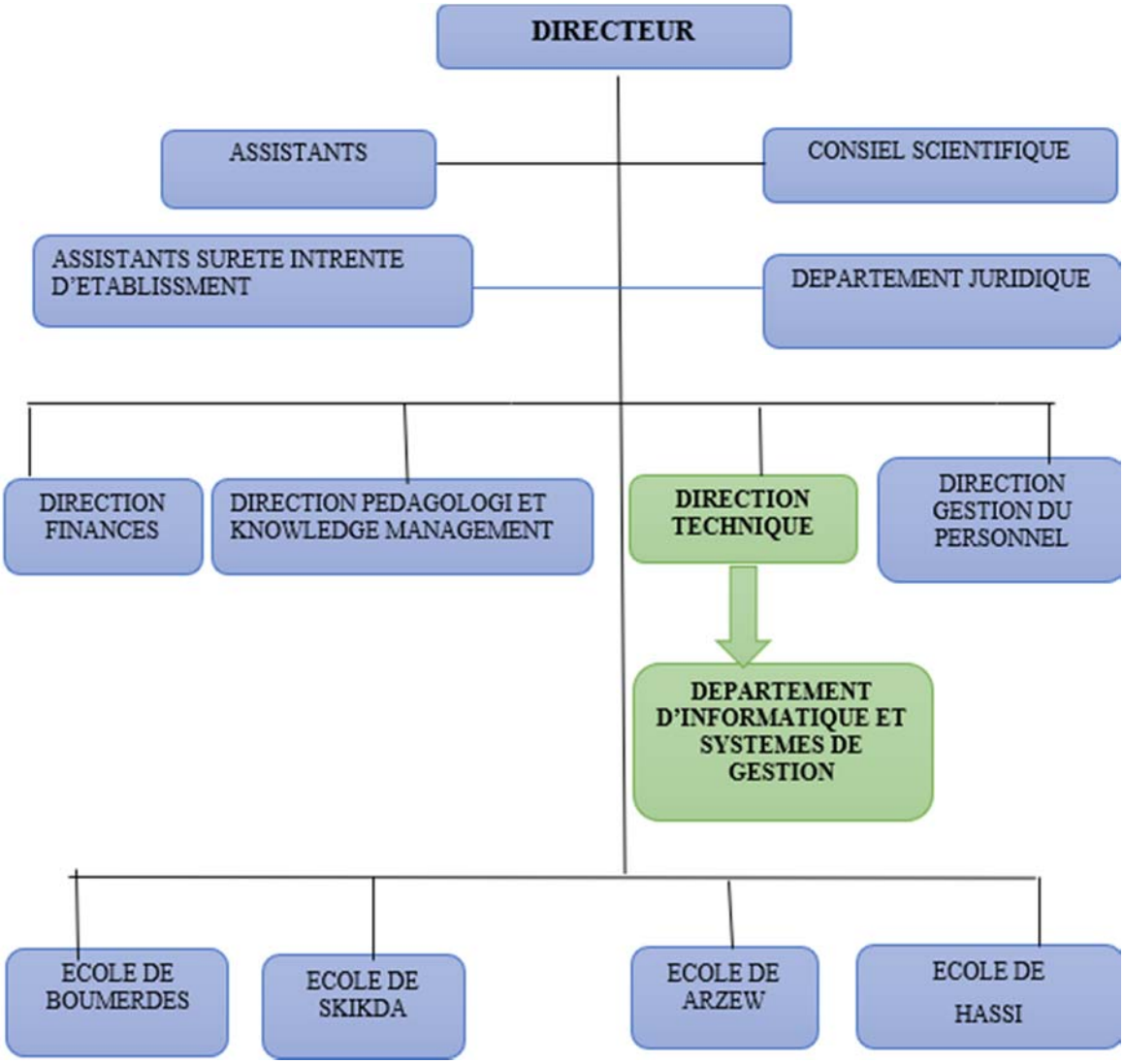


Figure I-2 : Organigramme de l'Institut algérien du pétrole (IAP) [3].

I.7. Missions actuelles de L'IAP

Les tâches principales de L 'Institut algérien du pétrole sont : [3]

- La formation, le perfectionnement et le recyclage dans les différents domaines d'activité de la Société ;
- L'édification en un pôle d'excellence et d'expertise technique et scientifique dans les domaines d'activité de la Société ;
- La recherche appliquée orientée vers les besoins de la Société ;

- Le développement et la mise en place des processus et outils d'évaluation de la formation au sein de la Société ;
- La réalisation de prestations de services d'études et d'expertises ;
- L'organisation des concours de formation-recrutement de la Société ;
- La création des espaces d'échange et d'interaction et l'organisation de forums ainsi que les manifestations scientifiques et techniques ;
- L'établissement d'échanges et de partenariats avec les universités et instituts nationaux et internationaux

Les Spécialités de l'Ecole de Boumerdes: [3]

- Géosciences (Géologie & Géophysique)
- Réservoir Engineering
- Forage & Production
- Exploitation des Hydrocarbures
- Raffinage, Pétrochimie
- Gaz Naturel Liquéfié
- Chimie & Analyse des Hydrocarbures
- Instrumentation Pétrolière
- Mécanique pétrolière
- Procurement/Economie Pétrolière

Les Spécialités de l'Ecole de Hansi Messaoud : [3]

- Géologie/Géophysique
- Forage pétrolier
- Production et intervention aux puits
- Exploitation des hydrocarbures
- Instrumentation pétrolière
- Mécanique pétrolière

Les Spécialités de l'Ecole d'Arzew et de Skikda: [3].

- Raffinage & Pétrochimie
- Chimie & Analyse des hydrocarbures
- Gaz Naturel Liquéfié
- Transport & Distribution du Gaz
- Oïl & Gaz Pressing
- Instrumentation pétrolière

- Mécanique pétrolière

I.8. Mission du Département Informatique et Systèmes de Gestion [3].

Le département **Informatique et Systèmes de Gestion** est en relation directe et permanente avec toutes les structures du groupement. Il offre une assistance aux utilisateurs et garantit la sécurité du système d'information.

Les tâches principales de ce département Mission du Département Informatique et Systèmes de Gestion sont les suivantes :

- L'administration du système informatique ;
- Le soutien et le support technique aux projets de digitalisation ;
- L'assistance technique pour la réalisation des projets d'infrastructures informatiques ;
- La veille technologique dans le domaine de l'informatique et systèmes d'information ;
- La veille à l'application de la charte informatique de la Société ;
- Le rapport à la Direction Technique.

Conclusion :

Ce chapitre a été conçu pour familiariser l'environnement du travail en présentant l'entreprise d'accueil.

Le chapitre suivant sera consacré à l'étude de l'architecture réseaux et système informatique dont elle dispose.

II. Introduction :

Le réseau et les systèmes informatiques sont devenu une ressource indispensable au bon fonctionnement d'une organisation, d'une entreprise, ou une d'université, ...

Dans ce chapitre, nous allons illustrer certains termes en relation avec notre thème. Des notions de bases ainsi que des définitions qui nous aiderons à réaliser notre projet, nous aurons à mettre en avant la partie théorique à savoir l'architecture de réseau d'entreprise.

II.1. Systèmes informatiques dans l'entreprise :

Les systèmes informatiques dans l'entreprise jouent un rôle de plus en plus important. En quelques années les ordinateurs se sont rapidement améliorés et démocratisés. Aujourd'hui, la société Sonatrach est de plus en plus dépendante des systèmes informatiques.

Un système informatique d'entreprise est un ensemble de moyens informatiques et de télécommunications, matériels et logiciels, ayant pour finalité de collecter, traiter, stocker, acheminer et présenter des données.

L'infrastructure technique de base de ce système est constituée par au moins ces éléments clés qui sont :

1. Computing (Serveurs)
2. Réseaux informatiques
3. Stockage

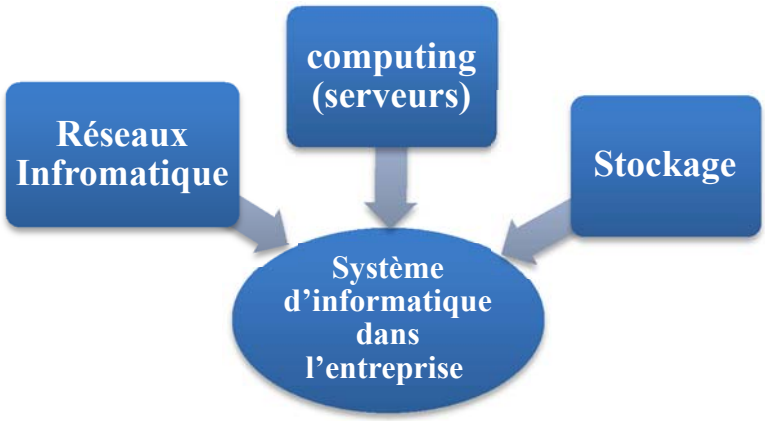


Figure II-1: Système d'informatique dans l'entreprise

II .1.1 Architecture des Réseaux informatique

II .1.1.1 Réseaux informatiques

Un réseau informatique est un ensemble d'équipements électroniques (ordinateurs, imprimantes, scanners, modems, routeurs, commutateurs...) interconnectés et capables entre eux physiquement ou grâce à des ondes radio dans le but d'échange d'information (messageries,

transfert de fichiers, interrogation de bases de données...) et une meilleure stratégie dans le domaine de la sécurité (centralisation et sauvegarde éventuellement automatisée des données).

Grâce à un réseau informatique d'entreprise, les collaborateurs peuvent partager entre eux des données et des applications, les sécuriser, communiquer, et accéder à Internet **[4]**

II .1.1.2 Importance des réseaux informatique

Le réseau informatique est devenu l'un des éléments essentiels du système d'information. Il permet d'utiliser les applications Saas, messagerie, Internet, les applications multi-sites ou même de voix sur IP, les applications cohabitent ensemble sur un même réseau informatique. Pourtant, elles ont des caractéristiques techniques et des besoins bien différents. D'autre part, leur valeur pour le métier et leur criticité sont variables. Il est donc primordial que le réseau soit géré optimiser et surtout supervisé pour garantir une expérience utilisatrice et une efficacité satisfaisante **[4].**

II .1.1.3 Connaître le réseau

Lorsque on installe des boitiers de monitoring de flux, on a souvent la surprise de découvrir à quoi sert vraiment son réseau informatique. Des applications métiers souvent inconnues ou oubliées s'entassent, mais surtout, les volumes sont la plupart du temps mal répartis **[5].** Internet, la messagerie, et les échanges de fichiers représentent plus de 90% du tout, étouffant les applications métiers utiles et les flux techniques type DNS ou SNMP.

II .1.1.4 La connectivité réseau

Il existe une multitude de types de réseaux informatiques. Chaque solution possède ses avantages et ses inconvénients, et toutes ne sont pas adaptées au même usage **[5]**

II .1.1.5 Le réseau Wifi

Le Wifi, pour Wireless Fidélité, est un ensemble de protocoles de communication sans fil, par ondes radio. Ces protocoles sont régis par les normes du groupe IEEE 802.11. Grace aux norme Wifi, il est possible de créer des réseaux locaux sans fils à haut débit. Ce type de connexion est utilisé sur divers matériels informatiques, comme les ordinateurs, imprimantes, box internet ou consoles de jeux. La portée dépend de l'appareil et peut aller de plusieurs dizaines à plusieurs centaines de mètres. Aujourd'hui, la quasi-totalité des périphériques peuvent se connecter en Wifi [**6].**

II .1.1.6 Le réseau LAN

Un réseau LAN (Local Area Network) **[2]**, désigne un ensemble d'ordinateurs appartenant à la même organisation reliée entre eux par un réseau dans une zone géographique limitée. Le réseau local est donc la forme la plus simple de réseau et peut compter plusieurs centaines d'utilisateurs.

La vitesse de transfert de données d'un réseau local peut s'échelonner entre 10 Mbit/s et 1Gbit/s

II .1.1.7 Le réseau WAN

Un réseau WAN (Wide Area Network), est un réseau étendu ou régional. Ce type de réseau informatique est généralement constitué de plusieurs sous-réseaux (LAN) et couvre une grande zone géographique comme un pays, ou un continent. Le type de liaison entre les sites et les technologies employées va conditionner les débits disponibles sur un WAN **[2].** Des routeurs permettent de déterminer le trajet le plus approprié pour atteindre un nœud du réseau. Le réseau WAN le plus connu et le plus grand est le réseau Internet.

II .1.1.8 Le réseau MPLS

Le Multi Protocol Label Switching, MPLS **[5],** fonctionne par commutation d'étiquettes (labels). Celles-ci sont attribuées aux paquets à l'entrée du réseau et sont ensuite retirées à la sortie. Cette technique de commutation est utilisée sur les gros réseaux informatiques

II .1.1.9 Architecture actuelle des réseaux informatiques

Le modèle le plus répandu de nos jours pour les topologies réseaux actuel, que ce soit, LAN ou WAN est un modèle hiérarchique (ou modèle à trois-couche : Core, Distribution, Access) Plus généralement nommé par sa version anglaise, « Three-Layered Hierarchical Model », ce modèle a été inventé et diffusé par Cisco.

Le principe est simple : créer un design réseau structuré en trois couches (layers), chacune ayant un rôle précis impliquant des différences de matériel, performances et outils **[7].**

Ces trois couches sont :

- ✓ la couche cœur, « Coré layer »
- ✓ la couche distribution, « Distribution layer ».
- ✓ la couche accès, « Access layer ».

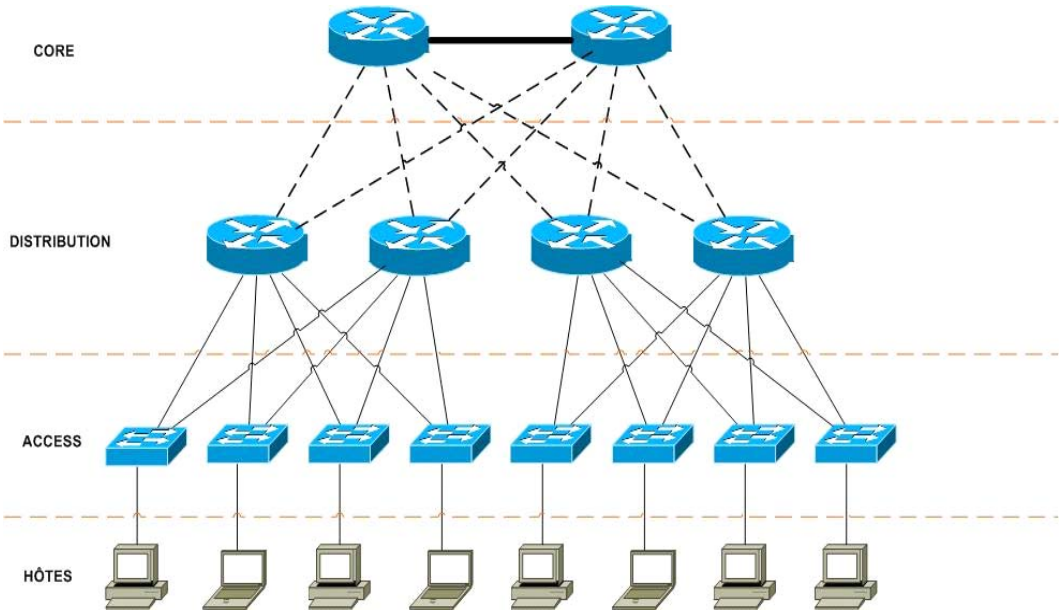


Figure II-2 : **Architecture actuelle des réseaux informatiques [7].**

II .1.1.9.1 couche cœur

C'est la couche supérieure. Son rôle est simple : relier entre les différents segments du réseau, par exemple les sites distants, les LANs ou les étages d'une société.

Nous trouvons généralement les routeurs ou des switched niveau à ce niveau.

Le Core est aussi appelé Back Bône.

II .1.1.9.2 couche distribution

Une fois nos routeurs/switches de la couche Core choisis et mis en place dans notre architecture, le designer s'intéresse à la couche Distribution.

Son rôle est simple : filtrer, router, autoriser ou non les paquets… Nous sommes entre la couche Core et la couche Access, c'est-à-dire entre la partie « liaison » et la partie « utilisateurs ». Ici, on commence à diviser le réseau en segment, en ajoutant plusieurs routeurs/switches de distribution, chacun étant connecté au Core d'un côté, et à la couche Access de l'autre.

Ces routeurs de distribution vont s'occuper de router les paquets, d'y appliquer des ACLs, d'assurer la tolérance de panne, de délimiter les domaines de broadcast, etc…

II .1.1.9.3 couche accès

C'est la dernière couche de notre modèle. Son rôle est simple mais très important : connecter les périphériques « end-users » au réseau.

Mais aussi, assurer la sécurité d'accès au réseau!

Ici, pas de routeur. Seuls des Switch, ou hubs parfois, sont implémentés. C'est normal, puisque tout le travail des routeurs est déjà effectué au niveau de la Distribution ou du Core.

Résultat, on ne s'occupe que de connecter nos end-users au réseau, que ce soit en Wi-Fi, Ethernet ou autre. Et si possible, on le fait de manière sécurisée, c'est-à-dire en utilisant switch port sur nos switches, en désactivant les interfaces non utilisées, etc…

II .1.2. Computing (serveurs) :

Un serveur informatique (figure II-3) offre des services accessibles via un réseau. Il peut être matériel ou logiciel tell que il nous offre un espace de calcul et traitement qui offrent des services, à un ou plusieurs clients (parfois des milliers) : Les services les plus courants sont :

- L'accès aux informations du World Wide Web
- Le courrier électronique
- Le commerce électronique
- Le stockage en base de données
- la gestion de l'authentification et du contrôle d'accès

Un serveur fonctionne en permanence, répondant automatiquement à des requêtes provenant d'autres dispositifs informatiques (les clients), selon le principe de client-serveur. Le format des requêtes et des résultats est normalisé, se conforme à des protocoles réseaux et chaque service peut être exploité par tout client qui met en œuvre le protocole propre à ce service.

Les serveurs sont utilisés par les entreprises, les institutions et les opérateurs de télécommunication. Ils sont courants dans les centres de traitement de données et le réseau Internet**[8].**

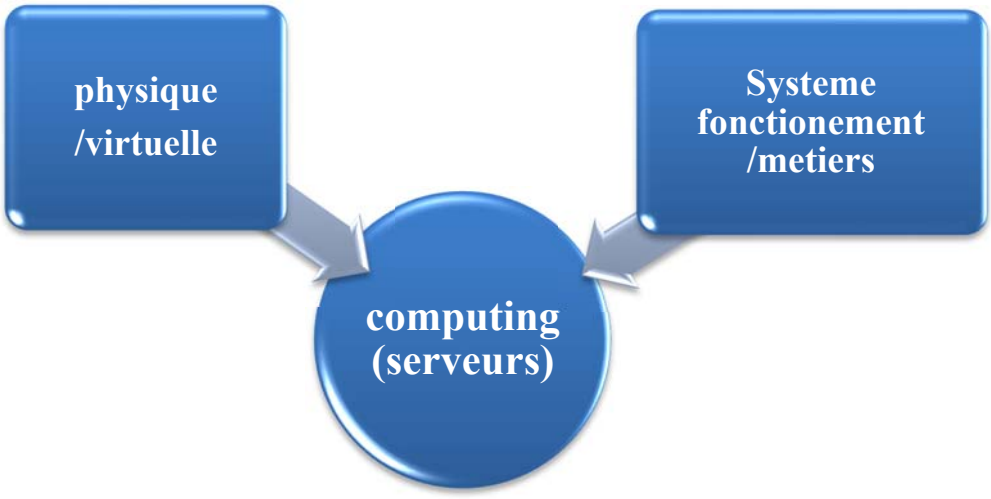


Figure II-3 : serveur informatique

II.2.1. Machine Physique :

Un serveur physique **[9]** (figure II-4) **,** couramment appelé serveur dédié est un serveur sur lequel on installe généralement un seul système d'exploitation pour gérer une application bien spécifique. C'est un serveur réservé à un usage personnel. L'applicatif s'exécutant sur ce serveur dispose de toutes les ressources de la machine. Ainsi, cette applicatif e a accès au système d'exploitation, à la mémoire vive, à la capacité de stockage, à la bande passante et à bien d'autres paramètres

Ce type de serveur permet aussi la centralisation de la gestion de tout le parc informatique d'une entreprise

Serveur messagerie Serveur AD Serveur DNS Serveur DHCP

Figure II-4 : machine phtisique

II.2 .2. Machine virtuelle

Au cours des dernières années, les avancées technologiques dans le domaine du matériel serveur ont largement devancé les besoins des logiciels exécutés. Le rythme des innovations dans le domaine des serveurs obéit à la loi de Moore, tandis que les besoins des applications exécutées sur ces serveurs augmentent modérément d'une année à l'autre. Le taux d'utilisation des serveurs qui exécutent un système d'exploitation et une pile d'applications directement sur le matériel est généralement inférieur à 15%. Les applications courantes n'exigeant que peu de ressources, telles que fichiers, impressions, etc., se trouvent souvent soit sur du matériel ancien et obsolète, soit sûr de nouveaux serveurs neufs, bien plus puissants que nécessaire. Comment les administrateurs informatiques peuvent-ils récupérer ce surplus de capacités ? **[10].** C'est avec les solutions de virtualisation qu'on peut exploiter les ressources d'une machine physique au maximum.

La virtualisation permet d'exécuter plusieurs systèmes d'exploitation sur un même ordinateur. Il faut d'abord installer un système d'exploitation spécial (l'hyperviseur) directement sur le matériel brut et installer les systèmes d'exploitation virtuels sur l'hyperviseur. Ces

instances de SE s'appellent machines virtuelles ou VM. Une seule machine physique peut en comprendre plusieurs dizaines, voire plusieurs centaines.

Principes de fonctionnement : chaque Système d'exploitation se voit attribuer sa propre part de ressources physiques, isolées par un séparateur logique des autres ressources disponibles sur la machine invitée. Cette séparation des ressources est la tâche principale de l'hyperviseur, en plus de l'intégration des services de mise en cluster, de sauvegarde et d'autres ressources permettant l'existence d'hôtes multiples. Les hyperviseurs les plus populaires actuellement sont fabriqués par Microsoft (Hyper-V), VMware (vSphere) et Citrix (XenServer), Proxmox, ou encore Oracle Virtual box

Exemple : un serveur physique (hôte) dispose de 12Go de RAM et de 4processeurs, un hyperviseur est installé sur ce serveur et 4machines virtuelles sont installées sur l'hyperviseur, chacune étant dotée de 2 à 4Go de RAM pour exécuter ses propres applications. Ce scénario peut être schématisé comme suit **[10]** :

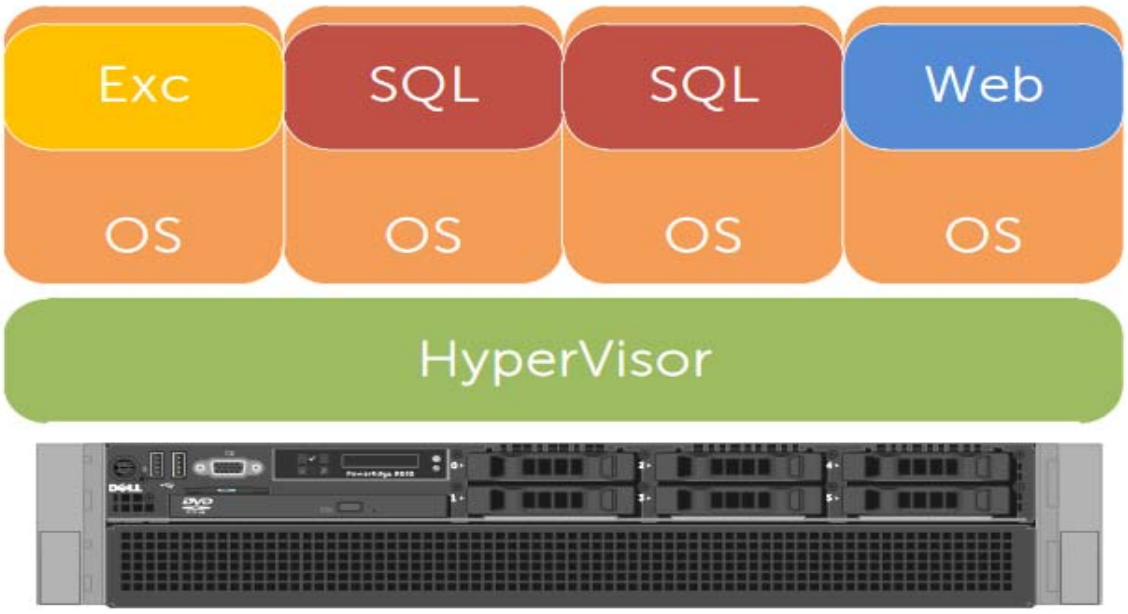


Figure II-5 : Machine virtuelle [10].

II.2 .3. Système de fonctionnement /métier :

Le système informatique a besoin, pour son fonctionnement, d'une part à des systèmes de base tel que l'Active Directory (AD), Messagerie, DNS, DHCP, … d'autre part, à des systèmes métier qui sont spécifiques au métier de l'entreprise, citant par exemple une qui exerce

dans le domaine de la formation a besoin d'un système de gestion de pédagogie tandis qu'une autre société qui fait de la commercialisation a besoin d'un système de facturation.

II.3. Système de stockage de donnée :

Le stockage des données et leurs exploitations sont au cœur du système d'information d'une entreprise. Pour cela différentes architectures sont possibles, ces architectures sont : DAS, NAS et SAN. Dans les paragraphes suivant nous allons présenter ces architectures. **[11].**

II.3.1 DAS : Direct Attached Storage

DAS [10] l'acronyme de Direct Attached Storage, c'est lorsque le disque de stockage est directement relié au serveur, le terme DAS a été créé après l'arrivée de NAS et de SAN pour catégoriser ce type d'accès traditionnelle direct.

L'échange de donne entre le serveur et les disques se fait en mode bloc évidement il ne pas possible de relier un disque a plusieurs machines simultanément, l'espace libre sur le disque de chaque serveur ne peut pas donc être redistribuer entre les machines ce qui fait l'allocation de l'espace disque est très peut optimiser dans sa forme la plus évoluée.

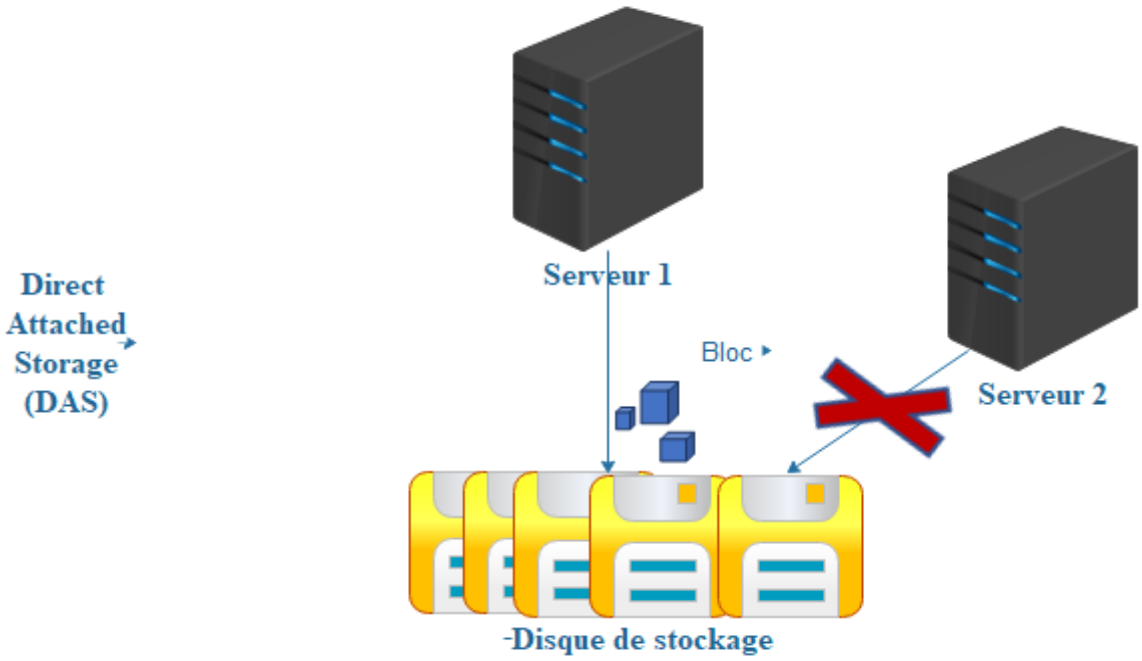


Figure II-6: DAS: Direct Attached Storage

II.3.2 NAS : Network Attached storage

Il s'agit d'une bais de stockage qui dispose à la fois de son propre système d'exploitation dédie à la gestion des données d'un logiciel, de configuration de son propre système, de fichier et ainsi un ensemble de disque Independent. Le NAS **[12],** est attaché au réseau d'entreprise

avant de servir de serveur de fichier, les disques dures ne sont pas reliés au serveur mai au NAS. De plus le NAS permet l'accès client aux donnés sans passe par le serveur d'application, il permet même d'offrir l'accès au même fichier a plusieurs serveurs simultanément et d'ailleurs très adapte pour les applications qui sollicites les systèmes de fichier de façon intuitive. Dans le NAS l'échange de donné entre le serveur et le disque se fait on mode fichier contrairement au SAN et au DAS en mode bloc.

Les échanges de donnes sur le NAS se font via l'utilisation des protocoles CFS/SMB pour Windows et NFS pour UNIX

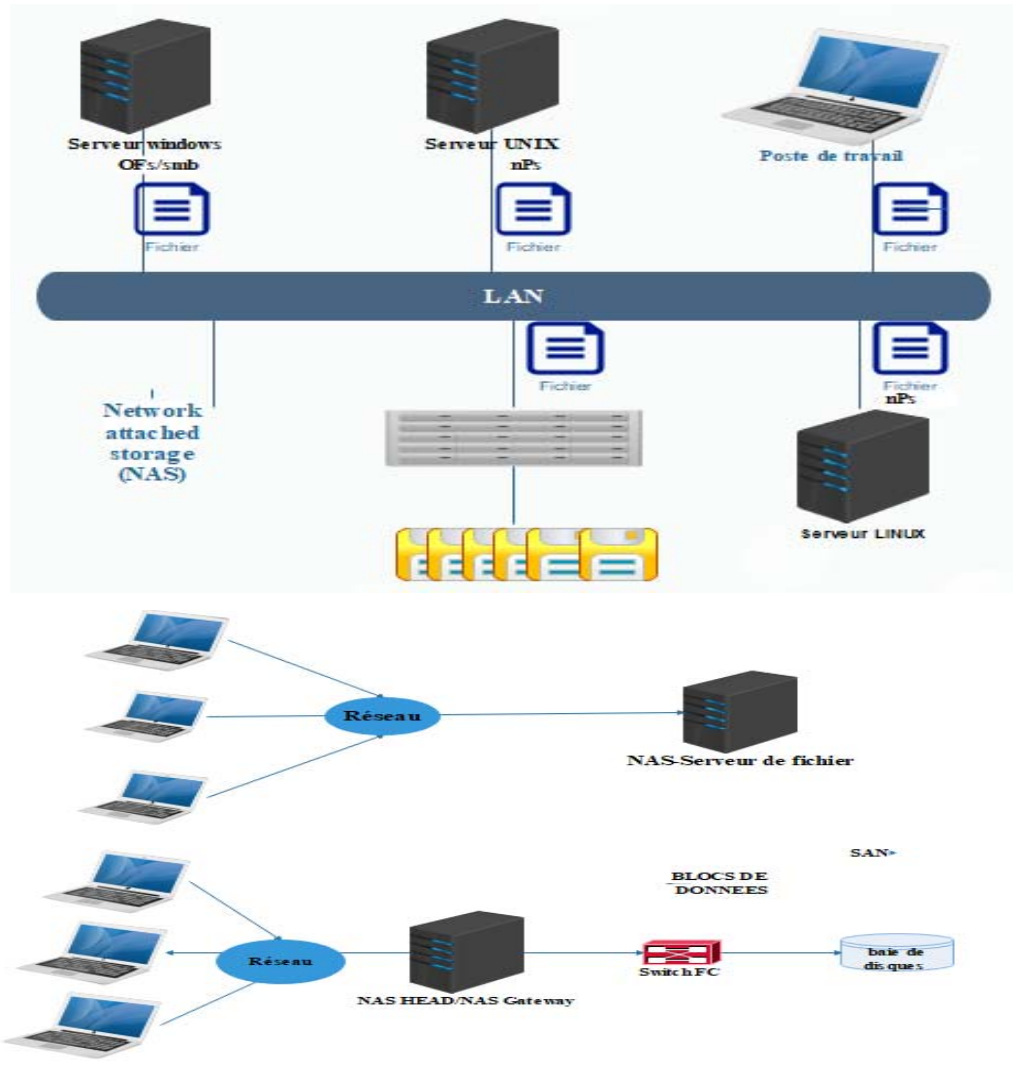


Figure II-7: NAS: Network Attached storage

II.3.3 SAN: Storage Area Network

Dans un SAN **[13]** c'est le serveur qui gère le système de fichier sur les espaces de stockage auxquels il a accès. Un périphérique de stockage peut être relié à plusieurs serveurs via le SAN, ce sont alors des espaces de stockage sur le même périphérique qui sont dédiés à

différents serveurs. Le SAN fait référence à un réseau de données à part entière, en parallèle du LAN

Un SAN **[12]** , ce présente sous forme d'armoire contient plusieurs bais de disque et relier au système d'information par un réseau dédié généralement en fibre Channel, pour un SAN câblé en fibre optique sera alors utilisé le protocole FC (Fibre Channel),les matérielle sont relier entre eux via un switch (FC) en parle alors de fabrique .des disques dure ne sont pas relier directement au serveur ce pendant les bais de stockage sont directement accessible en mode bloc par le système de fichier des serveurs. Chaque serveur vus l'espace de disque d'une des SAN auquel il a accès comme son propre disque dure la SAN permet alors de mutualise les ressources de stockage. Il est ainsi possible dans le cas de SAN de relier un disque a plusieurs machines simultanément l'espace disque ni plus limite parla caractéristique de serveur. Dans le fait le SAN est utilisé pour héberger les donnes applicatives alors que le DAS est utilisé pour la partition système**.**

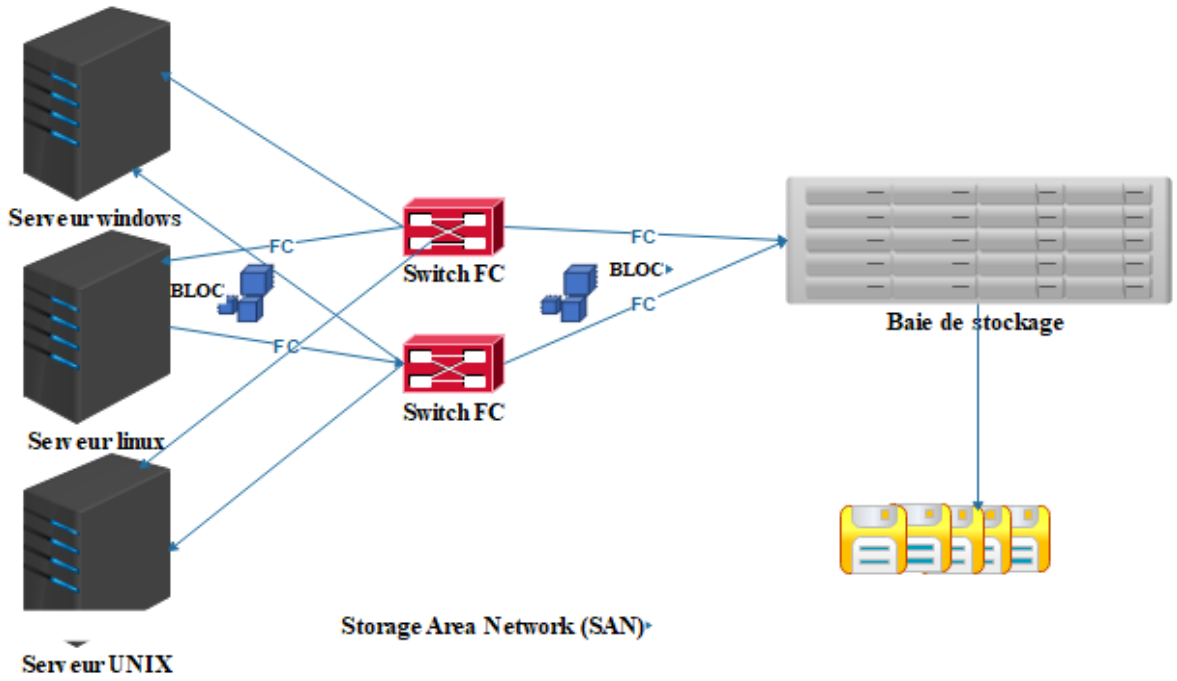


Figure II.8 -: SAN: Storage Area Network

II.4. Monitoring du système informatique de l'entreprise

La surveillance du système informatique dans l'entreprise est sans aucun doute l'une des tâches les plus importantes pour les administrateurs informatiques. Elle aide à garantir que tous les serveurs, le réseau de données et le réseau de stockage fonctionnent avec des performances optimales.

Chaque composante du système informatique utilise son propre outil de surveillance, ce qui oblige les administrateurs à utiliser plusieurs solutions différentes. Cette tâche (gérer plusieurs solutions) devient de plus en plus fastidieuse et difficile à gérer surtout avec l'acquisition des solutions nouvelles.

Le but de notre mémoire est de mettre en place une solution unique et centralisée qui surveille l'ensemble des systèmes et équipements. Cet outil de surveillance vous aidera à conserver toutes les informations sur la santé de vos infrastructures sous contrôle et vous informe de tout temps d'arrêt non planifié

II.5. Conclusion :

Dans ce chapitre, nous avons cité les différents concepts de système informatiques d'entreprise. Une introduction aux réseaux informatique, architecture actuelle des réseaux informatiques, et les différents éléments d'un système informatique ont été présentés. Nous avons terminé ce chapitre avec les principaux composants de système de stockage de données d'un réseau interne de l'entreprise.

III. Introduction

Les systèmes informatiques sont devenus indispensables au bon fonctionnement des entreprises et administrations. Tout problème ou panne survenu sur une partie de ce système pourrait avoir de lourdes conséquences aussi bien financières qu'organisationnelles. Donc, surveiller ou monitorer un tel système devient plus que nécessaire. Dans ce chapitre, nous allons définir précisément le concept de monitoring et de supervision ensuite nous procédons à une étude comparative des outils de supervision (solutions open-source). Cette étude ressemble à un banc d'essai puisque pour chacun des logiciels nous allons : Faire une courte présentation et expliquer son fonctionnement, puis finir sur les avantages et inconvénients.et à la fin on va préciser le choix de l'outil retenu.

III.1. C'est quoi Monitoring

Le terme **Monitoring** est couramment utilisé dans le jargon informatique, il provient de l'anglais, il signifie **Supervision**. Le monitoring permet, d'une part, de collecter et créer des historiques de données, d'y appliquer un traitement (des filtres par exemple) en extraire les données qui nous intéressent et de les présenter sous forme de graphiques. Cet historique des données permet si besoin d'apporter des correctifs au niveau des paramétrages des services, le juste pourcentage des ressources à utiliser...D'autre part, permet de recevoir des alertes qui se présentent au niveau des composants du système informatique. Le Monitoring est très important car il permet d'améliorer le service, et donc ainsi le rendu de l'utilisateur.

III.2. Principe du monitoring (Supervision)

La supervision se définit comme une technique utilisant au mieux les ressources informatiques pour obtenir des informations sur l'état des composants d'un système informatique. Ces données seront ensuite traitées et affichées afin de mettre la lumière sur d'éventuels problèmes. La supervision peut résoudre les problèmes automatiquement ou dans le cas contraire prévenir via un système d'alerte (email ou SMS par exemple) les administrateurs. Plusieurs actions sont ainsi réalisées : Acquisition de données, analyse, puis visualisation et réaction.

Un tel processus est réalisé à plusieurs niveaux d'un parc de machines : Au niveau interconnexions (Réseau), au niveau de la machine elle-même (Système) et au niveau des services offerts par cette machine (Applications).

• **Supervision réseau :** Par le terme réseau on entend ici l'aspect communication entre les machines. Le rôle est de s'assurer du bon fonctionnement des communications et de la performance des liens. C'est dans ce cadre que l'on va vérifier par exemple si une adresse

IP est toujours joignable, ou si tel port est ouvert sur telle machine, ou faire des statistiques sur la latence du lien réseau.

• **Supervision système :** La surveillance se cantonne dans ce cas à la machine elle-même tel que (les serveurs, périphériques, postes de client…) et en particulier ses ressources. Si l'on souhaite par exemple contrôler la mémoire utilisée ou la charge processeur sur le serveur voire analysé les fichiers de logs système.

• **Supervision applicative :** Cette technique est plus subtile, c'est elle qui va nous permettre de vérifier le fonctionnement d'une application lancée sur une machine Cela peut être par exemple une tentative de connexion sur le port de l'application pour voir si elle retourne ou demande bien les bonnes informations, mais aussi de l'analyse de logs applicatifs.**[1].**

III.2.1. Le monitoring, un outil indispensable en entreprise

La sécurité est le premier facteur à tenir en compte lors de la conception d'un système informatique en entreprise, donc la supervision des systèmes d'information et des parcs informatiques, afin d'assurer la haute disponibilité des services, est aussi cruciale pour cette entreprise.

La supervision en temps réel via des protocoles et les formats de données SNMP, les outils de monitoring réseau et solutions de supervision permettent de détecter rapidement les pertes de capacité du système d'information de l'entreprise. Le manager ou l'opérateur réseau reçoit alors des alertes (souvent par e-mail ou sms) en cas de surcharges, et peut ainsi intervenir directement via l'interface du système monitor**.**

En tant qu'outil de visualisation complet, le monitoring permet la détection des anomalies sur l'ensemble du système informatique, internet de l'entreprise, les serveurs, les disponibilités réseaux, les imprimantes, les applications, ainsi que tous les autres éléments actifs en contact avec le réseau (routeurs, switches, hubs, etc.). Une telle solution de supervision et de monitoring permet ainsi à l'administrateur de bien monitorer chaque point du réseau**,** et à distance lorsqu'il n'est pas sur place.

III.2.2 Pourquoi opter pour un logiciel de supervision ?

Si vous êtes une PME (petite ou moyenne Entreprise) ou une grande multinationale, une surveillance réseau efficace est très nécessaire par des logiciels de monitoring performants :

- Qui effectuent des analyses et des diagnostics réseau constants
- Veillent en permanence au bon fonctionnement des processus sur le réseau
- Centralisent les données clés à monitorer et l'information de la santé du réseau
- Et assurent l'envoi d'alertes aux agents de l'équipe informatique dès qu'une anomalie est détectée.

Les besoins en matière de supervision varient d'une entreprise et d'un métier à l'autre. C'est pour cela dans le marché il existe de nombreux outils de surveillance disponibles au téléchargement dans toutes les langues, qu'il s'agisse d'éditeurs de logiciels de monitoring open source (souvent gratuits) ou propriétaires (payants sous licence) **[14].**

III.3. Protocole d'administration réseau

III.3.1. Présentation de Simple Network Management Protocol (SNMP) :

SNMP est un protocole de gestion de réseaux proposé par l'IETF (Internet Engineering TaskForce), un groupe informel et international, ouvert à tout individu et participant à l'élaboration de standards Internet). Il reste actuellement le protocole le plus couramment utilisé pour la gestion des équipements en réseaux **[15].**

SNMP est un protocole principalement utilisé pour superviser des équipements réseaux (routeurs, switches…), des serveurs ou même des périphériques tels que baies de disques, onduleurs... **[16]**

Comme son nom l'indique SNMP est un protocole assez simple, mais sa principale force réside dans le fait de pouvoir gérer des périphériques hétérogènes et complexes sur le réseau. De ce fait ce protocole peut également être utilisé pour la gestion à distance des applications : bases de donnée, serveurs, logiciels**…...[15],** et de diagnostiquer les problèmes survenant sur un réseau**.[16]**

III.3.1.1 les buts du protocole SNMP sont de :

- Aonnaître l'état global d'un équipement (actif, inactif, partiellement opérationnel...).
- Gérer les évènements exceptionnels (perte d'un lien réseau, arrêt brutal d'un équipement...)
- Analyser différentes métriques afin d'anticiper les problèmes futurs (engorgement réseau...)
- Agir sur certains éléments de la configuration des équipements **[16].**

III.3.2. L'environnement de gestion SNMP est constitué de :

- **Le Manager** (station de supervision) exécute les applications de gestion qui contrôlent les éléments réseaux, la plupart du temps le manager est un simple poste de travail
- **Les éléments actifs du réseau**, sont les équipements que l'on cherche à gérer (switch, serveurs...)
- **La MIB** (Management Information Base), est une collection d'objets résidant dans une base d'information virtuelle

- **Le Protocole**, qui exécute la relation entre le Manager et les éléments actifs Chaque élément actif dispose d'une entité que l'on appelle un "agent", qui répond aux requêtes du Manager **[15].**

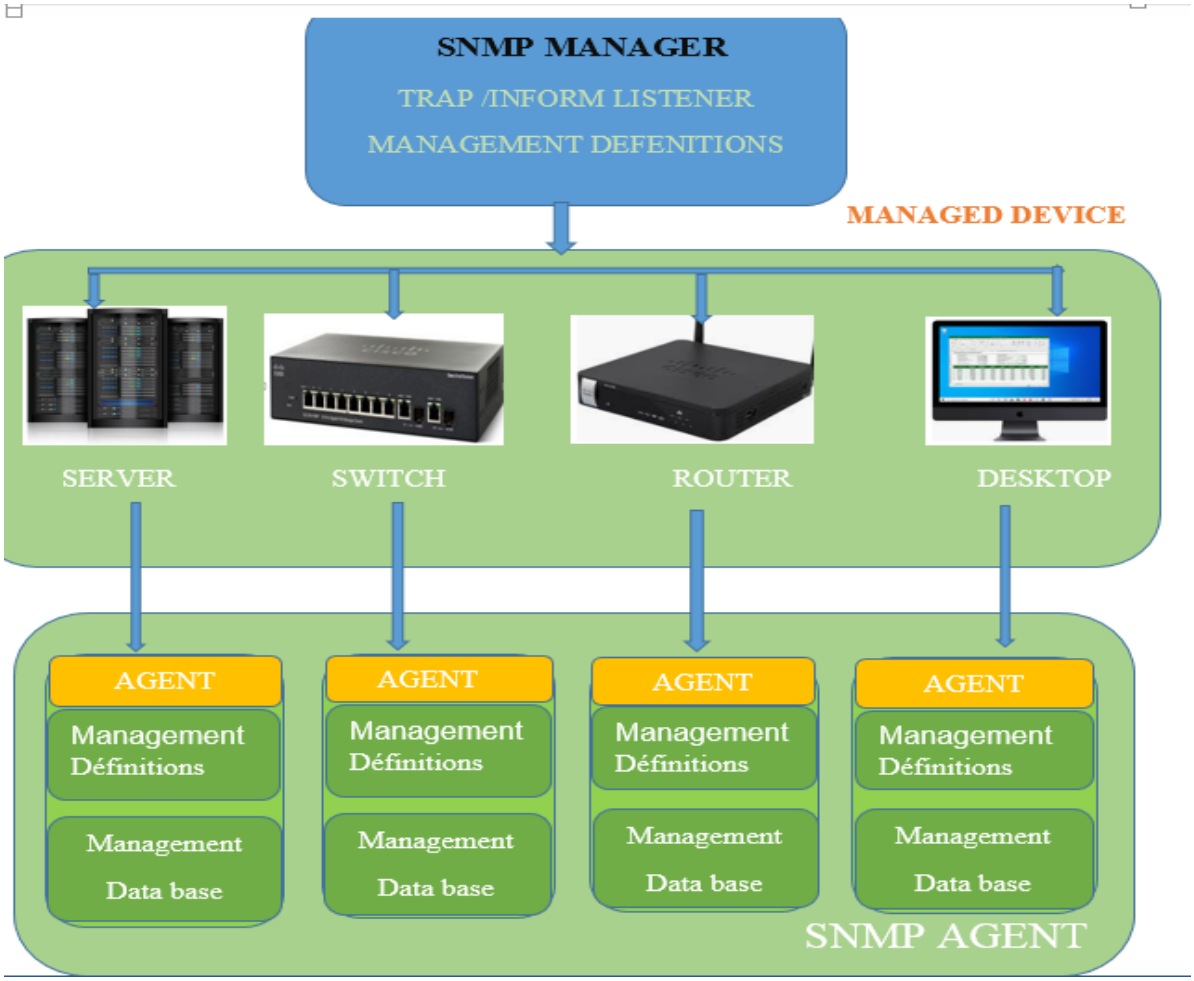


Figure III-1 : Schéma SNMP de communication de base

III.3.2.1 Architecture

Les différents éléments que l'on peut identifier avec le protocole SNMP sont synthétisés par le schéma ci-dessous.

- **Les agents SNMP** : ce sont les équipements (réseau ou serveur) qu'il faut superviser.
- **Le superviseur SNMP** : c'est une machine centrale à partir de laquelle un opérateur humain peut superviser en temps réel toute son infrastructure, diagnostiquer les problèmes et finalement faire intervenir un technicien pour les résoudre.
- **La MIB** : ce sont les informations dynamiques instanciées par les différents agents SNMP et remontées en temps réel au superviseur. **[1]**

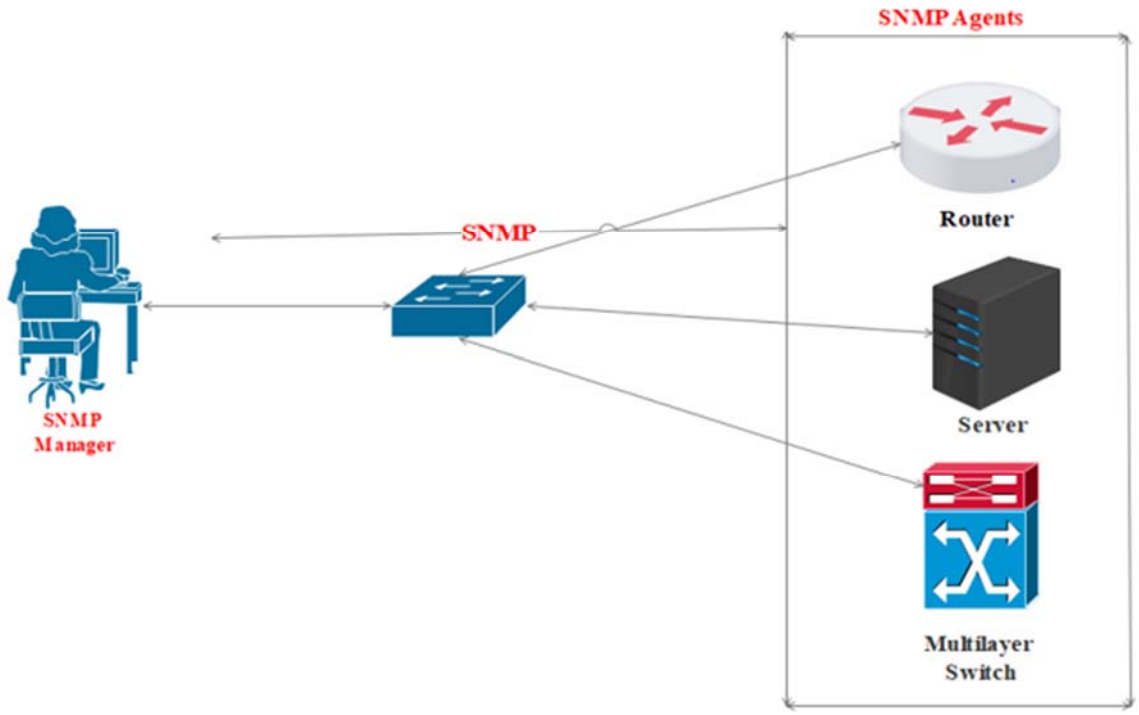


Figure III -2 : Architecture SNMP

III.3.3 Les principaux éléments de SNMP

III.3.3.1Le manager

Rappelons que le Manager se trouvera sur une machine d'administration (un poste de travail en général). Il reste un client avant tout, étant donné que c'est lui qui envoie les différentes requêtes aux agents. Il devra disposer d'une fonction serveur, car il doit également rester à l'écoute des alertes que les différents équipements sont susceptibles d'émettre à tout moment

Si l'on se base sur le schéma précédent, l'administrateur peut observer correctement le comportement de ses différents équipements en réseau.

Le Manager dispose d'un serveur qui reste à l'écoute sur le port UDP 162 ainsi que d'éventuels signaux d'alarme appelés des "traps".

Le Manager peut tout autant être installé sur une machine.

III.3.3.2 L'agent SNMP

L'agent est un programme qui fait partie de l'élément actif du réseau. L'activation de cet agent permet de recueillir la base de données d'informations et la rend disponible aux interrogations du Manager SNMP. Ces agents peuvent Être standards (Net-SNMP par exemple) ou encore spécifique à un fournisseur.

Cet agent doit rester à l'écoute d'un port particulier, le port UDP 161**[15].**

III.3.3.2. 1 Les principales fonctions d'un agent SNMP

- Collecter des informations de gestion sur son environnement local.
- Récupérer des informations de gestion tel que défini dans la MIB propriétaire.
- Signaler un évènement au gestionnaire.

Par ailleurs même si la principale fonction de l'agent est de rester à l'écoute des éventuelles requêtes du Manager et y répondre s'il y est autorisé, il doit également être capable d'agir de sa propre initiative, s'il a été configuré.

Par exemple, il pourra émettre une alerte si le débit d'une interface réseau, atteint une valeur considérée par l'administrateur comme étant critique. Plusieurs niveaux d'alertes peuvent ainsi être définis, selon la complexité de l'agent (température du processeur, occupation disque dur, utilisation CPU**...) [15]**

III.3.4. Management Information Base (MIB)

Chaque agent SNMP maintient une base de données décrivant les paramètres de l'appareil géré. Le Manager SNMP utilise cette base de données pour demander à l'agent des renseignements spécifiques. Cette base de données commune partagée entre l'agent et le Manager est appelée Management Information Base (MIB).

Généralement ces MIB contiennent l'ensemble des valeurs statistiques et de contrôle définis pour les éléments actifs du réseau. SNMP permet également l'extension de ces valeurs standards avec des valeurs spécifiques à chaque agent, grâce à l'utilisation de MIB privées.

En résumé, les fichiers MIB sont l'ensemble des requêtes que le Manager peut effectuer vers l'agent. L'agent collecte ces données localement et les stocke, tel que défini dans la MIB. Ainsi le Manager doit être conscient de la structure (que celle -ci soit de type standard ou privée) delà MIB afin d'interroger l'agent au bon endroit.**[1]**

III.3.4.1 Structure d'une MIB et Object Identifier

La structure d'une MIB est une arborescence hiérarchique dont chaque nœud est défini par un nombre ou un Object Identifier (OID). Chaque identifiant est unique et représente les caractéristiques spécifiques du périphérique géré. Lorsqu'un OID est interrogé, la valeur de retour n'est pas un type unique (texte, entier, compteur tableau...) Un OID est donc une séquence de chiffres séparés par des points.

Une MIB est un arbre très dense, il peut y avoir des milliers d'OID dans la MIB.

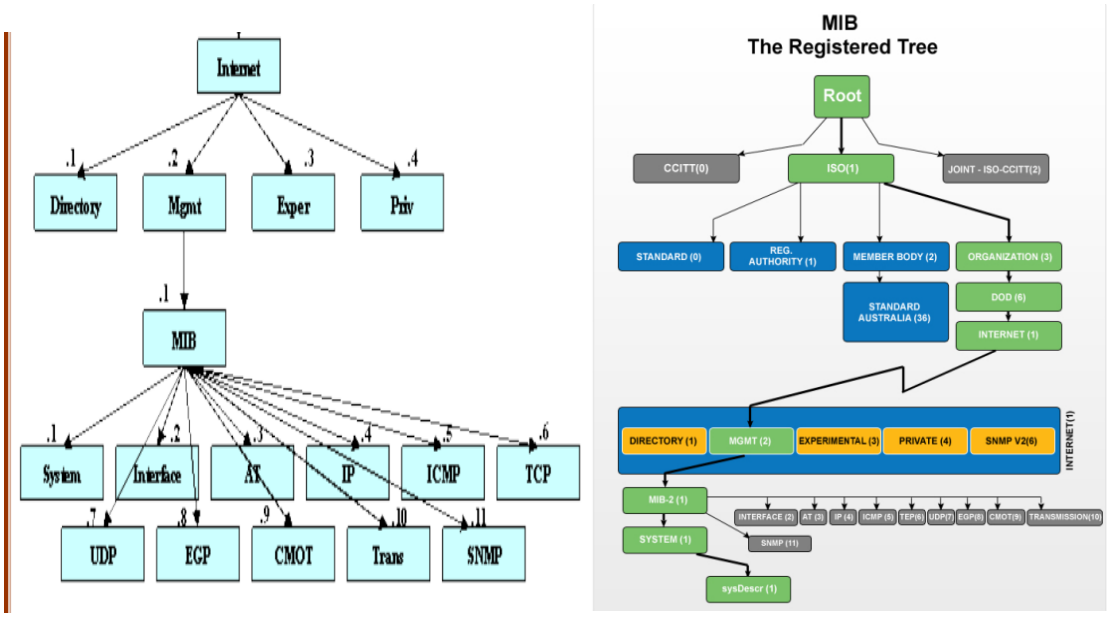


Figure III -3 : structure MIB

Cet exemple illustre d'ailleurs un Object typique qui est déclaré dans la RFC1213, à savoir le"sysDescr" (une description du périphérique interrogé) dont l'OID s'écrit .1.3.6.1.2.1.1.1.**[15]**

Ainsi, pour interroger les différentes variables d'activité sur un appareil, il faudra explorer son arborescence MIB. Celle-ci est généralement fournie par le constructeur mais il est aussi possible d'utiliser un explorateur de MIB tel que « Getif MIB Browser ».

Ensuite, pour accéder aux variables souhaitées, on utilisera l'OID (Object Identification) qui désigne l'emplacement de la variable à consulter dans la MIB. On aura par exemple sur un commutateur Nortel Passeport l'OID .1.3.6.1.4.1.2272.1.1.20 désignant le taux de charge du CPU **[1] .**

III.4 Les requêtes SNMP :

C'est un protocole de communication qui nous permettra de faire le lien entre l'agent (client) qui peut être le switch par exemple et le manager soit, le serveur qui va être la machine. Mais il permet aussi aux administrateurs réseaux de pouvoir gérer les équipements du réseau, de les superviser et de vérifier s'il y a d'éventuels problèmes.

Pour fonctionner et pouvoir recevoir les informations du switch vers le serveur, le protocole SNMP devra être installé sur l'agent. De plus, on devra s'appuyer sur deux principes à savoir : les alertes que l'agent émet vers le serveur, appelées « traps » et les requêtes du serveur vers l'agent. Soit, deux techniques de supervision avec SNMP, le polling et les traps.

Le polling consiste simplement à envoyer une requête pour obtenir une valeur particulière.

Les traps consistent à faire de la vérification passive, c'est-à-dire ce que configure l'agent SNMP pour qu'il contacte un autre agent SNMP en cas de problème. Autrement dit, on peut configurer un périphérique réseau (comme un routeur) pour qu'il envoie une trap SNMP **[17].**

Le protocole SNMP fonctionne avec les technologies utilisant les protocoles TCP/IP **[14]** et s'appuie sur le protocole UDP. L'agent aura le choix entre deux ports : 161 qui correspond à l'envoi de requêtes et de la réception des informations et le port 162, qui concerne l'envoi des traps. Même si le protocole UDP n'est pas sécurisé, le protocole SNMP est très utilisé par les administrateurs réseaux **[17].**

III.4.1. Les types de requêtes du manager SNMP vers l'agent SNMP sont :

- Get Request : Le manager interroge un agent sur les valeurs d'un ou de plusieurs objets d'une MIB.
- Set Request : Le manager positionne ou modifie la valeur d'un objet dans l'agent.

Les réponses ou informations de l'agent vers le manager sont :

- Get Réponse : L'agent répond aux interrogations du manager.
- Trap : L'équipement génère un envoi vers son manager pour signaler un événement, un changement d'état ou un défaut. L'agent n'attend pas d'acquittement de la part du Manager **[1].**

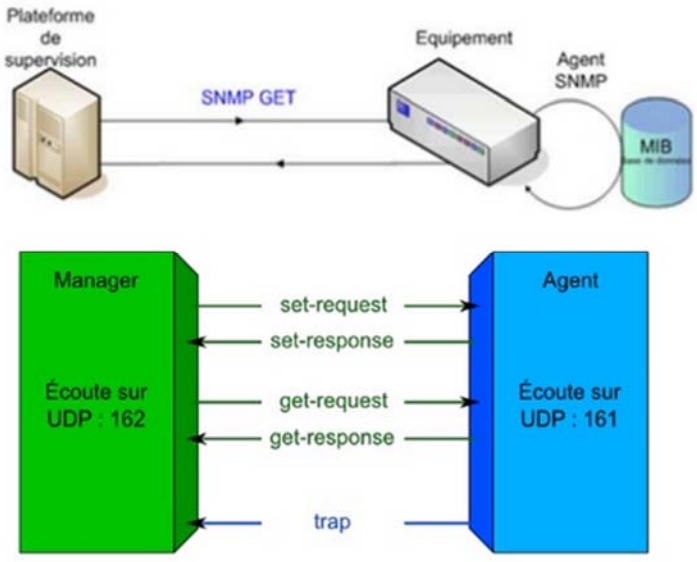


Figure III -4: Les échanges entre le Manager et l'Agent

III.4.2 Les communautés

La notion de communauté est utilisée dans les réseaux administrés à l'aide du protocole SNMP. Elle réunit à la fois le Manager et les différents agents. Chaque communauté est identifiée par un nom de communauté. Par défaut seules les communautés "public" et "private"

sont définies, cependant il est possible de nommer sa propre communauté, ceci à des fins évidentes de sécurité et donc de créer son propre domaine d'administration **[15].**

III.5. L'open source

Open Source (Source Ouverte), définit une licence qui permet d'accéder aux sources d'un programme informatique.

La désignation open Source s'applique aux logiciels dont la licence respecte des critères précisément établis par l'Open Source Initiative, c'est-à-dire la possibilité de libère la distribution, d'accès au code source et aux travaux dérivés.

Souvent un logiciel libre est qualifié d'« open source », car les licences compatibles open source englobent les licences libres selon la définition de la FSF « Free Software »**[18].**

III.5.1. Les solutions Open Source

Il faut savoir qu'il existe des dizaines de solutions Open Source dédiées au Monitoring, le principal critère de choix réside dans les différents cas d'utilisation **[15]**

Voyons à présent les solutions disponibles dans le monde de l'Open Source concernant le domaine de la supervision.

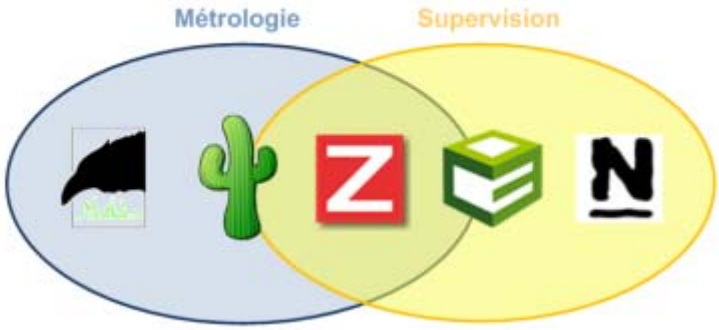


Figure III -5: métrologie ou supervision

III.5.2. Etude comparative des outils de supervision open source

Nous allons présenter les principaux outils de supervision réseau open source que nous avons choisi vu la diversité de ces outils tout en dégageant leurs avantages et inconvénients :

1. ZABBIX

➢ **Zabbix :**

Présentation de l'outil :

Zabbix est un outil de supervision libre (open source), qui permet d'offrir des vues graphiques (générés par RRDtool). Le « serveur ZABBIX » peut être décomposé en 3 parties séparées : Le serveur de données, l'interface de gestion et le serveur de traitement. Chacune d'elles peut être disposée sur une machine différente pour répartir la charge et optimiser les performances. Un agent ZABBIX peut aussi être installé sur les hôtes Linux, UNIX et Windows

afin d'obtenir des statistiques comme la charge CPU, l'utilisation du réseau, du système, l'espace (disque, processeur, mémoire…..) ce qui fait de lui un outil complet proposant des fonctionnalités relatives à la supervision (alertes sur seuil, mesures, actions sur conditions...). Le logiciel peut réaliser le monitoring via SNMP. Il est possible de configurer des « proxy Zabbix » afin de répartir la charge ou d'assurer une meilleure disponibilité de service **[1].**

Avantages :

- Une solution très complète : cartographie de réseaux, gestion poussée d'alarmes via SMS, Jabber ou Email, gestion des utilisateurs, gestion de pannes, statistiques.
- Une entreprise qui pousse le développement, et une communauté croissante
- Une interface vaste mais claire.
- Des performances au rendez-vous : l'application a été testée avec succès avec10000 équipements supervisés.
- Compatible avec MySQL, PostgreSQL, Oracle, SQLite.

Inconvénients :

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

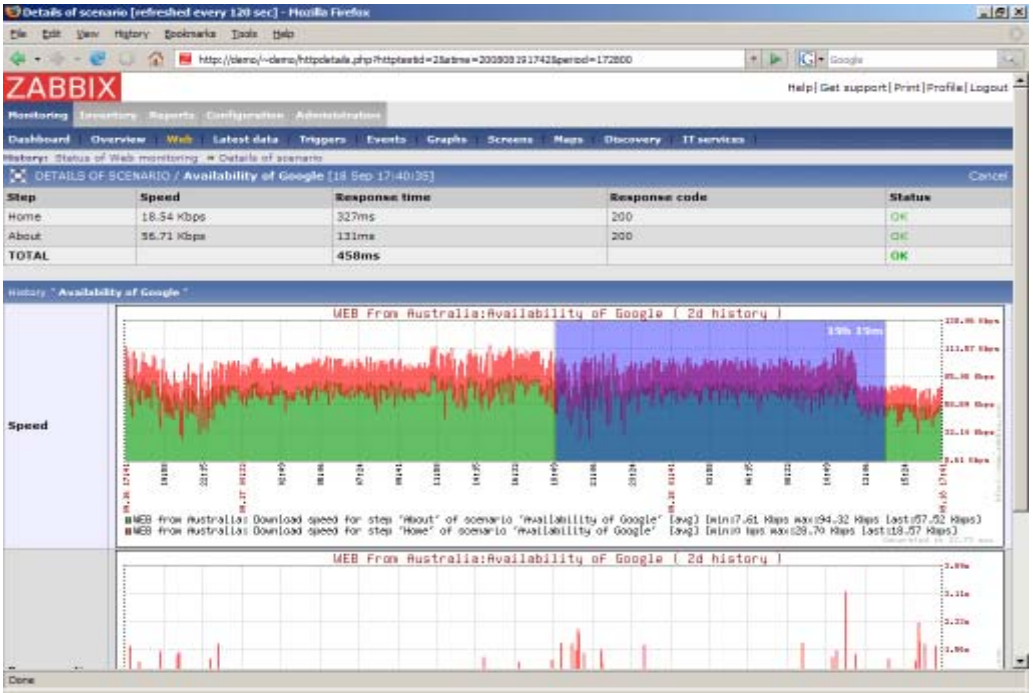


Figure III -6 : l'interface de Zabbix

Nagios®

➢ Nagios :

Présentation de l'outil :

Nagios un logiciel qui permet de superviser un système d'information. Il est avant toute chose, un moteur gérant l'ordonnancement des vérifications c'est-à-dire qu'il va lancer les déférents tests de supervision, appelés contrôles, sur les hosts et services, ainsi que les actions à prendre sur incidents (alertes, escalades, prise d'action corrective). L'interface web est la partie graphique visible, via un serveur web, et qui va permettre à l'administrateur d'avoir une vue d'ensemble de son réseau, de visualiser la supervision des équipements et de produire des rapports d'activité **[1]**.

L'inconvénient de Nagios reste son IHM (interface homme-machine) Il faut avouer que son interface ne donne pas spécialement envie d'être consultée, en étau delà de la pertinence de l'information, il faut de la compréhension et de l'interprétation. **[15]**

Avantages :

- Reconnu auprès des entreprises, grande communauté.
- Très puissant et modulaire.
- Une solution complète permettant le reporting, la gestion de panne et d'alarmes, gestion utilisateurs, ainsi que la cartographie du réseau.
- Beaucoup de documentations sur le web.
- Performances du moteur.

Inconvénients :

- Interface non adapté à l'utilisateur pour le confort et peu intuitive .
- Configuration fastidieuse via beaucoup de fichiers.
- Pour avoir toutes les fonctionnalités il faut installer des plugins, de base c'est assez limité. **[1]**

Figure III -7: l'interface de Nagios

➢ **Cacti:**

Présentation de l'outil :

Cacti est un logiciel de supervision réseau basé sur RRDTool, qui a la particularité d'avoir une " Plugin architecture" qui va lui permettre l'ajout de fonctionnalités grâce à l'importation et à la configuration, de plugins via l'interface web. L'aspect supervision proposé ici ne sera pas aussi développé que dans les autres logiciels (Nagios par exemple), on notera par exemple l'absence de panel de mesures, de groupes d'utilisateurs...Donc Cacti reste un outil de métrologie intégrant de nombreuses possibilités grâce aux plugins, avec la possibilité d'une mise en place de supervision mais uniquement dans les cas les plus simples **[15].**

Cacti permet de représenter graphiquement divers statuts de périphériques réseau utilisant SNMP pour avoir par exemple l'espace disque restant ou bien la mémoire utilisée, la charge processeur ou le ping d'un élément actif. Pour de meilleures performances un exécutable, nommé cactid, peut également effectuer les interrogations **[1].**

Avantages :

- Configuration : Avec l'utilisation des Template pour les machines, les graphiques, et la récupération des données tout se configure facilement et entièrement via l'interface web.
- Performance : Avec le choix du moteur de récolte des données, On peut opter pour la performance ou la simplicité
- Gestion des utilisateurs

- Communauté sur le web, présence d'une dizaine de plugins permettant d'étendre les fonctionnalités

Inconvénients :

- Pas de gestion d'alarmes, sauf avec un plugin nommé Thold.
- Pas de gestion de panne et absence d'une cartographie de réseau.
- Un développement lent **[1].**

➢ **Centreon**

Présentation :

Centréon (anciennement Oréon), 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.

Il reprend donc les avantages du moteur de Nagios et permet ainsi d'être entièrement compatible avec des solutions existantes.

Toujours visibles en haut à gauche, un tableau récapitulatif du nombre de machines actives et des éventuelles machines ne répondant plus pour toujours garder un œil sur l'ensemble du réseau **[19].**

Avantages

- Une interface beaucoup plus sympathique, permettant de tout configurer, de garder un oeil sur tout le réseau en permanence
- Les utilisateurs de Nagios ne seront pas perdus pour autant, l'interface reprenant avantageusement certaines vues Nagios
- Une solution complète permettant le reporting, la gestion de panne et d'alarmes, gestion utilisateurs, ainsi que la cartographie du réseau
- Peut-être décorrélé du serveur Nagios et tourner tout seul sur un autre serveur

Inconvénients

- L'interface peut paraître complexe car il existe beaucoup d'options, de vues…cela nécessite une petite formation
- Un développement qui n'est pas encore en phase avec celui de Nagios : Parfois des problèmes de compatibilité
- Un peu plus lourd que du Nagios pur

Figure III -8: l'interface de centreon

- **OBRSERVIUM**

Description :

Observium est un réseaux de découvert automatique et supervision de réseaux basé sur php / MySQL et orient pour les réseaux Cisco, LINUX, FreeBSD, Juniper….

Observium supporte une Large gamme de distribution et de matériel. Il est issu d'un manque de facilité d'utilisation des solutions de supervision resaux.il est destiné à fournir une interface facilement navigable pour supervise la sante et les performances de votre réseau **[18].**

Avantages

- Facile et rapide à mettre en place.
- Simple d'utilisation.
- Module "map" intégrer par défaut.
- Gratuit et libre.
- Possibilité d'installer des modules complémentaires (ex : Collectd).
- Pas de configuration des checks **[20].**

Inconvénients :

- Les checks via WMI sont difficiles à mettre en place => superviser les services Windows devient laborieux.

- Le niveau des checks n'est pas assez complexe, ils permettent principalement de superviser le hardware.
- Fonctionne via le DNS, c'est-à-dire que vous ne pouvez pas monitorer un serveur via son IP, mais uniquement via son nom dans le Dns **[20].**

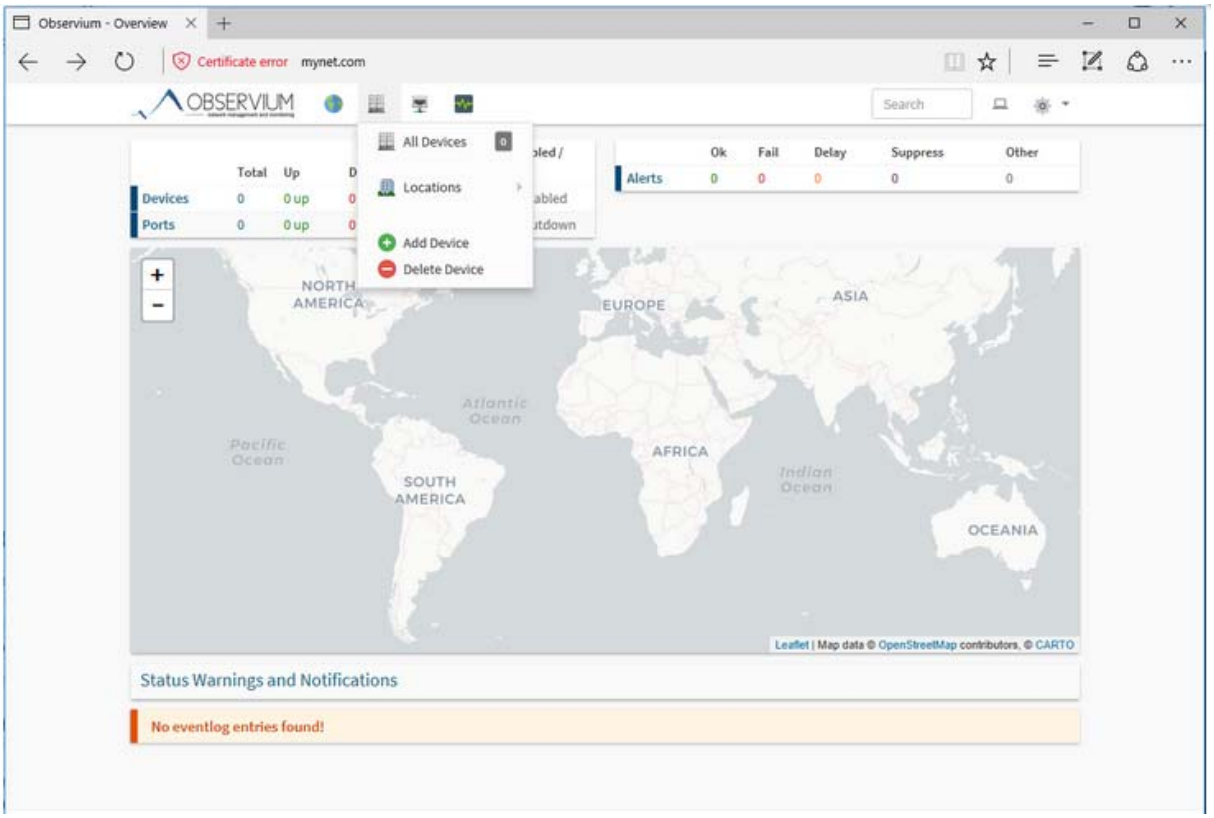


Figure III -09 : interface observium

Choix de l'outil :

Le monde des outils de supervision est très vaste, dans ce rapport on a eu recours à étudier quelques outils qui sont les plus connus sur le marché.

Selon les critères et les caractéristiques de chacun des logiciels libres cités a dessus nous avons décidés l'utilisation de **[16],** Observium comme logiciels de supervision à mettre en place.

Notre choix s'est basé sur les points forts de cet outil tell que :

- Cette solution possède une interface web assez simple d'utilisation mais un de ses avantages étant la Mape permettant de situer l'équipement distant superviser.
- Ce système étant le seul à ne pas utiliser d'agent pour effectuer le relais SNMP, le service SNMP doit être alors activé et configuré manuellement sur la machine à superviser mais il faut aussi rajouter une règle NAT sur le routeur du réseau qui permet de rediriger les paquets SNMP.

- La solution Observium, possède de nombreux graphiques pour chaque composant par jour, semaine, mois et année. Cela permet de voir l'évolution d'une entreprise et de lui proposer des solutions en adéquation avec ses besoins.**[21]**

Conclusion :

Le présent chapitre a été introduit avec une brève présentation de la notion de supervision et ses enjeux, les outils open sources dans le but de choisir le bon outil. Après avoir effectué le choix de l'outil de supervision open source convenable, nous allons faire une étude approfondie pour faciliter sa mise en œuvre.

IV. Introduction

Au cours de ce chapitre, nous nous intéressons à la description de la phase de réalisation de notre application. Nous commençons par la présentation de schémas globale de réseaux informatique de l'IAP et en particulier le réseau LAN du siège où on a fait notre stage. Ensuite nous décrivons les points les plus intéressants de la solution à savoir :

- Présentation de la solution et ses fonctionnalités
- Mise en place de la solution (installation et configuration)
- Etudes de cas

La solution mise en place dans notre stage, à savoir l'OBSERVIUM, est une solution open source répondant largement aux objectifs recherchés

Cette solution permet à l'administrateur réseaux/systèmes d'avoir une vision de l'infrastructure réseaux en temps réel grâce à une interface très claire et intuitive

IV.1. Schéma global du réseau IAP

Le réseau informatique de l'IAP est géographiquement réparti sur quatre sites : le site central (DG et école de Boumerdès) et trois écoles distants (Arzew, Skikda et Hassi Messaoud)

Ces quatre sites sont reliés par un réseau WAN de la SONATRACH. Aussi, l'ensemble des sites interconnectent avec le siège de la SONATARCH via ce réseau WAN

Le réseau informatique est segmenté en trois segments qui sont : le réseau LAN, WAN et DMZ.

Le segment WAN contient deux parties : le WAN SONATARCH et Internet

Le segment DMZ (démilitarise zone) : contient les serveurs qui hébergent les services publiquement accessibles comme le site web, web-mail, …

Le segment LAN : c'est le réseau LAN du siège de l'IAP. Un schéma détaillé de ce réseau sera donné par la suite.

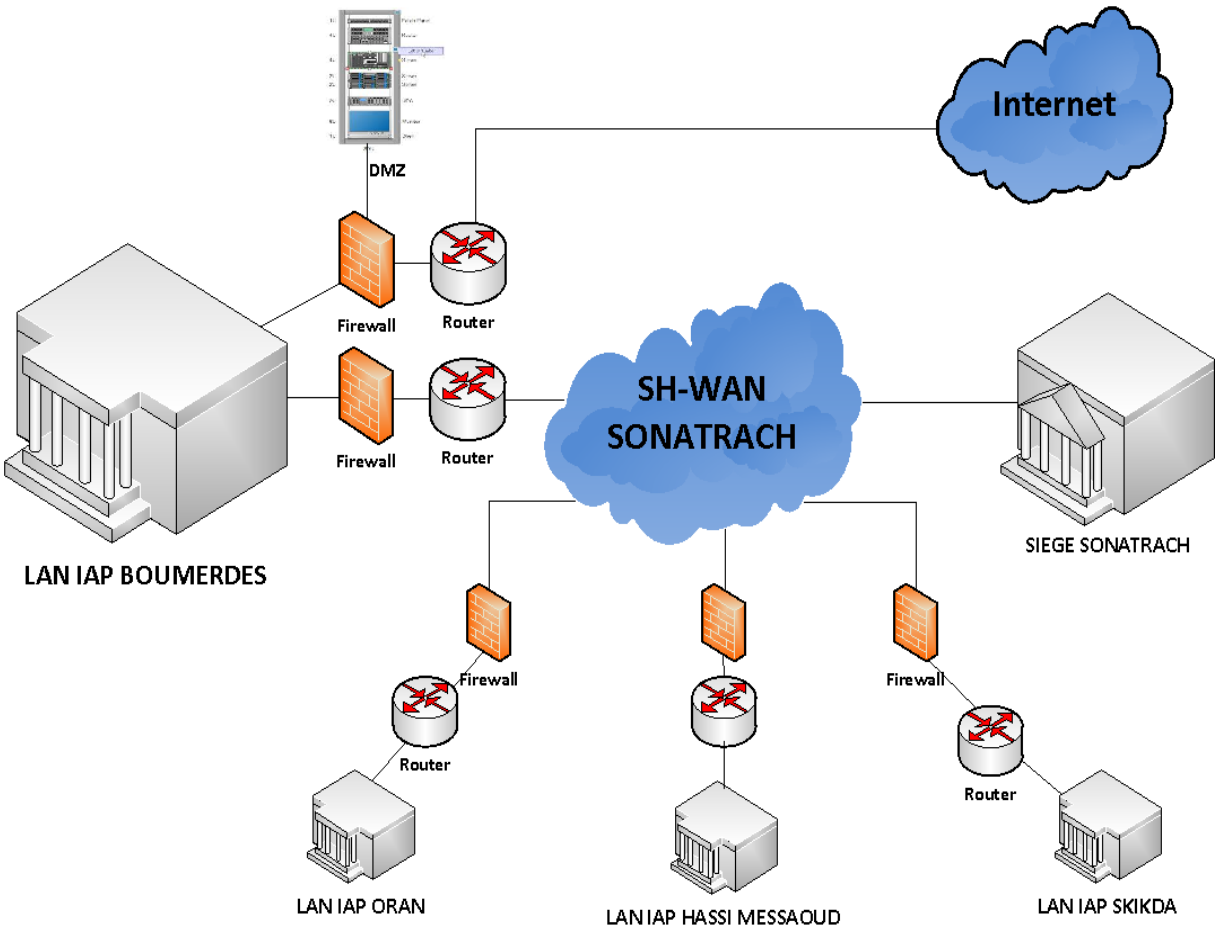


Figure IV.1 : Schéma global du réseau IAP

IV.1.1 Réseau LAN de IAP de Boumerdès

Ci-dessus, l'architecture simplifiée du réseau LAN de IAP Boumerdes qu'ils sont besoin d'une solution pour la supervision de cette architecture.

Les activités de l'entreprise dépendent des ressources informatiques placées dans la salle machine ou télécommunication ou convergent de toutes les lignes internet (fibres optiques).

Selon cette architecture de LAN IAP qui est hiérarchie en deux couches (core (cœur) et distribution) et appeler aussi colabset, ces dernier sont relier par une fibre optique mono mode représenté par deux switchs met en cascade leur références (2 CISCO 3750X-125), chaque une de ces couche a un rôle spicifier la couche core permet l'interconnexion entre les déférents équipements et la couche distribution (l'acheminement ,le filtrage, l'échange de donnes…….) on termine par une dernière couche qui est la couche accès présente les équipements (switch) réparté sur les déférent étage de la société.

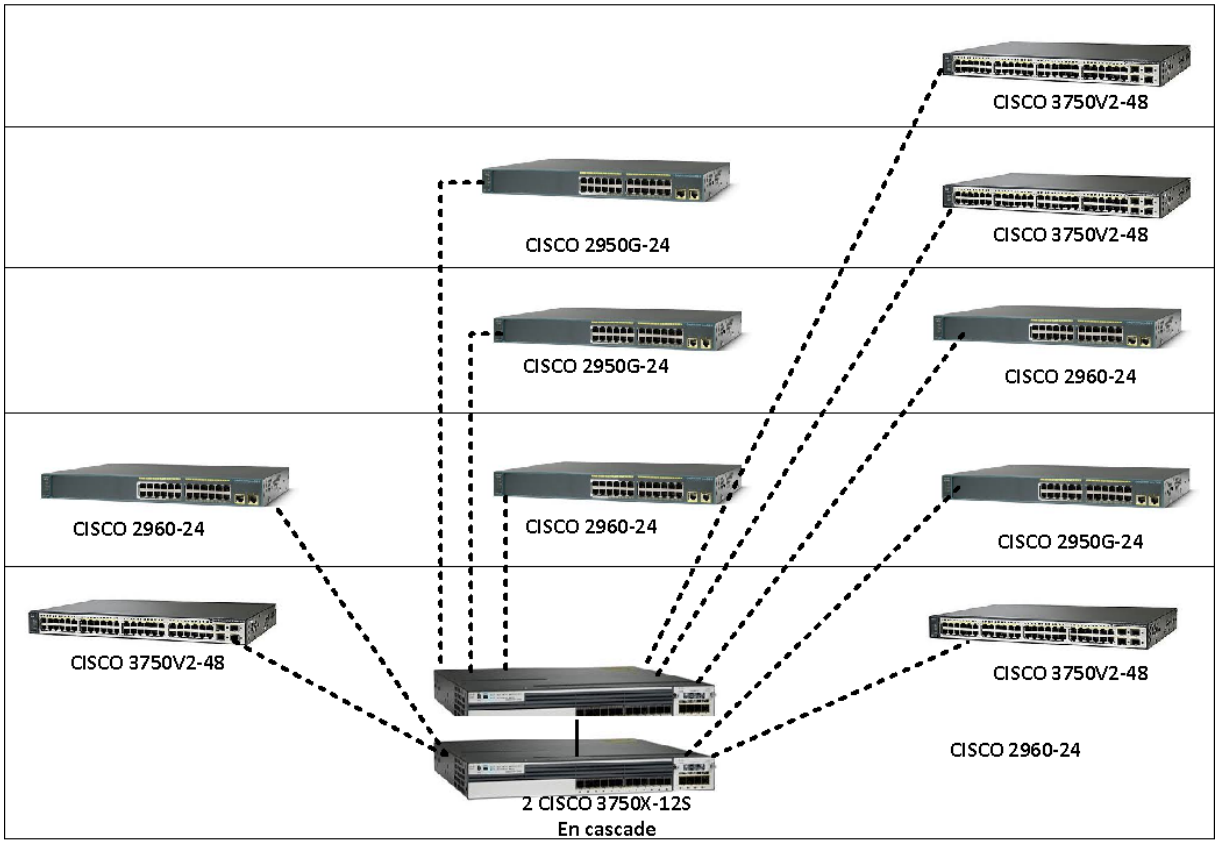


Figure IV -2: Réseau LAN IAP

IV.1.2 Datacenter

Le data center **[22]** appelé aussi centre de traitement de données est un site physique dans lequel se trouvent regroupe des équipements constituants du système d'information de l'entreprise **(**des serveurs, des sous-systèmes de stockage, des commutateurs de réseau, des routeurs, des firewalls etc) Ces équipement sont placé dans des armoires d'une façon bien organisé pour interconnecter tous ces équipements informatiques**.**

Pour le bon fonctionnement de ce data Center il doit avoir :

Un système distribution d'énergie, un commutateur électrique, des réserves d'énergie, des générateurs dédiés au backup, un système de climatisation, et une puissante connexion internet. Une telle infrastructure nécessite un espace physique suffisamment vaste et sécurisé pour contenir tout cet équipement.

IV.2. Présentation de OBSERVIUM

OBSERVIUM est un outil de supervision/monitoring au même titre que Centreon, Nagios ... C'est-à-dire que cet outil permet de connaître en temps réel l'état des équipements supervisés **[20].**

L'outil fonctionne sur un principe de check (vérification) via le protocole SNMP **[17].** Ce qui implique la configuration du SNMP sur les hôtes distants.

Pour la mise en place d'OBSERVIUM nous utiliserons la distribution CentOS7 (serveur et client).

IV.2.1 Fonctionnalités

OBSERVIUM nous permet d'assurer les tâches suivantes [**18]** :

- Découverte automatique des équipements de réseau
- Support de nombreux matériels réseaux et système
- Gestion des résultats (graphs, histogramme, ….)
- Notification par mail
- Gestion de Syslog (Système de Fichiers historiques)
- Support de système virtualisés
- Surveillance d'éléments physiques (Température, voltage...)
- OBSERVIUM fonctionne sur plusieurs environnements (Linux, Unix, …).

IV.3 Mise en place de OBSERVIUM

IV.3.1 Configuration de la machine virtuelle [23]

Voici les caractéristiques de la machine que nous avons utilisée :

- ✓ Processeur : 2 cœurs logiques (on peut aussi en mettre qu'un, mais l'interface graphique risque d'être lente).
- ✓ Mémoire: 2Go
- ✓ -Type de réseau : NAT (network adresse translation)
- ✓ Disque dur: 40Go

IV.3.2 Installation OBSERVIUM (Annexe B)

Pour l'installation de OBSERVIUM, il est recommandé de vérifier que certaines dépendances sont autorisées sur la machine.

Les principaux packagent installés sont : PHP, MySQL, snmp, fping, rrdtools.

- ➢ **PHP** pour le serveur web.
- ➢ **MySQL** : pour le stockage des données.
- ➢ **SNMP** pour la remonté d'information.
- ➢ **Fping**: permet d'envoyer un signal en ICMP vers les machines du réseau.
- ➢ **RRd-tool** car nous allons devoir l'utiliser pour créer des graphiques et sauvegarder les données critiques.

IV.3.3 Configuration du SNMP dans divers hôtes [20-21]

SNMP (Simple Network Management Protocol) est un protocole de couche d'application qui fournit un format de message pour la communication entre les gestionnaires et les agents. Il permet aussi de superviser plusieurs appareils de différentes marques.

La configuration d'un agent SNMP sur les périphériques se défaire d'un périphérique à un autre.

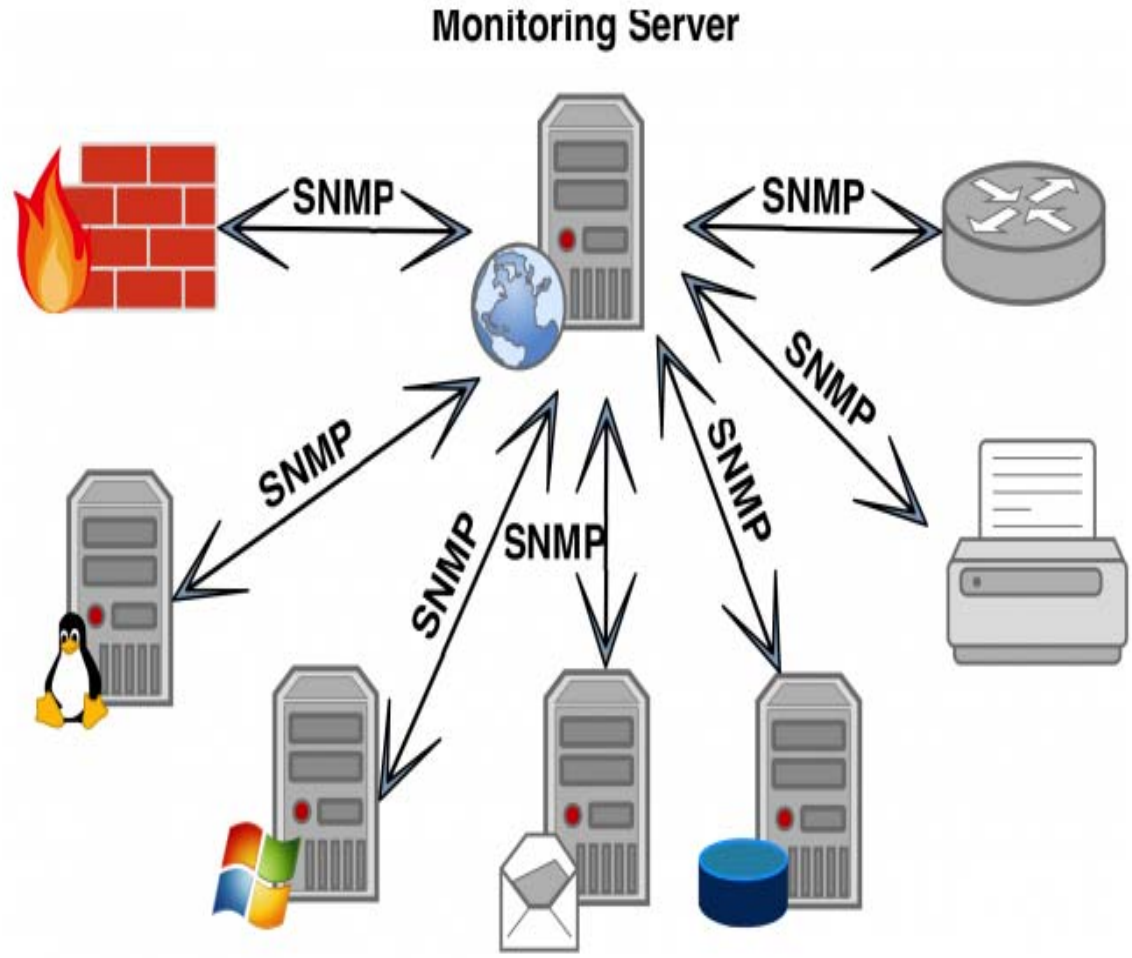


Figure IV -3: configuration SNMP dans divers hôtes [20-21].

IV.3.4. Configuration d'Observium

IV.3.4.1 Diagramme d'utilisation générale du système :

Afin de décrire les fonctionnelles de notre système, voici une description du cas d'utilisation globale.

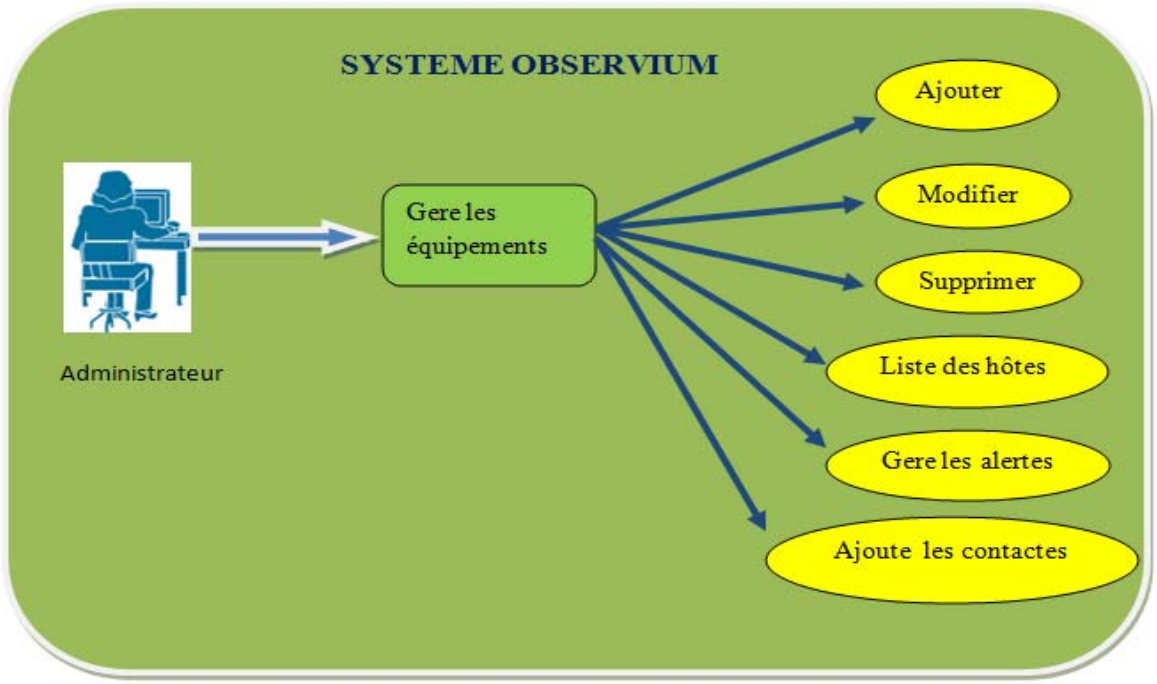


Figure IV -4 : Diagramme de cas d'utilisation générale du système .

IV.3.5 Les équipements superviser

Nous allons superviser des équipements existent dans la société et présenter les résultats finals obtenu. Nous avons six équipements (dispositifs) à supervise. Ces équipements sont :

Quatre équipements de sécurités (firewall), un poste de travail et un switch Cisco. La figure suivante montre ces équipements.

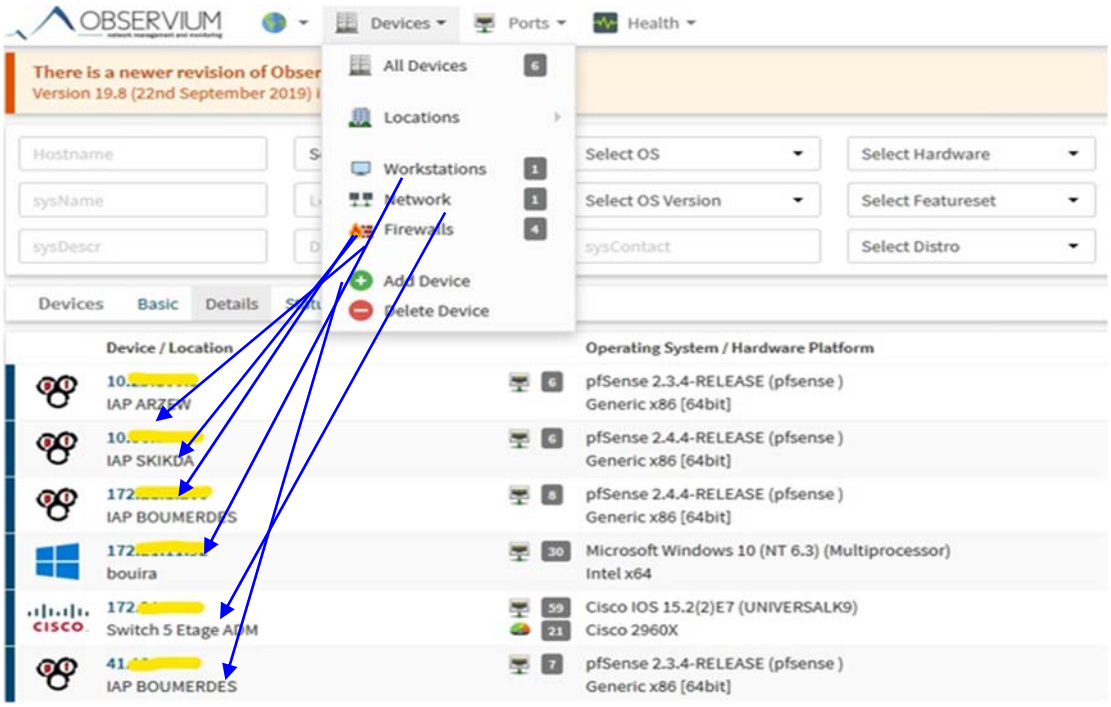


Figure IV -5 : Les équipements superviser

Pour chaque équipement OBSERVIUM donne son état en temps réel. L'état de ces équipements est représenté par des graphes comme la consommation de la bande passante (traffic), Disponibilité de l'appareil, Running process (Processus en cours)……..etc et d'autre part la consommation de la RAM, Processeur et le disk du stockage.

IV.3.6 Les vérificateurs d'alertes

Pour les alertes on a créé 3 alertes déférentes dans notre système. Nous avons sélectionné les éléments suivants : Processeur, Device et Sensor (capteur).

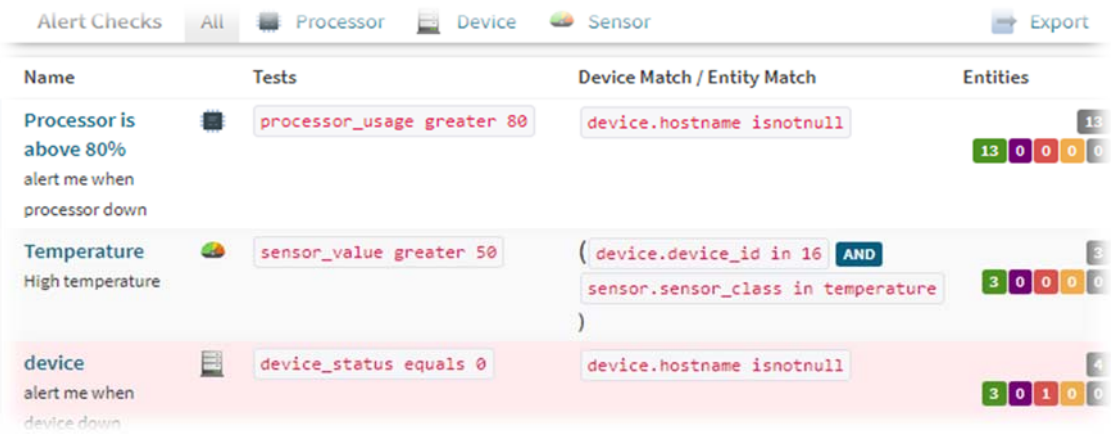


Figure IV -6 : type d'alerte utilisé

IV.3.7 Etude d'alerte a température :

Tout d'abord, lorsqu'on veut créer une alerte, on fait le choix de type d'entité. Des exemples de types d'entité Port, Device, Sensor et processor …

Dans notre cas on prend comme Entité « Sensor (capteur) » :

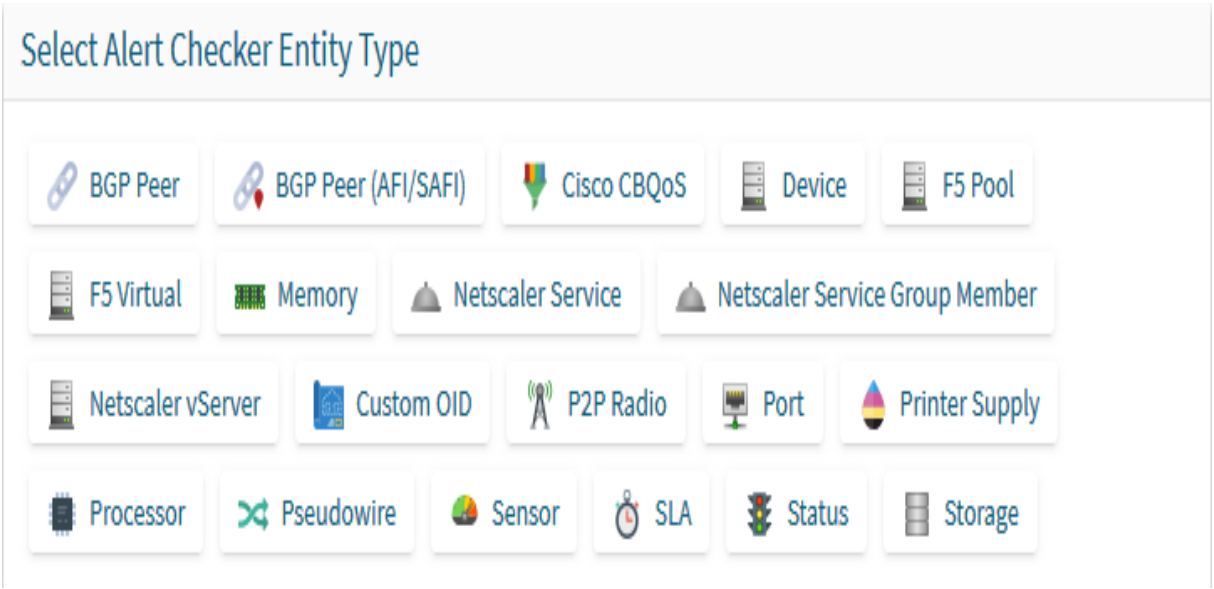


Figure IV -7 : déférent type d'entité

Après la sélection de l'entité on aura cette figure. On doit remplir ses différents champs.

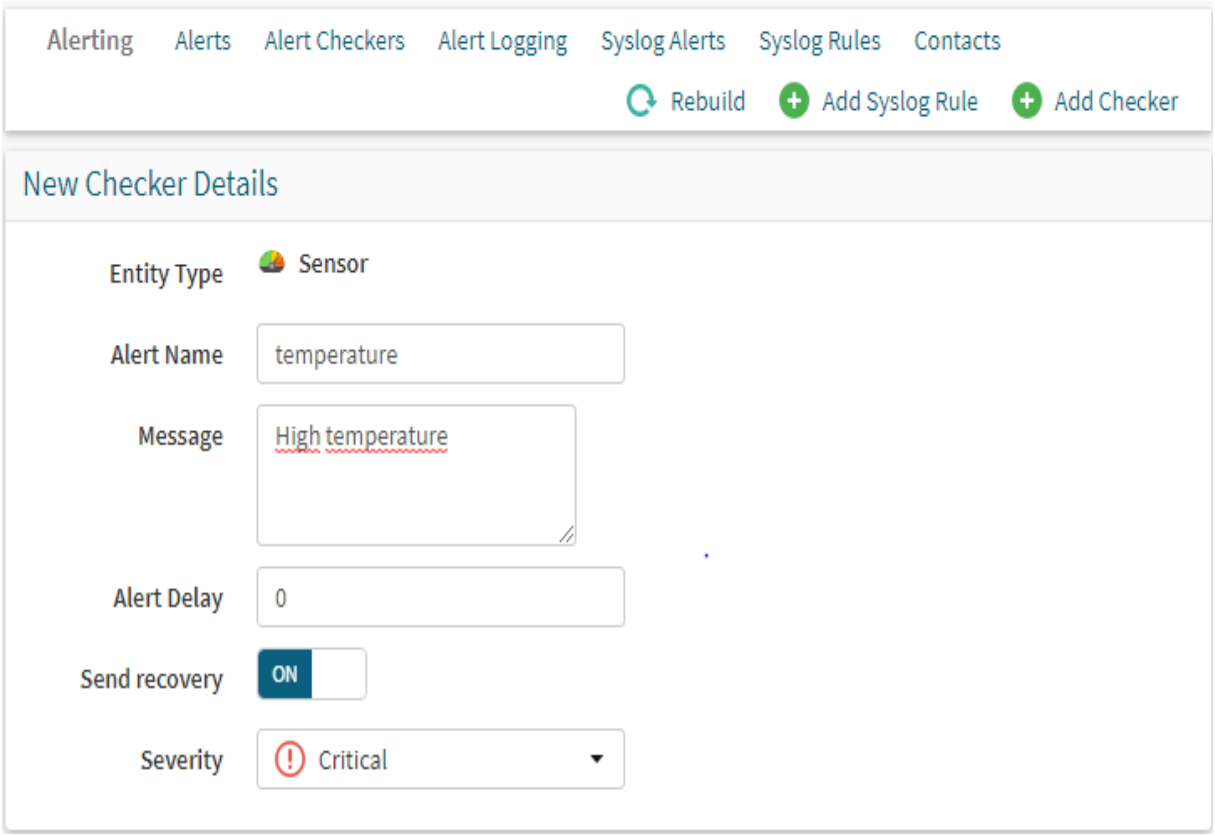


Figure IV -8: les détails de vérificateur d'alerte

Après nous devions choisir l'équipement (device) et le type de capteur dans notre cas c'est la température et nous pouvons également ajouter les adresses emails afin de contacter les responsables de réseau sur son état. La figure (4-9) Montre l'interface de configuration des contacts et le choix de l'équipement avec le type de l'alerte.

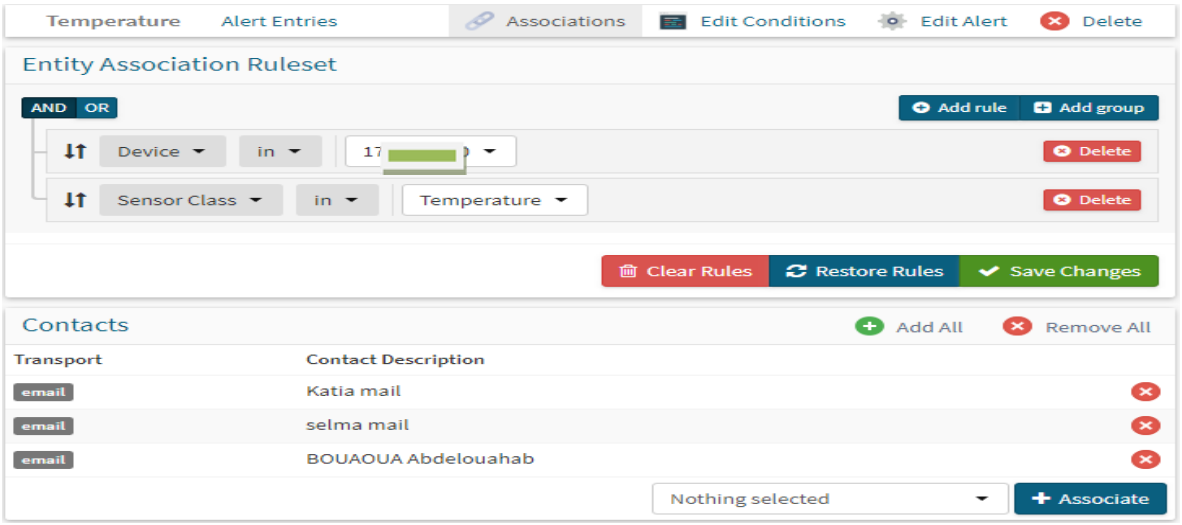


Figure IV -9 : liste des contacte

L'alerte est ajoutée avec succès, cet équipement a deux modules de température (Gigabit Ethernet 1/0/51 et Gigabit Ethernet 1/0/49) et un capteur. Le status (état) est « ok » qui signifier que l'équipement fonction bien pas de disfonctionnement ou de panne, le dernier foie vérifier est à 29s.

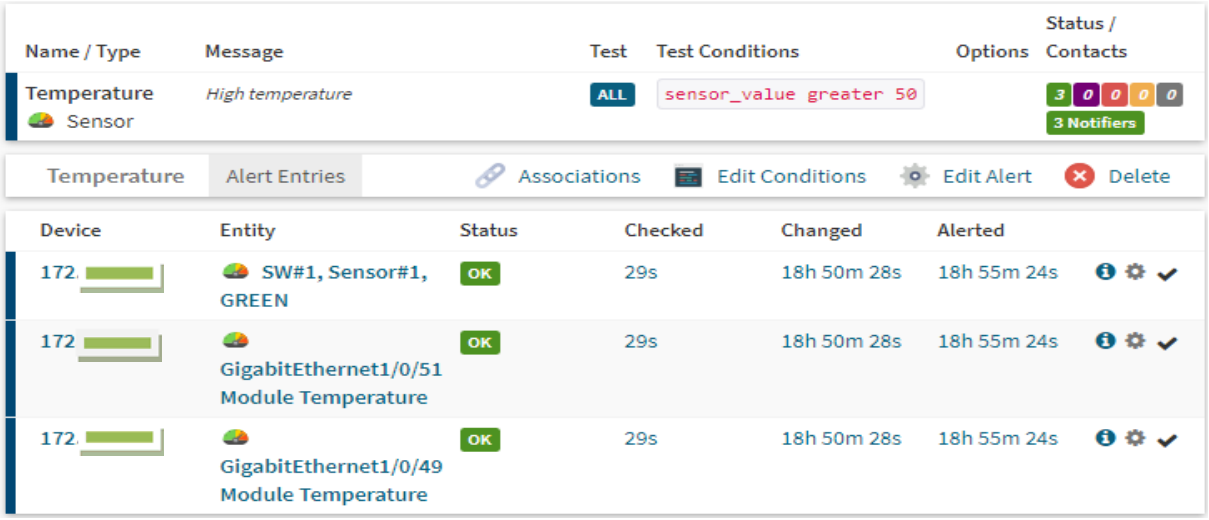


Figure IV -10 : alerte ajoute avec succès

IV.3.8 Diagramme d'activité « d'alerte » :

Ce diagramme décrit les différentes activités que prend le système lorsqu'il détecte un équipement non fonctionnel ou en panne. Le système commence par vérifier l'état du service correspondant au périphérique (dans notre cas la vérification est à chaque minute) jusqu'à la validation de l'état non-ok. Si on est dans l'état non-ok c'est-à-dire la condition est valide il récupère la liste des contacts et les notifie par un mail d'alerte (**ALERT**). Ensuite si l'intervalle de temps de la prochaine notification est écoulé et que l'état du service est encore non-ok, le système recommence la vérification des services, et lorsque on revient à l'état ok c'est-à-dire que le problème est résolu le système récupère la liste des contacts est les notifier par mail aussi (**RECOVER**).

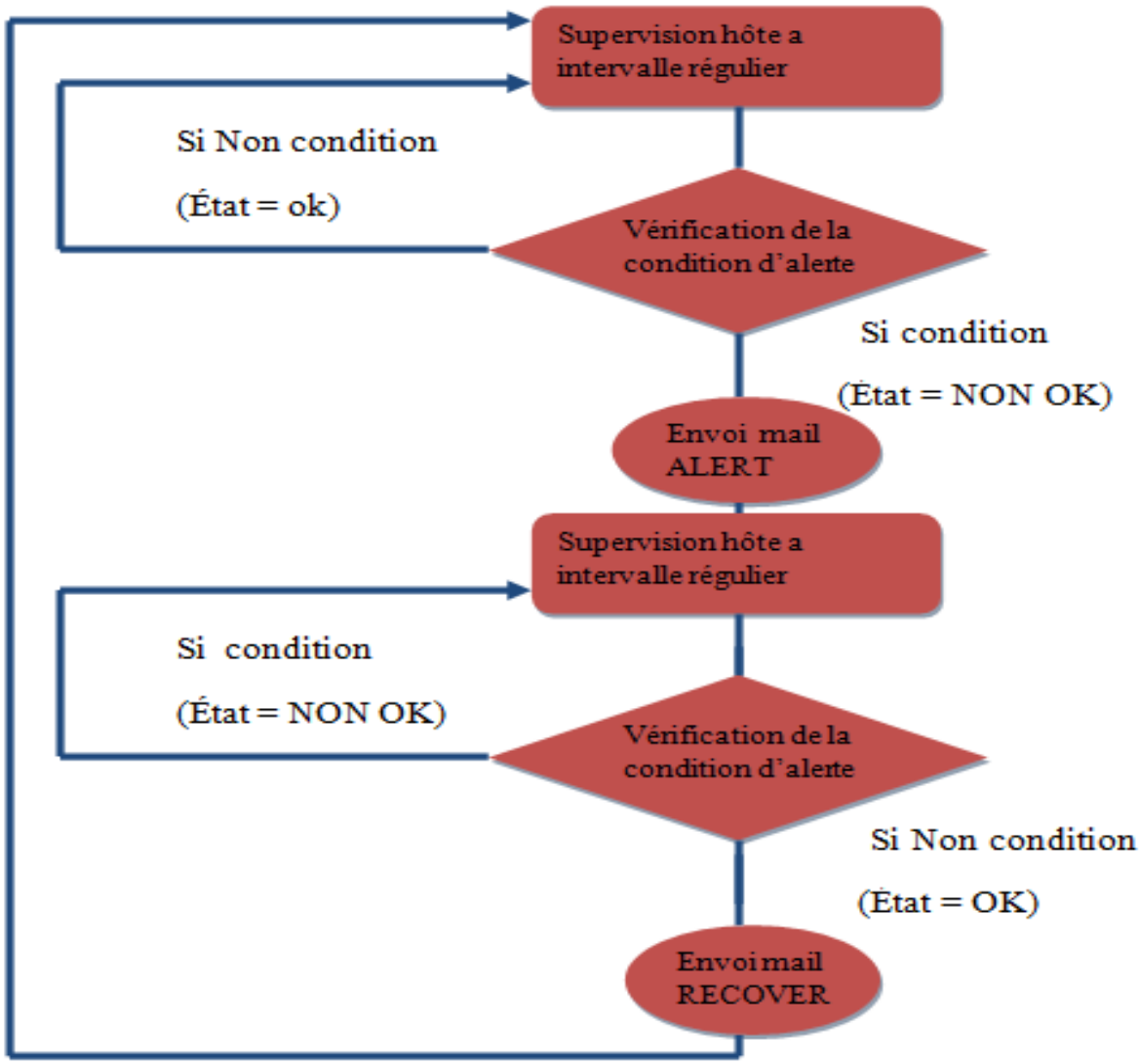


Figure IV -11: Diagramme d'activité « d'alerte »

IV.4 Résultat et Analyse

IV.4.1 Presentation des graphs

- **Pare-feu: IAP Boumerdes**

On a le premier équipement qui est un pare-feu (firewall). La figure suivante montre la quantité de bande passante consommée par cet équipement et le taux d'utilisation de la mémoire et le processeur. Nous remarquons une variation très importante de cette consommation par heure (il y'a une forte consommation). On peut revoir le graph pour un temps très important, 6 heures ,24 heures ,48heures…jusqu'a 3 ans.

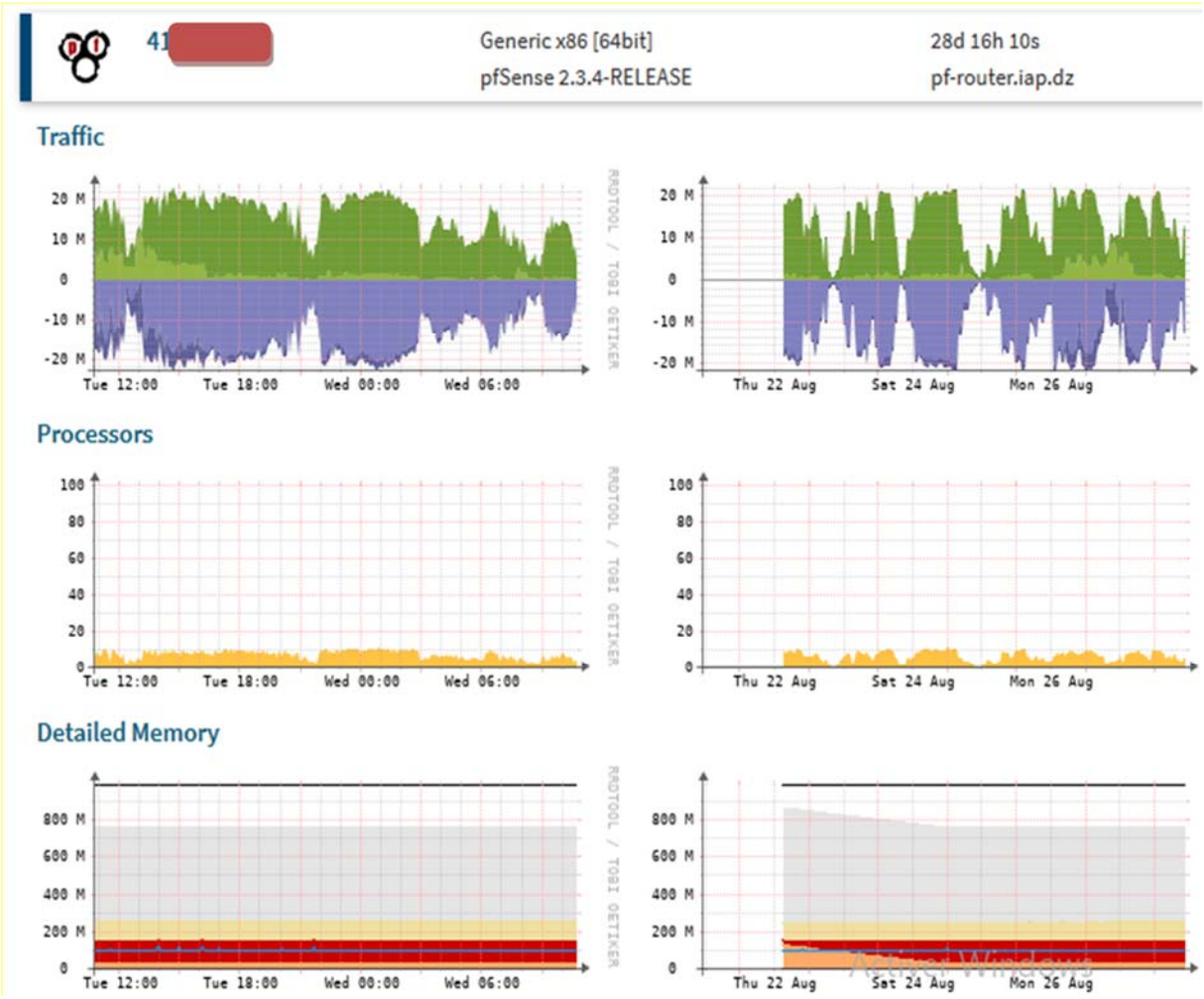


Figure IV -12 : Consommation de bande passante, processeur, mémoire par un pare-feu

- **Bande passante de Pare-feu : IAP Boumerdes**

La figure suivante présente la consommation de la bande passante tell qu'en remarque une variation de cette consommation en fonction de jour et heure.

Chaque couleur de ce graphe présente une interface physique (carte réseaux) de cet équipement :

A le vmax0 qui fait référence aux LAN de la société et vmax1 pour le taux d'utilisation des étudiants et a la fin vmax2 pour le WAN, tel que on peut consulte le taux de transmission et de réception pour chaque interface au moment actuel, la moyenne, le max et le min.

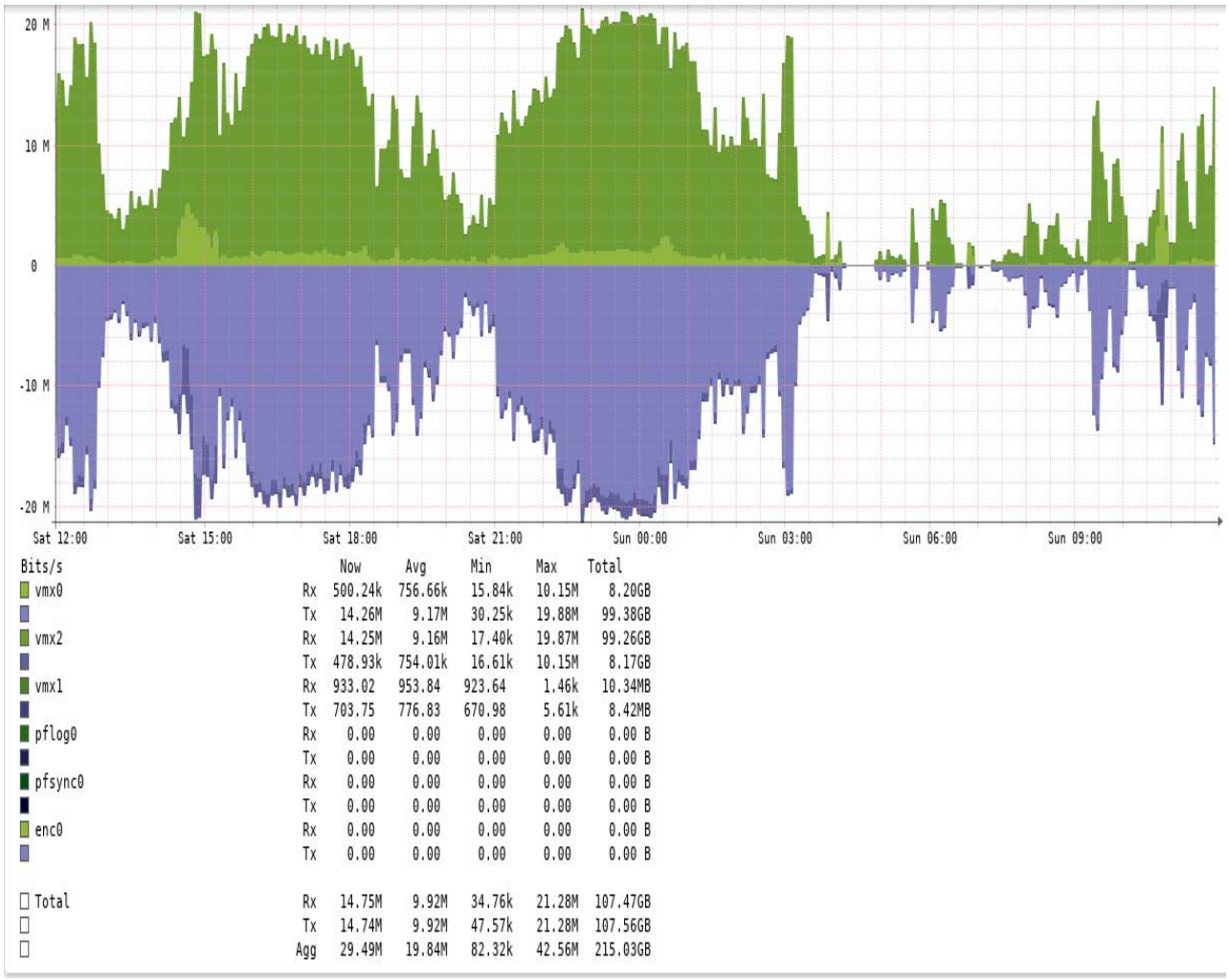


Figure IV -13 : consommation de bande passante de Pare-feu : IAP Boumerdès

- **Machine Cisco**

Cette figure (4-14) présente les déférents états de consommation de la bande passante pour un switch de 5 -ème étage de l'administration (ADM), telque selon le graphe on remarque peut de consommation à cause de manque d'utilisateur.

Et concernant le processeur et la mémoire disque de stockage en peut s'avoir pour chaqu'un de ces dernier l'espace utilise, et l'espace libre....

Figure IV -14: Consommation de bande passante, processeur, mémoire par machine Cisco

La figure (4-15) suivante en globe l'ensemble d'information que peut connaitre ce switch (Traffic, processeur, mémoire, stockage, status, courant, puissance, voltage……..) et pour les graphe de température chaque couleur d'un graph représente la température d'un module de ce switch, on peut même connaitre la température actuelle, moyenne et maximum pour ces derniers.

Figure IV -15 : graphe température switch Cisco

Le seuil de température pour les différents parties de switch est fixé à un certain intervalle par exemple le (Gigabit Ethernet 1/0/51 module température) sont intervalle est fixé a [-10°C(-5°C)—(80°C)85°C]. Lorsque la température est en dehors de cet intervalle on aura une alerte.

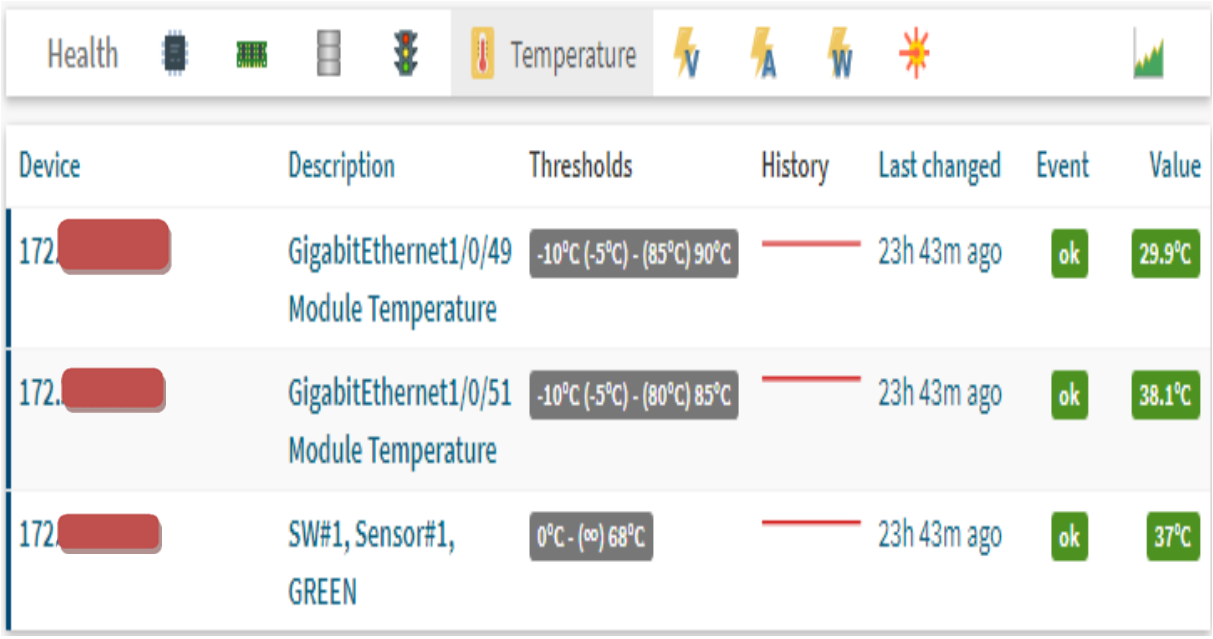
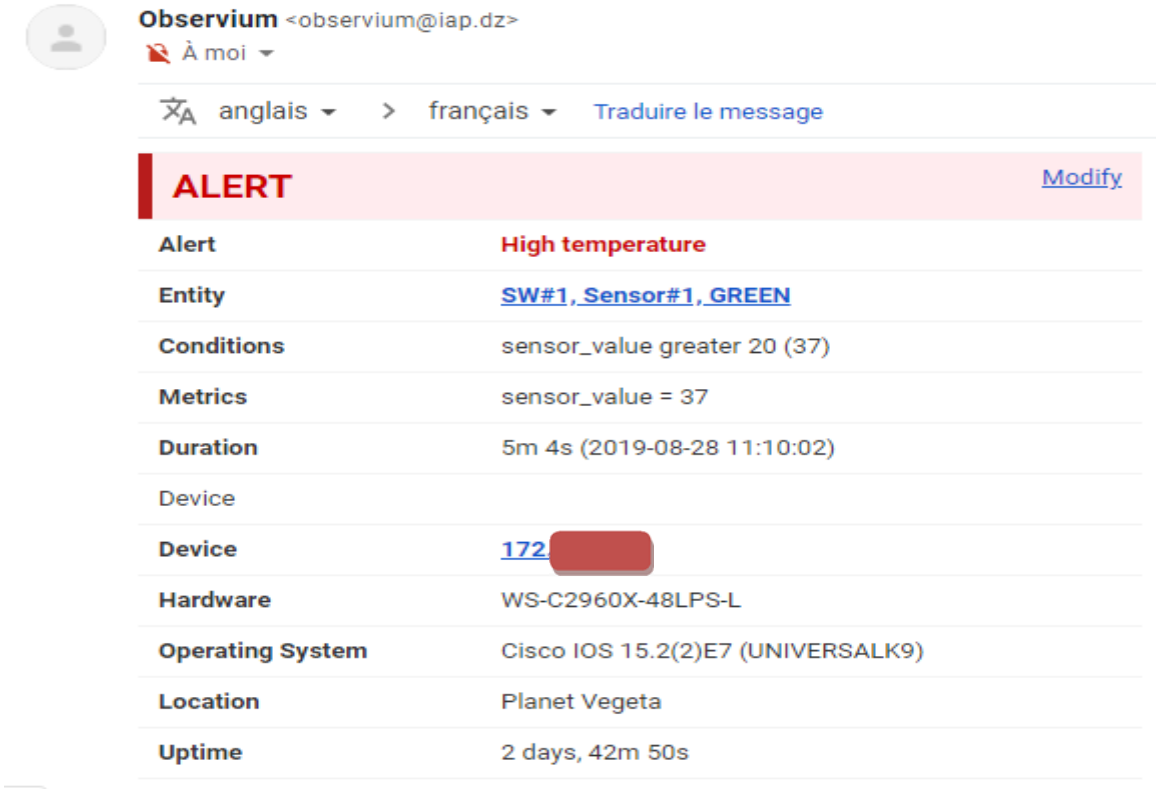


Figure IV -16: seuil de température pour switch

IV.5 Mail d'ALERTE / RECOVER reçu

Un message de notification de type alerte sera envoyé par mail au superviseur responsable indiquant le nom de la machine, son adresse IP et l'état de la machines, la localisation, la condition d'alerte, graph…….



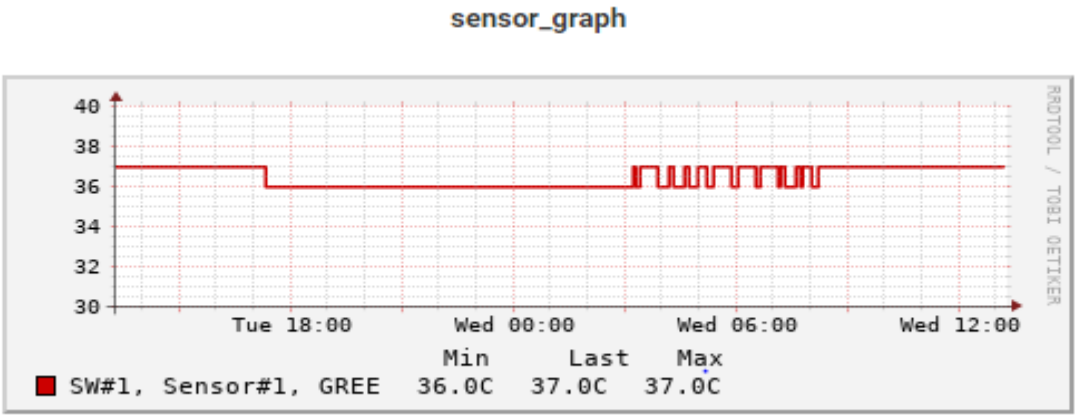


Figure IV -17: Mail d'alerte reçu

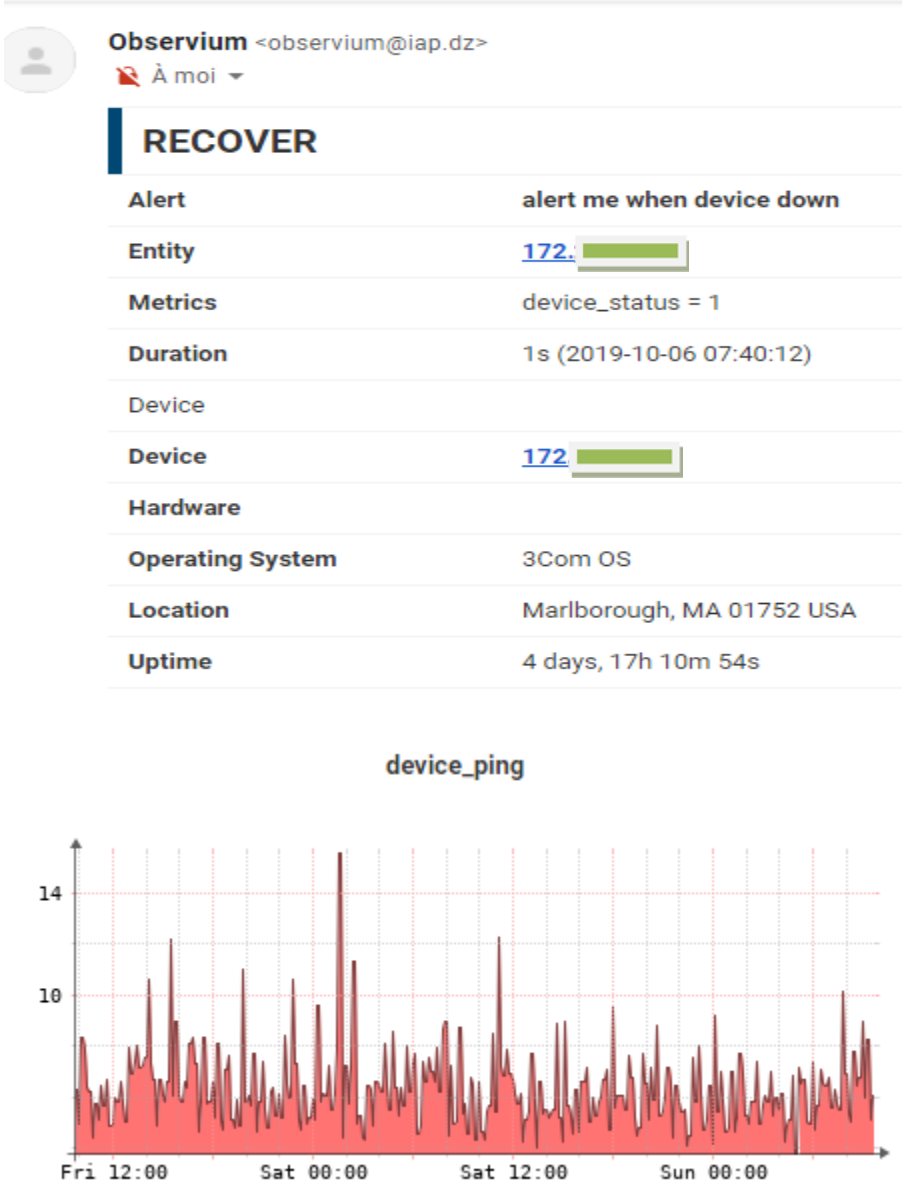


Figure IV -18: Mail de RECOVER reçu

Conclusion

Le présent chapitre a été introduit avec une brève présentation de réseaux de la société et son siège. Ensuite nous avons décrit l'aspect de notre solution, énuméré ses fonctionnalités et modélisé son architecture. Finalement nous avons ainsi prouvé l'importance de notre solution « OBSERVIUM », qui est principalement la facilite d'utilise et de configure cette solution, d'une manière beaucoup plus précise pour le seul but de gagner et optimiser la gestion de son temps, c'est-à-dire notre logiciel nous permet de supervise les dispositifs en temps réel et même la supervision à distance.

Bibliography

[1] : TRABELSI, A. Mise en place d'un outil de supervision système et réseau open source. Mémoire de Mastère Professionnel. Université Virtuelle de Tunis, (2015).

[2] : OTHMAN, S. Mise en place d'un système de supervision Open source. *Mémoire de master*. Université Virtuelle de Tunis,(2011).

[3] : Disponible sur www.sontrach.com,(2018, avril).

[4] : KHAILA, R. Installation configuration et administration d'un réseau local avec contrôleur de domaine. Mémoire de fin d'étude : Réseaux et système informatique. Guelma: institut national spécialisé de la formation professionnelle de gestion Djebabla kaddour, (2018).

[5]: Le réseau informatique en entreprise. Disponible sur e-Qual:< https://www.e-qual.fr/accueil-2/reseau-informatique-entreprise/>, (2019, Juin 4).

[6]: ZAHIRA, D et SAMIRA, *B.* Conception des Réseaux sans fils IEEE 802.11 En modes infrastructure et AD HOC. Mémoire Master. Université Abou bker belkaid tlemcen. Algerie ,(2016).

[7] : PORTE, L. Topologie réseau : le modèle hiérarchique en 3 couches. Disponible sur bibabox:<https://bibabox.fr/topologie-reseau-le-modele-hierarchique-en-3-couches/>,(2011, août 3).

[8] : Syloé. Serveurs. Retrieved from Syloé: <https://www.syloe.com> ,(2019, Mars).

[9] : wp_leshebergeurs496. Différences serveur physique et serveur virtuel. Disponible sur Serveur web:< http://leshebergeurs.net>,(2018, mars 13).

[10] : Manuel. D'un système physique à une solution virtuelle:Éléments de réflexion sur la conversion etle déploiement d'une solution de virtualisation dans les datacenters de . Disponible sur dell: http://www.dell.com/virtualization, (2011, janvier 05).

[11] : SZUSCIAK, F. DAS, NAS, SAN, kesako par Ludovic ROUCOU. (Modifié le 10/11/2012). Disponible sur :<https://ticalternancecesiarras.wordpress.com/2012/11/10/das-nas-san-kesako-par-ludovic-roucou> ,(2019, juillet 18).

[12] : BoucheCousue, G. D. In Comprendre le stockage (SAN, NAS, DAS et Cloud).Mise en ligne le 28 avril 2016. Disponible sur :<https://bouchecousue.com/blog/comprendre-stockage-san-nas-das-cloud/ >,(2019, juillet 18).

[13] : SZUSCIAK, F. Actualité des Promotions Informatiques du Campus Cesi Arras.(DAS, NAS, SAN, kesako ? par Ludovic ROUCOU) Mis en ligne le 10 nov 2012. Disponible sur :<https://ticalternancecesiarras.wordpress.com>,(2019, aout 6).

[14] : PAUPIER, F. e Top 4 des logiciels de monitoring réseau [en ligne]. (modifié le 24.08.2017). Retrieved from < https://www.appvizer.fr/magazine/services-informatiques/supervision-reseau/monitoring-reseau-4-outils-pour-detecter-les-anomalies/> ,(2019, aout 7).

[15] : IRSAPOULLE., P. Mise en place d'un outil de supervision et de contrôle distant. *Mémoire de Master M2*. Université de la Réunion, (2014).

[16] :BEN SASSI, G. Mise en place d'un outil de supervision de réseau d'entreprise. *Mémoire de Mastère Professionnel*. Université Virtuelle de Tunis, (2015).

[17] :EL BARRANI, N. *Supervision SNMP. (Modifié le 19/09/2017).* Disponible sur :< https://www.supinfo.com/articles/single/5484-supervision-snmp > ,(2012, Janiver 05).

[18] : Dubroeucq, P. Y.Étude et mise en œuvre d'une solution open source de supervision systèmes et réseaux. Mémoire d'ingénieure. Université Lille, France. Retrieved from Informatique. Mémoire d'ingénieure, (2012).

[19] :MARQUET, H.Etude des outils de surveillance (monitoring) réseau. Mémoire de Mastère Professionnel. Université Lille, France, (2009).

[20] : BERGERON, N. Supervision via Observium - Installation/configuration (Modifié le 01/09/2016). Retrieved from <https://www.supinfo.com/articles/single/2095-supervision-via-observium-installation-configuration> ,(2019, Juillet 24).

[21] : BILLON, A.Rapport de stage. Sygmalab informatique et media,(2017).

[22] : DJOUHRA, D. Optimisation des performances des data centers des cloud sous contrainte d'énergie consommée. . Thèse de doctorat : Ingénierie des données et des connaissances. Universite de Oran,Algerie,,116p. Retrieved from Thèse de doctorat : Ingénierie des données et des connaissances, (2016).

[23] : CLEM*ENT* OBER, A. Comment installer CentOS 7 [en ligne].2018 *)*. Disponible : <https://www.supinfo.com/articles/single/7083-comment-installer-centos-7> (2019, nov 21).

[24] :RHEL/CentOS Install. Retrieved from observium: <https://docs.observium.org/install_rhel7/> ,(2013-2017).

Conclusion général

Dans ce mémoire nous avons décrit le travail effectué durant la période de notre projet. Nous avons atteint presque l'objectif initial de ce projet qu'était de permettre à l'administrateur réseaux/systèmes de l'entreprise de mieux superviser les équipements et les services de son système informatique. En effet une solution de supervision permet de diminuer le temps de diagnostic des pannes et faciliter les tâches de l'administrateur.

Plus le nombre des équipements et des services informatiques augmente plus les tâches de l'administrateur deviennent trop compliquées et il n'arrive pas à les assurer convenablement ce qui engendre une perte du temps.

Notre travail consistait à mettre en place un outil de supervision système et réseau. Dans un premier lieu et après avoir réalisé une étude comparative entre les différentes solutions open source existantes sur le marché. Nous avons déterminé la solution à mettre en place. Dans la partie réalisation, nous avons mis en place l'outil OBSERVIUM et le configuré sur le système d'exploitation LINUX (CentOS 7).

Cette application comporte une cartographie présentant les différents équipements surveillés et elle permet de renseigner l'administrateur sur l'état des machines, le trafic écoulant, etc.

Enfin, l'administrateur peut être averti par un message textuel, sous forme de Mail, dont le contenu indiquera la machine défectueuse.

Comme perspectives, nous proposons l'amélioration de ce travail par :

- Ajouter des modules a l'outil,
- Amélioration de l'interface graphique,
- Intégration d'autre module,
- Prédiction de l'état du réseau au future,
- Utiliser ce boitier dans d'autre réseaux.

Annexe A : Configuration d'Observium

Observium est un système d'exploitation linux installer sur le serveur ou nous aurons mise en place notre solution. Nous vons choisé d'utilisé Centos7 pour le télécharger dans notre serveur.

I. Présentation d'accueil

Ici vous aurez une vue d'ensemble de votre infrastructure.

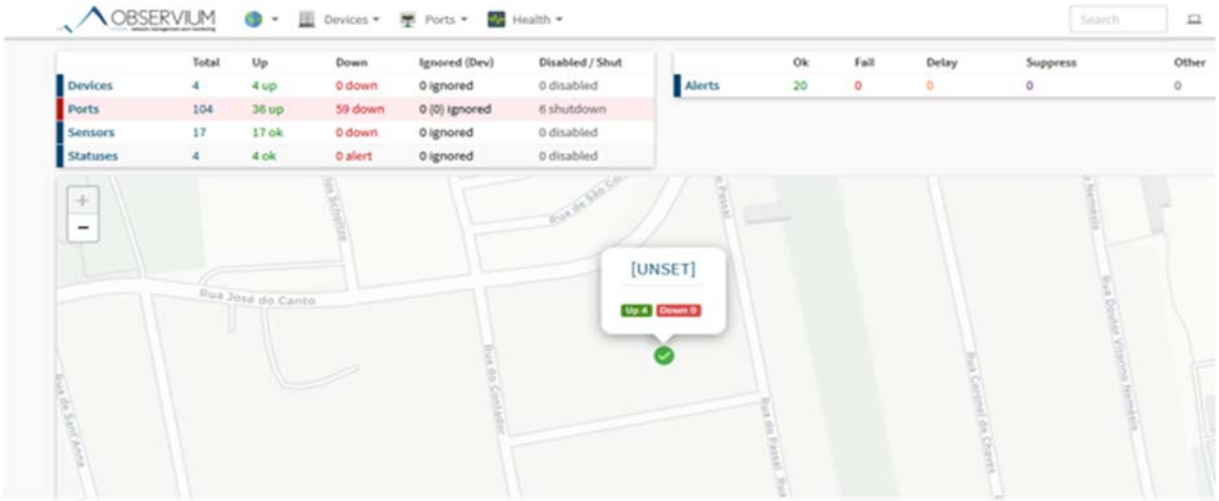
En haut : une barre de menu pour un accès rapide à toute l'interface web.

En haut à gauche : le nombre d'hôtes Up, le nombre de ports ouverts.

En haut à droite : le nombre d'alerte qui sont OK, Fail ou sans réponses.

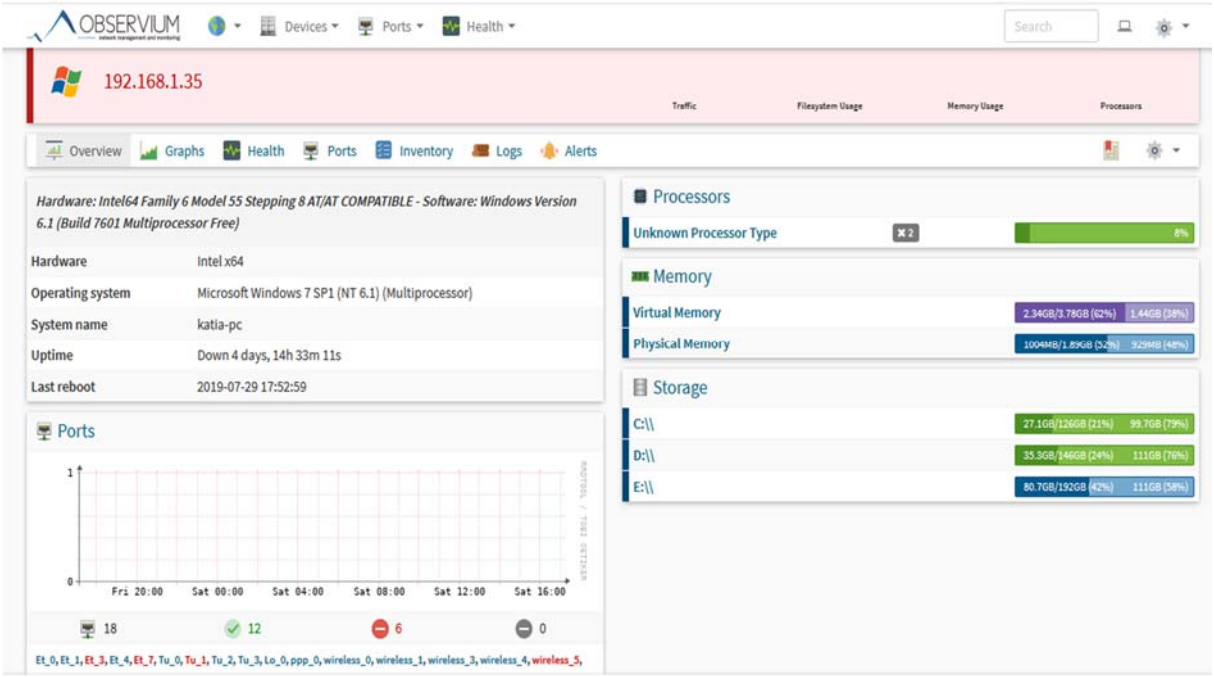
Au centre : la carte avec les serveurs UP en vert, et les serveurs down en rouge (le nombre indique qu'il y a plusieurs serveurs au même endroit).

En bas : les derniers changements d'état sur toute l'infrastructure **[20].**



I.1 Les équipement :

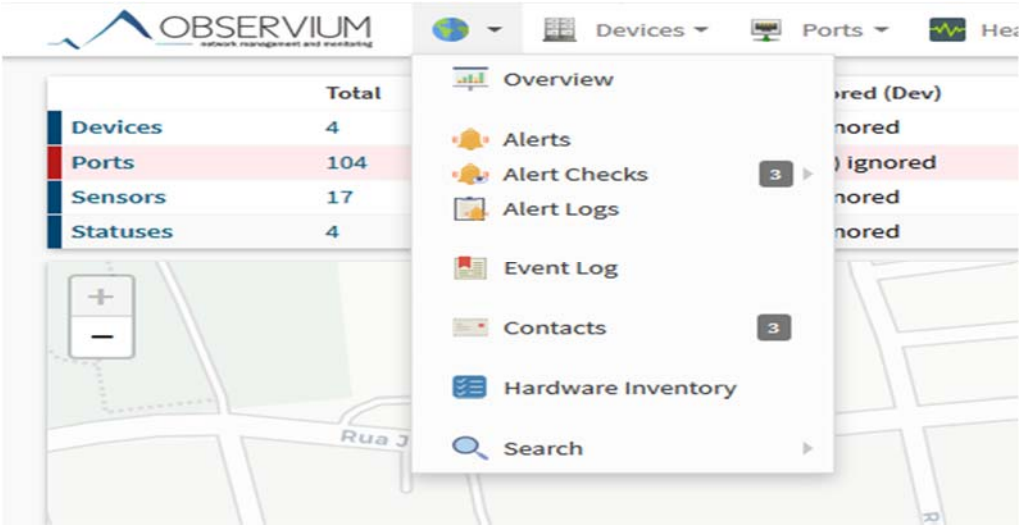
Si l'on sélectionne un hôte (par exemple en allant dans "Devices> All devices>Workstations", on peut accéder à une interface semblable à celle-ci **[20]** :



La première page nous permet d'avoir une vue globale sur le device avec les pourcentages d'utilisation des trois composants principales (à droite).

Depuis cette page, nous pouvons accéder à toutes les informations remonter par l'agent SNMP via les onglets **[20]** :

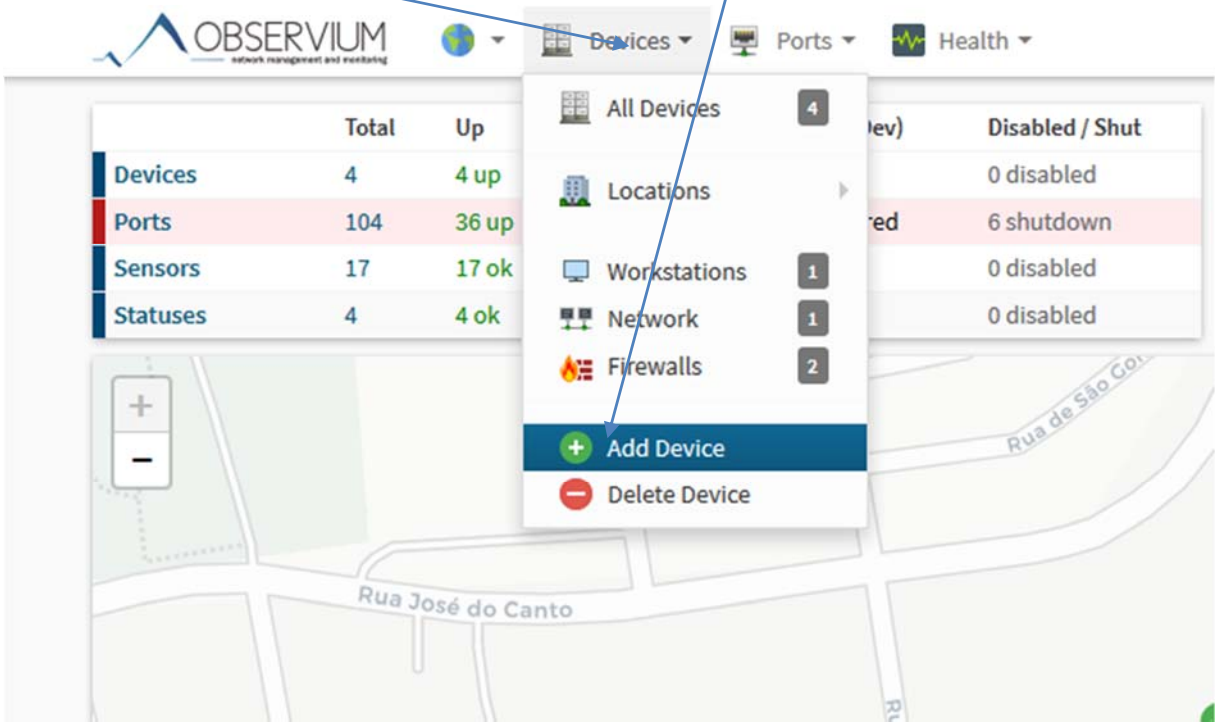
- Overview (vous y êtes déjà
- Graphs.
- Health.
- Ports.
- Inventory.
- Logs.
- Et Alerts.



II. Configuration :

II.1 Ajouter un équipement :

Aller dans l'onglet « Devices » et cliquer sur « AddDevices » **[21]** :



Puis nous allons faire entrer les paramètres suivants :

Hostname : nom de l'hôte à superviser, essayer de le pinger avant depuis le serveur où Observium est installé (pingIP_hôte).

Protocol Version : A moins d'utiliser un protocol particulier, le v2c est parfait, mais dans certains cas, il faudra utiliser le v1 ou v3.

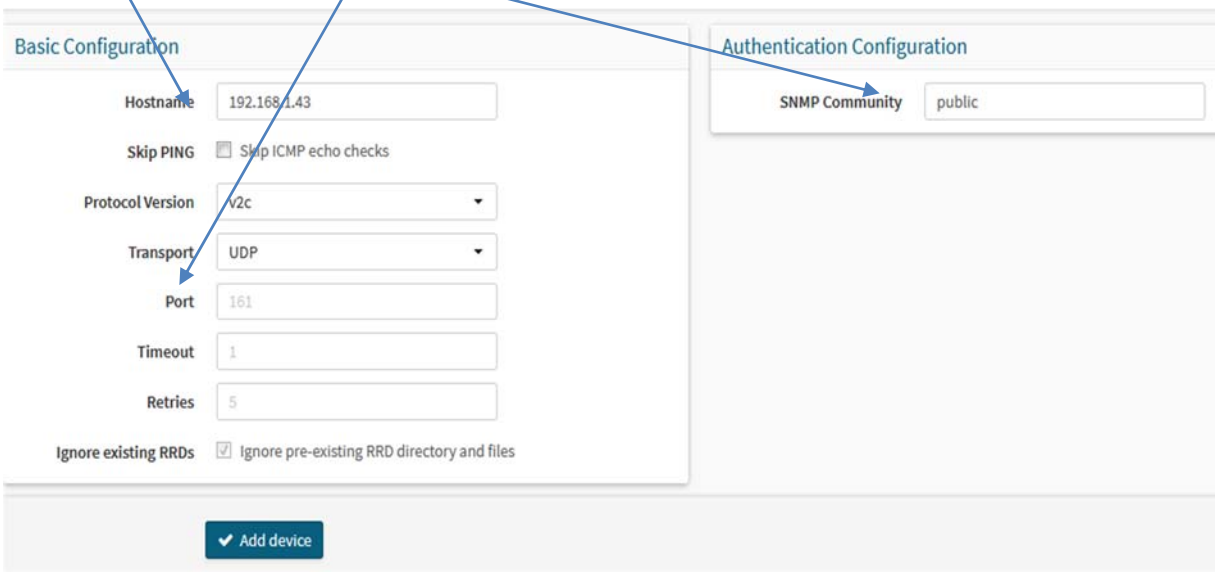
SNMP Community : Notre communauté dans ce cas est "public".

Puis cliquer sur ajouter device.**[20]**

Exemple :

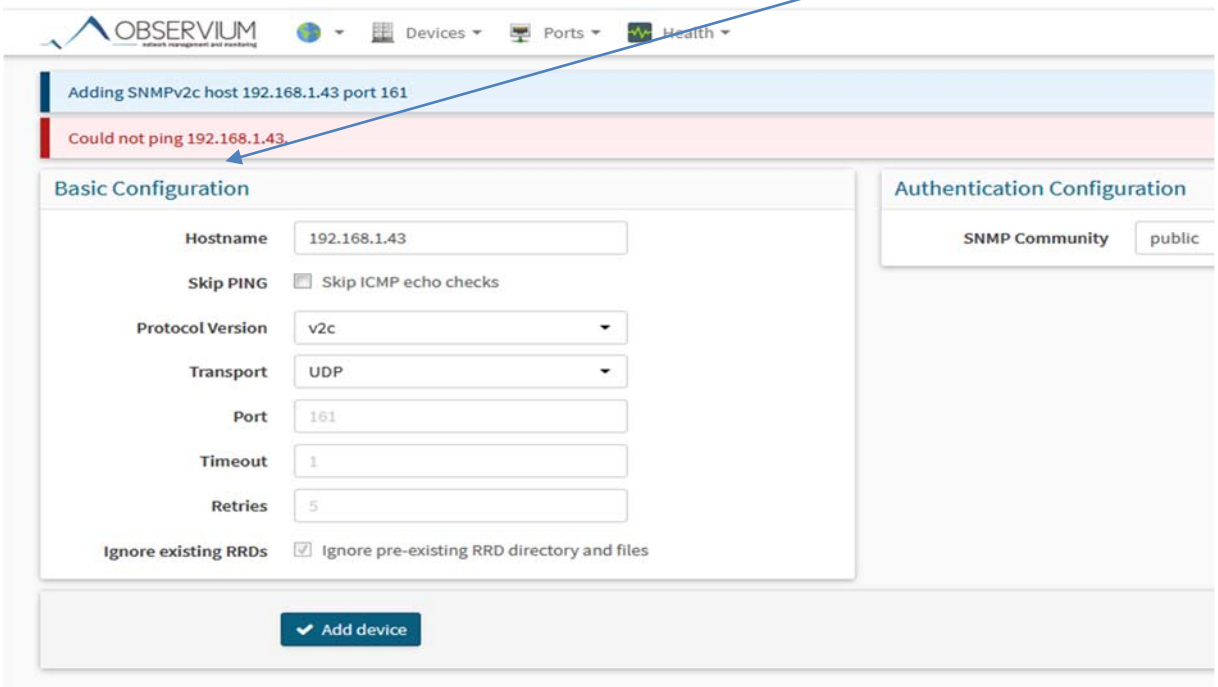
Saisir l'IP publique du client et leportconfigurer sur le routeur du client.

Saisir sur SNMP COMMUNITY : « public»**[21]**

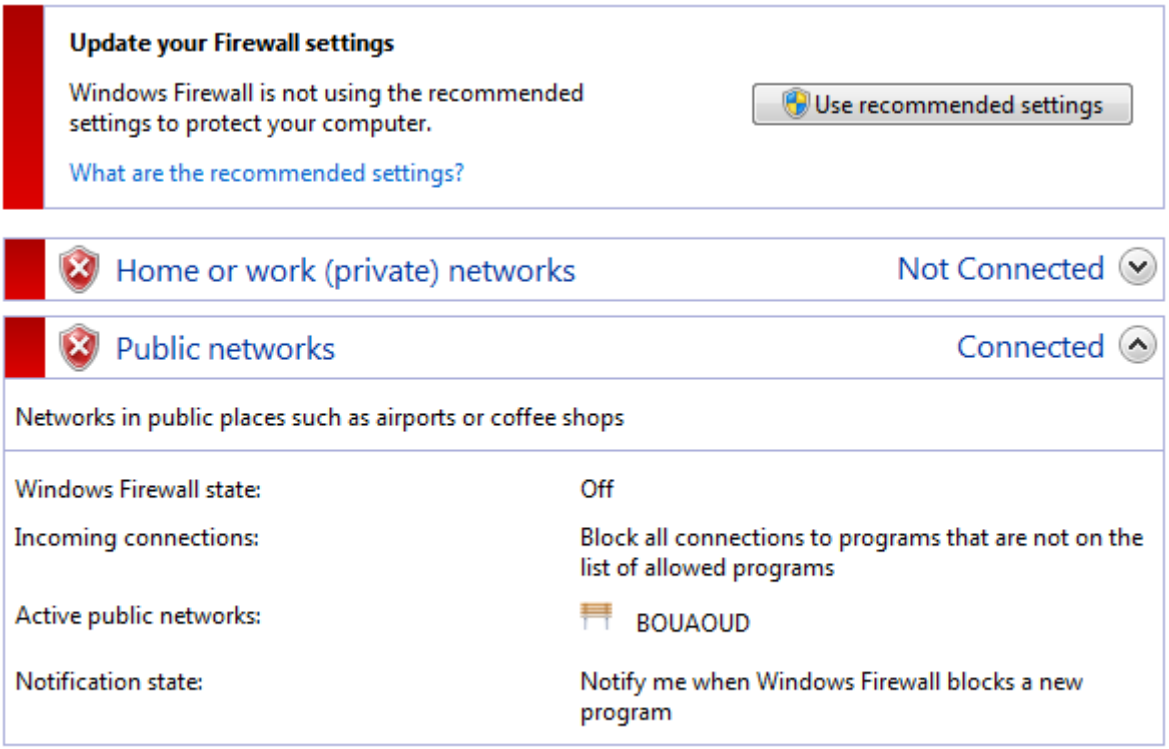


Voilà, votre machine est ajoutée. Lorsque l'on regarde la machine en question, il est alors normal qu'elle affiche des messages d'erreur pour l'affichage des graphiques car il faut attendre minimum 10 minutes pour que cela disparaisse. Ou alors vous n'avez pas encore configurer la machine à surveiller.**[21]**

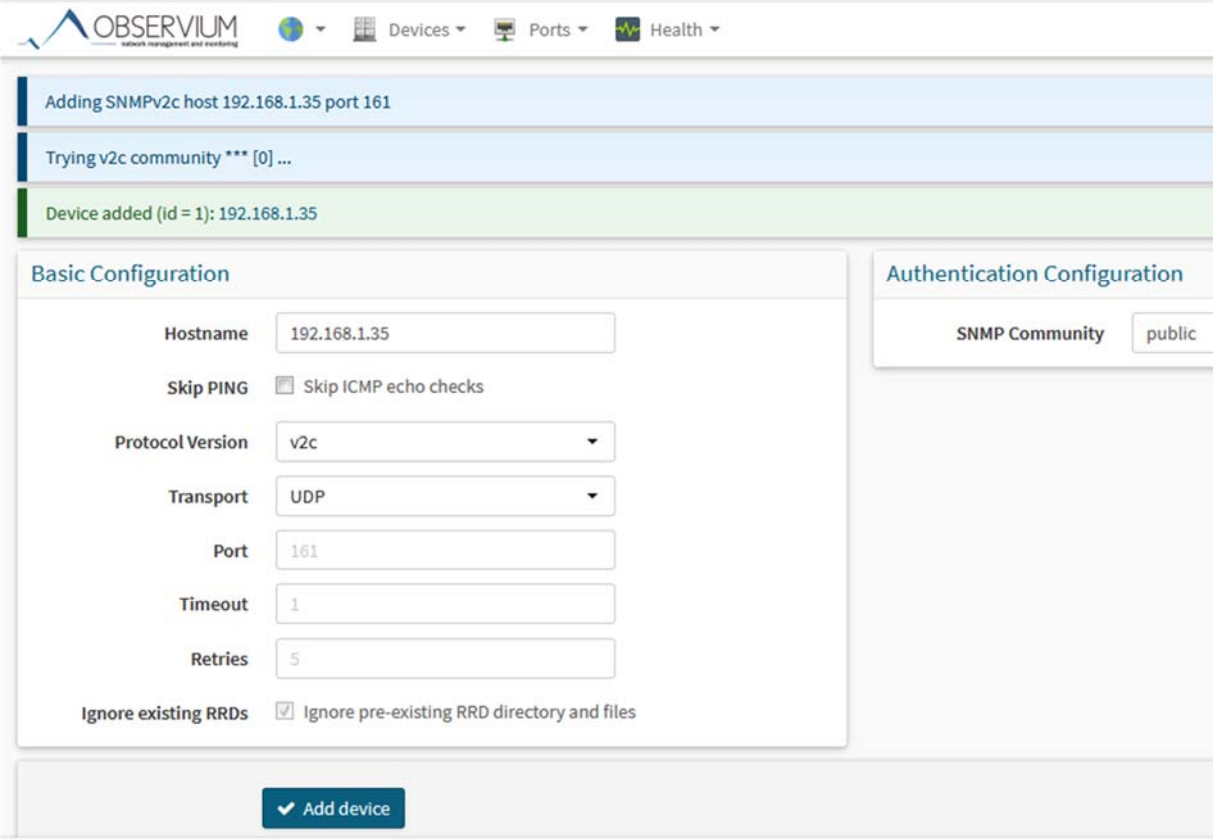
Comme vous voyez ici lorsque on a ajouté le host, il apparaitre une **erreur**



Pour résoudre cette erreur on doit désactivé notre pare-feu

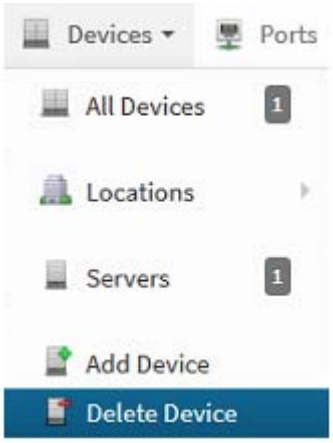


après on refère l'étape d'ajout de host eston aura :

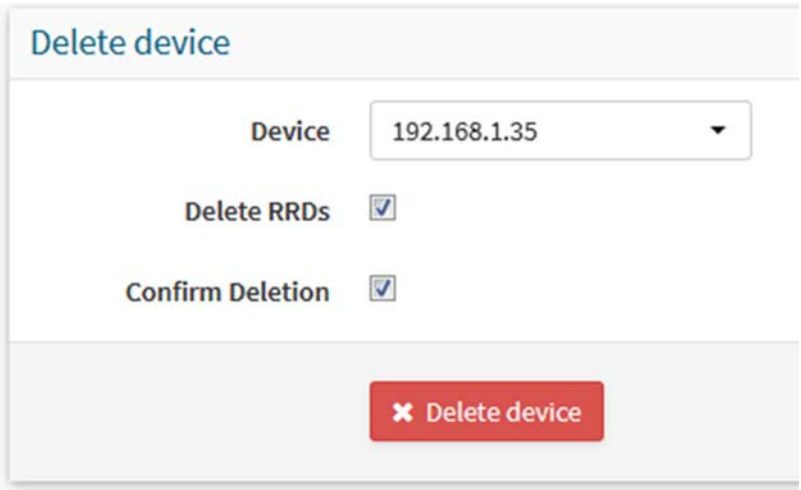


II.2 Supprimer un équipement :

Pour supprimer un équipement, allez dans le menu puis dans Devices>Delete Device :



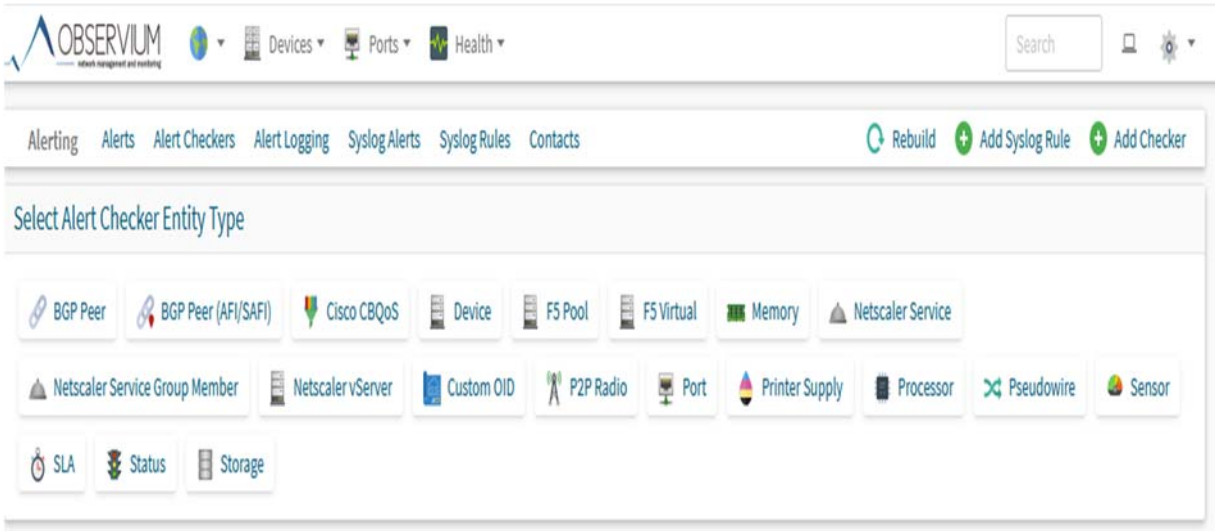
Sélectionner l'équipement à supprimer, cocher bien "Confirm Deletion" et "Delete RRDs" (Delete RRDs : pour supprimer les graphiques de l'hôte afin de diminuer la taille de la base de données)**[20] :**



II.3 Ajouter un Alèrt cheker *:*

Aller dans l'onglet « Alert Checks » et cliquer sur « Create New Chcker »

Il apparaitre cette fenêtre des types d'entité:



II.3.1 Type d'entité [24]:

Tout d'abord, lorsque vous créez une alerte, vous devez choisir le type d'entité pour lequel vous créez l'alerte. Des exemples de types d'entité incluent Port, Device, Sensor et processor.

Exemple pour un processor :

Entity type : doit être défini sur le type d'entité pour lequel vous créez un vérificateur

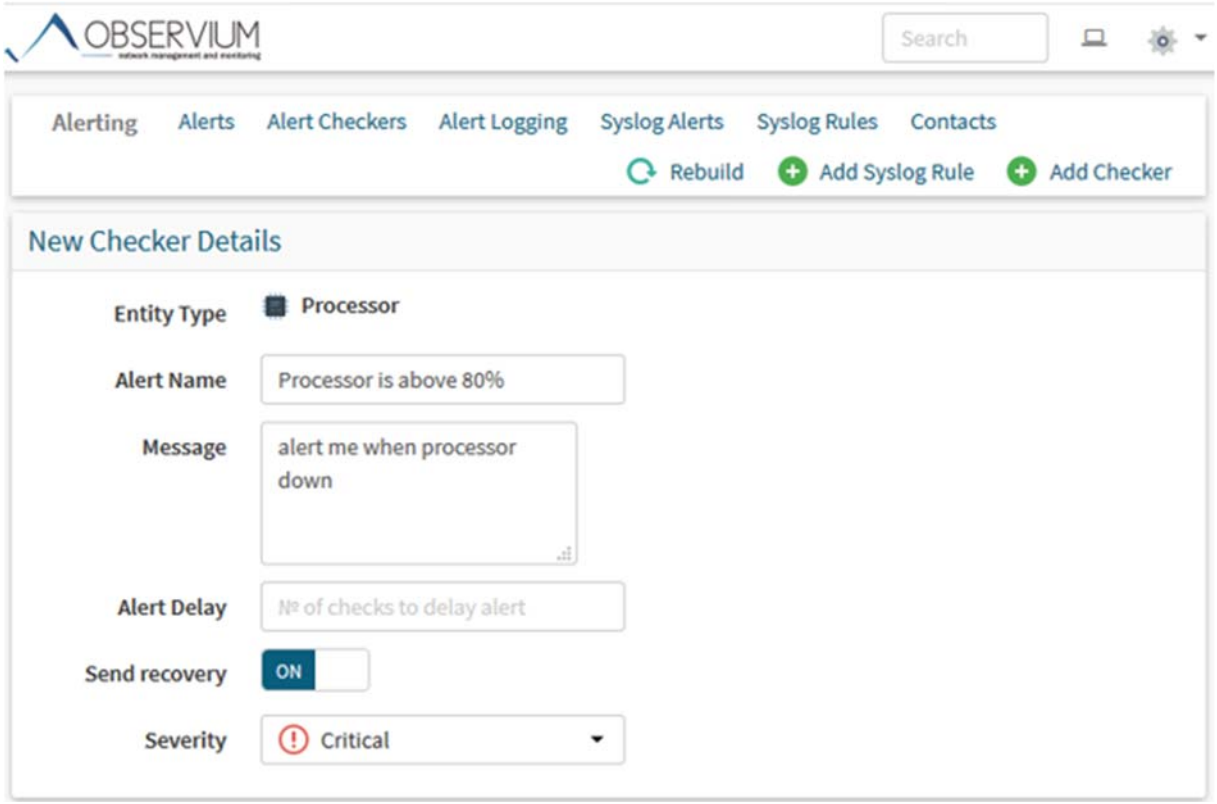
Alert Name : est un identifiant textuel unique utilisé pour identifier votre vérificateur dans l'interface utilisateur. Il doit être unique ou l'ajout du vérificateur échouera.

Message : est un message texte significatif envoyé avec toutes les alertes générées par ce vérificateur. Il devrait être utilisé pour diriger le destinataire vers la cause et l'importance du problème.

Alert Delay : permet de retarder une alerte pour X vérifie avant qu'il ne soit alerté.

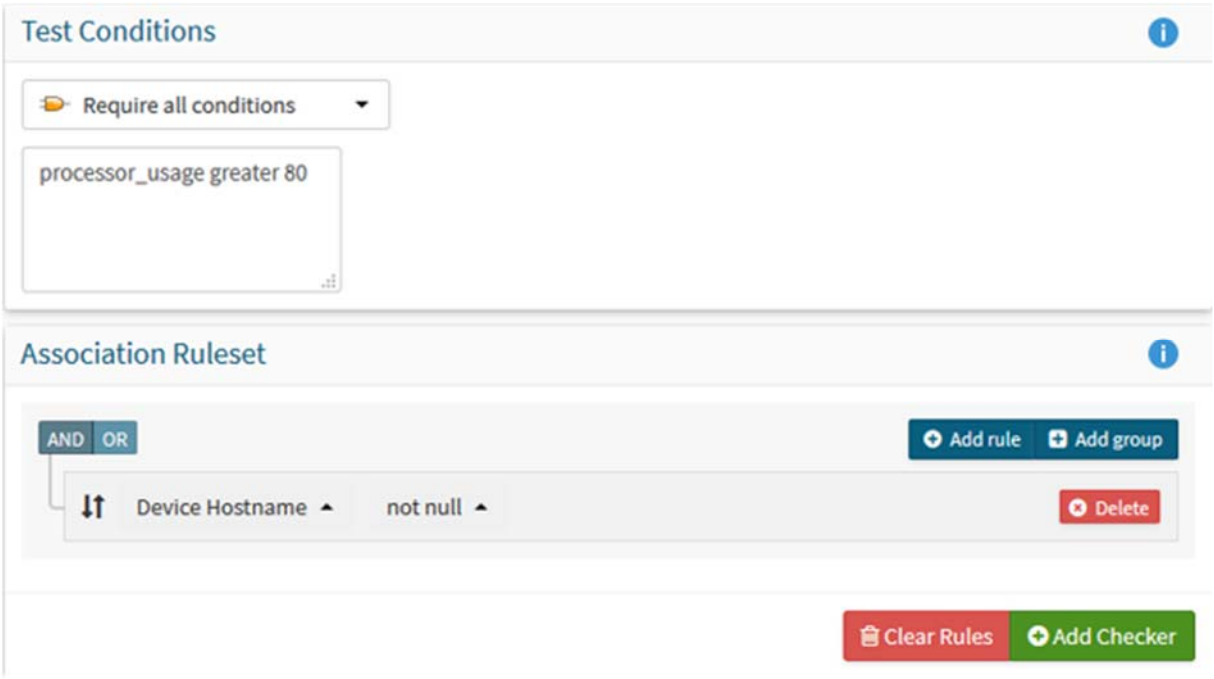
Send Recovery vous permet d'activer ou de désactiver l'envoi de notifications de récupération.

Severity est actuellement bloquée à critique.



II 3.2 Checker Conditions

Ensuite, nous avons la fenêtre de Conditions Checker



Elle permet de configurer les règles réelles qui déclencheront votre alerte. Les conditions sont entrées sous forme d'un texte, avec une condition par ligne.

On auras a la fin :