UNIVERSITE SIDI MOHAMMED BEN ABDELLAH
FACULTE DES SCIENCES ET TECHNIQUES FES
DEPARTEMENT DE GENIE ELECTRIQUE

Diplôme de Licence

Electronique Télécommunication et Informatique
(ETI)

RAPPORT DE FIN D'ETUDES

Intitulé :

Etude de la supervision informatique du réseau MARSA MAROC ;

Réalisé Par :
Hanae ZAIM - Nabila ZAOUI

Encadré par :

M^R Fahd BENBOUBKER
P^r Ali AHAITOUF
P^r Farid ABDI

Soutenu le 18 Juin 2010 devant le jury

Pr	**Ali AHAITOUF**	**(FST FES)**
Pr	**Farid ABDI**	**(FST FES)**
Pr	**Abdellah MECHQRANE**	**(FST FES)**
Pr	**Nor-Said ECHATOUI**	**(FST FES)**

Remerciements

Nous tenons à remercier vivement M. AZMI, chef de la division technique département système d'information, qui nous a accordé ce stage.

Nous adressons nos remerciements également à M. M'BARKI, chef de département des ressources humaines, aussi nous témoignons de notre reconnaissance à l'égard de l'ingénieur M. BENBOUBKER qui était si patient et de qui on a appris « que pour réussir sa carrière, on doit faire preuve de l'esprit d'équipe et d'efficacité ».

Nos grands remerciements à M. AHAITOUF, notre professeur, à qui nous devons énormément de respect et grâce à qui, on a pu bénéficier de ce stage, ainsi que notre chef de la filière ETI, M. ABDI.

Nous remercions vivement tous nos professeurs qui nous ont accompagnés tout au long de nos études.

Enfin, merci à tout le corps enseignant de département génie électrique à la Faculté Sciences et Techniques de Fès.

Dédicaces

A ceux qui nous ont procuré soutien et courage,

A nos chers parents qui nous ont toujours honorés par leur fierté,

A nos chers professeurs qui n'ont épargné aucun effort en vue de nous faciliter les tâches et à qui nous devons respect et estime,

A tous les ami(e)s et à tous ceux qui nous avons eu la chance de croiser dans notre carrière,

Nous dédions ce travail modeste tout en souhaitant qu'il puisse susciter leur admiration,

A vous tous, nous disons Merci.

Sommaire

Introduction

Le stage en entreprise est pour tout étudiant le moyen d'exprimer ses compétences et de mettre en exergue ses connaissances.

Ce stage vient terminer notre formation en licence Electronique, Télécommunication et Informatique (ETI), il dure deux mois et a été effectué à MARSA MAROC, le sujet qui nous a été attribué est : « Supervision informatique »

Pendant la période de stage, on s'est familiarisé avec un environnement technique et un ensemble d'outils de supervision. Le projet réalisé s'est avéré très intéressant pour notre expérience professionnelle.

Le but de ce rapport n'est pas de faire uniquement une présentation exhaustive de tous les aspects techniques qu'on a pu apprendre ou approfondir, mais aussi, de faire un tour d'horizon des aspects techniques et humains auxquels on a été confrontés.

Ce rapport se décline en quatre chapitres :

Chapitre I : Présentation de l'entreprise MARSA MAROC

Chapitre II : Supervision informatique

Chapitre III : Etude comparative des outils de supervision

Chapitre IV : Conception des solutions choisies

A la fin de ce document, nous présenterons une annexe qui introduit les concepts techniques utilisés pour la conception de notre projet, à savoir la plateforme linux version « Ubuntu ».

(*) : Ces mots seront expliquer dans le glossaire.

Chapitre1

Présentation de "MARSA MAROC"

1) Présentation de MARSA MAROC:

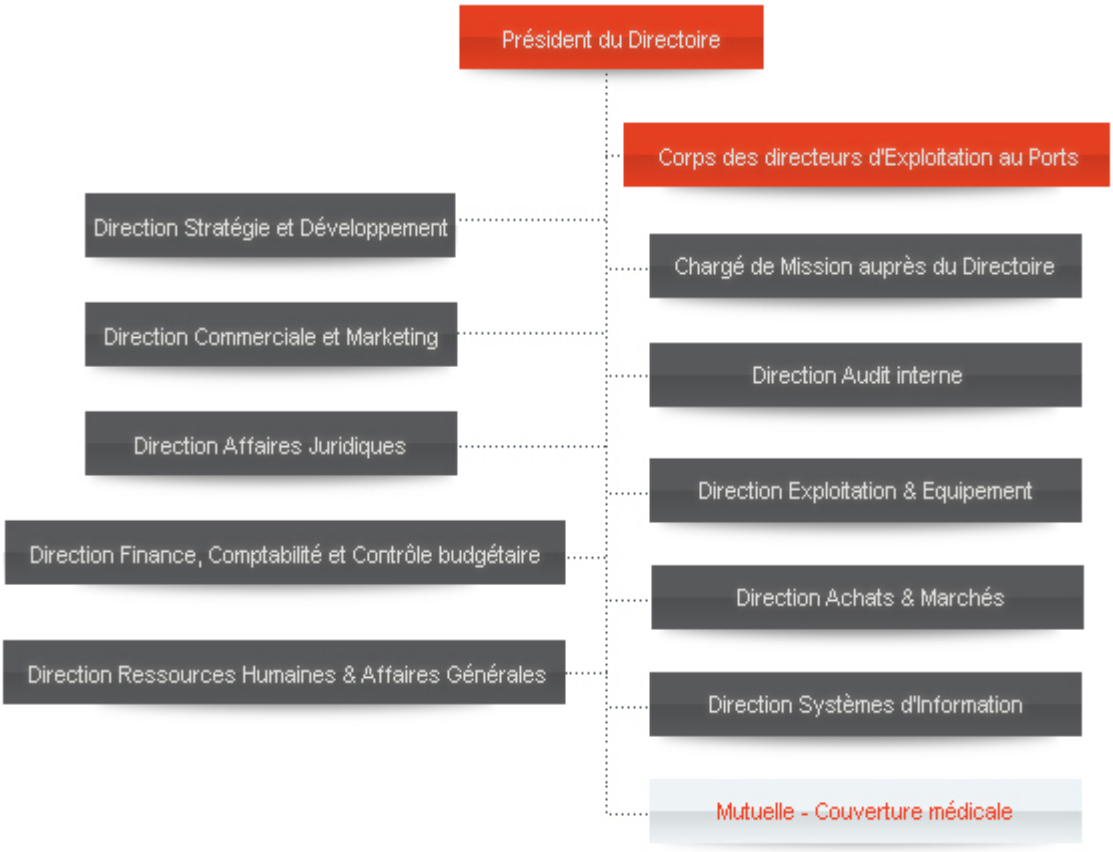
Marsa Maroc (anciennement ODEP, Office D'Exploitations des Ports) est une entreprise marocaine spécialisée dans l'exploitation de terminaux et quais portuaires, créée en 2006.

Le tableau ci-dessous présente quelques caractéristiques de cette entreprise :

Raison sociale	: Société d'Exploitation des Ports
Nom de marque	: Marsa Maroc
Date de création	: 1er Décembre 2006
Statut juridique	: Société Anonyme à Directoire et Conseil de Surveillance
Capital Social	: 733.956.000 DH
Siège social	: 175, Bd Zerktouni-20 100 Casablanca - Maroc
Président du Directoire	: Mohammed ABDELJALIL
Secteur d'activité	: Gestion de terminaux et quais portuaires
Chiffre d'Affaires *	: 2.372 MDH
Effectif *	: 2251 collaborateurs
Trafic global *	: 36 Millions de tonnes
Sites opérés	: 10 à savoir Nador, Al Hoceima, Tanger, Mohammedia, Casablanca, Jorf Lasfar, Safi, Agadir, Lâayoune, Dakhla

2) Organisation :

Étant donné que le port de Casablanca est le plus important port du Maroc et pour mettre en œuvre l'organisation recherchée, la direction d'exploitation du port de Casablanca (DEPC) est structurée selon l'organigramme suivant :



3) Présentation du Département Information de Gestion et Informatique (DIGI) :

a. *Mission de la DIGI :*

Le Département Information de Gestion et Informatique a pour mission de :

➔ Mettre à la disposition des différentes entités de la DEPC, les moyens nécessaires au recueil, à la fiabilisation, au transport et au traitement de l'information susceptible de contribuer à la réalisation de leurs objectifs.

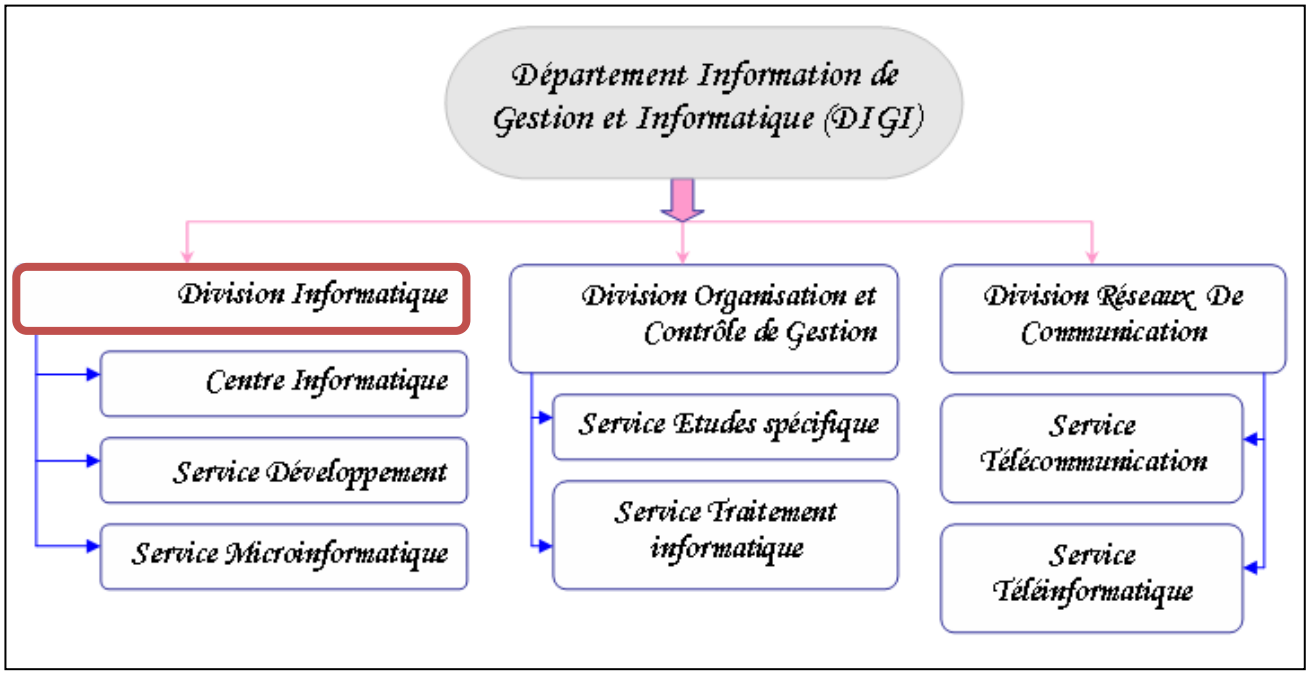
➔ Assurer la cohérence du système d'information à la DEPC et au sein de la MARSA MAROC.

➔ Assurer la réception et le bon fonctionnement du port à la DEPC.

➔ Gérer les tableaux de bord et le manuel d'organisation de la DEPC.

b. *Organigramme de la DIGI* **:**

Le département Information de Gestion et Informatique comprend trois divisions présentées d'une manière succincte dans l'organigramme ci-dessous :



Notre stage a été effectué au sein de la division informatique.

Chapitre2

Supervision informatique

1) Introduction :

Dans le domaine des entreprises modernes, l'adoption d'un système informatique facilite énormément les processus d'administration (personnelle et matérielle) et de productivité.
Un tel outil aide à bien satisfaire les exigences croissantes non seulement des administrateurs, mais aussi des utilisateurs, c'est pourquoi les développeurs conçoivent ce système d'une telle façon que tous les besoins soient satisfaits à travers une bonne gestion de toutes les branches de l'entreprise.

En effet, toutes les entreprises, de nos jours, sont équipées d'un réseau local au minimum, et pour les plus importantes d'entre elles de réseaux longue distance WAN (Wide Area Network), leurs parcs informatiques englobent des centaines, voire des milliers de terminaux engendrés par des serveurs de bases de données et des serveurs de traitements.

L'apparition de ces nouveaux environnements informatisés rend la surveillance des éléments clefs de réseau et de système une opération indispensable, afin de minimiser la perte d'exploitation et garantir que les utilisateurs ne s'aperçoivent pas des anomalies de fonctionnement au niveau de système d'entreprise. En effet, l'arrêt d'un service de messagerie n'est pas aussi coûteux que la perte de la base de données de son entreprise due à un disque défectueux.

Vu que le système informatique est au cœur des activités d'entreprise, sa maîtrise devient primordiale, puisque, il doit fonctionner pleinement et en permanence pour garantir la fiabilité et l'efficacité exigées, d'une part. D'autre part, les problèmes liés au système informatique tels que les défaillances, les pannes, les coupures et les différents problèmes techniques doivent être réduits, du fait qu'une indisponibilité du système ou du réseau peut causer des pertes considérables.

Afin de minimiser le nombre de ces pertes, une sorte de surveillance et de contrôle s'avère obligatoire ; la notion de la « supervision informatique » fût apparue et devenue une tâche vitale pour tout système informatique. Cette nouvelle branche d'administration système/réseau doit assurer trois fonctionnalités :

- ✓ Garantir la disponibilité de leurs système et réseau ;
- ✓ Tenter de prévenir en cas de problème ;
- ✓ Garantir une durée d'intervention et de résolution minimale.

En résumé, le but majeur attendu d'un système de supervision (Monitoring system :en Anglais) est d'assurer le plus possible le bon fonctionnement du système informatique, en surveillant les services et les entités logicielles (software) ainsi qu'en contrôlant le matériel (hardware).

❖ *Problématique :*

Actuellement, dans un environnement d'entreprise géré par l'informatique, il est plus important que jamais d'identifier et de résoudre les interruptions de service et les goulets d'étranglement (*) qui menacent les applications vitales, et ce avant tout impact sur la productivité du système et la satisfaction de l'utilisateur.

De ce fait, ces entreprises ont suivi plusieurs démarches pour surveiller et assurer la bonne gestion de leurs systèmes. Ces dernières peuvent nécessiter beaucoup de personnel et d'argent s'il s'agit de gérer des systèmes éloignés à l'aide de systèmes d'exploitation différents.

De plus, il ya souvent peu d'informations disponibles pour aider les administrateurs à comprendre les problèmes actuels et à prévoir les défaillances du système. Donc, il peut leur être difficile d'atteindre les niveaux de service requis par l'entreprise.

Plus important encore, avec tous les nouveaux équipements et les nouvelles technologies apparues et qui évoluent chaque jour. Les réseaux se complexifient et la tâche de la surveillance devient de plus en plus difficile. Cette complexité permet l'accès à un nouveau marché pour les constructeurs qui désormais se lancent dans le développement et la vente de logiciels de supervision.

Mais bien que leur efficacité ait été prouvée, presque toutes les solutions de supervision actuelles se limitent à effectuer des vérifications locales ou distantes sur les machines et services du réseau, et d'en communiquer les résultats ou signaler des pannes éventuelles le cas échéant. Dans ce dernier cas, le logiciel de supervision alerte l'administrateur qui doit intervenir manuellement pour le bon fonctionnement du système. Cela rend les choses plutôt pénibles et exige toujours la présence humaine et l'intervention manuelle, parfois même tardive. Ce qui devient à la limite coûteux et influe sur l'efficacité et la fiabilité du système informatique de l'entreprise.

D'un autre point de vue, les applications d'aujourd'hui deviennent de plus en plus distribuées dans de multiples objets et fonctionnalités qui sont amenées à coopérer. La décentralisation est donc la règle et une organisation coopérative entre modules logiciels est un besoin. En contrepartie, la taille, la complexité et l'évolutivité croissantes de ces nouvelles applications informatiques font qu'une vision centralisée, rigide et passive atteint ses limites.

❖ *Objectifs :*

Devant ce constat et dans le cadre de notre projet de fin d'études, nous avons fixé l'objectif de concevoir et de réaliser un système de monitoring informatique. Pour le mettre en œuvre et en réduire le coût, nous nous sommes dirigés naturellement vers une solution opensource.

Notre travail consiste, alors, à implémenter une solution adaptée à la supervision informatique assurant la détection des pannes dans un système informatique donné. Puis, nous allons tenter de résoudre, s'il y a possibilité, les problèmes qui apparaissent dans un environnement de réseau informatique pour offrir un meilleur service.

Pour réaliser ce travail, il nous a été fixé d'atteindre les objectifs suivants :

- Comprendre le concept « supervision »,
- Etudier les systèmes de supervision et leurs principes,
- Proposer des solutions de supervision convenables pour les besoins,
- Tester et estimer les solutions proposées.

2) Supervision informatique :

a. *Définition :*

En informatique, la supervision est une technique de suivi, qui permet de surveiller, analyser, rapporter et d'alerter sur les fonctionnements normaux et anormaux des systèmes informatiques.

D'un point de vue théorique, ERIC D'HEM (*) explique : « Dans le Monitoring il s'agit de répéter de manière régulière un processus de test ou de surveillance d'une personne ou d'un bien, le

but étant d'obtenir très rapidement et simplement une vision précise des événements ou des anomalies sur la période analysée » **[1]**.

L'objectifs de la supervision informatique est de surveiller le système et de garantir sa disponibilité même en cas d'anomalie pour cela deux étapes essentielles sont nécessaires pour les administrateurs :

- Tenter de prévenir en cas de problème (défaillances matérielles ou interruption des services) et garantir une remontée d'information rapide.

- Automatiser les tâches de récupération des applications et des services en assurant des mécanismes de redondance en une durée d'intervention minimale (par exemple : le redémarrage des services interrompus, l'arrêt de la machine en cas du surcharge du CPU, la sauvegarde des données en cas du risque de perte d'un disque dur, etc.)

En outre, la supervision informatique consiste aussi à indiquer et /ou commander l'état d'un serveur, d'un équipement réseau ou d'un service software pour anticiper les plantages ou diagnostiquer rapidement une panne.

La supervision peut porter sur plusieurs aspects de l'informatique qu'on peut classer dans trois catégories principales :

- Fiabilité
- Performance
- Contenu

b. Fonctionnalités et niveaux d'information :

Généralement, la plateforme de supervision regroupe les fonctionnalités illustrées dans la figure1 suivante :

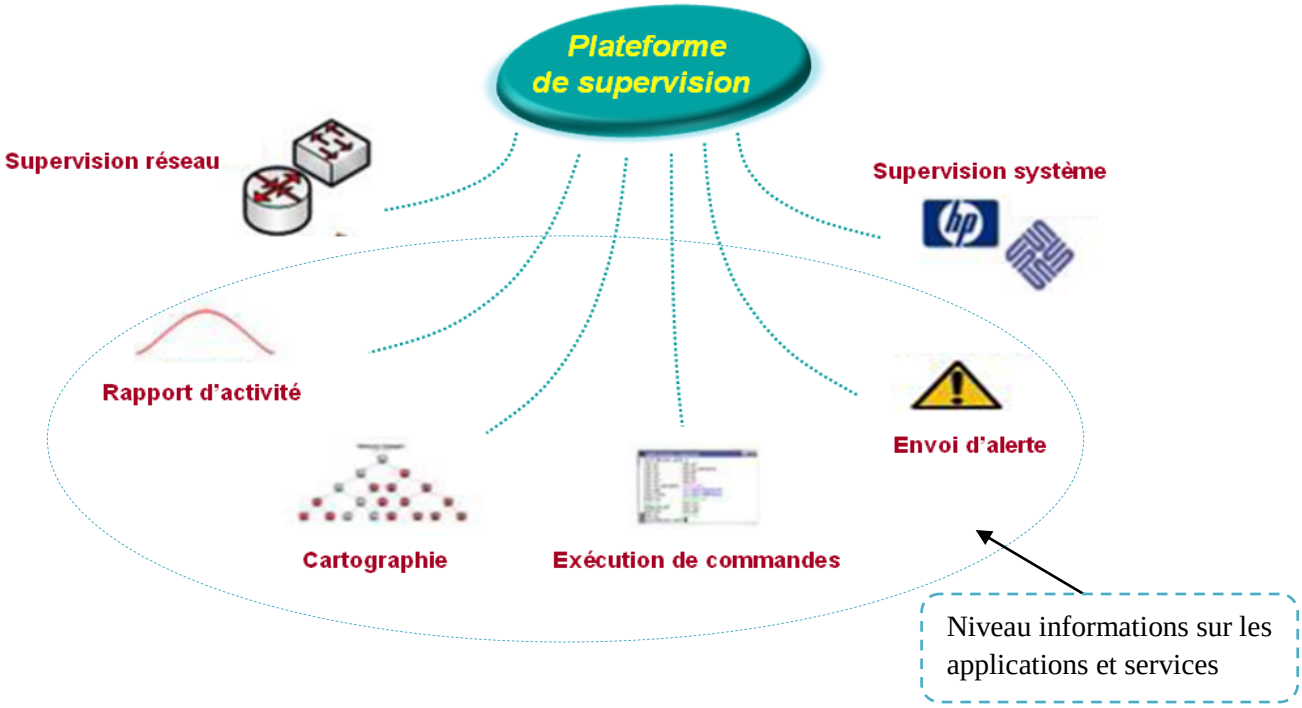


Figure 1 : Fonctionnalités de la supervision.

Trois niveaux principaux d'informations se dégagent de ce synoptique :

- Un niveau informations sur les systèmes : **supervision système**, cette supervision fournira des informations sur le fonctionnement du système.
- Un Niveau informations sur les applications et services il regroupe : **exécution de commandes**, **envoi d'alerte**, **cartographie** et **rapport d'activité**.
- Un Niveau informations sur les réseaux : **supervision réseau**, Ce type de surveillance permet de diagnostiquer la disponibilité d'un équipement physique connecté à un réseau
-

3) Protocole SNMP :

a. *Définition :*

SNMP signifie **S**imple **N**etwork **M**anagement **P**rotocol, c'est un protocole qui permet comme son nom l'indique, de gérer les équipements réseaux ainsi que les machines informatiques et de diagnostiquer les problèmes du réseau.

b. Principe de fonctionnement :

Avec le protocole SNMP, le système de gestion du réseau est basé sur trois éléments principaux : Les équipements gérés, des agents et Les systèmes de management de réseau.

- Les équipements gérés : ce sont des éléments du réseau (ponts, hubs, routeurs ou serveurs), contenant des "objets de gestion" pouvant être des informations sur le matériel, des éléments de configuration ou des informations statistiques ;
- Les agents : c'est-à-dire une application de gestion de réseau résidant dans un périphérique et chargé de transmettre les données locales de gestion du périphérique au format SNMP ;
- Les systèmes de management de réseau (*network management systems* notés NMS), c'est-à-dire une console à travers laquelle les administrateurs peuvent réaliser des tâches d'administration.

Le schéma suivant présente quelques éléments du protocole SNMP :

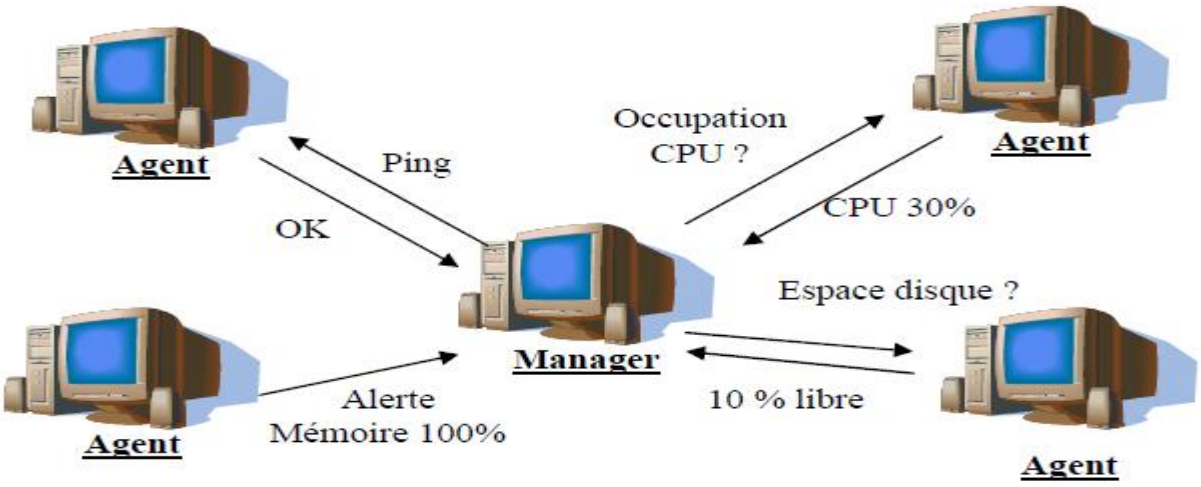


Figure 2 : éléments de base du protocole SNMP

Ces objets sont classés dans une base de données nommée **MIB** ("*Management Information Base*") qui est un ensemble d'informations structuré hiérarchiquement sur une entité réseau.

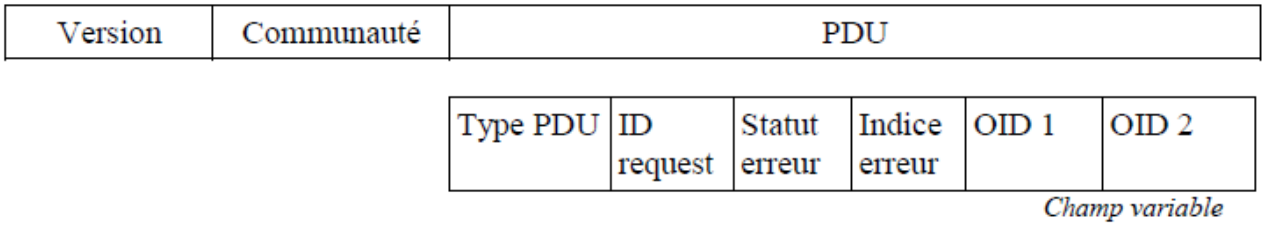
c. *Différentes versions de SNMP*

✓ **SNMP v1**

C'est la première version de SNMP qui a été très utilisée et qui l'est encore mais la principale faiblesse de cette version est qu'elle n'était absolument pas sécurisée. En effet, il n'y a pas de cryptage des données et aucune authentification n'est nécessaire. C'est pour cela qu'une appelée SNMPSec a été développé mais elle n'a quasiment pas été utilisée.

Format des messages SNMP :

Le message se présente sous la forme :



- Version : Le champ version contient la version de SNMP utilisée
- Communauté : Ce champ identifie l'utilisateur auprès de l'administrateur avant de lui accorder un accès.
- PDU : Ce champ est composé de :
  - Type PDU : il s'agit du type de requête
  - ID request : permet d'associer les réponses aux requêtes
  - Statut erreur : Type d'erreur (0 si aucune)
  - Indice erreur : position de l'erreur, s'il y a une erreur, ce champ indique quelle variable a causé l'erreur.
  - Champ variable : OID1 et OID2 ➔ correspond à la valeur de la variable.

✓ **SNMP v2**

C'est une évolution de la version SNMPv1. Elle a été publiée comme un avant projet du standard. Cette version est toujours restée à l'état expérimental et a vite laissé place à la version 3.

De nombreuses autres évolutions ont existés sans jamais être adoptées : SNMPv2p, SNMPv2c, SNMPv2u **[2]**.

- ✓ **SNMP v3**

La version 3 de SNMP a permis essentiellement d'introduire la sécurité des transactions. Elle comprend l'identification des deux parties qui communiquent mais aussi s'assure que les messages échangés ne puissent pas être lus par n'importe qui.

La sécurité est basée sur différents concepts :

- ✓ USM (User-based Security Model)
- ✓ VACM (View-based Access Control Model)

L'USM permet d'assurer plusieurs fonctions :

- o *L'authentification*

L'authentification permet de s'assurer que le paquet n'est pas modifié pendant la transmission et que le mot de passe est valide. Elle se fait grâce à HMAC-MD5-96 ou de
HMAC-SHA- 96 qui sont des fonctions de hachage (*). Grâce a ceci tout les paquets vont être authentifiés, cette authentification ne nous garantie pas encore la confidentialité des données.

- o *Le cryptage*

Le cryptage permet de s'assurer que personne ne puisse décrypter un message SNMP échangé sur le réseau. La version 3 de SNMP utilise pour cela le cryptage symétrique DES (*) avec des clés de 64 bits.

- o *L'estampillage du temps*

Lors de l'envoi d'une requête SNMP, le cryptage et l'authentification ne permettent pas d'éviter qu'une personne récupère cette requête et la retransmette plus tard sur le réseau (Replay Attack).
On a donc un timestamp de 150s sur les messages qui nous assure qu'il sera automatiquement refusé après ce délai fini.

Le format d'une trame SNMP v3 est très différent de celle de la version 1, pour rendre plus facile la distinction entre les versions, le numéro de la version SNMP est placé tout au début du paquet. La figure suivante montre la trame SNMPv3:

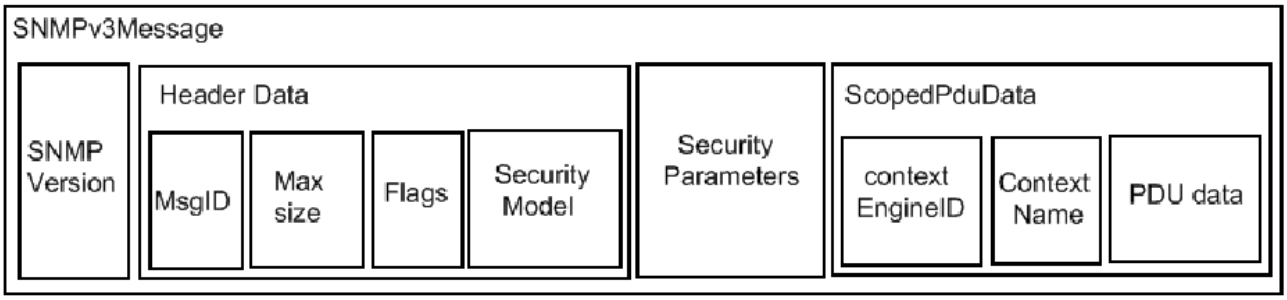


Figure 3 : trame SNMP V3.

- Version : utilisé pour envoyer le paquet vers le bon module de décodage.
- MsgID : identificateur de message utilisé pour associer les requêtes et les réponses.
- Max size : grandeur maximale du paquet réponse.
- Flags : drapeaux indiquant si une réponse est attendue et si un modèle de sécurité a été utilisé.
- Security model : modèle de sécurité utilisé pour envoyer le paquet vers le bon module de sécurité.
- Security parameters : informations de sécurité.
- Context EngineID et Conext Name : identifie le contexte.
- PDU data : informations utiles

4) Conclusion :

La supervision informatique est indispensable pour une entreprise et dont la défaillance d'un quelconque de ses services informatiques et l'indispensabilité de son système d'information influent négativement sur le rendement global de sa productivité.

Pour pouvoir être efficace, la surveillance doit donc impérativement être effectuée depuis différents points de contrôle sur une architecture distribuée, avec des techniques permettant d'analyser et gérer en permanence les flux.

Le chapitre suivant donnera une vue détaillée des différentes infrastructures de monitoring existantes.

Chapitre3

Etude comparative des outils de supervision réseau

1) Introduction :

Le marché de la supervision informatique déborde de logiciels de monitoring, certains sont payants et d'autres font parti du monde libre où on peut même trouver des Open Source. Nous allons dans ce qui suit citer quelques uns et nous détaillerons les plus connus et répandus dans le milieu des entreprises.

Le choix d'un type de logiciel se fait selon divers critères, le tableau ci-dessous dresse une comparaison relative entre les avantages et limitations des logiciels libres et sous licence commerciale :

	Open source (logiciel libre)	Closed source (logiciel payant)
Avantages	-Faible coût d'acquisition -Développements additionnels peu coûteux et riches -Respect des standards -Indépendance des fournisseurs	-Solutions globales et approuvées -Périmètres techniques et fonctionnels étendus
Limitations	-Support difficile -Périmètres techniques et fonctionnels encore limités.	-Coût d'acquisition et de support -Incompatibilités entre fournisseur à choix d'un fournisseur unique -Développement additionnel restreint et coûteux

2) Closed source : (sous licence commerciale)

Les gros éditeurs de logiciels ont rapidement compris que la supervision était une ressource clé pour les entreprises qui, de plus en plus, utilisent de systèmes d'information performants

et complexes et ont donc besoin d'une disponibilité toujours plus grande de leur infrastructure informatique. Par conséquent, la supervision est un domaine dans lequel les sociétés n'hésitent pas à investir depuis quelques années pour développer et proposer des moyens de surveillance de plus en plus performants.

Parmi les outils de supervision, on trouve: la gamme Openview de HP et Tivoli d'IBM.

a. *HP OpenView :*

HP OPEN VIEW [3] est un outil de supervision reconnu sur le marché. Son principal avantage est la centralisation des informations sur un seul poste. Il permet le management d'équipements réseau. Ce logiciel est donc destiné aux moyennes et grandes entreprises qui souhaitent avoir une vue globale de leur réseau et de son état.

Le tableau ci-dessous regroupe les principales caractéristiques de ce logiciel :

Fonctionnalités de base :	sondes et protocoles:	Indication et évaluation:
• Gestion de l'infrastructure, réseau, stockage,.... • Réduction des coups de maintenance et augmentation de la productivité, • Surveillance préventive afin d'éviter les erreurs repétitives, • Système de base SQL server avec une autre prioritaire à HP, • Serveur web integré, • Envoi d'alertes,	• Protocoles :protocole de communication RPC (*), SMTP , HTTP .... • Analyse des performances d'un client à travers un agent;	• Graphiques pour afficher les données surveillées, • Cartes pour visualiser l'architecture du réseau, • Compte rendus en HTML, • Canaux pour l'information : mail,syslog ..., • Rédaction des rapports d'activités;

b. IBM Tivoli Monitoring :

IBM Tivoli Monitoring [4] est une solution de surveillance unifiée avec collecte des indicateurs disponibles, historisation des données et visualisation graphique pour un pilotage centralisé. Ce moniteur de supervision se classe parmi les leaders du domaine, puisque il offre de nombreux avantages.

Le tableau ci-dessous regroupe les principales caractéristiques de ce logiciel :

Fonctionnalités de base :	sondes et protocoles:	Indication et évaluation:
•Surveiller de manière proactive les composants vitaux de l'infrastructure, •Réduire le temps de diagnostic et de correction d'un incident, •Visualise les mesures de performances historisées et en temps réél sous forme de tableaux, •Une interface simple et personnalisable;	• Technologie avec ou sans agent , •Protocoles : HTTP, SMTP (*), PING ...;	•Envoi d'alertes, •Puissantes fonctions d'automatisation, •Historisation et reporting integrés;

D'autres logiciels moins connus existent, on en cite par exemple :

a. OpManager :

OpManager [5] est un logiciel de surveillance du réseau qui offre une surveillance combinée des applications, du réseau à grande échelle et des serveurs avec des fonctionnalités

intégrées de service d'assistance, d'administration et d'analyse du trafic sur le réseau.

Le tableau ci-dessous regroupe les principales caractéristiques de ce logiciel :

Fonctionnalités de base :	sondes et protocoles:	Indication et évaluation:
• Mesure de l'utilisation et du traffic sur la bande passante, • Garantit une disponiblité elevée, • Identification des sources du trafic elévé ou à forte utilisation, • Surveillance du traffic sur les ports, • Surveillance des applications, • Surveillance des composants du réseau;	• Protocoles : HTTP, SMTP, PING ,POP (*), telnet (*), HTTPS, IMAP (*)..;	• Un rapport détaillé sur la machine, • Graphique en temps réél pour avoir une idée plus significative, • Visualiser la table de routage, • Visualiser les services,le journal d'évenement et les processus actifs, • Envoi d'alertes via mail ou sms

b. PRTG :

PRTG (Paessler Router Traffic Grapher) **[6]** est un logiciel qui permet grâce à l'analyse de trames SNMP, de créer des graphiques sur le trafic réseau.

Le tableau ci-dessous regroupe les principales caractéristiques de ce logiciel :

PRTG

Fonctionnalités de base :	sondes et protocoles:	Indication et évaluation:
• Surveilance de bande passante, d'activité, de disponiblité et des SLA, • Surveillance LAN,WAN,WLAN et VPN à l'aide de probes, • Acquisition de données via SNMP, packet sniffing, netflow ou mesure de latence, • Version Freeware disponible pour les petits réseaux, • Système de base de données interne avec un serveur web;	• Protocoles : HTTP, SMTP, PING ,POP3, SNMP, WMI, DNS (*), RDP (*)... • Modèles préconfigurés pour des routeurs cisco, serveurs SQL..	• Réalisation de comptes rendus (HTML,PDF)et de logfiles • Différents canaux pour l'information (email, SMS,syslog...) • Graphiques attrayants;

3) Open source :

Depuis une dizaine d'années déjà, plusieurs projets de supervision ont vu le jour au sein de la communauté du logiciel libre. Nous en présenterons ici, les plus populaires **:**

a. Zabbix :

Zabbix [7] est un logiciel de monitoring réseau Opensource et multiplateforme créé en 2002 par, Alexei Vladishev. Il permet de surveiller le statut de divers services réseau, serveurs, postes de travail et autres matériels (routeurs, pare-feu, imprimantes, etc.).

Le tableau ci-dessous regroupe les principales caractéristiques de ce logiciel :

Fonctionnalités de base :	sondes et protocoles:	Indication et évaluation:
• Surveillance des ressources matérielles : CPU, mémoire vive.., • Surveillance des sites web : temps de réponse, vitesse de transfert.., • Surveillance de l'integrité des fichiers, • Analyse des logs;	•Protocoles : HTTP, FTP (*),SMTP,SSH (*),IMAP... •Ports : 21, 80, 1434, 10050...	• Surveillance via simples test , SNMP ou agent zabbix, • Alerte par mail, sms ou jabber, • Réalisation de graphiques, cartes ou screens;

*Ce logiciel a fait l'objet de notre projet.

b. Nagios :

Nagios [8] est un logiciel de monitoring et de supervision libre sous licence GPL. Il offre une solution de surveillance efficace dans un système informatique complexe. Il permet de surveiller le bon fonctionnement des services d'une ou plusieurs machines dans un réseau hétérogène. Il est écrit en C et fonctionne grâce à un ensemble de plugins (qui eux peuvent être écrits dans n'importe quel langage).

Le tableau ci-dessous regroupe les principales caractéristiques de ce logiciel :

Fonctionnalités de base :	sondes et protocoles:	Indication et évaluation:
• Surveillance des ressources des hôtes (utilisation des disques..), • Interface web optionnelle , • Archivage automatique des données collectées;	• Protocoles : HTTP (*), SMTP, POP3, NNTP (*),	• Alerte par mail ou autre méthode personnalisée, • Interface permettant l'integration simple des plugins;

c. *Cacti :*

Cacti est un logiciel de supervision réseau sous licence GNU GPL qui fonctionne sur les plateformes Linux/Unix et Windows.

Il est utile pour connaître et comprendre les flux circulant sur le réseau.

Le tableau ci-dessous regroupe les principales caractéristiques de ce logiciel :

Fonctionnalités de base :	sondes et protocoles:	Indication et évaluation:
•Surveillance du traffic lié aux ports et traffic lié aux interfaces réseau des équipements, •Nombre d'utilisateurs connectés, •Utilisation des scripts personnalisés, •Interface web conviviale et configurable, •Import / Export de modèles en XML;	•Protocoles : HTTP, SNMP,	•Interface permettant l'intégration simple des plugins;

*Ce logiciel a fait l'objet de notre projet.

Conclusion

Dans ce chapitre, on a présenté les caractéristiques principales des principaux logiciels de supervision en open et closed source.

Il en ressort qu'un bon moniteur de supervision doit englober le maximum des avantages et pouvoir se remédier aux maximum des lacunes et limitations afin de converger et atteindre un niveau de supervision et de fiabilité optimum.

Pour cela, la mise en place d'un tel moniteur exige un bon choix de plate-forme de développement pour conduire à la réalisation d'une architecture distribuée fiable et robuste.

Chapitre4

Conception des solutions choisies

a. *Présentation de CACTI*

Cacti est un outil de graphage à la fois puissant, rapide et relativement simple d'utilisation et de prise en main. Il se distingue par l'interface graphique complète de paramétrage qu'il propose et les nombreuses options de personnalisation qu'il offre. Il possède les caractéristiques suivantes :

- Gratuit/Sous licence GNU v2 Open Source.
- Fonctionne sous différentes plateformes dont GNU/Linux et Microsoft Windows.
- Basé sur RRDTool pour le système graphique et la conservation des données.
- Permet de récupérer les données à grapher en SNMP ou grâce à des scripts librement réalisables.
- Configurable grâce à une interface web sécurisée très conviviale.
- Graphiques totalement personnalisables avec un système de modèles exportables en XML

Nous allons tout d'abord voir les pré-requis à posséder avant d'installer cet outil, en présentant aussi les outils annexes qu'il requiert. Nous allons ensuite nous attacher à expliquer les bases concernant l'installation du programme et l'utilisation de celui-ci.

b. *Pré-requis*

❖ *RRDTool*

RRDTool (Round Robin Database Tool) n'est pas un logiciel à proprement parler. C'est un ensemble d'outils permettant de stocker des données et de les restituer sous forme de graphiques.

Les données sont organisées selon un format très compact (les bases RRD), qui ne retient que les données nécessaires à la création des graphes.

L'auteur de cette suite d'outils est Tobias Oetiker, le créateur de MRTG. On peut dire que Cacti est une sorte de frontend à RRDTool, car il sert d'interface graphique à la création et à la manipulation de ces bases RRD (bien que ce ne soit pas son seul rôle).

❖ *SNMP en cacti*

L'utilisation que Cacti fait du SNMP est en mode pull (Cacti vient récupérer des données sur le matériel réseau en l'interrogeant). Il faut savoir que le matériel réseau lui-même peut envoyer des informations (des « trappes ») via le protocole SNMP à un collecteur de données lorsqu'il se produit un évènement important (coupure réseau, défaillance matérielle, etc.) mais Cacti ne sait pas les exploiter.

c. *Installation de CACTI* **[9-14]**

Cacti utilise RRDTool, PHP, SNMP et MySQL. Tous ces graphiques permettront à l'administrateur réseau d'anticiper et de résoudre les problèmes réseaux et systèmes.

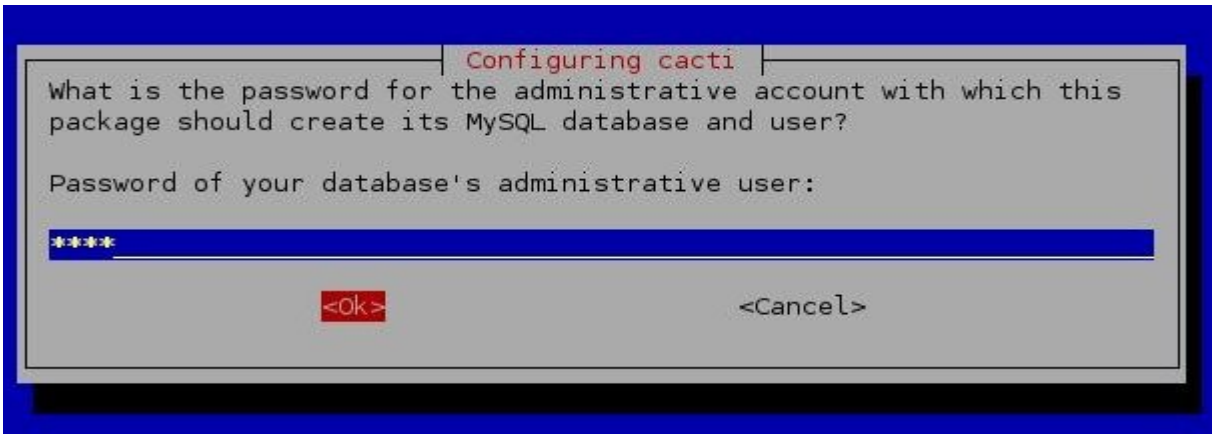
✓ Installer les dépendances (dont un LAMP)

```
# apt-get install apache2 libapache2-mod-php5 php5 php5-cli php5-mysql php5-gd php5-snmp mysql-client mysql-server libmysqlclient15-dev snmp  snmpd rrdtool
```

✓ *Installer CACTI*

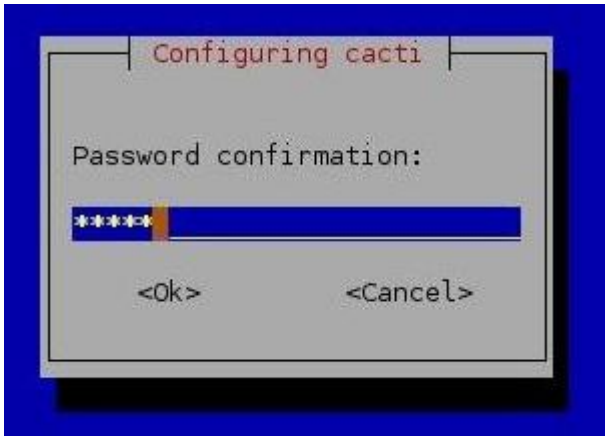
```
#apt-get install cacti
```

✓ O*n doit configurer les paramètres de MYSQL via un Assistant*

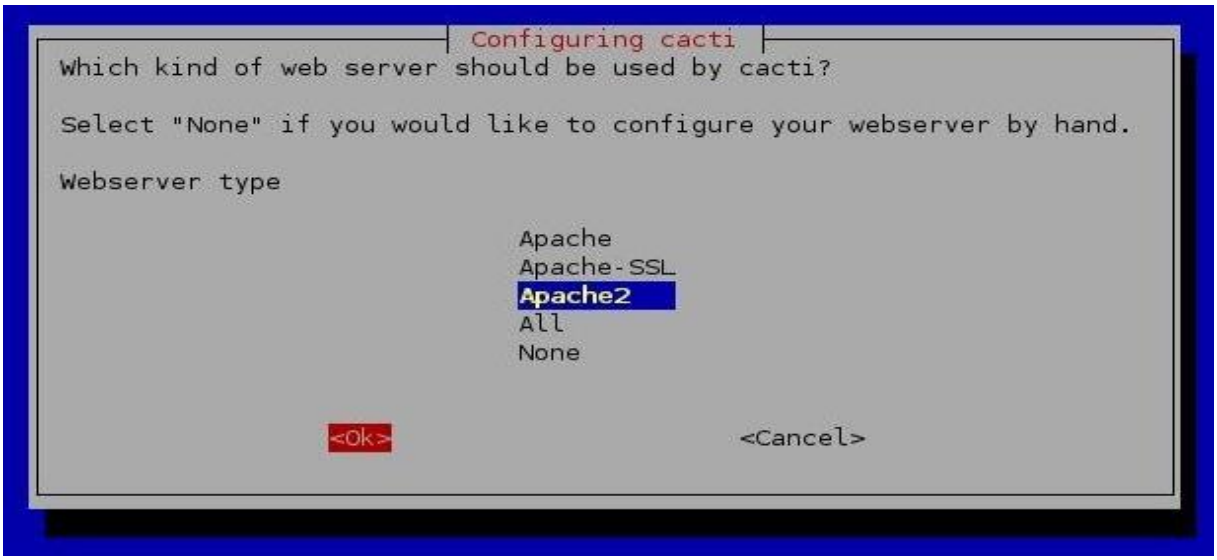


✓ Nouveau MySQL cacti user password:

✓ Confirmer MySql cacti user password

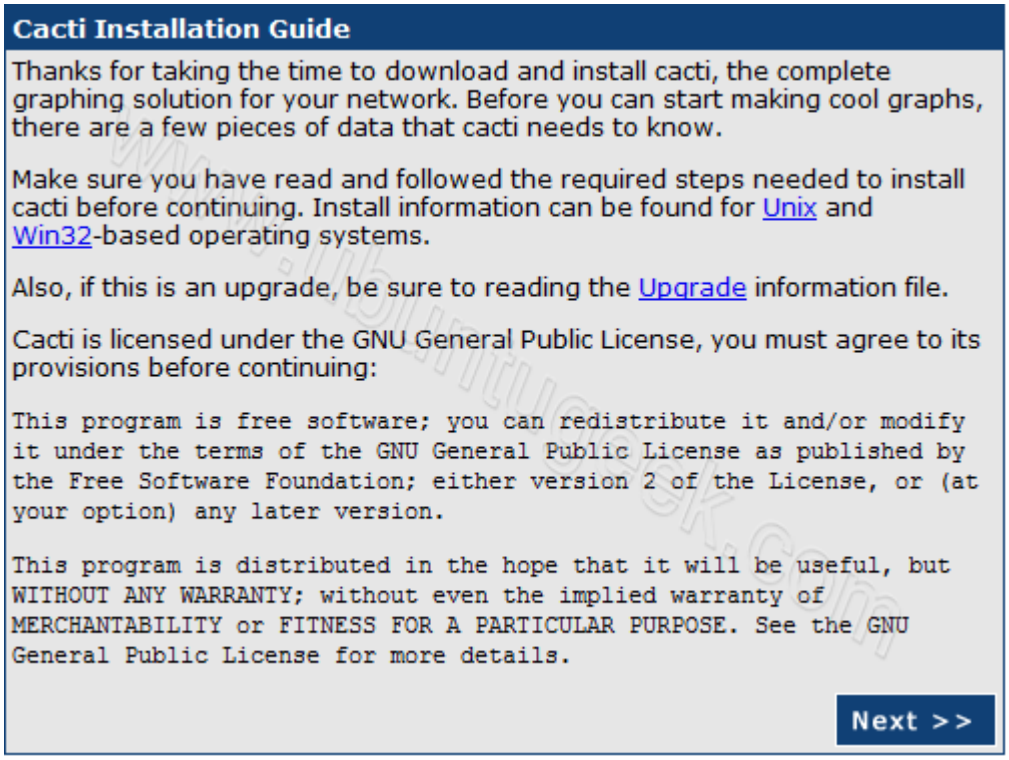


✓ Web server utilisé par cacti :

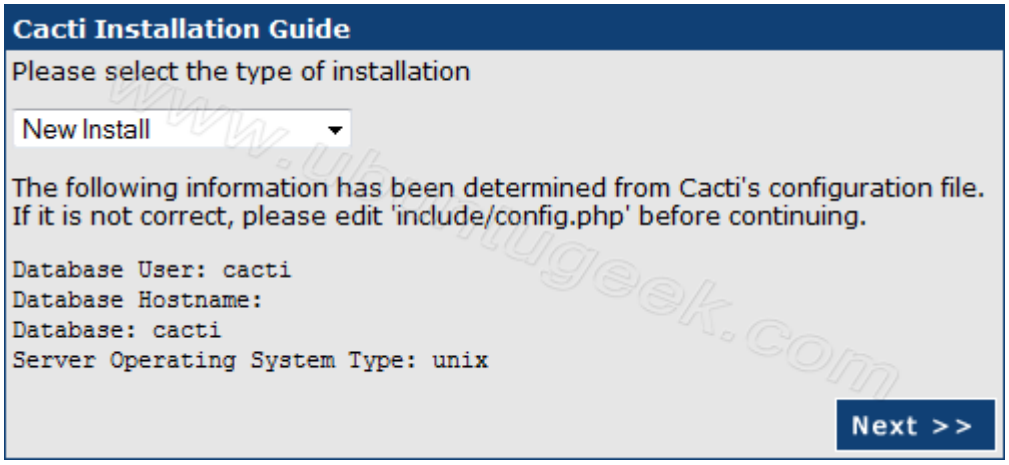


Cacti est maintenant prêt a être utilisé via: **http://localhost/cacti**

Cacti License:



Vous devez sélectionner le type d'installation comme nouvelle installation et cliquez sur continuer.

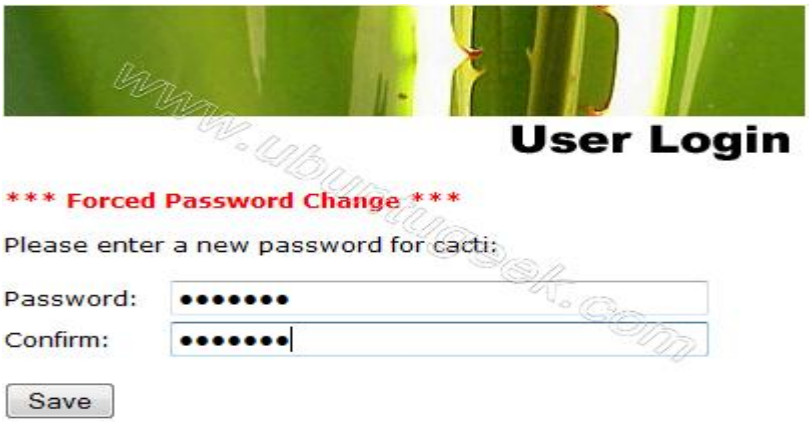


Vérifiez si les outils requis sont correctement vu par cacti

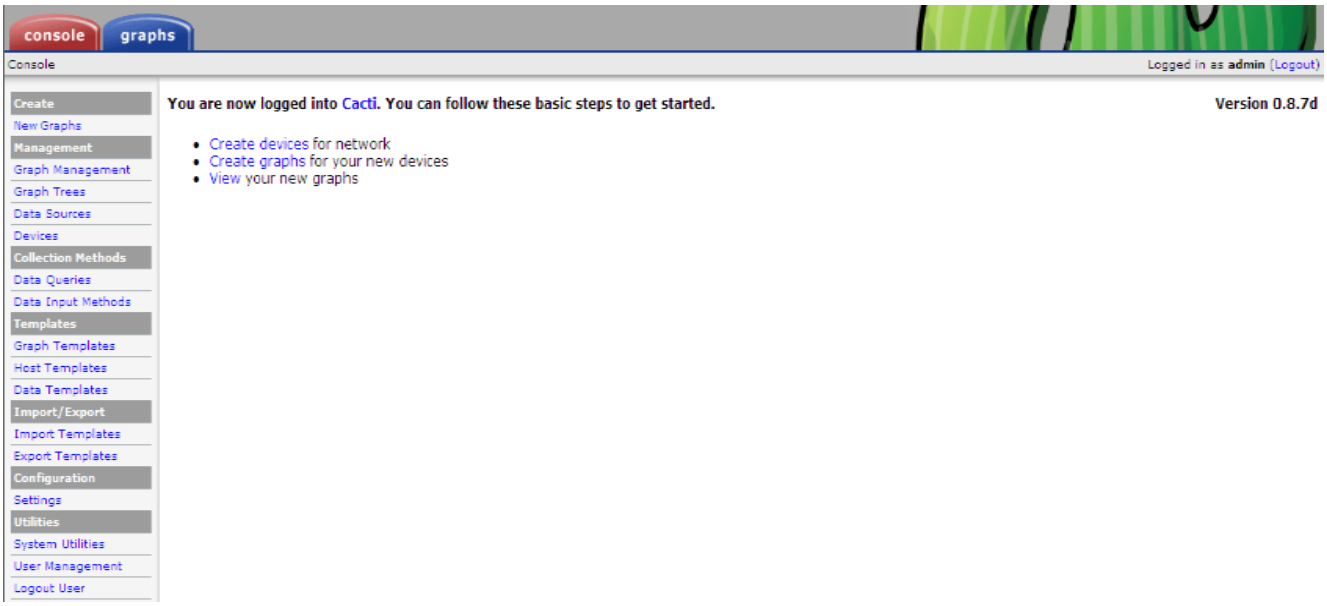
Maintenant l'écran de connexion de cacti s'affiche comme suit :

Ici, on a avait besoin d'entrer le nom d'utilisateur et le mot de passe comme admin/admin, puis cliquez sur login

La première fois il nous invite à changer le mot de passe de l'utilisateur admin cacti pour des raisons de sécurité, puis on clique sur Enregistrer



Une fois vous connecter, l'écran suivant s'affiche comme ci-dessous :



d. *Configuration de CACTI :*

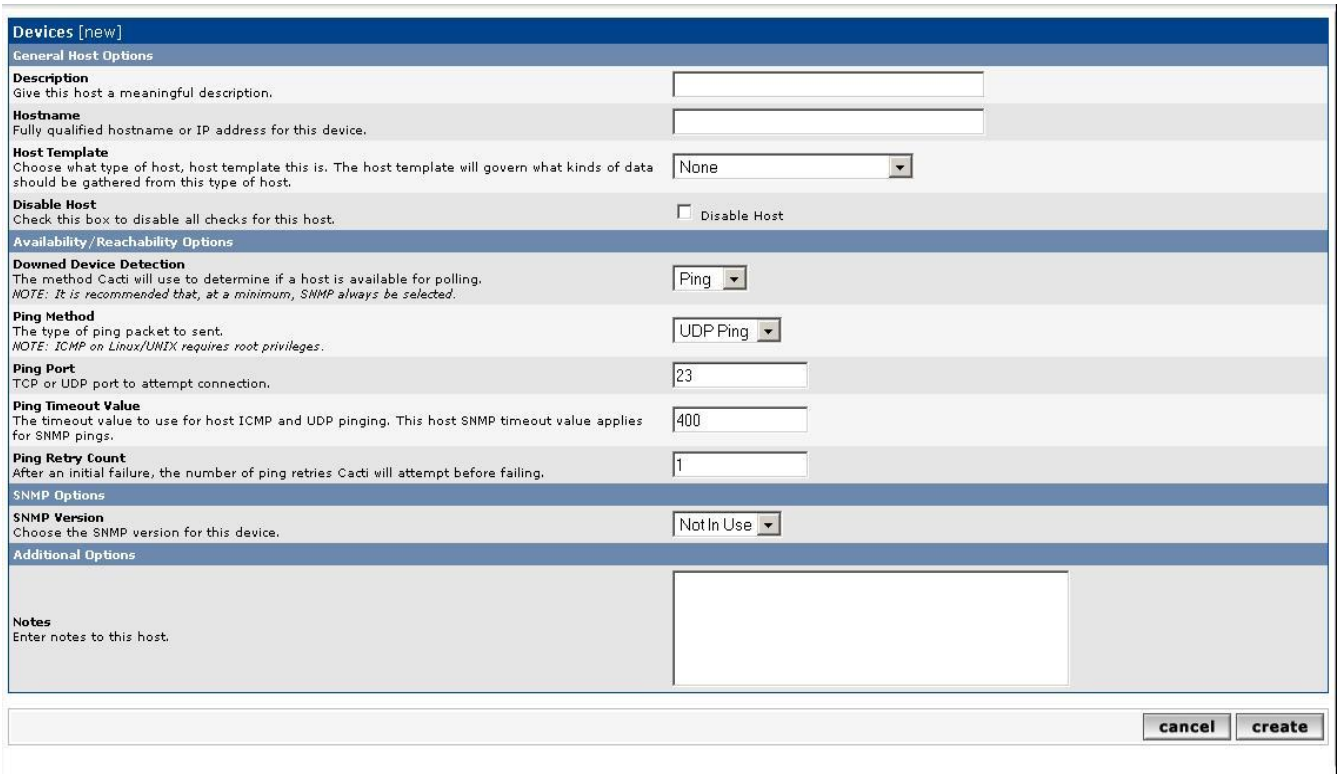
Faire un graphique d'un hôte pour la première fois se fait simplement en 3 étapes :

1. Créer l'hôte
2. Créer le graphique
3. Déclarer l'hôte dans l'arbre de présentation

- **Créer l'hôte :**

  Dans la catégorie MANAGEMENT, cliquez sur DEVICES, puis sur ADD en haut à droite.

Le formulaire propose les champs suivants :



- **Description** : nom de l'hôte qui apparaîtra dans Cacti et non une véritable description
- **Hostname** : adresse IP ou nom DNS de l'hôte
- **Host Template** : modèle de template qui sera appliqué sur l'hôte (on peux créer un modèle dans lequel on indique tous les scripts qui s'appliqueront sur un hôte)

- **Disable Host** : désactive l'hôte
- **SNMP Community** : nom de la communauté SNMP utilisé pour la lecture (par défaut : public)
- **SNMP Username** et **SNMP Password** : login et mot de passe de l'utilisateur autorisé lorsque le SNMP est de version 3
- **SNMP Version** : version du protocole SNMP (par défaut : 1)
- **SNMP Port** : port UDP du serveur SNMP (par défaut : 161)
- **SNMP Timeout** : temps de réponse maximum à Cacti

Cliquez sur CREATE. Cacti affiche alors la liste des hôtes créés, c'est-à-dire celui que l'on vient de faire à l'instant, ainsi que le localhost.

- **Créer le graphique :**

Dans la catégorie CREATE, cliquez sur NEW GRAPHS. Choisissez dans le menu déroulant, l'hôte qui nous intéresse. On choisit les graphes qu'on veut afficher puis on clique sur create.

- **Déclarer l'hôte dans l'arbre de présentation :**

Nous allons indiquer à Cacti comment nous présenter les différents graphiques que vous allez créer. Dans la catégorie MANAGEMENT, cliquez sur GRAPH TREES.
Nous choisissons ici la catégorie dans laquelle va apparaître notre hôte. Par défaut il en existe déjà une, DEFAULT TREE.

Pour cela, cliquez sur ADD en haut à droite. Dans la case NAME, donnez un nom à votre catégorie. La case SORTING TYPE permet de choisir la façon dont Cacti va trier les différents hôtes :

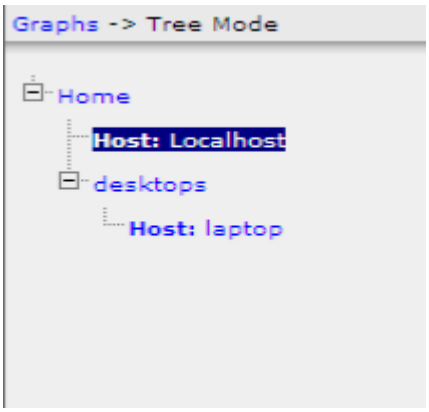
- **Manuel Ordering** : tri manuel
- **Alphabetic Ordering** : tri par ordre alphabétique
- **Numeric Ordering** : tri par valeurs numériques

Puis cliquez sur CREATE. Dans la nouvelle fenêtre, nous allons y inscrire l'hôte. Cliquez sur ADD.

Le menu TREE ITEM TYPE contient trois options :

- **Header** : la branche d'un arbre. Title contient le nom de la branche, et Sorting Type la méthode de tri.
- **Graph** : affiche un graphique. Graph permet de choisir quel graphique afficher, Round Robin Archive permet de choisir sur quelle période s'étend le graphique
- **Host** : affiche tous les graphiques d'un hôte, l'option Host permet de choisir quel hôte, Graph Grouping Style indique l'ordre de présentation

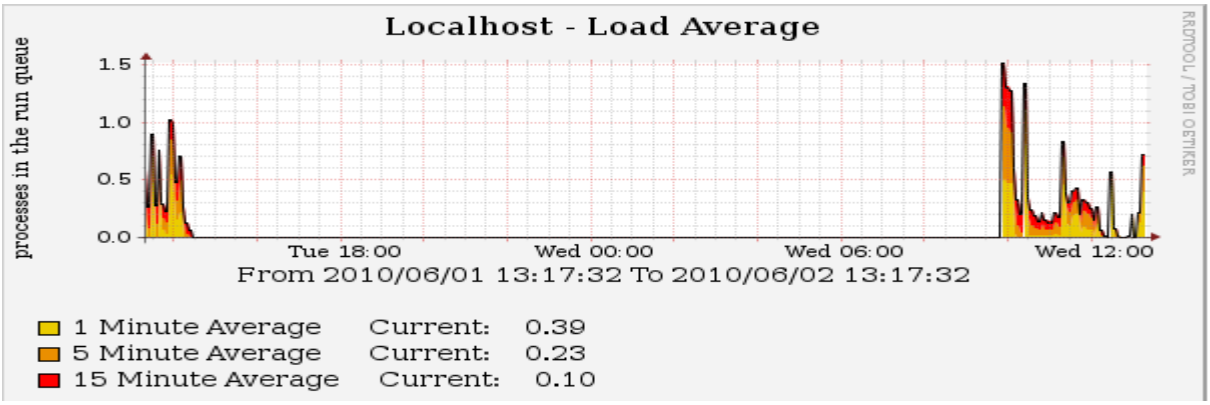
Puis cliquez sur CREATE. Maintenant votre hôte apparaît dans la catégorie que vous avez créée. Vous pouvez admirer le résultat en cliquant sur le bouton GRAPHS en haut à gauche. Il se peut que le graphique mette quelques minutes à se créer.



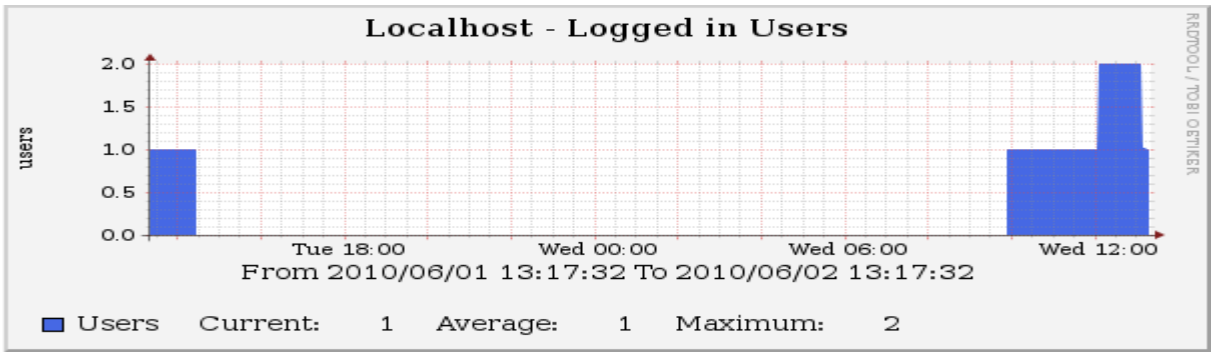
Une fois ces étapes réalisées les graphes choisis sont affiché dans l'onglet graphe comme suit :

Exemples de graphe pour localhost :

Graphe « Moyenne de téléchargement »

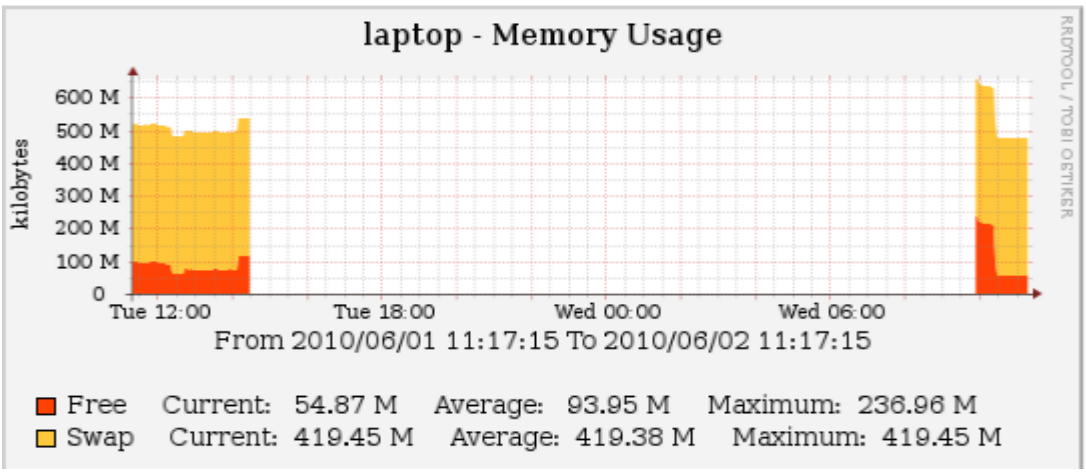


Graphe « Utilisateurs en ligne »

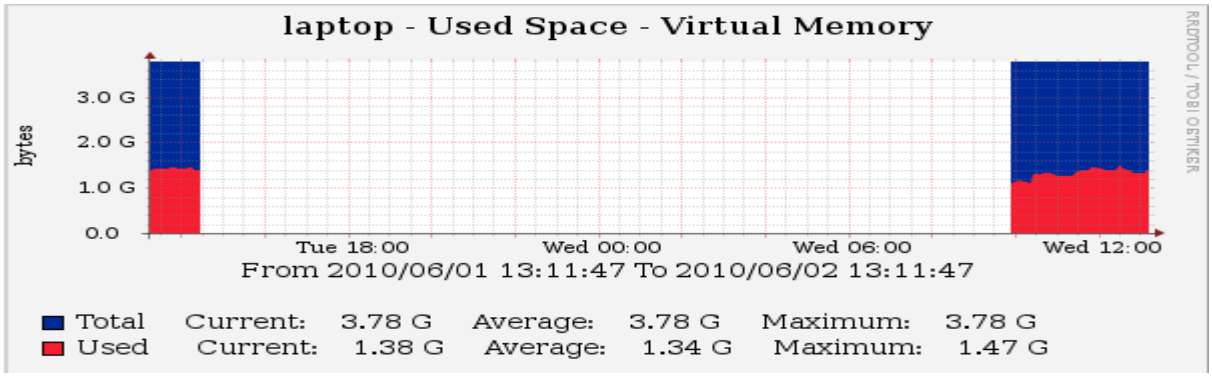


Exemples de graphe pour le host nommé laptop :

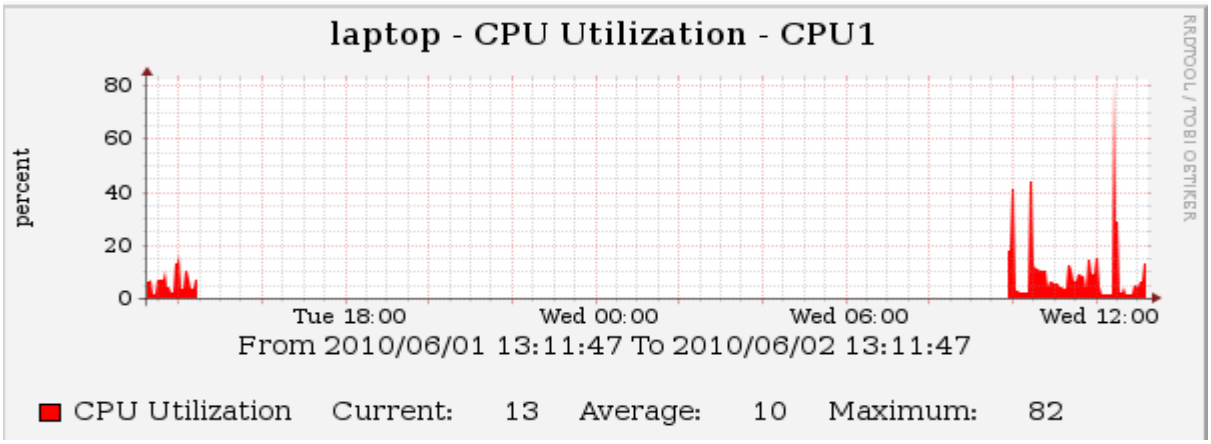
Graphe « Utilisation de mémoire »



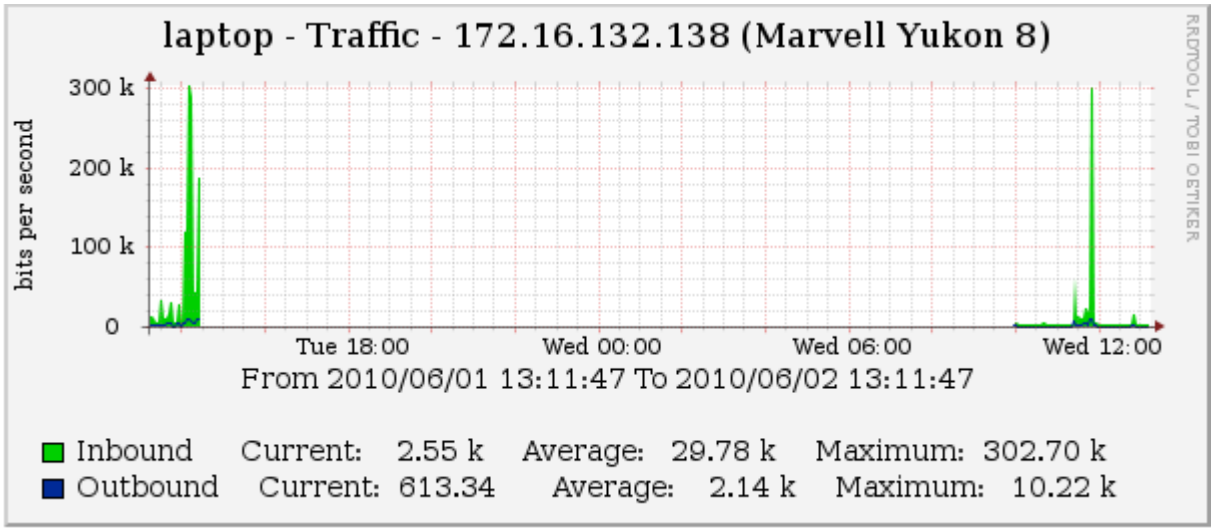
Graphe « Espace utilisé dans la machine virtuelle »



Graphe « Utilisation de CPU »



Graphe « Traffic du carte réseau »



a. *Présentation :*

Zabbix est un logiciel open source créé par Alexei Vladishev et développé sous licence GPL. Ce projet existe depuis 2002, il permet notamment de :

- S'assurer du bon fonctionnement de l'ensemble du parc informatique ;
- Détecter d'éventuelles baisses de performance ;
- Anticiper les pannes ;
- Remonter les pannes.

Un autre intérêt de Zabbix est son architecture complète et extensible de type client/serveur. Le serveur collecte les données et les stocke dans une base de données (Mysql, PostgreSQL...). Pour fournir ces données, zabbix propose trois mécanismes :

- collecte directe : effectuée par le serveur et permet d'effectuer des tests simples (ping, port actif...).
- requêtes SNMP
- agent zabbix : qui donne accès à des données prédéfinies (consommation mémoire, occupation CPU...) et peut être étendu par le biais de scripts. Ces scripts peuvent être réalisés en tout langage, ils doivent juste écrire leurs résultats sur la sortie standard.

Les graphes proposés par Zabbix sont nombreux et très finement configurables. Surtout Zabbix intègre un mécanisme d'alerte par mail ou SMS permettant d'attirer votre attention d'où l'émergence d'un problème ou de la dégradation de performances de votre machine.
Enfin Zabbix est multiutilisateurs. Les données mesurées sont mises en forme et disponible à la consultation à partir d'une interface WEB.
Il est clair que l'activation de toutes ses fonctionnalités va requérir du temps et des ressources que le suivi d'un seul PC personnel ne justifie probablement pas.

b. Structure du logiciel

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.

- Le serveur de données

ZABBIX utilise MySQL, PostgreSQL ou Oracle pour stocker les données. Selon l'importance du nombre de machines et de données à surveiller, le choix du SGBD influe grandement sur les performances. Il existe une section relative à ce choix dans le manuel officiel.

- L'interface de gestion

Son interface web est écrite en PHP. Elle agit directement sur les informations stockées dans la base de données. Chaque information nécessaire au serveur de traitement étant réactualisée automatiquement, il n'y a pas d'action à effectuer sur le binaire pour lui indiquer qu'il y a eu une mise à jour.

Cette interface dispose des fonctionnalités principales suivantes:

- Affichage des données et état des machines
- Génération de graphiques (évolution des données et état des machines/liens)
- Classement et groupement des machines surveillées
- Auto découverte de machines et ajout automatique
- Gestion fine des droits d'accès pour les utilisateurs de l'interface

- Le serveur de traitement

Il s'agit d'un daemon binaire existant pour Linux, BSD et divers Unix. Il offre diverses options de monitoring. La vérification simple permet de vérifier la disponibilité ainsi que le temps de réponse de services standards comme SMTP ou HTTP sans installer aucun logiciel sur l'hôte surveillé. 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, l'espace disque... Le logiciel peut réaliser le monitoring via SNMP.

Fonctionnalité intéressante, il est possible de configurer des "proxy Zabbix" afin de répartir la charge ou d'assurer une meilleure disponibilité de service.

c. *Pré-requis*

- Disposer des droits d'administration
- Avoir activé l'accès aux dépôts Universe ;
- Avoir un serveur Web installé et gérant le PHP et MySQL (ou PostgreSQL), apache2,
- Net-Snmp libraries

d. *Installation de Zabbix* [15-19]

✓ *Préparation du serveur*

On tape la commande ci-dessous:

```
sudo apt-get install build-essential gnustep-make

sudo apt-get install linux-headers-$(uname -r)
```

✓ Création de l'utilisateur zabbix:

```
sudo adduser zabbix

enter your password
```

✓ Ajout de l'utilisateur zabbix au groupe Admin

```
Sudo adduser zabbix admin
```

✓ Installation des paquets nécessaires:

```
sudo su zabbix
```

```
sudo apt-get install apache2

sudo apt-get install postgresql-8.3 postgresql-server-dev-8.3

sudo apt-get install php5 php5-gd php5-pgsql snmp libsnmp-dev snmpd libcurl4-openssl-dev fping libiksemel3 libiksemel-dev
sudo apt-get install phppgadmin
```

✓ Maintenant on se connecte en tant que root

```
sudo su -
```

✓ Configuration de la base de données:

```
sudo -u postgres psql postgres
\password postgres
password: maroc
\q;

sudo -u postgres createuser --superuser zabbix

sudo -u postgres createdb zabbix
```

```
sudo  gedit /usr/share/phppgadmin/conf/config.inc.php

CHANGE:     $conf['extra_login_security'] = true;

TO:              $conf['extra_login_security'] = false;

sudo  gedit /etc/phppgadmin/apache.conf

CHANGE:      deny from all

TO:               allow from all
```

✓ Installation de zabbix :

```
sudo su zabbix

cd /home/zabbix

 wget http://optusnet.dl.sourceforge.net/sourceforge/zabbix/zabbix-1.6.6.tar.gz

tar zxvpf zabbix-1.6.6.tar.gz

cd zabbix-1.6.6/create/schema

cat postgresql.sql | psql zabbix

cd ../data

cat data.sql | psql zabbix
```

```
cat images_pgsql.sql | psql zabbix

cd ..

cd ..

sudo ./configure --enable-server --enable-agent --with-pgsql --with-net-snmp --with-jabber=/usr/ --with-libcurl

sudo make install
```

✓ Préparation du reste du système :

On ajoute les ports ci dessous au fichier services :

```
sudo gedit /etc/services

zabbix_agent 10050/tcp
zabbix_trap 10051/tcp
```

✓ Création de répertoire zabbix :

```
sudo mkdir /etc/zabbix

sudo chown -R zabbix.zabbix /etc/zabbix/

cp misc/conf/zabbix_* /etc/zabbix/
```

On édite le fichier configuration de l'agent comme suit :

```
sudo gedit  /etc/zabbix/zabbix_agentd.conf
```

Server=127.0.0.1

On supprime # de ListenIP=127.0.0.1

On édite le fichier configuration du serveur comme suit:

```
sudo gedit  /etc/zabbix/zabbix_server.conf
```

Database user

DBUser=zabbix

Database password

DBPassword=maroc

On supprime # de ListenIP=127.0.0.1

```
Sudo  /etc/init.d/zabbix-agent restart

Sudo   /etc/init.d/zabbix-server restart
```

✓ Création de l'interface web zabbix :

```
# sudo mkdir /var/www/zabbix
# sudo cp -rf ./frontends/php/* /var/www/zabbix/
# sudo gedit /etc/php5/apache2/php.ini
max_execution_time = 300
date.timezone = Africa/ Casablanca
# sudo  /etc/init.d/apache2 restart
```

✓ Lancement du serveur:

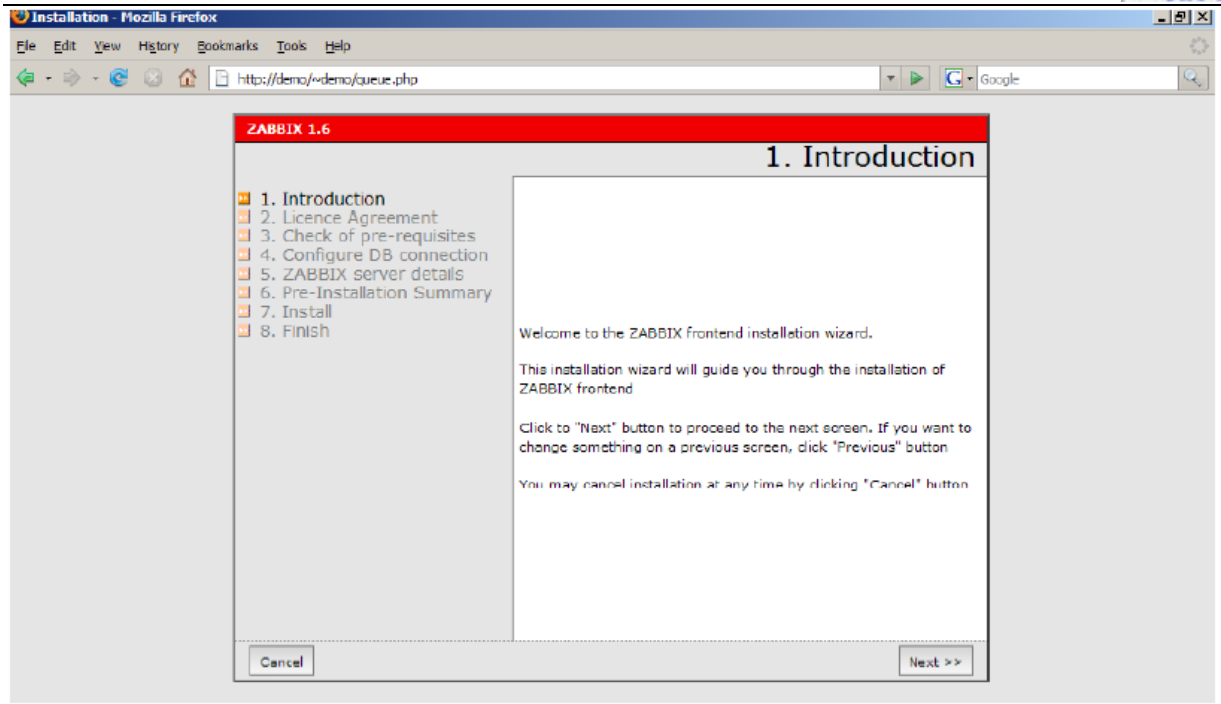
```
# /usr/local/sbin/zabbix_server
```

En cas de problème, le serveur génère des logs dans le fichier */tmp/zabbix_server.log*.

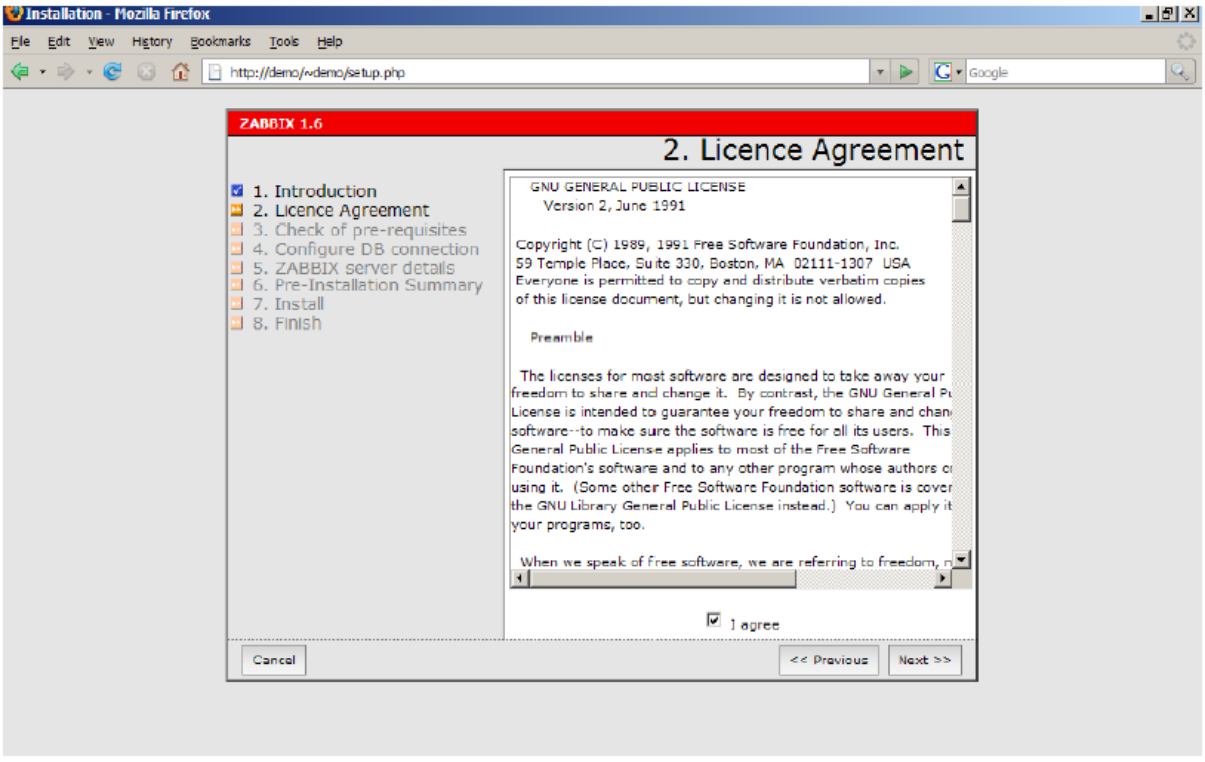
Se connecter à l'interface Web: http://localhost/zabbix/ ou http://127.0.0.1/zabbix/

Puis suivre le wizard de configuration:

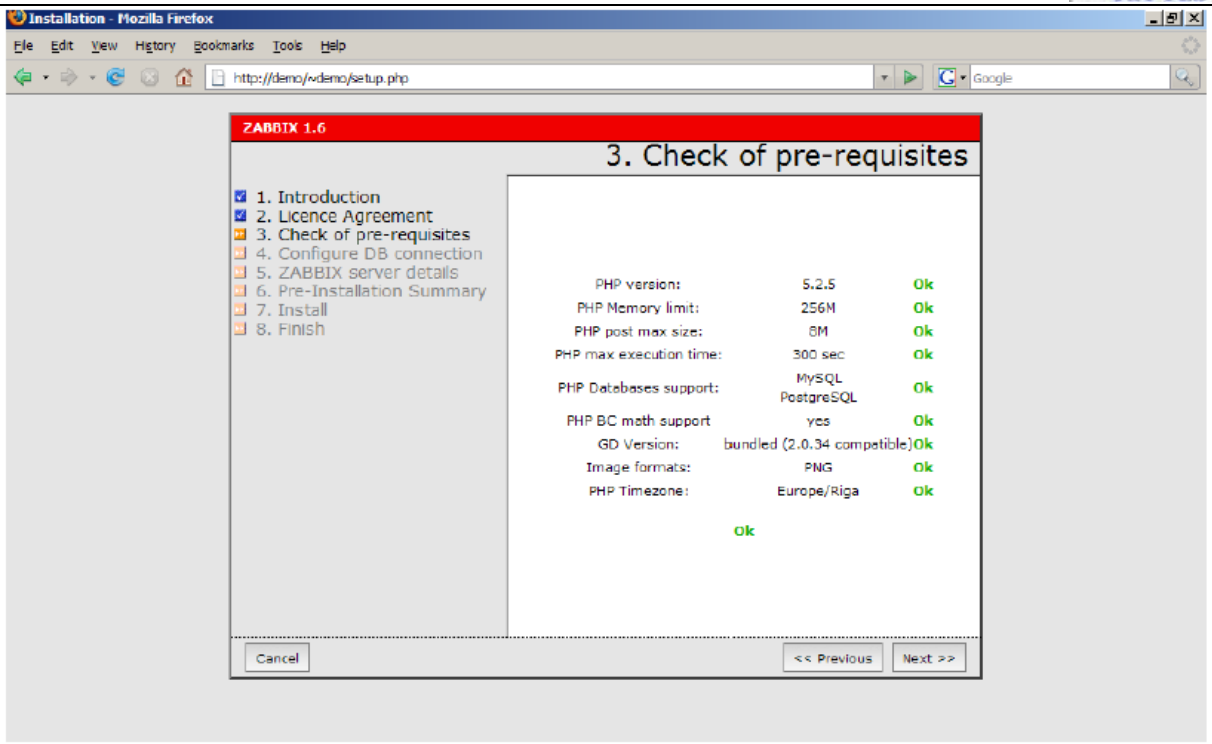
❖ Introduction



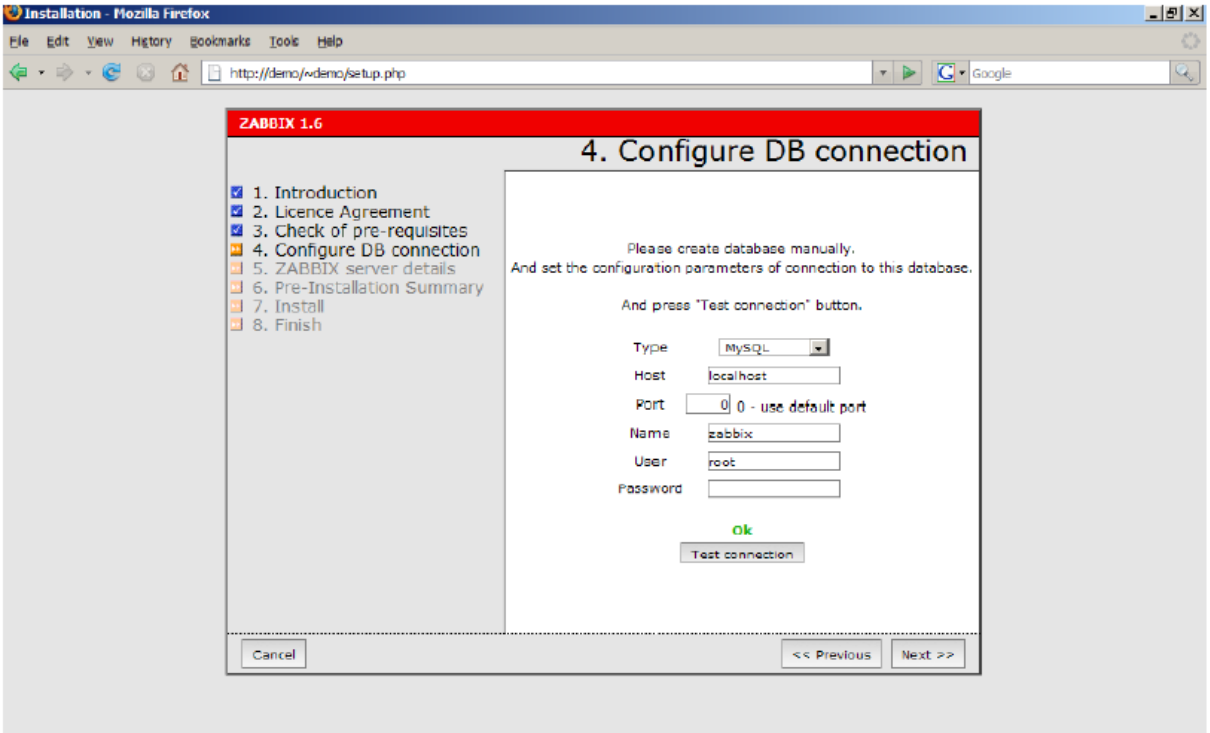
❖ Licence - I agree / suivant

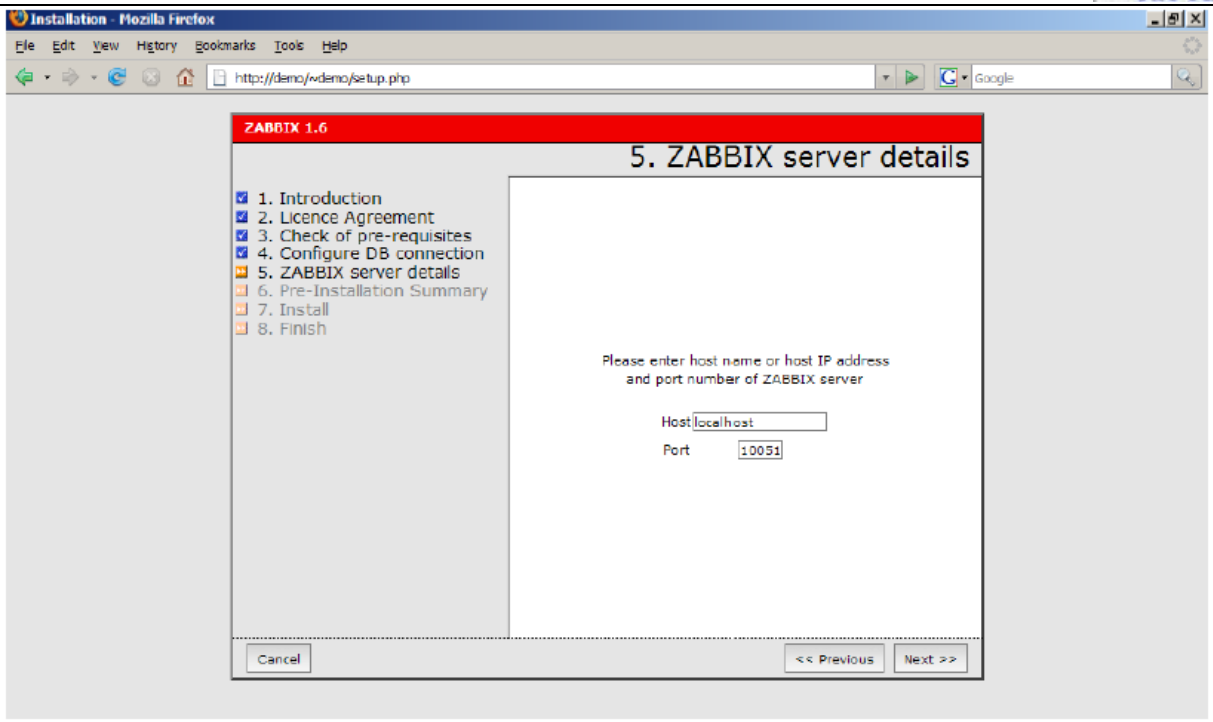


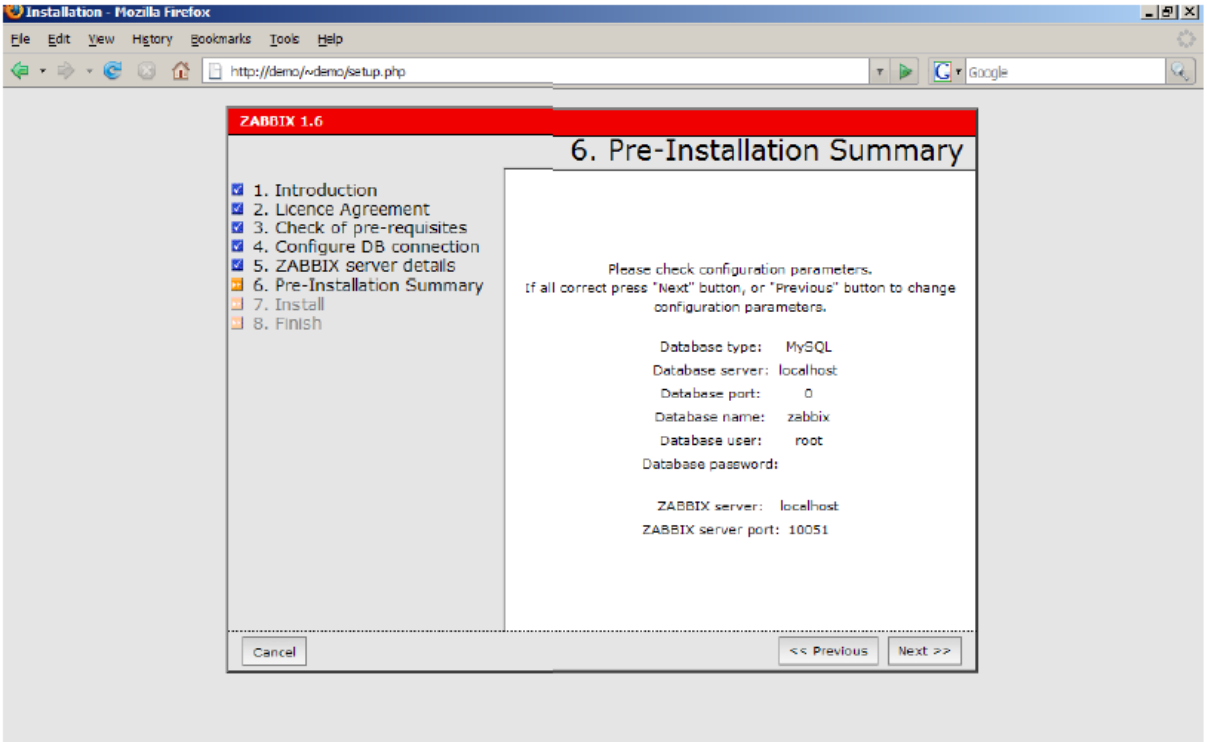
❖ Pré-requis - Vérifier que tout est OK puis suivant



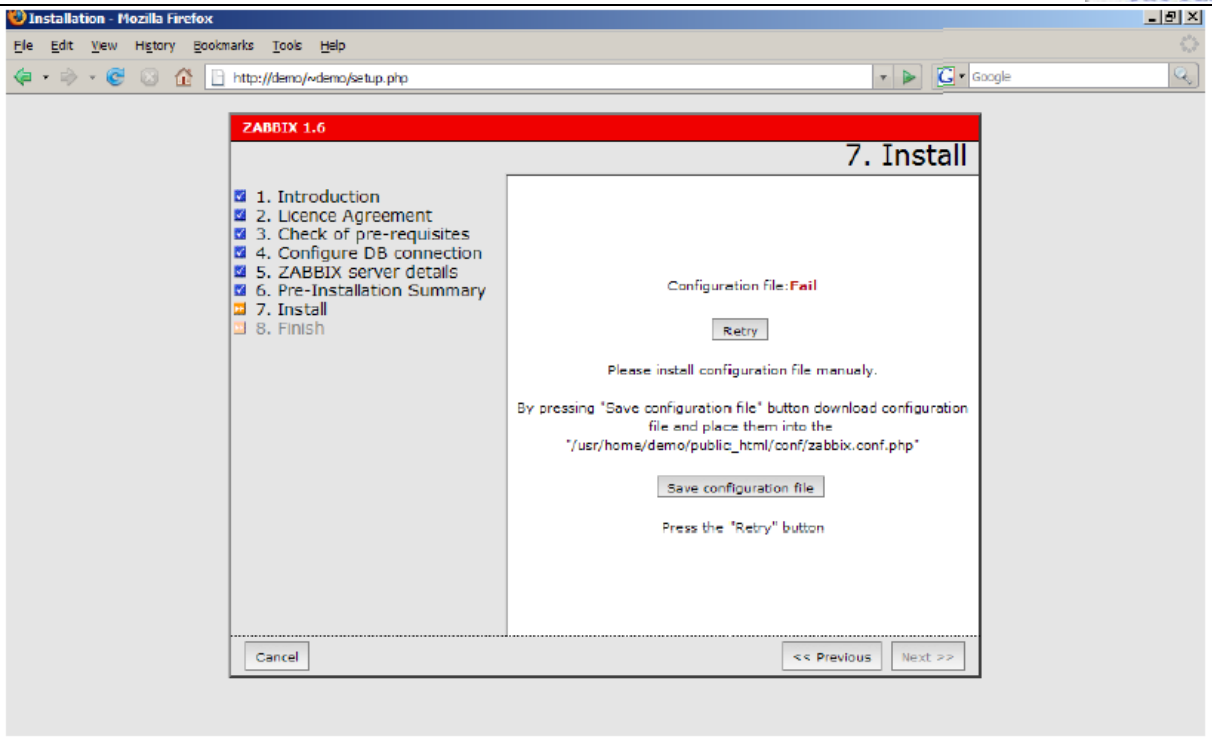
❖ Configuration base de données puis suivant :

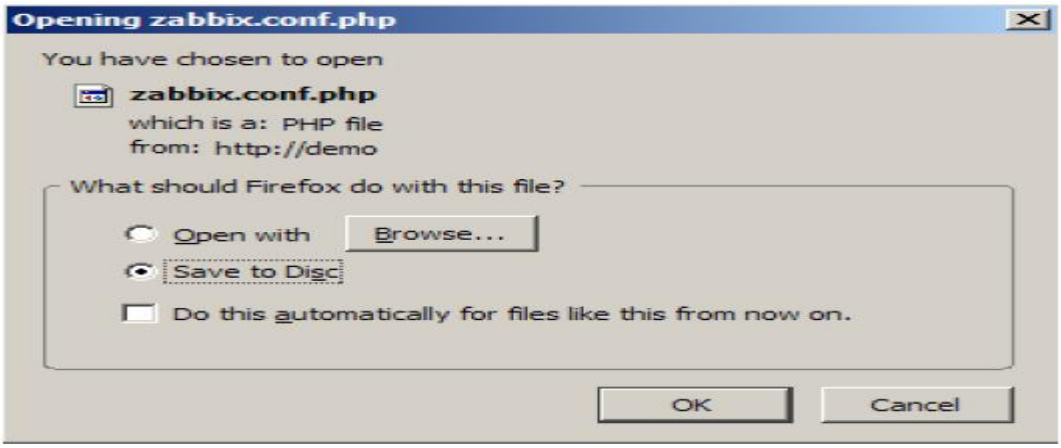


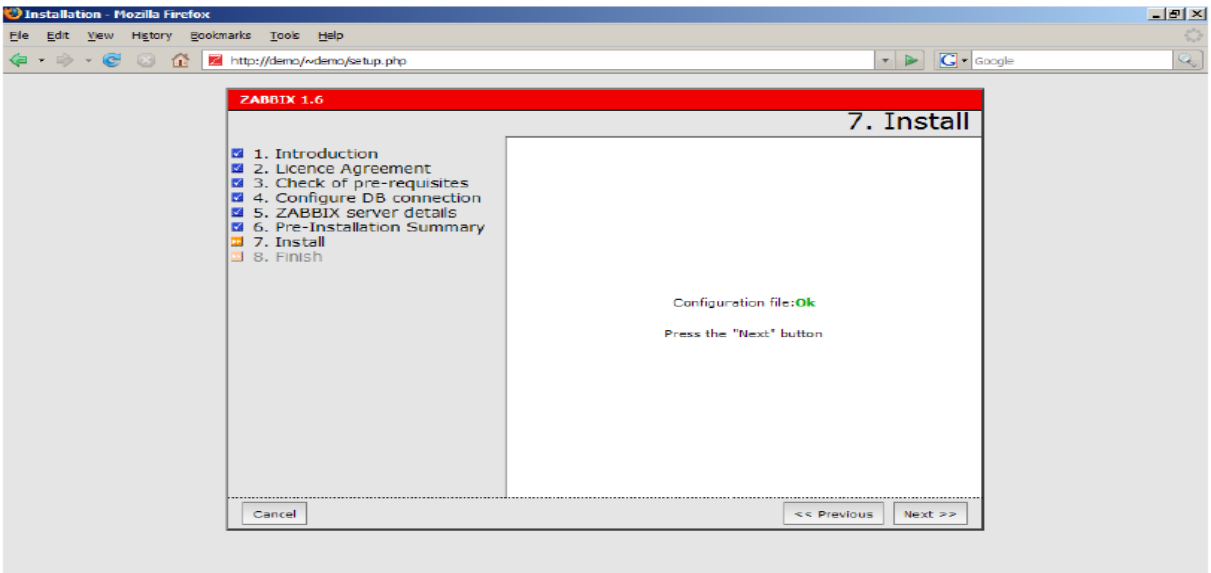




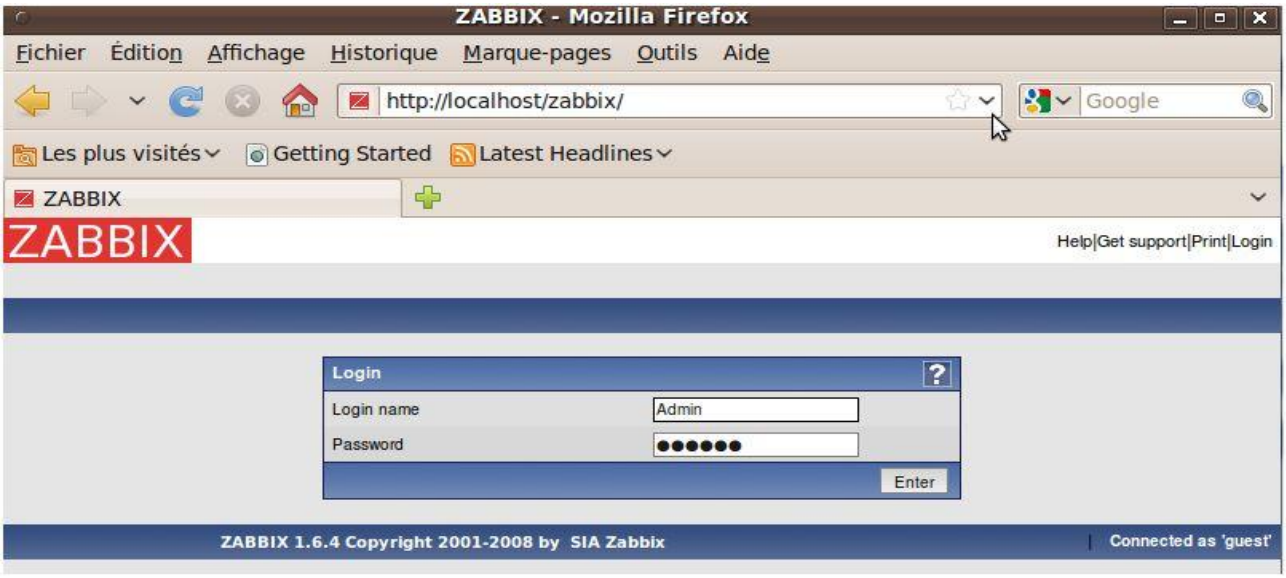
- Install - Cliquer sur le bouton "Save configuration file" et télécharger manuellement le fichier zabbix.conf.php dans le répertoire /var/www/zabbix/conf puis cliquez sur Next

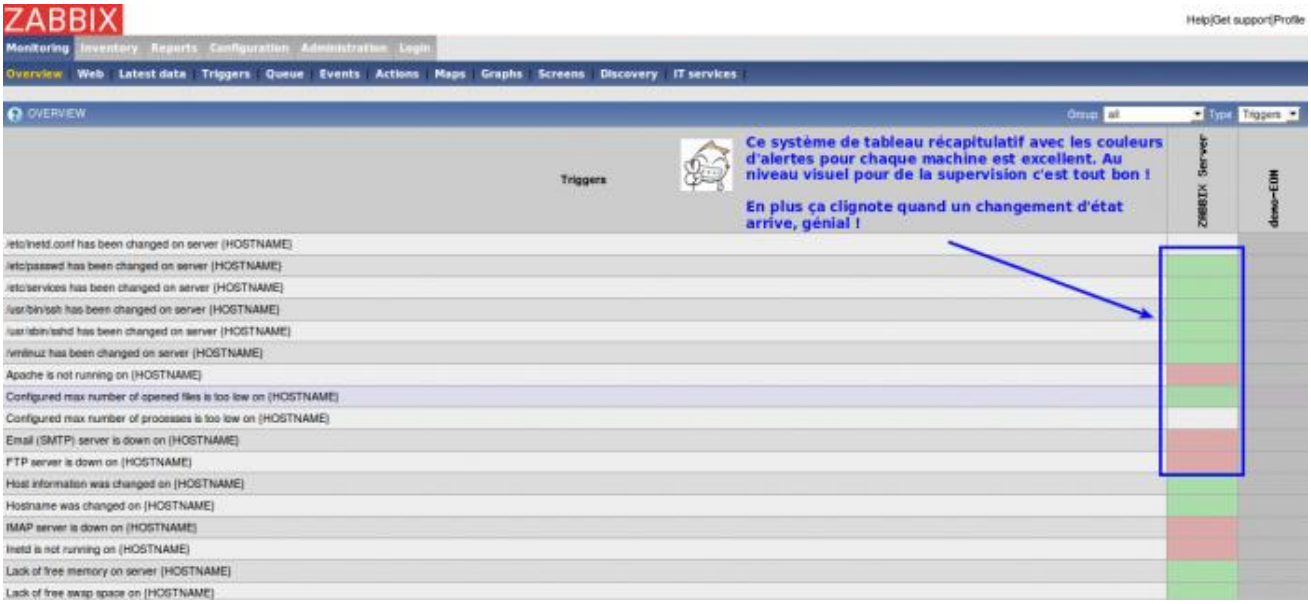

Installation - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://demo/wdemo/setup.php
Google
ZABBIX 1.6
7. Install
1. Introduction
2. Licence Agreement
3. Check of pre-requisites
4. Configure DB connection
5. ZABBIX server details
6. Pre-Installation Summary
7. Install
8. Finish
Configuration file:Fail
Retry
Please install configuration file manualy.
By pressing "Save configuration file" button download configuration file and place them into the "/usr/home/demo/public_html/conf/zabbix.conf.php"
Save configuration file
Press the "Retry" button
Cancel
<< Previous
Next >>


Opening zabbix.conf.php
You have chosen to open
zabbix.conf.php
which is a: PHP file
from: http://demo
What should Firefox do with this file?
Open with
Browse...
Save to Disc
Do this automatically for files like this from now on.
OK
Cancel


Installation - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://demo/wdemo/setup.php
Google
ZABBIX 1.6
7. Install
1. Introduction
2. Licence Agreement
3. Check of pre-requisites
4. Configure DB connection
5. ZABBIX server details
6. Pre-Installation Summary
7. Install
8. Finish
Configuration file:Ok
Press the "Next" button
Cancel
<< Previous
Next >>

Si l'installation se passe sans problème vous devriez être redirigé vers la page d'authentification du serveur Zabbix (login: Admin / password: zabbix).





d. ***Installation du client Zabbix***

Cette installation est à faire sur toutes les machines à surveiller. L'agent (le client) Zabbix existe précompilé sur de nombreux OS (Linux Ubuntu / Fedora, FreeBSD, Windows...).

Par exemple pour installer l'agent Zabbix sur une machine Linux Ubuntu, il suffit de faire:

```
# sudo apt-get install zabbix_agent
```

Il faut ensuite configurer les fichiers zabbix_agent.conf et zabbix_agentd.conf:

```
# sudo vi /etc/zabbix/zabbix_agent.conf
...
Server=adresse IP du serveur Zabbix
...
# sudo vi /etc/zabbix/zabbix_agentd.conf
...
Server=adresse IP du serveur Zabbix
...
```

Puis lancer le client:

```
# sudo /etc/init.d/zabbix-agent start
```

Pour installer un agent Zabbix sous Windows, il suffit de récupérer le binaire sur le site : http://www.suiviperf.com/zabbix/, de décompresser l'archive (via WinRAR) à la racine de votre disque c: et de créer un fichier c:\zabbix_agent.conf contenant la ligne suivante:

Server=*adresse IP du serveur Zabbix*

Puis de lancer l'exécutable c:\bin\win32\zabbix_agentd.exe

c. ***Paramétrage de Zabbix***

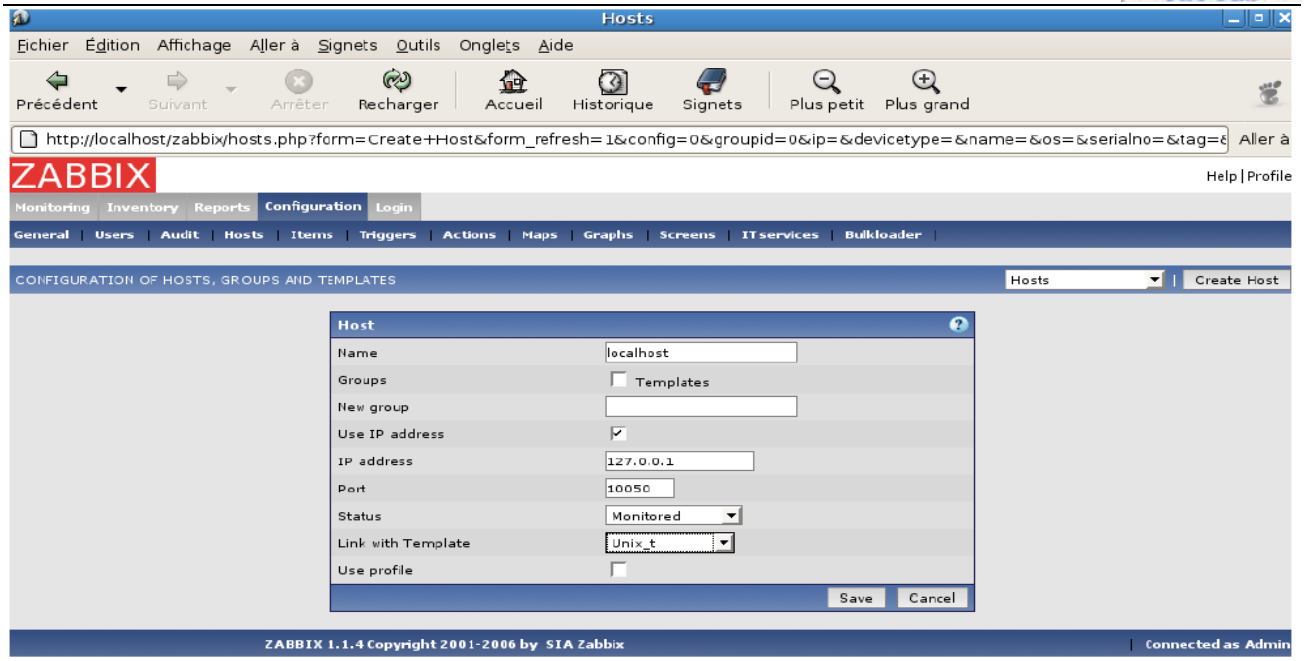
La première chose à faire une fois logué dans l'interface Web du serveur est de cliquer sur le lien Profile (en haut à droite) afin de modifier le mot de passe et la langue (Zabbix est traduit en Français).

Ensuite il faut ajouter des machines à surveiller (les machines ou l'on a installé le client Zabbix).

- **Création d'un hôte**

Vous allez intégrer votre PC local dans la liste des équipements que vous souhaitez que Zabbix suive. Cliquez sur le menu « Configuration » puis sur le sous-menu « hosts ».

Cliquez sur le bouton « create host » en haut à droite de la fenêtre. Vous allez alors voir apparaître le masque de saisie ci-dessous :



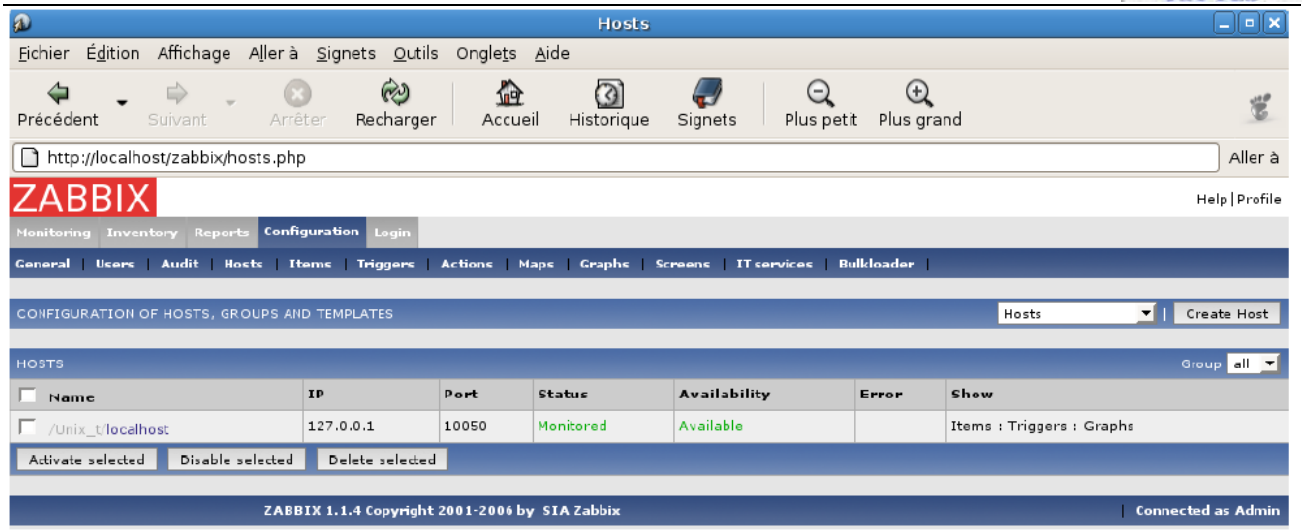
- Indiquez le nom de l'hôte local « localhost ».
- Cochez la case « use Ip Adress » et indiquez l'IP «127.0.0.1 » dans le champ « IP Adress »; Zabbix utilisera le port TCP 10050 pour communiquer avec l'agent installé sur cet hôte
- En choisissant l'option « Monitored » dans le champ « Status », vous allez activer le suivi de ce PC.

Enfin, choisissez le modèle « Unix_t » dans le champ intitulé « link with Template ». Ceci aura pour effet d'appliquer un certains nombres de réglage prédéfinis pour les hôtes de type « linux ». Il existe également un modèle pour les hôtes Windows. Vous pouvez aussi créer/modifiés autant de modèle d'hôte que vous le souhaitez.

Quand vous avez terminé la saisie, cliquez sur le bouton « Save ».

Zabbix va alors intégrer votre hôte et lui appliquer le modèle « Unix_t »

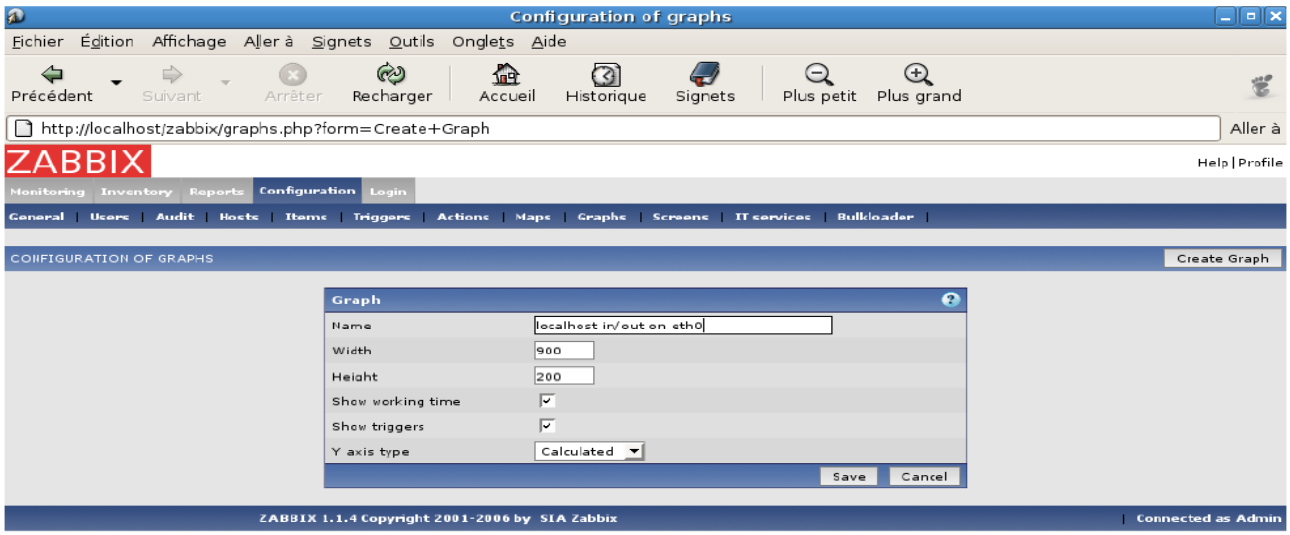
Désormais, le PC nommé « localhost » est présent dans la liste du menu « configuration » « host ». Vous remarquerez que le statut de cet hôte est « monitered » ce qui signifie que Zabbix l'a bien intégrée dans sa liste de PC à mesurer. La colonne "availability » contient la valeur «available » ce qui signifie que le serveur Zabbix a réussi a établir le dialogue avec l'agent installé sur « localhost ».



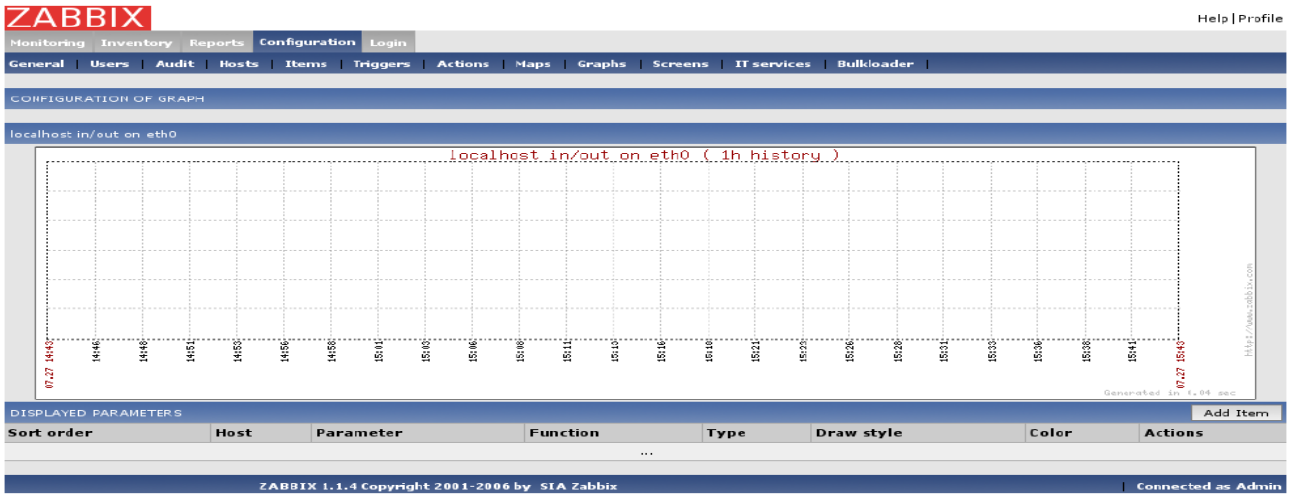
- **Création d'un « graph »**

Un « graph » dans le jargon de Zabbix est une représentation graphique de l'évolution d'une ou plusieurs donnes mesurées sur un ou plusieurs hôtes. Les données les plus récentes sont à droite du graphique. Par défaut, l'historique des données est affiché sur une période d'un n heure mais un filtre en bas de graphique permet de modifier la période consultée. Nous allons créer un « graph » montrant l'évolution dans le temps du trafic entrant et sortant sur la carte réseau eth0 du PC « localhost ». Pour cela, cliquez sur le menu « configuration », « graphs » puis sur le bouton « create graph ».

Remplissez le formulaire en nommant votre graphique (champs name). Laissez tous les autres réglages par défaut et validez la création du « graph » en cliquant sur le bouton « save ».



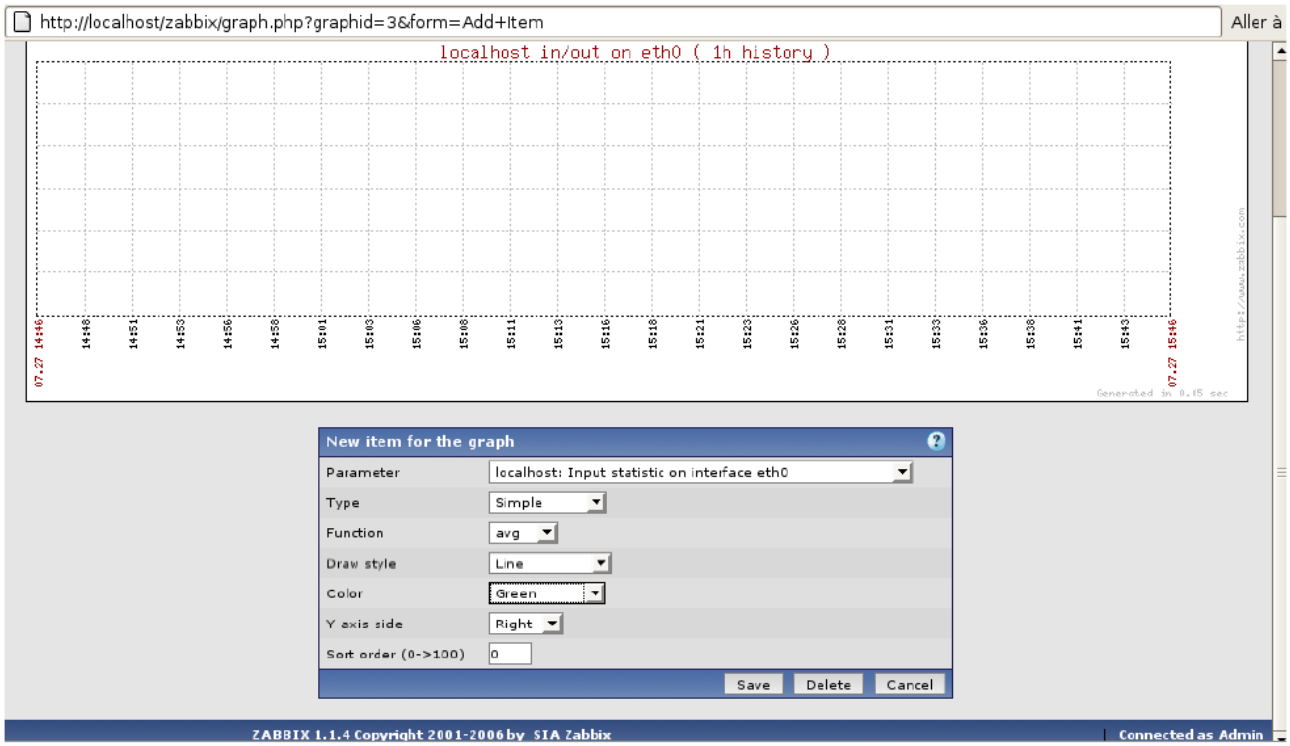
Zabbix vous affiche alors un graphique vide puisque nous n'avons pour l'instant indiqué aucune donnée.



Cliquez une première fois sur le bouton « add item » et remplissez le formulaire d'ajout de données au « graph ».

Dans le liste nommée « parameter », choisisssez « localhost: Input Statistic on interface eth0 » et choisissez la couleur verte (« green »).

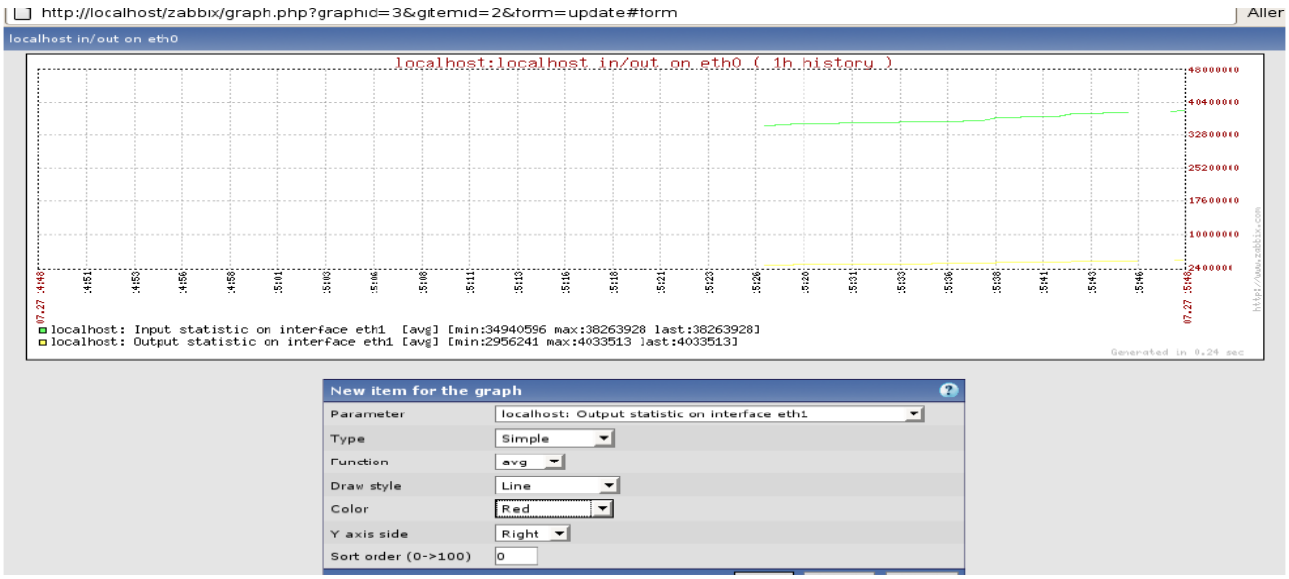
Validez en cliquant sur le bouton « save ».



Vous voyez déjà apparaître quelques informations graphiques. Cliquez une seconde fois sur « add item » et remplissez le formulaire d'ajout de données au « graph ».

Dans le liste nommée « parameter », choisissez « localhost: Output Statistic on interface eth0 » et choisissez la couleur rouge (« red »).

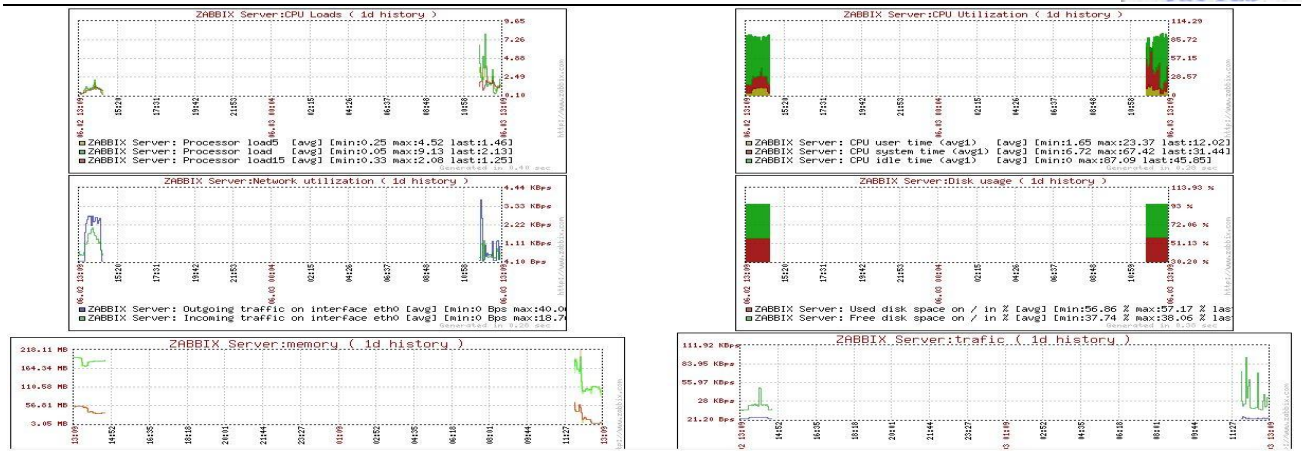
Validez en cliquant sur le bouton « save ».



On peut aussi créer :

- Ecran :« screen »

Ils vous permettent de paramétrer un affichage avec plusieurs éléments en aperçu. Par la suite, en cliquant sur le graphique, vous aurez accès à celui-ci dans sa taille originale. Un écran est une grille de graphiques, composée entièrement par l'administrateur. Ouvrez l'outil « Screens » puis cliquez sur le bouton « Create screen ». Vous n'aurez qu'à lui rentrer un nom (pertinent) et une dimension (en lignes et en colonnes). Ces dimensions pourront être changées plus tard.



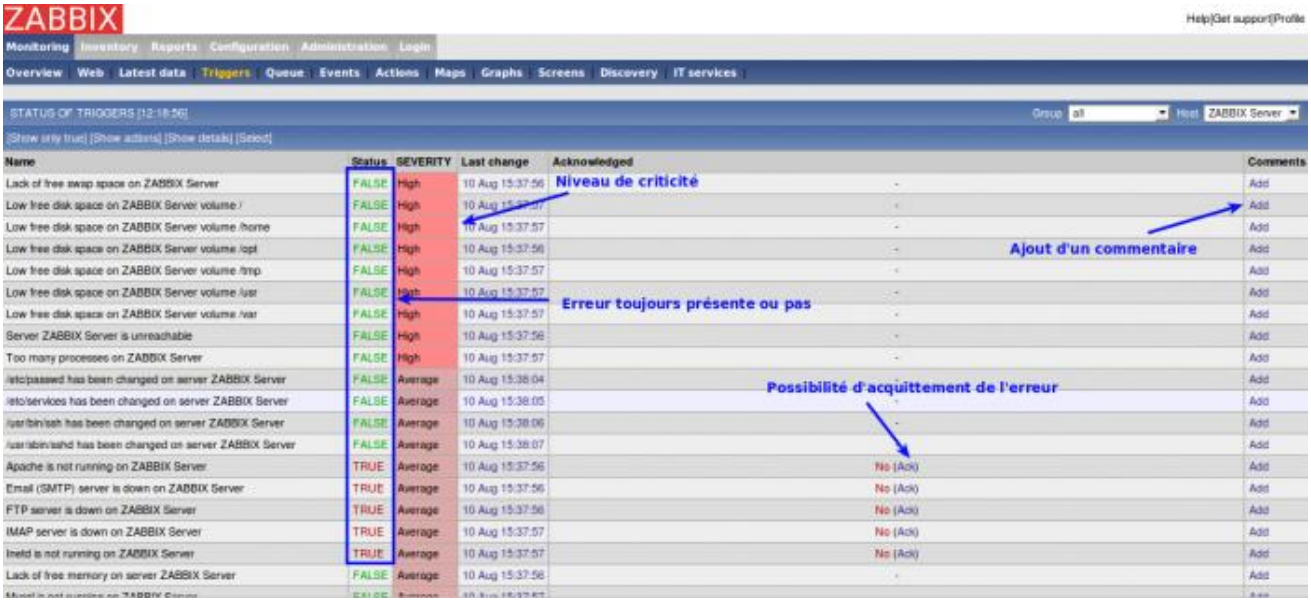
❖ <u>Les Triggers :</u>

Comme dans les bases de données, ils ne se déclenchent que sur un événement précis. Zabbix dispose d'un ensemble de triggers déjà définis et il est possible d'en créer d'autres ou de modifier les existants.

Un trigger est défini par :

- son nom
- son évènement déclencheur
- son parent : le trigger ne se déclenche que si un autre c'est déclenché
- son niveau de sévérité

Pour définir un évènement, dans le formulaire de création de trigger, dans « Expression » cliquer sur le bouton « Insert ».



❖ Les actions

Elles sont déclenchées sur condition(s), pour palier à un éventuel problème ou pour simplement prévenir une personne.

Une action est le regroupement :

- d'un évènement source déclencheur (trigger ou découverte)
- d'une ou plusieurs conditions
- de la procédure effectuée par l'action (envoi d'un message, commande à exécuter etc...).

Pour envoyer un message, sélectionnez l'utilisateur puis préparez le modèle de votre message. Pour une commande distante, tapez : <hote> :<commande> ou <groupe>#<commande

Pour ouvrir les ports de l'agent zabbix et serveur zabbix, on a installé le par-feu « **Firestarter** ».

Conclusion

Les outils que nous venons de décrire permettent à l'administrateur d'avoir des informations sur le comportement de son infrastructure réseau. L'association de ces deux outils en augmente sa compréhension.

Conclusion

Ce stage de fin d'études a été une expérience supplémentaire dans le métier d'informaticien. Il a été très formateur, il nous a permis d'élargir notre expérience en entreprise.

Les nombreuses personnes qu'on a rencontrées nous ont permis de confirmer la vision du travail en équipe. On a pu mettre en pratique nos connaissances informatiques mais aussi relationnelles en répondant à de nombreux problèmes.

On a aussi découvert l'organisation et le règlement d'une grande entreprise à dimension nationale qui met en avant une qualité de service et d'étude très élevée.

Ce stage de fin d'étude de la licence « Electronique, Télécommunications, Informatiques » est donc une très bonne occasion de confirmer son projet professionnel et de cerner toutes les facettes du métier d'informaticien. Même si le stage n'est pas en rapport direct avec la formation acquise en licence, on pense que c'est une bonne expérience et un bon complément à cette année.

« Il n'est pas tant important de tout savoir que de connaître la valeur exacte de chaque chose, d'apprécier ce que nous apprenons, et de faire avec ce que nous savons. » .

Hannah More

Annexe :

LINUX

Linux ou GNU/linux est un système d'exploitation libre multitâches (plusieurs applications peuvent être lancées en même temps sans qu'aucune n'affecte les autres), multiplateformes et multiutilisateurs (plusieurs personnes peuvent en même temps travailler sur le même ordinateur), de type Unix.

Il tire son nom d'une de ses parties, à savoir de son noyau, il s'agit d'un composant central et de bas niveau qui s'occupe de fournir aux logiciels une interface pour communiquer entre eux et le matériel.

Linux est considéré comme un système fiable, robuste et puissant. Il est d'ailleurs capable de fonctionner avec très peu de ressources sur des ordinateurs bas de gamme très peu puissants.

Linux

Le logo et mascotte du noyau Linux : Tux

Famille	Systèmes Unix
Type de noyau	Noyau modulaire (depuis la version 2.0)
État du projet	en constant développement
Licence	Licence publique générale GNU
Dernière version stable	2.6.34 (16 mai 2010) (Noyau Linux) [+/-]
Dernière version avancée	2.6.35-rc2 (le 5 juin 2010) (Noyau Linux) [+/-]

Le système Linux possède notamment les avantages suivants :

- Le support des standards de l'internet, c'est-à-dire des protocoles TCP/IP, la famille de protocoles utilisée sur Internet. Linux est donc un moyen gratuit de créer un réseau local, de se connecter à Internet et de mettre en place un serveur.
- Une sécurité accrue due à la transparence de son code source et de la réactivité de la communauté lors des annonces de vulnérabilités.

- Un cloisonnement des espaces mémoire et de l'espace disque couplé à une gestion pointue des droits permettant de gérer un grand nombre d'utilisateurs avec un niveau de risque minimal.
- Un noyau entièrement configurable en fonction du matériel de la machine sur laquelle le système est installé afin de maximiser les performances.

Linux n'est pas le produit d'une seule société, mais de nombreuses sociétés et groupes de personnes qui y contribuent. En fait, *le système GNU/Linux* est un composant fondamental, dérivé en de multiples produits différents, nommés distributions**.**

Ces distributions changent entièrement l'aspect et la fonction de Linux. Elles s'étendent du système complet (développé par des entreprises) à des systèmes légers (souvent développés par des volontaires) qui s'installent sur une clé mémoire USB ou sur des ordinateurs anciens.

Il existe de très nombreuses distributions : Mandriva, RedHat Fedora, Debian,….. Une distribution performante et conviviale pour passer à Linux est Ubuntu.

Ubuntu linux est une distribution GNU/Linux nom commerciale basée sur Debian ; Ubuntu vise à créer une distribution qui fournit un système linux à jour et cohérent pour les machines de bureau et les serveurs ; Ubuntu inclut de nombreux paquets rigoureusement choisis et conserve aussi son puissant gestionnaire de paquets qui permet l'installation facile de programmes et leur suppression de façon propre.

En se focalisant sur la qualité, Ubuntu produit un environnement informatique robuste et riche en fonctionnalité qui peut convenir aussi bien à une utilisation domestique que commerciale.

Ubuntu linux est conçue principalement pour les ordinateurs de bureau avec un objectif de convivialité et d'ergonomie.

Il existe de nombreuses façons de se procurer une copie d'Ubuntu ; elles sont décrites sur la page de téléchargement http://www.ubuntu.com/download du site web d'Ubuntu

Terminal :

Le terminal est souvent appelé invite de commandes

Les commandes les plus utilisés sont :

- **Sudo** *command* : exécute command en mode super-utilisateur ;
- **Ifconfig :** affiche toutes les interfaces réseau disponible,
- **etc/ network/interfaces :** contient les informations de configuration des interfaces
- **apt-get install** *soft* : installer le logiciel soft en gérant les dépendances
- **tar xvf archive.tar.gz :** extraire les fichiers archive.tar.gz, en affichent les noms des fichiers
- **gedit** *fichier* :éditer un *fichier*
- **cd :** se déplacer vers le dossier /home/utilisateur
- **/etc/init.**d/ restart/start : sert à démarrer ou à redémarrer une application
- **Wget siteweb :** télécharger directement le programme voulu

VirtualBox est un logiciel de virtualisation des systèmes d'exploitation permettant de disposer de plusieurs systèmes d'exploitation sur une même machine en cours d'utilisation. La virtualisation se faisant de plus en plus présente, VirtualBox trouve de plus en plus souvent sa place sur les postes simples.

Sun VirtualBox est une collection d'outils puissants de machine virtuelle, ciblant les ordinateurs bureaux, serveurs d'entreprise et les systèmes. Intégré, avec VirtualBox vous pouvez virtualiser les systèmes d'exploitation 32 bits et 64 bits.

Glossaire :

Goulot d'étranglement : un point d'un système limitant les performances globales, et pouvant avoir un effet sur les temps de traitement et de réponse.

ERIC D'HEM : créateur et directeur technique de NETvigie spécialiste du monitoring avancé d'infrastructure IP.

Fonction de hachage : fonction particulière qui, à partir d'une donnée fournie en entrée, calcule une empreinte servant à identifier rapidement la donnée initiale. Ex : HMAC-MD5-96 HMAC-SHA- 96.

DES : Data Encryptions Standard un algorithme de chiffrement par bloc utilisant des clés de 56 bits.

HTTP/S : **HyperText Transfer Protocol /*Secured***, un protocole de communication client-serveur développé pour le World Wide Web.

SMTP : **Simple Mail Transfer Protocol** est un protocole de communication utilisé pour transférer le courrier électronique vers les serveurs de messagerie électronique.

POP : **P**ost **O**ffice **P**rotocol un protocole qui permet de récupérer les courriers électroniques situés sur un serveur de messagerie électronique.

Telnet : **Télécommunication NET**work est un protocole réseau utilisé sur tout réseau supportant le protocole TCP/IP le but du ce protocole est de fournir un moyen de communication très généraliste.

IMAP : **I**nternet **M**essage **A**ccess **P**rotocol (**IMAP**) est un protocole utilisé par les serveurs de messagerie électronique, fonctionnant pour la réception.

DNS : **D**omain **N**ame **S**ystem est un service permettant d'établir une correspondance entre une adresse IP et un nom de domaine.

RDP : Remote **D**esktop **P**rotocol un protocole qui permet à un utilisateur de se connecter sur un ordinateur faisant tourner Microsoft Terminal Services.

RPC : **R**emote **P**rocedure **C**all est un protocole permettant de faire des appels de procédures sur un ordinateur distant à l'aide d'un serveur d'applications.

SSH : **S**ecure **Sh**ell : un protocole de communication sécurisé.

FTP : **F**ile **T**ransfer **P**rotocol : un protocole de communication destiné à l'échange informatique de fichiers sur un réseau TCP/IP.

NNTP : Network **N**ews **T**ransfer **P**rotocol un protocole réseau correspondant à la couche application du schéma OSI, NNTP est utilisé en particulier par les forums de discussion.

Web-graphie :

[1] : http://www.netvigie.com/Societe/Presse/Articles/la_securite_par_le_monitoring.html
[2] : http://www.frameip.com/snmp/,
[3] : http://www.supinfo-projects.com/fr/2006/hp_open_view/
[4] :http://www-01.ibm.com/software/fr/c-est_simple_clients/informatique/tivoli/tiv_monitoring-description.html
[5] : http://www.supinfo-projects.com/fr/2006/supervision_reseau/
[6] : http://www.forumdz.com/archive/index.php/t-15039.html
[7] : http://wiki.monitoring-fr.org/supervision/zabbix-ubuntu-install
[8] : http://www.hlecorche.fr/nagios/rapport.pdf

[9] : http://tuxtraining.com/2008/10/11/how-to-install-cacti-on-debian

[10] : http://openmaniak.com/fr/cacti_plugins.php

[11] :http://gregsowell.com/?p=115

[12] : http://www.supinfo-projects.com/fr/2004/graphe_cacti/introduction/

[13] :http://gregsowell.com/?p=115

[14] :http://cacti.net/

[15] : http://zabbix.com

[16] : http://www.synergeek.fr/wp-content/uploads/monitoring.pdf

[17] : http://www.zabbix.com/documentation.php

[18] : http://wiki.monitoring-fr.org/supervision/zabbix-ubuntu-install

[19] :http://www.ubuntugeek.com/how-to-setup-zabbix-monitoring-application-in-ubuntu-9-04-jaunty-server.html