République Algérienne Démocratique et Populaire
Université Abou Bakr Belkaid– Tlemcen
Faculté des Sciences
Département d'Informatique

Mémoire de fin d'études

pour l'obtention du diplôme de Master en Informatique

Option: *Modèles intelligent et de décisions I (M.I.D)*

Thème

Supervision d'un réseau virtuel par l'outil NAGIOS

Réalisé par :

- **Mr BELKHODJA Lakhdar**
- **Mme BELKHOUCHE Souheyla**

Présenté le 19 Septembre 2013 devant le jury composé de MM.

- *BENAMAR Abdelkarim* *(Président)*
- *BENAISSA Mohamed* *(Encadreur)*
- *LEHSEINI Mohamed* *(Examinateur)*
- *BELABED Amine* *(Examinateur)*

Année universitaire : 2013-2014

Remerciements

.

Nous tenons à remercier sincèrement Mr BENAISSA Mohamed, qui, en tant que encadreur de mémoire, s'est toujours montré à l'écoute et très disponible tout au long de la réalisation de ce mémoire, ainsi pour l'inspiration, l'aide et le temps qu'il a bien voulu nous consacré.

Nous exprimons également notre gratitude aux membres du jury Mr BENAMAR AbdelKarim et Mr LEHSEINI Mohamed et Mr BELABED Amine, qui nous ont honoré en acceptant d'examiner ce modeste travail.

Dédicaces

.

Je dédie ce travail à mes parents
À mes frères et ma sœur
À mon époux pour sa patience et son soutien
Et à mon fils adoré
Mohamed El Amine

Souheyla

Dédicaces

.

Je dédie ce travail à mes parents
À mes frères Ali ,Abdelwaheb et mohammed
A mes sœurs Souad,Zoubida,Nouria ZAHIA
A mes tentes et cousines
À mes amis de travail

Lakhadar

Tables des Matières

Table des matières

Chapitre IV:LES DIFFERENT TESTS DE SUPERVISION PAR NAGIOS

Introduction Générale

Introduction générale

Actuellement aucune entreprise ne peut se passer d'outils informatiques, et très souvent un réseau informatique de taille plus ou moins importante est mis en œuvre. La maintenance ainsi que la gestion de ces parcs informatiques devient alors des enjeux cruciaux, d'autant plus qu'une panne du réseau peut parfois avoir des conséquences catastrophiques.

C'est pourquoi les administrateurs réseau font appel à des logiciels de surveillance et de supervision de réseaux. Ces logiciels vérifient l'état du réseau 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. Grâce à un tel système, les délais d'interventions sont fortement réduits.

Dans ce domaine, un logiciel fait office de référence: Nagios. En effet Nagios est très performant et possède une prise en main assez intuitive. Il s'installe sur une machine possédant un système d'exploitation Linux, mais peut superviser aussi bien des machines Linux que Windows.

Notre mémoire est composé de deux parties :

Une partie théorique contenant trois chapitres ; le premier chapitre comporte une introduction à la virtualisation, le deuxième chapitre détaille les notions de la supervision réseaux, le troisième chapitre comporte l’étude de l’outil de supervision Nagios et le dernier chapitre comporte les différents outils de la supervision dans un réseau virtuel.

Une partie pratique qui fait l’objectif de notre projet, elle est réservée pour la configuration sous Linux l’outil de supervision Nagios dans un réseau virtuel.

Chapitre I

INTRODUCTION A LA VIRTUALISATION

INTRODUCTION A LA VIRTUALISATION

I.1Introduction

Pour l'optimisation des coûts la virtualisation est devenue une réelle nécessité pour les entreprises. Introduction à un concept vieux de plus de 30 ans mais qui correspond à l'avenir des architectures informatiques

La virtualisation permet de faire fonctionner simultanément plusieurs systèmes d'exploitation sur une même machine physique. Dans l'esprit, il y aura plusieurs machines virtuelles sur une machine physique se partageant les ressources de celle-ci. L'évolution exponentielle des composants informatique et de leur puissance de calculs donnèrent de nouvelles optiques à l'informatique. La loi liée à l'évolution des composants informatique est la loi de Moore :

La loi de Moore veut que tous les 18 mois, une des 3 variables suivantes : la « puissance » , la « vitesse » ou « l'espace » soit doublée.

Dans la logique, la virtualisation est basé sur le principe, au lieu de multiplier les machines physiques avec un seul système d'exploitation, on utilise une machine physique pour virtualiser plusieurs systèmes d'exploitations. La virtualisation a notamment été créée pour répondre à la problématique de la sous-utilisation des ressources matérielles.

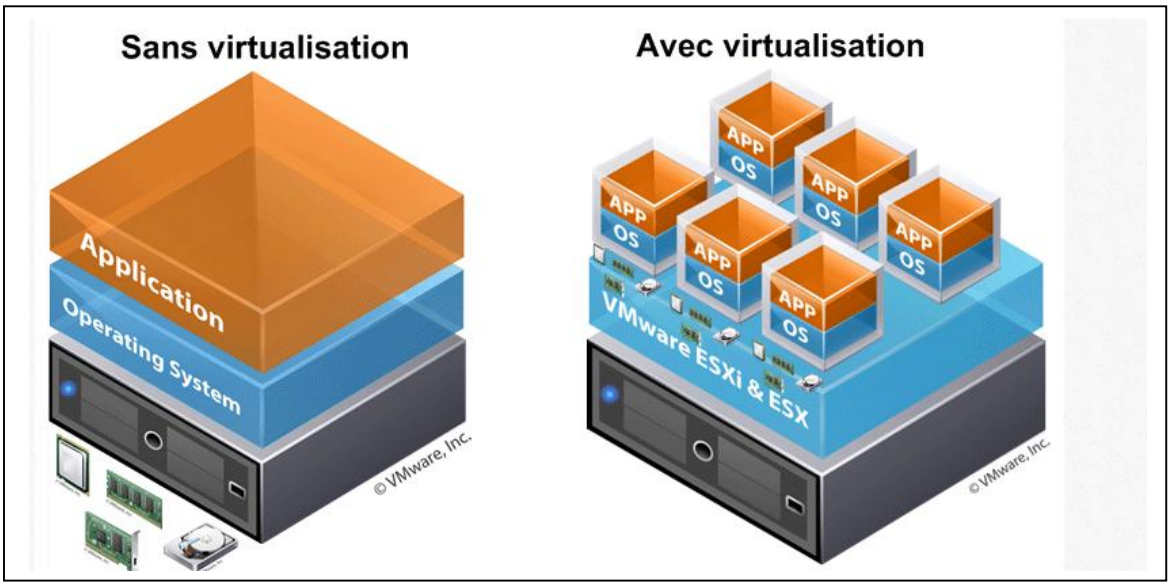


Figure I.1 : virtualisation

I.2Virtualisation

La virtualisation se compose:

- **D'une machine physique (Host)**

Équipée de plusieurs cartes réseau, de beaucoup de mémoire et d'une grande capacité de stockage.

- **Un logiciel de gestions des ressources matérielles (Hyperviseur)**

L'Hyperviseur permet à plusieurs systèmes d'exploitation de travailler et de partager les ressources d'une seule et même machine, le Host.

- **Des Machine virtuelle**

Une machine virtuelle est un logiciel qui est installé sur un système d'exploitation appelé hôte (OS hôte, « host OS »). Cette machine virtuelle est capable d'émuler d'autres systèmes d'exploitation appelés invités (OS invités, voire OS clients, « guest OS »). Par abus de langage, on appellera une « machine virtuelle » (VM) le fichier représentant le système invité. La machine virtuelle émule les périphériques (carte graphique, carte son, réseau, etc.) mais pas le processeur. A la différence des émulateurs de jeux de consoles, qui eux émulent également le processeur. Une machine virtuelle est donc plus performante qu'un émulateur « classique »[1].

I.3Les types de virtualisation

I.3.1 Hyperviseur de type 1

L'hyperviseur de type 1 ou bare-metal est un outil qui s'interpose entre la couche matérielle et logicielle. Celui-ci a accès aux composants de la machine et possède son propre noyau. C'est donc par dessus ce noyau que les OS seront installés. Il pilote donc les OS à partir de la couche matérielle, il s'administre via une interface de gestion des machines virtuelles. Il est beaucoup plus puissant que les hyperviseurs de type 2 notamment grâce à sa proximité au matériel.

Les couches sont organisées comme suit :

- Couche matérielle
- Couche de virtualisation (hyperviseur)
- Virtualisation d'OS

Parmi ces hyperviseurs on trouve :

- VmWare vSphere
- Microsoft Hyper-V
- XEN
- KVM (open source)

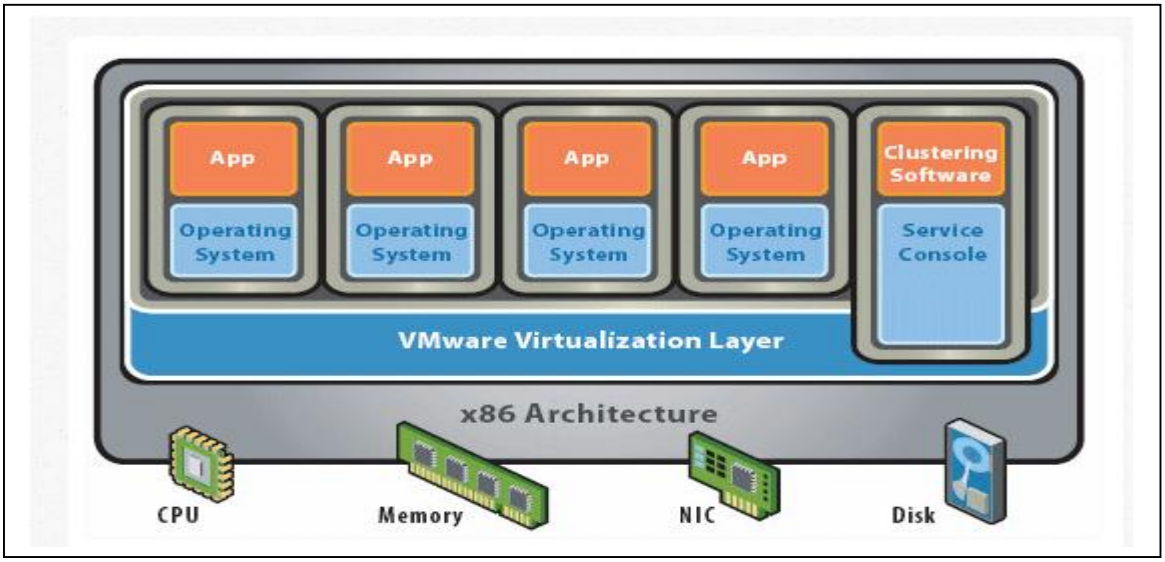


Figure I.2 : Hyperviseur de type 1

I.3.2 Hyperviseur de type 2

L'hyperviseur de type 2 ou architecture hébergée est une application installée sur un système d'exploitation, elle est donc dépendante de celui-ci. Les performances sont réduites en comparaison des hyperviseurs de type car l'accès au matériel (CPU, RAM…) se fait via une couche intermédiaire. Néanmoins il propose une parfaite étanchéité entre les systèmes d'exploitations installés.

Les couches sont organisées comme suit :

- Couche matérielle
- Système d'exploitation hôte
- Couche de virtualisation
- Virtualisation d'OS

Parmi ces hyperviseurs on trouve :

- VmWare Workstation, Fusion, Player
- Oracle VirtualBox
- Microsoft Virtual PC
- QEMU (open source)

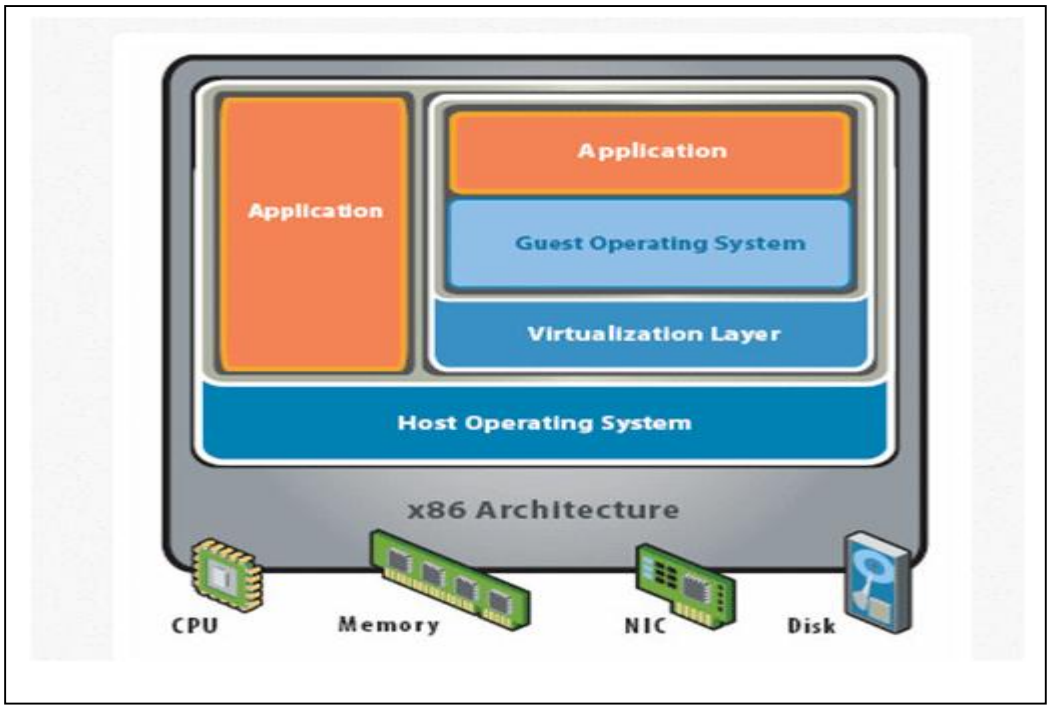


Figure I.3 : Hyperviseur de type 2

I.4 Avantages de la virtualisation

Le premier avantage c'est de diminuer les coûts associés à l'achat d'équipement informatique. Dans une grosse entreprise les économies peuvent atteindre des centaines de milliers de dollars. Les plus petites peuvent quant à elles, envisager d'être plus productives avec moins d'équipement. Cela pourrait faire décoller des projets en attente faute de budget.

Réduction des coûts directs

- Réduction des frais associés à la désuétude informatique (Réduction du matériel)
- Réduction de la maintenance (Réduction du matériel)
- Coût d'électricité et de climatisation (coût significatif avec le nombre d'équipement)
- Meilleure compatibilité des logiciels avec les systèmes d'exploitation (Réponse à la désuétude avec les multi-OS, réponse aux incompatibilités avec la compartimentation)

- Aisance dans le processus de migration des plateformes (Multi-OS) (Intervention sur un nombre limité de machine et activation à distance).

Accroissement de la sécurité

- Meilleur contrôle grâce à un surveillance plus efficace des serveurs en temps réel.
- Portabilité et sécurité des activités en temps réel (Possibilité de redondance intersites en cas de sinistre). Avec la notion du « *cloud computing* », nous ajoutons encore plus de flexibilité.
- Meilleure sécurité grâce à la rapidité de se relever d'un désastre avec un plan de continuité.

Accroissement de l'efficacité et de la productivité

- Meilleure efficience informatique parce que vous faites plus avec moins (Moins de matériel et plus d'environnement compartimentés)
- Rapidité pour monter un nouveau serveur. En effet, tous les éléments sont toujours à porter de mains pour reprendre les activités.
- Meilleure protection grâce à la facilité de revenir en arrière en cas de sinistre
- Façon efficace de monter un environnement de test peu coûteux et complet. Avec une photo de l'environnement, il devient facile de tester sans tout bousiller et à sans dépenser trop en temps.
- Gestion des licences avantageuse motivant l'usage de la virtualisation, car vous aurez besoin de moins de licences pour être aussi efficace. Microsoft permet une gestion proactive de vos besoins en licences.

I.5 Inconvénients de la virtualisation

- C'est une technologie, non pas un protocole normalisé
- Mise en œuvre par des technologies différentes non standardisées..
- Repose sur des concepts différents, et Technologie « parfois » complexe à mettre en œuvre.
- Performances inégales selon la technologie de virtualisation employée
- Certaines technologies n'offrent pas de performances ou de stabilités suffisantes.
- Les serveurs n'ont plus d'E/S dédiées, chaque machine virtuelle partage les E/S sur disque.
- Baisse de performance possible à évaluer.

- Nécessité d'un serveur hôte plus puissant.
- Pertes plus importantes en cas de panne de la machine hôte plusieurs services indisponibles
- Nécessité de sauvegarder les machines virtuelles pour les relancer ailleurs en cas de problèmes

I.6Virtualbox

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. En effet, l'intérêt de virtualiser un système d'exploitation sur un serveur de production visible à partir de l'internet reste un cas rare.

Bien que VirtualBox soit nettement plus jeune que certains de ses concurrents comme par exemple VMWare, Sun a su rattraper son retard en proposant un logiciel tournant aussi bien sous Mac que sous Windows et également sous GNU/Linux (Linux, OpenBSD, FreeBSD).

Le virtualbox c'est l'objet de notre travail dans la configuration de notre réseau virtuel [2].

I.7Conclusion

La virtualisation est une technologie de plus en plus incontournable. Les environnements virtuels sont très en vogue au sein des entreprises de toutes tailles.
Il est vrai que les avantages de cette technologie sont nombreux en termes de productivité, de coûts et d'exploitation. En effet, elle permet des baisses de coûts importantes par la réduction du nombre de machines physiques, mais aussi par toutes les autres économies induites : énergie, temps de mise en œuvre.

La virtualisation d'un seul ordinateur physique n'est qu'un début. Durant, notre projet
nous allons mettre en place une infrastructure virtuelle complète, en intégrant des machines virtuels interconnectés entre eux par un réseau virtuel.

Chapitre II

SUPERVISION RESEAU

Chapitre2

SUPERVISION RESEAU

II.1Introduction

Depuis le développement de l'informatisation des entreprises, il y a quelques années, la question de la sécurité et de la robustesse du système d'information est au cœur des préoccupations.
Ces craintes sont à l'origine de la création et du succès des outils de surveillance : Des logiciels de supervision permettant de faciliter la gestion des parcs informatiques devenant de plus en plus complexes.
Leur but principal est la collecte de données et la présentation de celles-ci pour que l'administrateur puisse consulter aisément les écrans de contrôle pour mesurer l'état du réseau. Toutefois, ces outils se sont étoffés offrant des services d'alertes sur panne ou préemption de pannes, de configuration d'équipements à distance ainsi que de cartographie.

II.2Présentation

II.2.1Définition de la supervision

La supervision se définit comme une technique utilisant au mieux les ressources informatiques pour obtenir des informations sur l'état des réseaux et de leurs composants. Ces données seront ensuite traitées et affichées afin de mettre en lumière 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. Cette définition de la supervision est décrite plus en détail dans la norme ISO7498/4.
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).

II.2.2Supervision 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 (débit, latence, taux d'erreurs). 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.

II.2.3Supervision système

La surveillance se cantonne dans ce cas à la machine elle-même et en particulier ses ressources. Si l'on souhaite par exemple contrôler la mémoire utilisée ou la charge processeur sur le serveur voire analyser les fichiers de logs système.

II.2.4Supervision 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.
En effet rien ne garantit qu'un port X ouvert veut dire que l'application qui tourne derrière n'est pas "plantée".

II.3Les protocoles existants

Il existe des protocoles réseau qui permettent de récupérer des informations sur le parc informatique. Nous allons en étudier deux particulièrement importants qui possèdent des rôles très différents mais qui ont un point en commun : Ils sont tout deux largement utilisés par les logiciels de supervision.

I.3.1ICMP (Internet Control Message Protocol)

ICMP est un protocole de couche réseau (couche 3 du modèle OSI) qui vient palier à l'absence de message d'erreur du protocole IP (Internet Protocol). En effet si il y a un incident de transmission les équipements intermédiaires vont utiliser ce protocole pour prévenir la

machine émettrice. Les paquets ICMP sont encapsulés dans des paquets IP (malgré qu'ils soient au même niveau OSI), et peuvent contenir des bouts de paquets IP pour citer celui ayant généré l'erreur. Afin de catégoriser les erreurs, elles sont divisés en types eux-mêmes parfois redivisés en codes. Par exemple le type 3 représente un destinataire inaccessible : Il existe 16 codes différents en fonction de la raison pour laquelle le destinataire n'est pas joignable.
C'est un protocole très simple, qui n'a pas pour fonction directe la supervision d'un réseau mais qui est utilisé comme source d'information sur la qualité du réseau ou sur la présence d'une machine.

II.3.2SNMP (Simple Network Management Protocol)

- **Présentation**

  SNMP (Simple Network Management Protocol) est un protocole de couche applicative qui a pour but de superviser les réseaux. Il a été conçu en 1988 par l'IETF (Internet Engineering Task Force) avec pour idée directrice de créer un protocole simple qui ne vienne pas gêner le trafic du réseau qu'il supervise.
  Depuis sa création, le protocole a évolué par soucis de sécurité: La version 2 qui est pour l'instant la plus utilisée possède une notion de communauté qui est utilisée comme un mot de passe, la version 3 durcit un peu plus le protocole en y ajoutant le chiffrement.

- **Fonctionnement**

  Par soucis de simplicité et donc de rapidité, SNMP ne transporte que des variables et s'appuie sur le protocole UDP (User Datagram Protocol). SNMP va créer un dialogue entre des agents installés sur des machines à superviser et un serveur de supervision.

  Les échanges entre agents et serveur se résument à trois opérations, les alarmes, les requêtes et les réponses :

  - Une requête est émise du serveur vers un agent via le port 161 UDP si le serveur veut demander ou imposer quelque chose à cet agent. La requête peut être de quatre types
    - **GetRequest** : Demande la valeur d'une variable à un agent

- **GetNextRequest** : Demande la valeur suivante de la variable
- **GetBulk** : Demande un ensemble de variables regroupées
- **SetRequest** : Demande la modification de la valeur d'une variable sur un agent

- L'agent va ensuite traiter cette requète et emettre une réponse via le même port. Si tout se passe bien, l'agent répond un GetResponse accompagné de la valeur demandée. Mais dans le cas contraire l'agent ajoutera un code d'erreur en réponse (par exemple No Access ou Read Only)
- Une alarme est créée par un agent en cas d'évènement et utilise un message dit de type trap ou de type inform pour prévenir le serveur. Ce message SNMP transite via le port 162 UDP. Les alarmes peuvent prendre les formes suivantes :
  - **ColdStart(0)** : Redémarrage à froid du système
  - **WarmStart(1)** : Redémarrage à chaud du système
  - **LinkDown(2)** : Le lien réseau n'est plus opérationnel
  - **LinkUp(3)** : Le lien réseau est opérationnel
  - **AuthentificationFailure(4)** : Tentative d'accès à l'agent avec un mauvais nom de communauté
  - **EGPNeighboorLoss(5)** : La passerelle adjacente ne répond plus
  - **EntrepriseSpecific(6)** : Alarme propre aux constructeurs

Étant donné que ces requêtes utilisent des noms de variables, ceux-ci doivent être communs à tout matériel que l'on souhaite monitorer (et supportant SNMP).
C'est pour cette raison que les données sont stockées dans une base normalisée nommée MIB (Managed Information Base). Cette base organisée de manière hiérarchique et est assez compliquée à lire pour un humain. Chaque information (les fameuses variables précédentes) est identifiée par un OID (Object IDentifier).

II.4Conclusion

Avertissant l'administrateur en cas de problème, suggérant une évolution afin de prévenir une panne, centralisant les données sur une console, la supervision fait gagner du temps et est devenu un outil indispensable de la fiabilisation d'un réseau.
Il existe actuellement des solutions complètes qui gèrent l'ensemble des aspects de la supervision et permettent d'administrer des parcs de machines de grande ampleur. Mais si le nombre d'équipements à gérer est très réduit, les petits outils sur lesquels se basent les grands logiciels de supervision sont largement suffisants et permettent de réaliser des choses intéressantes .

Chapitre III

LES DIFFERENTS OUTILS DE SUPERVISION

Chapitre3

LES DIFFERENTS OUTILS DE SUPERVISION

III.1Introduction

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

III.2Le marché de la supervision

Le marché de la supervision peut être découpé en deux grandes sous-parties : Les offres éditeurs : qui permettent de fournir des moniteurs de supervision payants. Les offres du monde libre : qui permettent d'avoir des moniteurs gratuits (Open-source).

III.2.1 Les offres éditeurs

Les gros éditeurs logiciels ont rapidement compris que la supervision était une ressource clé pour les entreprises qui, de plus en plus, utilisent leur système d'information 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. Ayant rapidement compris cela, les gros éditeurs logiciels sont donc très vite entrés dans la course aux logiciels de supervision.

Aujourd'hui, la majorité des gros éditeurs logiciels propose des outils complets de supervision. On retrouve, parmi les plus connus :

- HP : la gamme Openview (NNM, OVO, ...); IBM : Tivoli ; BMC : Patrol ; Computer ; Associates : Unicenter TNG.

Ces outils, véritables *frameworks* de la supervision, possèdent tous leurs avantages et inconvénients face à la concurrence. Et bien entendu, tous ont également le même défaut, à savoir: *leurs prix coûteux*

Cette constatation faite, il est alors logique de voir de plus en plus de sociétés aujourd'hui regarder du côté du logiciel libre, où les projets commencent depuis quelques années à devenir de plus en plus professionnels et suivis.

Dans ce qui va suivre, nous présenterons deux leaders des logiciels payants de supervision: HP OpenView et IBM Tivoli.[4]

- ✓ **HP OpenView**

HP OPEN VIEW est un outil de supervision reconnu sur le marché. Son principal avantage est la centralisation des informations sur un seul poste. Il a pour rôle de gérer et de surveiller entre autre les infrastructures et services réseaux. Ce logiciel est donc destiné aux moyennes et grandes entreprises qui souhaitent avoir une vue globale de leur réseau et de son état.

Principe de fonctionnement

HPOV est un produit qui propose, aux personnes chargées de l'exploitation des systèmes d'information, un outil favorisant :

Une vue globale du système d'information ;
Un contrôle homogène des différents composants du système informatique ;
Une vision des incidents et leur impact.

La plate-forme HP OpenView est composée principalement de :

OVOW (OpenView Opération for Windows): composé d'une base SQL SERVER;
Le logiciel est assorti d'un serveur HTTP Apache pour l'accès aux interfaces Web des outils.

- ❖ **La console OVOW**

La console OVOW permet à l'opérateur d'avoir une vision globale de son réseau informatique. L'opérateur peut visualiser d'un seul coup d'oeil la disponibilité globale d'un service, la gravité d'une erreur, la raison principale de cette erreur.

Les noeuds

Pour OVOW, chaque client est un « noeud ». Un noeud correspond donc à un élément surveillé (un noeud peut être un serveur, un photocopieur ...).

Les agents OVOW

OVOW a besoin d'un agent pour pouvoir surveiller un élément. Un agent OVOW est un programme que l'on déploie à partir du serveur HPOV sur un noeud. On doit spécifier à cet agent un domaine cible.

L'agent OVOW est composé d'une mini base de données très sécurisée nommée base Coda. L'agent stocke ses les informations liées aux métriques de performances du matériel surveillé dans la base Coda ensuite le serveur se connecte à cette base toutes les 4 minutes (variable paramétrable), et récupère les informations et les stockent dans sa base SQL SERVER.

✓ ***IBM Tivoli Monitoring***

Les solutions IBM Tivoli Monitoring sont conçues pour une meilleure gestion des applications en ligne essentielles à l'entreprise en :

- surveillant de manière proactive les ressources système vitales ;
- en détectant efficacement les goulets d'étranglement et les problèmes potentiels ;
- en répondant automatiquement aux événements.

En s'appuyant sur les meilleures pratiques pour identifier et résoudre les problèmes d'infrastructure, il a été conçu pour aider les opérateurs à surveiller et gérer les matériels et logiciels essentiels, comprenant les systèmes d'exploitation, les bases de données et les applications sur des environnements répartis.

Ce moniteur de supervision se classe parmi les leaders du domaine, puisque il offre de nombreux avantages. En effet, il :

- Surveille de manière proactive les composants vitaux de votre infrastructure à la demande, en vous aidant à isoler et prévenir rapidement les problèmes de performance ;

- Visualise les mesures de performances historiques et en temps réel sous forme de tableaux et graphiques, avec en plus des conseils spécialisés et des actions.

automatiques au sein d'IBM Tivoli Enterprise Portal ; Consolide la surveillance et la gestion de systèmes répartis et de systèmes hôte à l'aide d'une seule console de travail personnalisable Fournit des outils de surveillance puissants et personnalisables à davantage d'opérateurs nécessitant beaucoup moins de compétences et formation en programmation pour déployer le produit

- Aide à réduire les coûts opérationnels informatiques globaux en simplifiant l'installation et la configuration, et en déployant des règles allégées avec des fonctionnalités de surveillance automatique ;

- Effectue automatiquement le suivi de l'état des principaux composants de votre environnement informatique complexe et reçoit des alertes uniquement en cas d'incident ; Aide à optimiser l'offre de services informatiques en intégrant des produits de gestion et des processus informatiques pour stimuler les performances et respecter les accords de niveau de service ;

- Aide à optimiser le temps de réalisation en simplifiant l'installation et la surveillance, avec également des fonctionnalités de gestion s'appuyant sur des technologies pointer-cliquer.

III.2.2 Les offres du monde libre

Depuis une dizaine d'années déjà, plusieurs projets de supervision ont vu le jour au sein de la communauté du logiciel libre. Il suffit pour cela d'aller faire une simple recherche sur le Net pour se rendre compte de la multitude de projets émergeants autour de la supervision système et réseau.

Nous présenterons ainsi, les systèmes de monitoring plus populaires.

NAGIOS ou Net saint est le principal logiciel Open Source de supervision de réseaux et de systèmes; c'est le plus rependu et le plus suivi par la communauté de développeurs. Par conséquent, il est adapté aux systèmes d'information de taille moyenne ou importante ;

MRTG est un outil de supervision du trafic de liens réseaux. Il peut s'intégrer étroitement à des solutions comme Nagios.

MRTG (Multi Router Traffic Grapher) génère des pages HTML de représentation en temps réel du trafic réseau. Le logiciel prend toute sa dimension comme produit fini, mais également

comme brique spécialisée d'une solution intégrée plus large. Il s'intègre notamment parfaitement dans la solution de supervision de Nagios. Son architecture logicielle permet l'intégration sur des plates-formes et composants hétérogènes.

CACTI est un logiciel de supervision réseau basé sur RRDTool Il peut-être considéré comme un successeur à MRTG et également comme une interface à RRDTool. Cacti permet de représenter graphiquement divers statuts de périphériques réseau utilisant SNMP ou encore grâce à des scripts (Bash, PHP, Perl, VBs...) pour avoir par exemple l'espace disque restant ou bien la mémoire utilisée, la charge processeur ou le ping d'un élément actif. Les données sont récoltées auprès des différents agents SNMP (ou auprès des scripts locaux) grâce à un script php. Pour de meilleures performances un exécutable, nommé cactid, peut également effectuer les interrogations.

ZENOOS représente une alternative à des plates-formes de supervisions comme Tivoli ou OpenView, notamment pour les entreprises de taille moyenne Il assure des fonctions de découverte, d'inventaire, de supervision de la disponibilité, de gestion de la performance, de gestion des évènements et des alertes qui peuvent être envoyées par email Le produit fédère et s'interface avec de nombreux utilitaires de supervision et d'administration open source. Zenoss est disponible en version GPL ou commerciale (avec support).

Le moniteur **Nagios** qu'utilise actuellement le client d'INEODEV Limited et que nous allons le décrire, ainsi dessous, est considéré comme la solution la plus aboutie dans son genre et la plus utilisée dans le monde du logiciel libre de supervision.

III.3 NAGIOS

Nagios, le successeur de Netsaint, 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).

Prévu à l'origine pour fonctionner sous Linux, Nagios devrait fonctionner également sous les autres systèmes Unix.

Plusieurs améliorations ont été apportées à Nagios pour qu'il devienne un partenaire simple à utiliser et remarquablement fiable et efficace.

III.3.1 Fonctionnalités de Nagios

Nagios offre à l'utilisateur plusieurs fonctionnalités, à savoir **:**

- Surveillance des services réseaux (SMTP, POP3, HTTP, NNTP, PING, etc.) ;

- Surveillance des ressources des hôtes (charge processeur, utilisation des disques, etc.) ;

- Permettre aux utilisateurs de développer facilement leurs propres vérifications de services grâce à son système de plugins ;

- Paralléliser la vérification des services ;

- Possibilité de définir la hiérarchie du réseau en utilisant des hôtes "parents", ce qui permet la détection et la distinction entre les hôtes qui sont à l'arrêt et ceux qui sont injoignables ; Notifications des contacts quand un hôte ou un service a un problème et quand celui-ci est résolu

- Possibilité de définir des gestionnaires d'évènements qui s'exécutent pour des évènements sur des hôtes ou des services, pour une résolution proactive des problèmes
- Rotation automatique des fichiers log ; Support pour l'implémentation de la surveillance redondante des hôtes ;
- Interface web optionnelle, pour voir l'état actuel du réseau, notification et historique des problèmes, fichiers log, etc. ;
- Une interface permettant l'intégration simple de plugins ;
- De prévenir par email ou par toute autre méthode personnalisée en cas de problème ;
- Déclencher des procédures personnalisées pour résoudre les problèmes ;
- La consultation des différents événements et données collectés via une interface web ;
- Archivage automatique des données collectées ;

Dans la figure suivante, les fonctionnalités de Nagios se résument **:**

Figure III.1 : Fonctionalités de Nagios

Cependant, pour pallier aux éventuelles lacunes du Nagios, des plugins peuvent être ajoutés qui sont personnalisés selon les besoins d'utilisation, pour accomplir ou améliorer d'autres services et tâches.

III.3.2 Architecture de Nagios

Nagios est un programme modulaire de telle sorte que son évolution puisse être facile, il se compose principalement de trois parties :

- L'ordonnanceur : c'est le moteur de l'application qui s'occupe de l'ordonnancement des tâches de supervision.

- L'interface Web : qui permet d'avoir une vue d'ensemble du système d'information et des possibles anomalies, Nagios s'appuie sur simple serveur

Web tel apache basé sur des CGI.

- Les sondes : Les sondes de Nagios (Plugins ou Greffons) sont de petits scripts ou programmes qui sont à la base des vérifications. Ces minis programmes que l'on peut compléter selon nos besoins pour superviser chaque tache Nagios peut aussi gérer ses données dans des bases de données (MySQL ou PostgreSQL) ou bien dans des fichiers textes.

La figure suivante montre cette architecture:

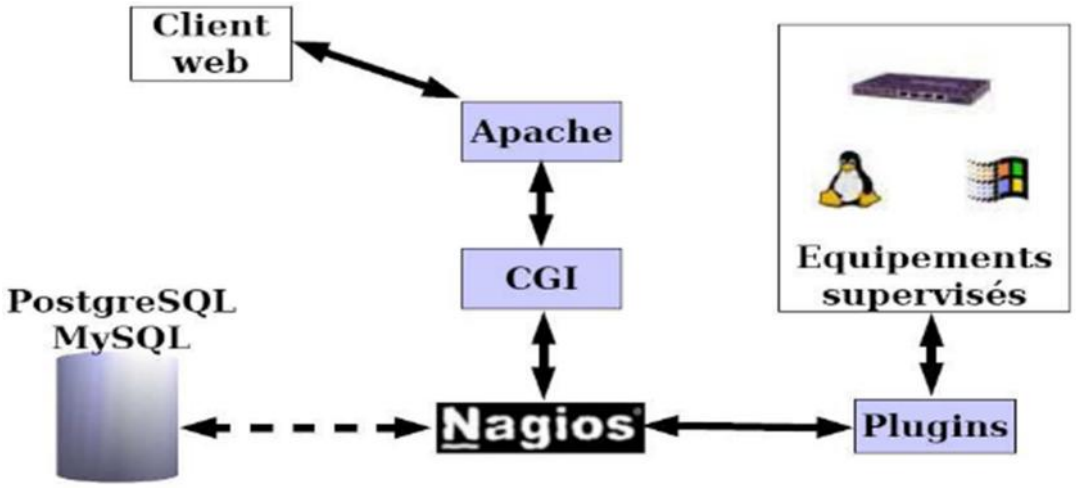


Figure III.2 : Architecture de Nagios

III.3.3. Principes de bases de Nagios

Les Common Gate Interface (CGI) : C'est une technologie standard implémentée à tous serveurs Web. Elle permet l'échange de données entre un programme et le contenu d'une page Web visualisée par un internaute distant. Un tel programme peut être écrit à l'aide de n'importe quel langage de programmation : les plus utilisée sont le langage C, Perl ou encore Python.

Les Plugins : A la différence de beaucoup d'autres outils de supervision. Nagios ne dispose pas de mécanisme interne pour vérifier l'état d'un service, d'un hôte.

Il utilise des programmes externes appelés Plugins, Les Plugins sont des programmes exécutables ou scripts (Perl, Shell, Etc.) qui peuvent être lancés depuis une ligne de commande pour tester un hôte ou un service. Nagios utilise le résultat de cette action pour déterminer le statut des hôtes ou services sur le réseau. Pour Nagios peu importe ce que fait un Plugin, seul le résultat compte. Les Plugins permettent aux utilisateurs de développer facilement leurs propres vérifications de services. Ces plugins fonctionnent soit en local sur la machine supervisée, soit exécutent des tests à distance (tels sur des protocoles réseaux tels Http, Smtp ou exécution distante via Ssh ou autres).

Ce concept est illustré dans la figure suivante :

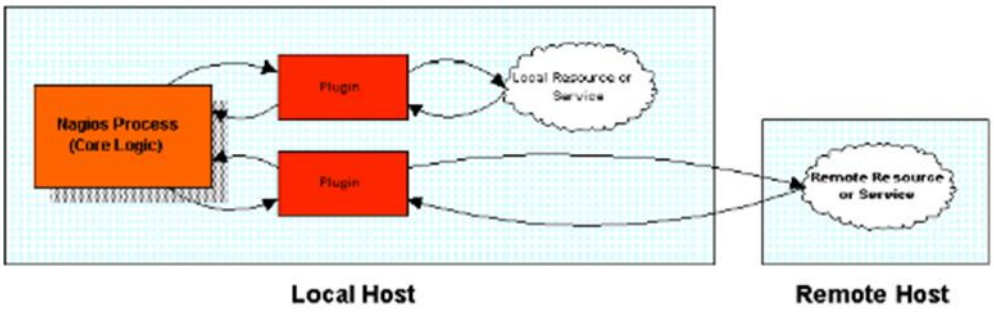


Figure III.3 : Fonctionnement d'un Plugin de NAGIOS

III.3.4 Mise en réseau de la supervision avec Nagios

Les plugins locaux au serveur de supervision sont exécutés directement par Nagios. La vérification d'un service à distance (par l'exécution d'un Plugin situé sur une autre machine ou par SNMP) se fait elle aussi par le biais de l'exécution d'un Plugin local au serveur Nagios qui n'est en fait qu'un ordonnanceur de tâches dédiées à la supervision. Nagios n'a pas pour vocation d'intégrer des fonctionnalités de vérification de bon fonctionnement quelconques autres que ses fonctions internes.

Pour l'exécution de plugins à distance, plusieurs possibilités existent :

- Par le biais d'autres serveurs de supervision Nagios distants : dans le cas de la supervision distribuée qui concentre la vérification sur un site distant, et ne remonte que les problèmes.

- Les agents de transport ou d'exécution des tests, tels :

- NRPE (Nagios Remote Plugin Executor) qui permet l'exécution à la demande de Plugins à distance, à choisir parmi un certain nombre de services disponibles. C'est ce qu'on appelle la ***supervision active.***

- NSCA (Nagios Service Chek Acceptor) qui permet de son coté la remontée d'information de façon passive vu du point de vue de Nagios, c'est ce qu'on appelle la ***supervision passive***.

L'ordonnancement des vérifications est assuré de façon locale à chaque machine et surtout permet d'inverser le sens des connexions entre serveur supervisé et serveur superviseur qui peut avoir un intérêt dans un réseau sécurisé.

- NSClient++ : qui est un greffon (plugin) lourd pour la supervision des serveurs Windows NT/2K/XP.

- Check_Snmp : pour la supervision basée sur SNMP à travers le réseau.

III.4 CENTREON

III.4.1 Présentation de centreon

Surcouche applicative au-dessus de Nagios.

Intégration d'une interface multi-utilisateurs complète et intuitive.

Ajout de nouvelles possibilités de supervision.

Utilisation du langage PHP pour réaliser le client Web.

Projet français basé sur la licence GPL v2 :

Large communauté d'utilisateurs.

Création d'une activité de services par les fondateurs du projet.

III.4.2 Les fonctionnalités de centreon

Interface de configuration des différents éléments de Nagios :

Hôtes, services, contacts, alertes, etc.

Formulaires complets et intuitifs.

Gestion graphique des fichiers de configuration et des plugins. nagios.cfg et resource.cfg

Politique de gestions des profils utilisateurs (droits, langues, accès aux ressources).

Stockage des informations de configuration dans des fichiers textes et une base de données.

L'ensemble des fichiers de configuration de Nagios est accessible via l'interface graphique.

Les éléments sont liés entre eux via des formulaires complets et intuitifs.

Module d'auto-détection des ressources présentes sur le réseau (via NMAP).

Création de graphes au sein des modules :

mécanismes de patrons/modèles.

un module unique, donc moins de ressources systèmes consommées.

pas d'outil externe.

Test de validité des configuration de Nagios avant mise en production.

III.4.3. Génération des graphes à partir de RRD

Supervision graphique des données, ce qui permet d'avoir un historique.
Possibilité de comparer des graphes.
Centreon génère les fichiers de configuration de Nagios (/etc/nagios) à partir des informations saisies dans l'interface Web.
A cela, nous avons ajouté un « toolkit » offrant des fonctionnalités avancées :
Traceroute, Nmap, WOL, reboot, ping, etc.

III.5 NAGIOS et CENTREON

III.5.1 Présentation

Centréon, 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, Centréon (anciennement Oréon) a été repris par une nouvelle entreprise nommée Merethis.

Centréon reprend donc les avantages du moteur de Nagios et permet ainsi d'être entièrement compatible avec des solutions existantes. Son interface reprend un découpage classique :
Home : Page d'accueil avec Le "Tactical Overview" de Nagios permettant un coup d'oeil rapide aux problèmes survenus et accès aux statistiques des performances du moteur et de ses composants.
Monitoring : Possède plusieurs vues, mais reprend la grande idée de l'arbre des groupes d'équipements. Reprend également la vue Nagios.
Views : Permet d'accéder à tous les graphiques avec un menu arborescent.

III.5.2. Avantages

La robustesse et la renommée de Nagios ;
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 ;
Une entreprise qui pousse le développement ;

Peut être décorelé du serveur Nagios et tourner tout seul sur un autre serveur.

III.5.3. 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.

III.6 MRTG (Multi Router Traffic Grapher)

MRTG est un logiciel dédié à la supervision réseau. Il permet d'obtenir toute une série de statistiques *(visualisation de charge sur un réseau, utilisation de bande passante...)* concernant un appareil informatique *(tels que routeurs, serveurs, ou PC)* sous forme de représentations graphiques. Il va pour cela chercher des informations directement sur les interfaces des machines du réseau via le protocole SNM P *(Simple Network Management Protocol, protocole facilitant l'administration de systèmes à distance).*

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

MRTG est un outil réalisé en Perl et en C dans le but de surveiller la charge des liens réseaux. Il génère des pages html contenant des images au format PNG qui représentent graphiquement l'état en temps réel de la ressource surveillée. Le principe est simple : un script Perl recherche les données via le protocole SNMP et envoi celles-ci à un programme C qui va les stocker et générer les graphiques.

A la base l'auteur avait dans le but de surveiller le trafic passant par des routeurs, mais MRTG se basant sur SNMP, les possibilités se sont étendues à toute variable. Encore mieux, on peut aussi créer un script qui surveillera n'importe quelle type de donnée non disponible dans SNMP. On possède ainsi un système de surveillance déjà conséquent qui permet sur une même page de surveiller un réseau et de garder les traces des anciennes données.

III.6.1Les avantages du MRTG

MRTG possède de nombreux avantages :

- MRTG est un logiciel gratuit, développé par une communauté de développeurs passionnés.

- MRTG est un outil multi plateforme (Linux,Unix,Windows), car il utilise un script perl.

- MRTG étant basé sur le protocole SNMP, il n'est pas limité au simple contrôle du trafic mais on peut contrôler n'importe quelle variable SNMP que l'on a choisie car MRTG réalise une commande SNMPGET. De plus on peut même employer un programme externe pour recueillir les données qui doivent être contrôlées via MRTG. Enfin on peut contrôler plus de 50 liens réseaux à partir d'une machine UNIX ou LINUX.

Sa configuration se fait par l'intermédiare d'un fichier de configuration, ce qui permet un contrôl total de ses fonctionalités.

III.6.2 Les inconvénients du MRTG

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

III.7 Conclusion

Tous ces logiciels que nous avons décris ci-dessus sont considérés comme un aboutissement et une réussite dans leur branche, cependant, on voit qu'ils ont tous leurs propres inconvénients qui doivent être résolus.

Un bon moniteur de supervision doit englober tous les avantages de ces derniers et aussi remédier à leurs lacunes et inconvénients afin de converger vers la perfection et atteindre un niveau de supervision et de fiabilité optimum.

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

Chapitre IV

les différentes tests de la supervision par NAGIOS

Chapitre4

LES DIFFERENTS TESTS DE LA SUPERVISION PAR NAGIOS

IV.1 Introduction

Nagios est un logiciel de surveillance de systèmes et de réseaux. Il permet de monitorer toute une liste d'ordinateurs et d'avoir pour chacune d'entre elle une vue de son état. Cette vue s'effectue via une interface Web et permet donc une vision d'ensemble des systèmes monitorés. Le serveur Nagios possède donc une large panoplie de services, telle que la surveillance de disques durs, de mémoires, de services réseaux. Ce chapitre vous explique comment mettre en place Nagios sur un Ubuntu 9.10 server.

Dans notre cas, nous avons crées 3 machine virtuelles a l aide de virtualbox.

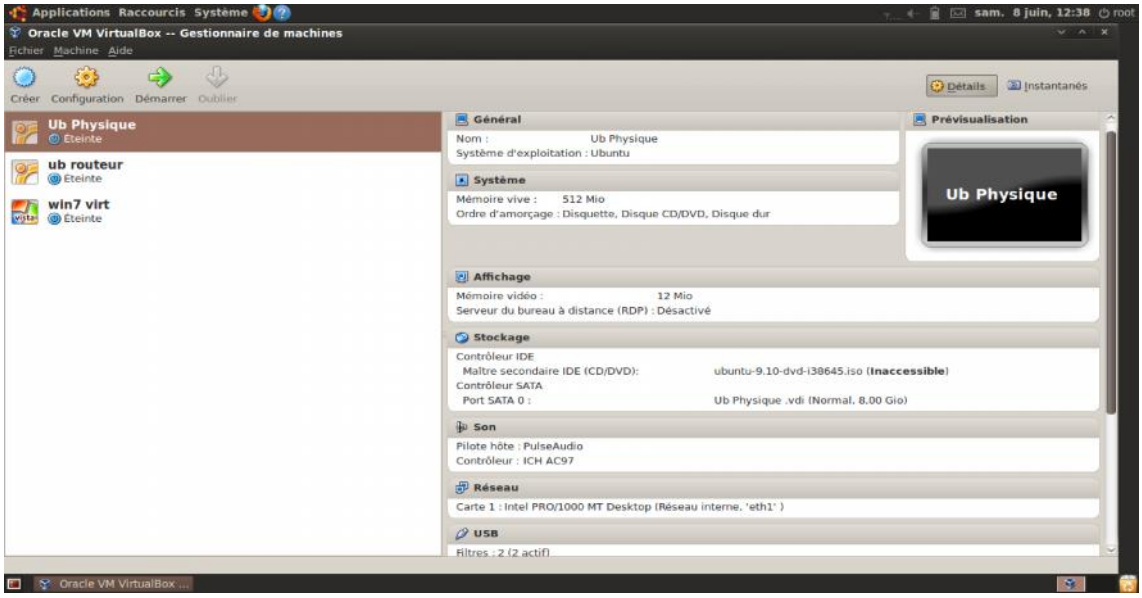
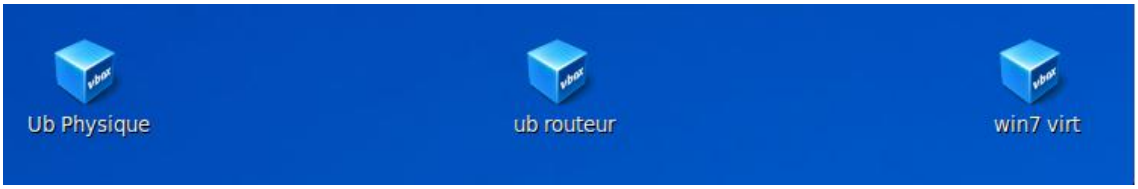


Figure IV.1 : Virtualbox

IV.2La conception de notre réseau virtuel

La 1er machine est considéré comme une machine physique ubuntu 9.10 dans le rôle d un serveur de supervision. A la fin de son installation on met au point sa configuration de carte réseau qui devient interne en la nommant « eth1 », et de la même façon on installe la 2em machine virtuel ubuntu 9.10 dans le rôle d un routeur. Dans la configuration de cette machine on active 2 carte réseau interne la 1er on la nomme « eth0 » relié a la 3em machine, et la 2em « eth1 » qui relie le routeur avec le serveur. En fin on crée une dernière machine virtuelle en

utilisant le système windows7 qui devient dans notre théorie un client avec les configurations nécessaires(réseauinterne«eth0 »).

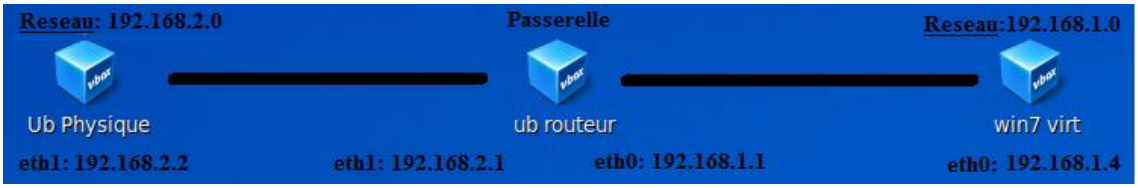


Âpres la création des machines on doit faire la liaison entre eux par les adresse IP

1er machine : ub physique IP: 192.168.2.2/24 avec une passerelle: 192.168.2.1

La 3em machine: win7 virt IP: 192.168.1.4/24 avec une passerelle: 192.168.1.1

La 2em machine: ub routeur a 2 adresse IP ce sont les passerelle utiliser 192.168.1.1 et 192.168.2.1.



La 1er étape est accomplie on a fait les configurations nécessaires ; la 2em consiste à installer tout les paquets nécessaires au machines.

IV.3 Architecture complet de notre de réseau virtuel avec la configuration des cartes réseaux

Notre réseau virtuel est composé par 3 machines virtuelles comme suite :

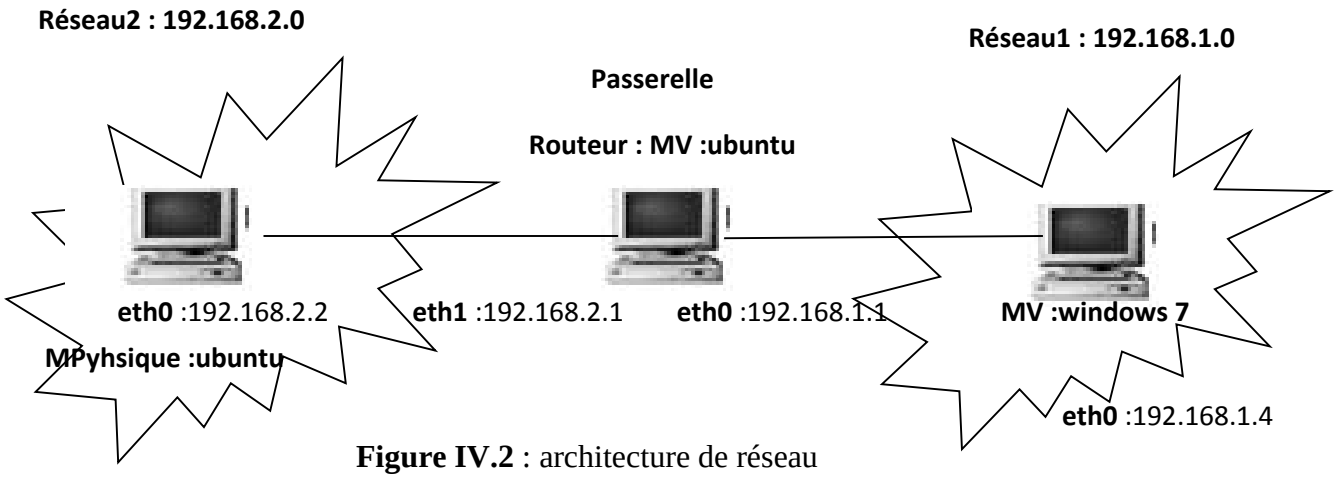


Figure IV.2 : architecture de réseau

machine virtuelle ubuntu 9.10 : routeur ou passerelle entre le résau 192.168.1.0 et 192.168.2.0

dans la machine virtuelle nous avons crées deux cartes réseaux virtuel :

dans la configuration réseau : nous avons ajoutés deux cartes réseaux
carte réseau1 :
choisir réseau interne (eth1)
carte réseau2:
choisir accès par pont (eth0)

Créer deux cartes réseaux :
eth0 : 192.168.1.1
eth1 : 192.168.2.1

dans le fichier /etc/netwok/interfaces nous avons ajouté les lignes suivantes :

auto eth0
iface eth0 inet static
address 192.168.1.1
netmask 255.255.255.0

auto eth1
iface eth1 inet static
address 192.168.2.1
netmask 255.255.255.0

activation la propriété de routage de la passerelle:

dans le fichier /etc/sysctl.conf nous avons activés la ligne suivante (enlever la #) :
net.ipv4.ip_forward=1

machine virtuelle hote physique ubuntu :

ajouter la configuration suivante dans le fichier /etc/network/interfaces :

auto eth1
iface eth1 inet static
address 192.168.2.2
netmask 255.255.255.0

up route add -net 192.168.1.0/24 gw 192.168.2.1

machine virtuelle xp :

Sur la machine virtuelle : paramètre : configuration réseau
Nous avons ajoutés une carte réseau1 eth0:
Nous avons choisis réseau interne (nommé votre carte réseau par eth0)

Nous avons démarrés la machine virtuelle xp et nous avons configurés l'adresse ip de notre machine

exemple @ip : 192.168.1.4
mask : 255.255.255.0
passerelle : 192.168.1.1 (passerelle de machine virtuelle ubuntu)

Nous avons aussi desactiver le parefeu de windows 7

Teste de la configuration entre les trois machines

machine physique ubuntu @ ip : 192.168.2.2 (reseau2 192.168.2.0)

machine virtuelle ubuntu passerelle possede eux adresses ip :
@ip 192.168.1.1 (réseau1 192.168.1.0)
@ip 192.168.2.1 (réseau2 192.168.2.0)

machine virtuelle xp : @ip 192.168.1.4 (réseau1 192.168.1.0)

teste le ping :

machine physique ubuntu:@ip: 192.168.2.2
ping 192.168.1.1 (carte réseau1 de passerelle machine virtuelle ubuntu)
ping 192.168.2.1 (carte reseau de passerelle machine virtuelle ubuntu)
ping 192.168.1.4 (carte réseau de machine virtuelle xp)

machine virtuelle ubuntu : passerelle :
ping 192.168.1.4 (machine virtuelle xp)
ping 192.168.2.2 (machine physique hote ubuntu)
ping 192.168.1.1 (carte réseau1 de passerelle)
ping 192.168.2.1 (carte reseau2 de la passerelle)

machine virtuelle xp : @ip : 192.168.1.4
ping 192.168.2.2 (machine physique hote ubuntu)
ping 192.168.1.1 (carte réseau1 de passerelle virtuelle ubuntu)
ping 192.168.2.1 (carte réseau2 de passerelle virtuelle ubuntu)

Si on a 3 machines virtuelles alors la configuration est comme suite :

Machine virtuelle 1 : reseau intern (eth0)
Machine virtuelle 2 : reseau intern (eth0)
Machine virtuelle 3 : reseau intern (eth0)

IV.4 Les types de connections réseaux avec Oracle VirtualBox

L'utilisation des machines virtuelles avec Oracle VirtualBox nécessite une configuration adéquate de notre réseau virtuel. Nous distinguons plusieurs « type » de connections et de configuration réseau.

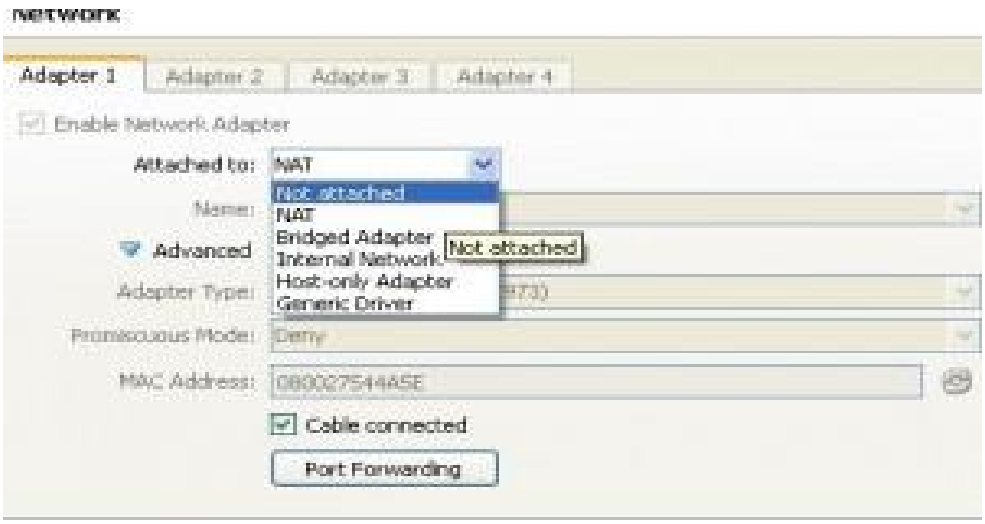


Figure IV.3 : connexion réseau virtualbox

- ✓ **Pour le type « *NAT* »**
  -Les Machines Virtuelles communiquent entre elles
  -Les Machines Virtuelles communiquent avec l'hôte et l'extérieur
  -L'hôte et l'extérieur ne voient pas les VM

  Dans ce type, les trames allant vers l'extérieur de votre machine virtuelle auront la même adresse que votre machine hôte (peut importe l'adresse IP de votre machine virtuelle).

  Particularité : Dans ce mode, la machine virtuelle ne peut être utilisée qu'en client. Elle ne peut pas recevoir de requêtes directes de l'extérieur (ex : un ping ne fonctionnera pas).

- ✓ **Pour le type « *Réseau Interne* » :**
  -Les Machines Virtuelles communiquent entre elles
  -Les Machines Virtuelles ne communiquent pas avec l'hôte
  -Les Machines Virtuelles ne communiquent pas avec l'extérieur

  Ce type permet de connecter des machine virtuelle entre-elles sur un réseau virtuel isolé.

- ✓ **Pour le type : « *Réseau Privé Hôte* »**
  -Les Machines Virtuelles communiquent entre elles
  -Les Machines Virtuelles communiquent avec l'hôte
  -Les Machines Virtuelles ne communiquent pas avec l'extérieur

  Avec ce type de connexion réseau votre machine virtuelle ne peut communiquer qu'avec votre machine hôte de la même manière qu'avec deux cartes physiques standard.

- **Pour le type « *Pont* » :**
  -Les Machines Virtuelles sont sur le même réseau que l'hôte

  Avec ce type de connexion, les trames qui sortent de votre machine virtuelle auront leurs particularités propres (adresse MAC et adresse IP).

IV.5 Installation de Nagios

IV.5.1 Installation des paquets

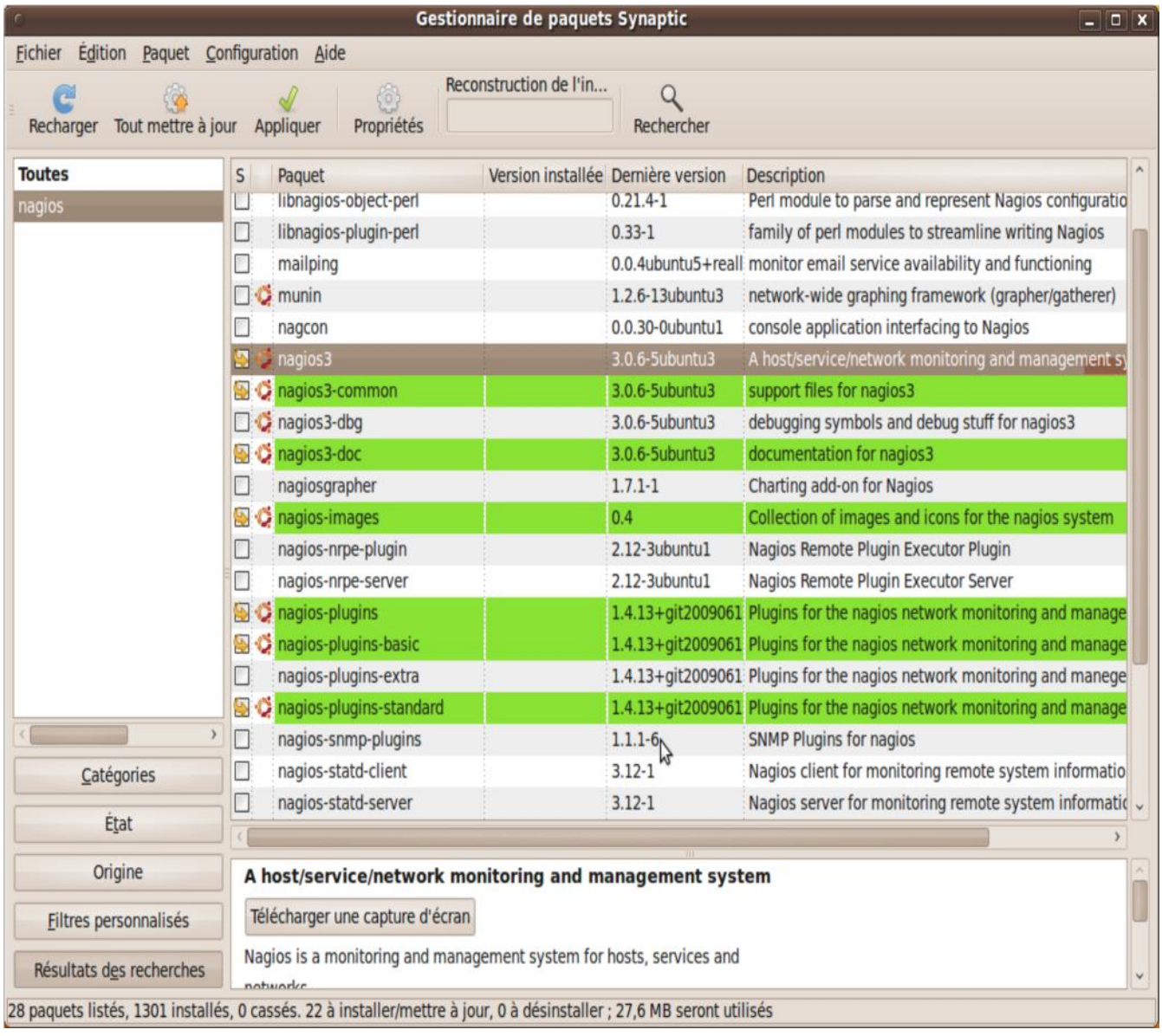


Figure IV.4 : Sélection package nagios

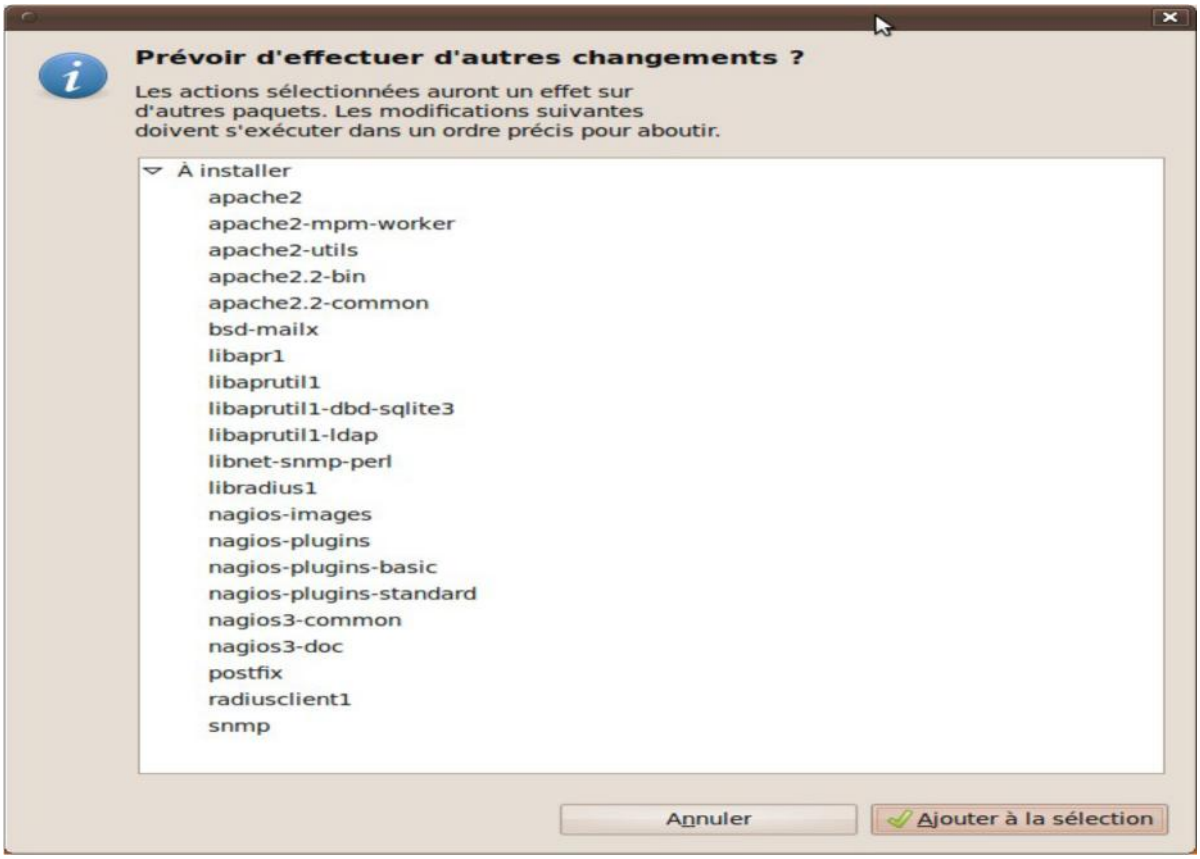


Figure IV.5 : Installation package nagios

IV.5.2 Téléchargement et installation des paquets

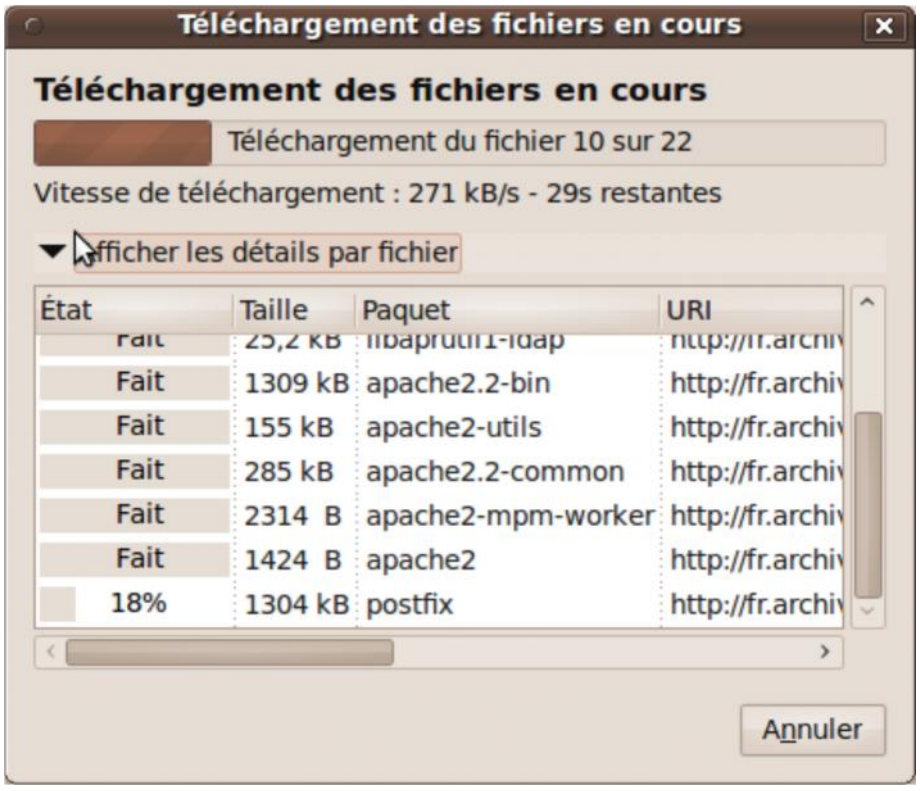


Figure IV.6 Téléchargement et installation des paquets

IV.5.3 Fichiers de configuration nagios

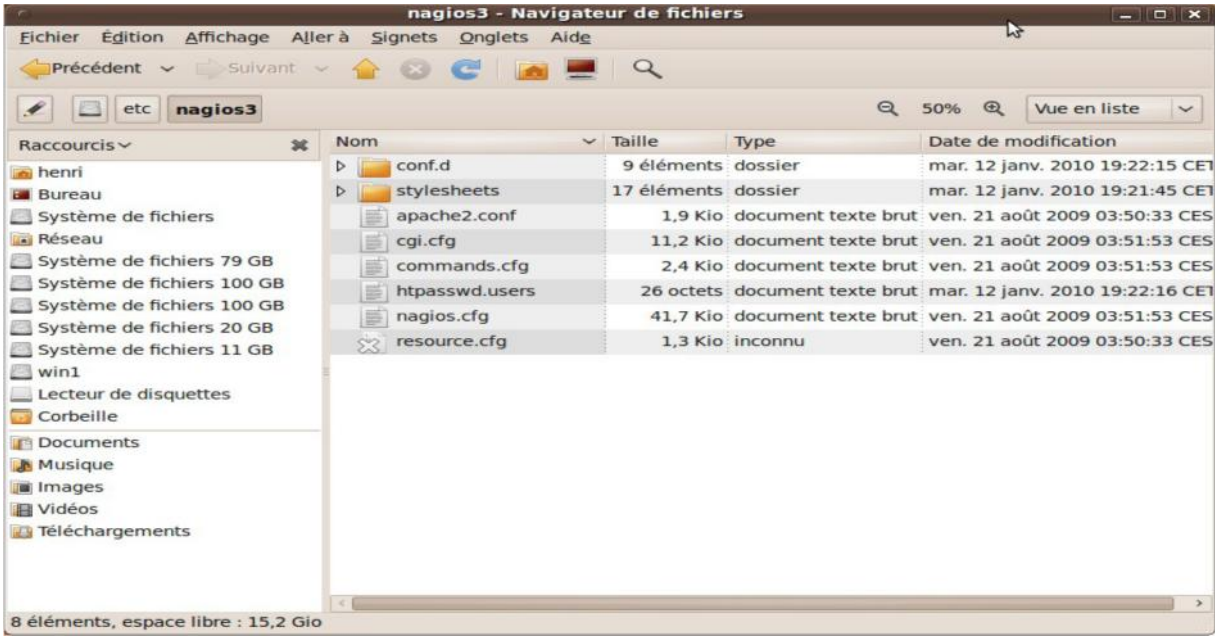


Figure IV.7 Fichiers de configuration nagios dans le dossier /etc/nagios3/

/etc/nagios.cfg

Le fichier pour htacces est déjà prêt, il contient nagiosadmin:JafIU8XLDjbyw c'est-à-dire le login et mot de passe de l'administrateur nagios.

Les fichiers à configurer sont dans le répertoire /etc/nagios3/conf.d

IV.5.4 Configuration des hôtes et services

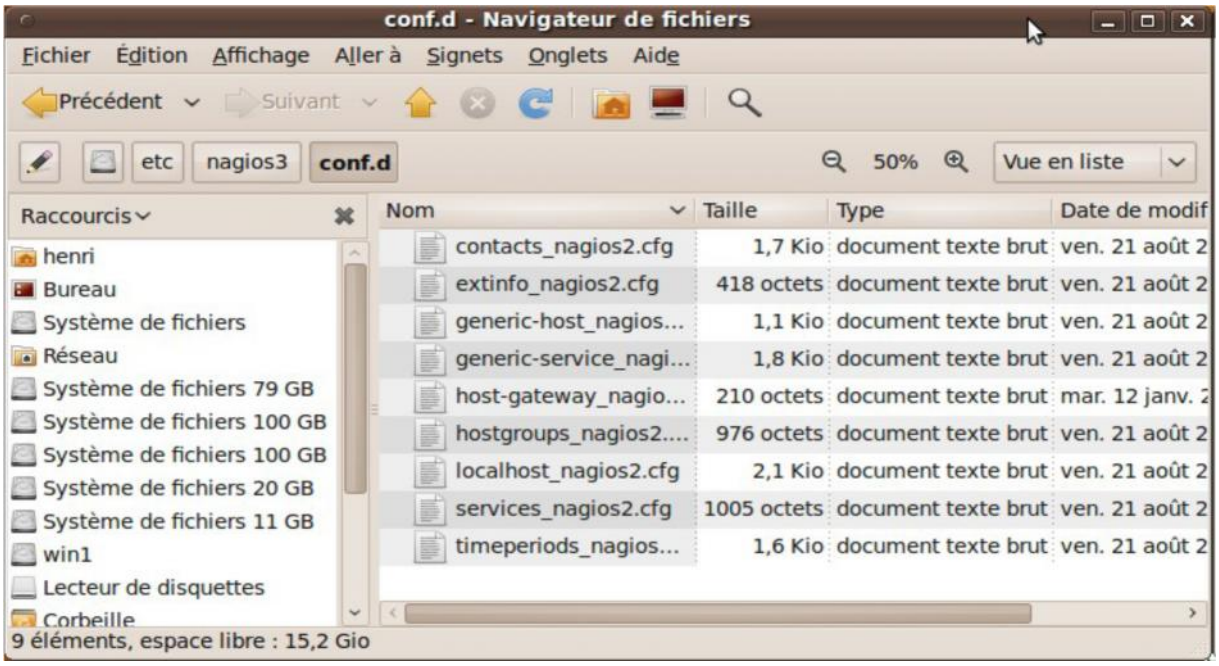


Figure IV.8 Liste des hôtes et services

Accédons au répertoire /etc/nagios3/conf.d qui contient 9 fichiers de configuration et examinons les.

localhost_nagios2 : c'est l'un des fichiers les plus importants. Il contient le paramétrage des hôtes et services à monitorer. Il constitue une fusion des deux fichiers des hôtes «hosts.cfg» et «services.cfg» dans une configuration mieux structurée.

```
# Déclaration de la machine localhost, seule à surveiller pour l'instant.
define host             {
                          use generic-host      ; utilisation d'un modèle d'hôte
                          host_name localhost ; nom de la machine
                          alias localhost
                          address 127.0.0.1
                           }
```

On peut ajouter un nouveau serveur de la manière suivante :

```
define host             {
                          use generichost ; utilisation d'un modèle d'hôte
                          host_name  BELKHODJA-PC  ; nom de la machine
                          alias ma machine win
                          address 192.168.1.4 ;   adresse IP
                           }
```

Un nouveau service concernant belkhodja-pc sera déclaré ainsi :

```
# Se contente de pinger l'hôte merlin
define service          {
                                host_name belkhodja-pc
                           service_description PING
                          check_command c**heck_ping!100.0,20%!500.0,60%**

                          use                           genericservice
                            notification_interval 0 ; s et > 0 if you want to be renotified
                                }
# Définition d'un service qui va surveiller le nombre n d'utilisateurs connectés
# sur la station localhost. Warning si n > 20 users, état critique si n > 50 users.
define service          {
                              use generic-service; utilisation d'un modèle de service
                         host_name localhost
                        service_description Current Users : nom du service
                              check_command check_users!20!50 # commande check=users
                         }
# Define a service to check the number of currently running procs
# on the local machine. Warning if > 250 processes, critical if
# > 400 processes.
define service          {
                          use generic-service   ; Name of service template to use
                          host_name localhost
                          service_description Total Processes
                          check_command check_procs!250!400
                           }
```

```
# Define a service to check the load on the local machine.
define service  {
                    use generic-service; Name of service template to use
                    host_name localhost
                   service_description Current Load
               check_command check_load!5.0!4.0!3.0!10.0!6.0!4.0
                  }
```

IV.5.5 Test de la configuration

Test de la configuration
commande : exécuter #nagios3 v
/etc/nagios3/nagios.cfg
Si la vérification ne fournit pas d'avertissement (warning) ni de message on a réussi a finir l'installation avec succès .
d'erreur (error). Elle doit se terminer de la manière suivante :
Checking time periods...
Checked 4 time periods.
Checking for circular paths between hosts...
Checking for circular host and service dependencies...
Checking global event handlers...
Checking obsessive compulsive processor commands...
Checking misc settings...
Total Warnings: 0
Total Errors: 0
Things look okay No
serious problems were detected during the preflight
check

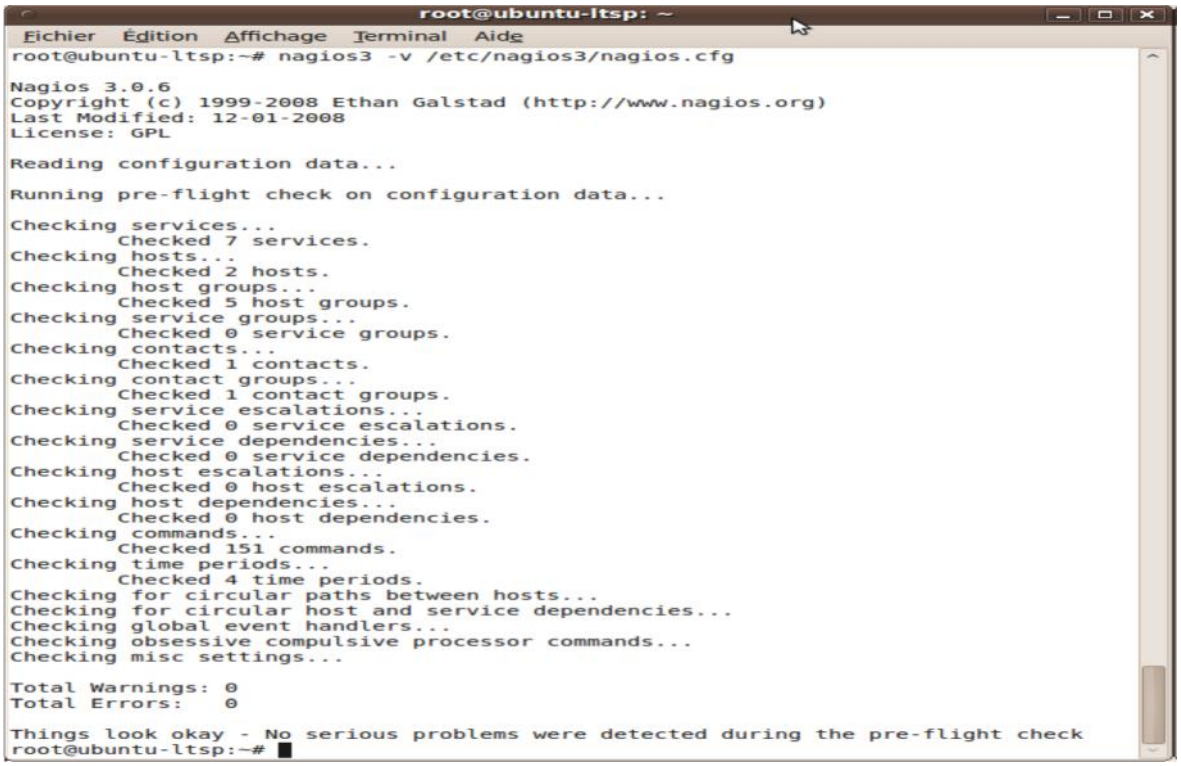
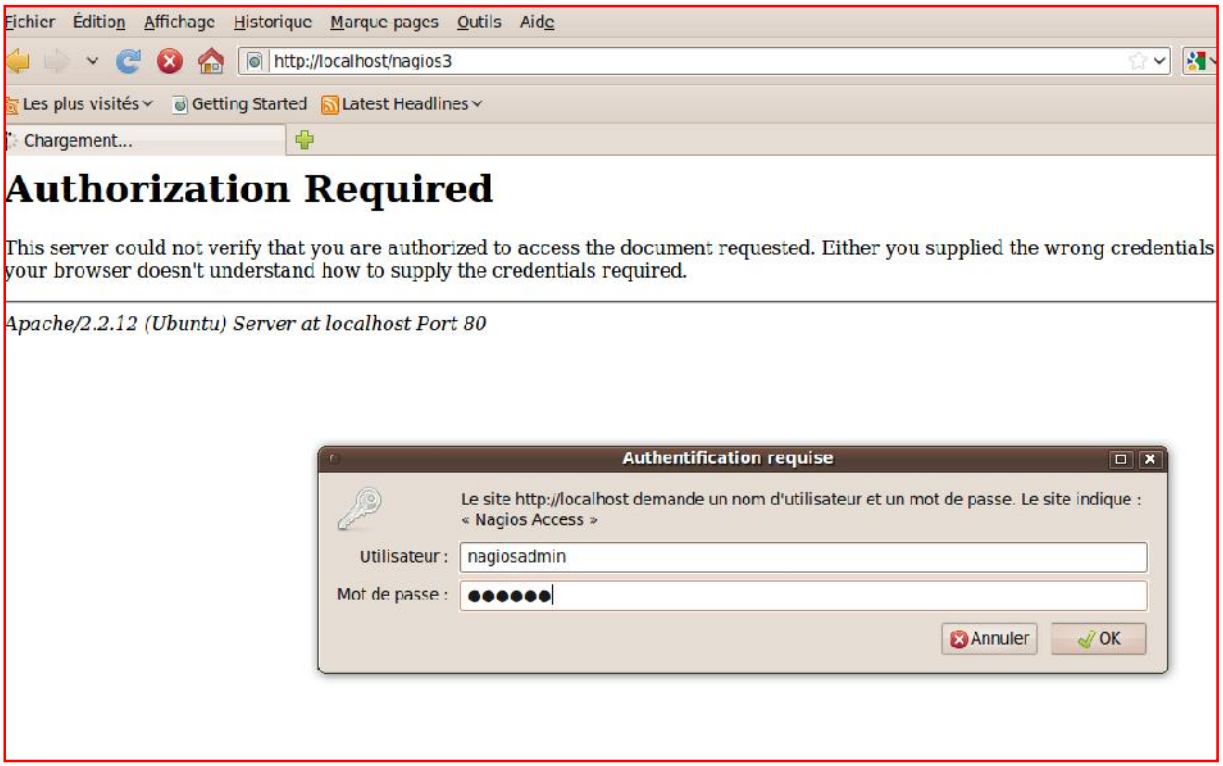
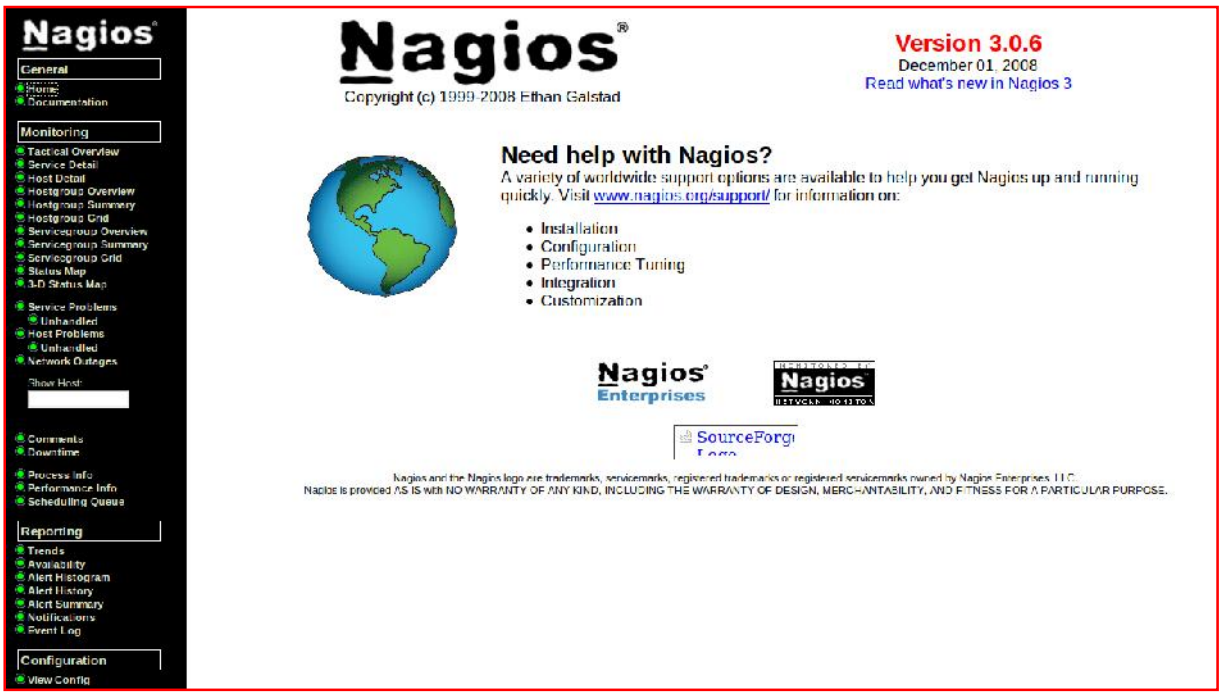


Figure IV.9 éxecution test configuration

Connexion à l'interface Web

Vous devriez pouvoir maintenant accéder à l'interface Web de Nagios avec l'adresse ci-dessous. Le nom d'utilisateur (nagiosadmin) et le mot de passe définis précédemment vous sont demandés. http://localhost/nagios/





Cliquez sur le lien "Service Detail" de la barre de navigation pour voir ce qui est surveillé sur votre machine locale. Quelques minutes seront nécessaires à Nagios pour vérifier tous les services associés à votre machine.

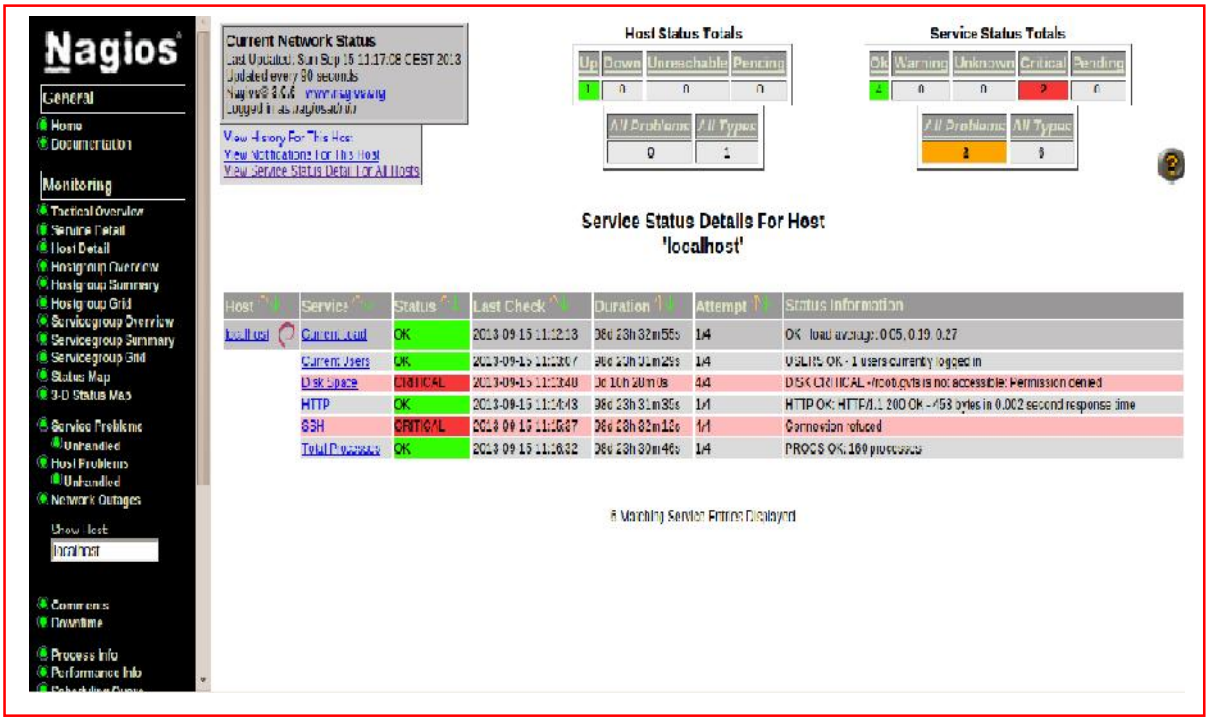


Figure IV.10: service détail pour une machine localhost

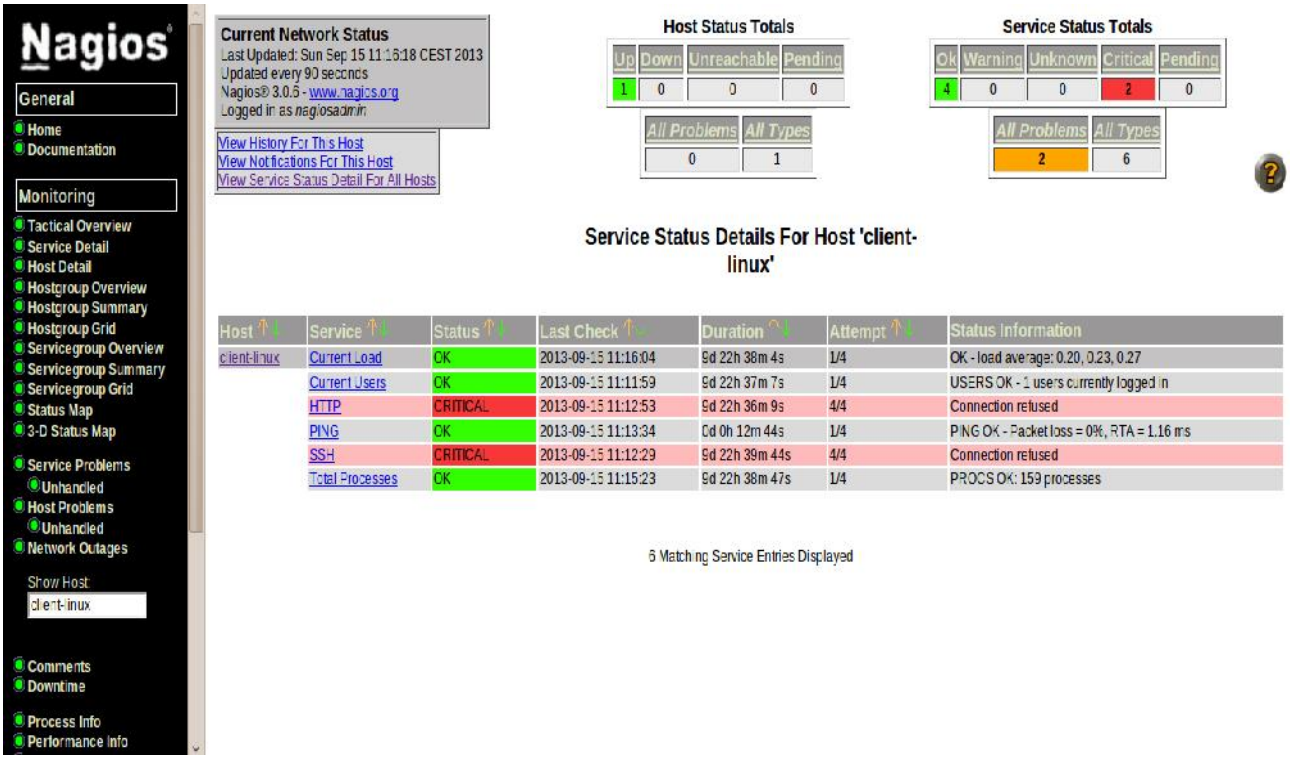


Figure IV.11 : service détail pour une machine linux

Maintenant, nous allons lister les principaux fichiers de configuration de Nagios. Ils ne sont pas tous mentionnés, seulement les plus importants. Ces fichiers se trouvent dans le répertoire /etc/nagios du répertoire d'installation de Nagios.

Fichiers	Description
cgi.cfg	Configuration du site web et des cgi (authorization).
checkcommands.cfg	Définition des tests.
contactgroups.cfg	Définition des groupes d'administrateurs.
contatcs.cfg	Définition des administrateurs (droits, adresse mail, nature des alertes…)
hostextinfo.cfg	Définissions complémentaires des machines pour la cartographie du réseau par les cgi de l'interface web (icône, emplacement…)
hostgroups.cfg	Définition des groupes de machines.
hosts.cfg	Définition des machines
miscommands.cfg	Définition des commandes. Notamment celle d'envoie par mail (host-notify-by-email)
nagios.cfg	Fichier de configuration principal (emplacement des fichiers, gestion des logs, user et group, comportement général…).
resource.cfg	Définition des variables. Notamment $USER1 = chemin d'accès aux plugins)
services.cfg	Définition des services à superviser. C'est le plus gros fichier à écrire. On y renseigne tous les services de toutes les machines que Nagios devra gérer.

Table IV.1 : Les fichiers de configuration

IV.6 Nsclient++

NSClient se base sur une architecture client/serveur. La partie cliente (nommée **check_nt**), doit être disponible sur le serveur Nagios. La partie serveur (**NSClient++**) est à installer sur chacune des machines Windows à surveiller.

IV.6.1. Configuration de Nagios pour surveiller vos machines Windows

Une fois le client et le serveur installé, il faut configurer Nagios de la manière suivantes. Il faut dans un premier temps éditer votre fichier de configuration des hosts (hosts.cfg par défaut) et y ajouter votre machine Windows:

```
Define host {
use generic-hosthost_name  belkhodja-PC

alias Ma machine Win
address 192.168.1.4}
```

Puis ajouter les services offerts par NSClient (dans le fichier services.cfg):

```
# Affiche la version du NSClient
define service {
use generic-service
host_name belkhodja
service_description VERSION
check_command check_nt!CLIENTVERSION
}

# Temps écoulé depuis le dernier reboot (uptime)
define service {
use generic-service
host_name  belkhodja-PC
service_description UPTIME
check_command check_nt!UPTIME
}

# Charge CPU
# WARNING si charge > 80% pendant plus de 5 minutes
# CRITICAL si charge > 90% pendant plus de 5 minutes
define service {
use generic-service
host_name  belkhodja-PC
service_description CPU
check_command check_nt!CPULOAD!-l 5,80,90}
# Etat de la mémoire vive libre
# WARNING si mémoire > 80%
```

```
  # CRITICAL si mémoire > 90%
  define service {
use generic-service
host_name  belkhodja-PC
  service_description MEM
  check_command check_nt!MEMUSE!-w 80 -c 90}
  # Etat de la mémoire disque libre (sur disque c:)
  # WARNING si mémoire > 80%
  # CRITICAL si mémoire > 90%
  define service {
  use generic-service
  host_name belkhodja-PC
  service_description DISK
  check_command check_nt!USEDDISKSPACE!-l c -w 80 -c 90}
```

Pour monitorer des clients Windows avec Nagios il faut passer par l'installation d'un agent nagios, ici le choix se portera sur **NSClient**

mais il en existe d'autres comme NCNET. NSClient communiquera directement avec Check NT (voir schéma fonctionnel).

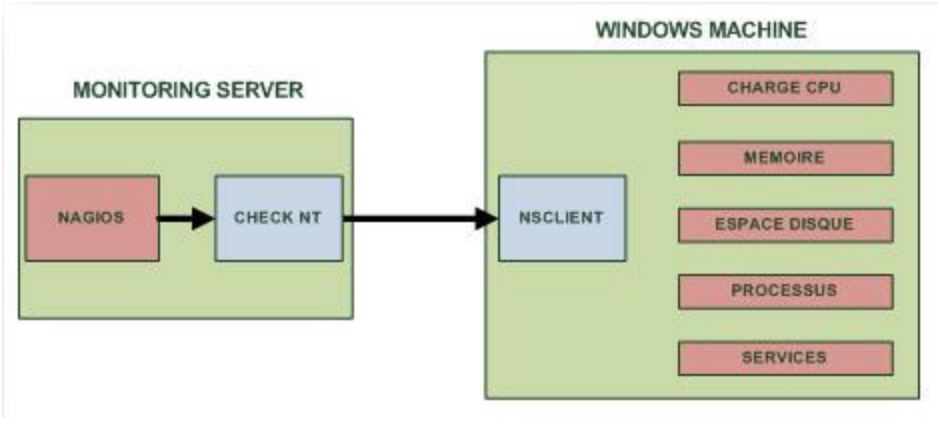


Figure IV.12 : Schéma fonctionnel de Nagios couplé à NSClient

Configuration de NAGIOS pour accueillir des hôtes Windows

On va modifier la configuration de Nagios pour qu'ils connaissent l'hôte que l'on va superviser, pour cela on va modifier le fichier de config principal de Nagios pour accepter les clients Windows:

```
vim /usr/nagios/etc/nagios.cfg
```

Dans ce fichier on va dé commenter cette ligne :

```
#cfg_file=/usr/nagios/etc/objects/windows.cfg
```

Une fois décommenté on l'enregistre et on ferme. Maintenant on va ouvrir le fichier **windows.cfg** pour y rajouter le nom d'hôte à monitorer et les services à surveiller

```
vim /usr/nagios/etc/objects/windows.cfg
```

Une fois ce fichier ouvert il faut rajouter le nom du serveur :

```
define host{
        use             windows-server
        host_name       servfichier
        alias           servfichier
        address         192.168.0.225
        }
```

Ensuite suivant les services que vous voulez surveiller il faut rajouter le nom d'hôte toujours dans le même fichier :

```
define service{
        use                     generic-service
        host_name               servfichier
        service_description     NSClient++ Version
        check_command           check_nt!CLIENTVERSION
        }
```

Maintenant il faut ouvrir le fichier de configuration commands.cfg pour mettre un mot de passe pour la communication entre NSClient et le CHECK NT de Nagios

```
vim /usr/nagios/etc/objects/commands.cf
```

```
# 'check_nt' command definition
define command{
        command_name    check_nt
        command_line    $USER1$/check_nt -H $HOSTADDRESS$ -p 12489 -v $ARG1$
$ARG2$ -s Ton_password
        }
```

Il faudra se rappeler de ce mot de passe car on l'utilisera plus tard pour la config client.

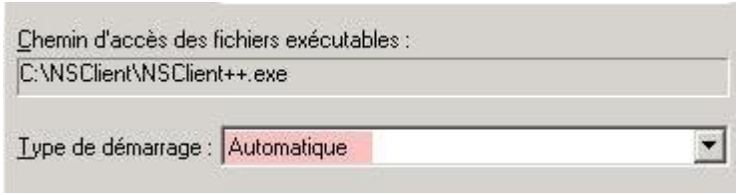
Installation de NSClient sur le serveur Windows:

Le logiciel NSClient est disponible à cette adresse : http://sourceforge.net/projects/nscplus

Une fois télécharger il faut dézipper l'archive par exemple dans C : maintenant il faut ouvrir une invite de commande dans C:\NSClient Et tapez ce qui suit :

```
nsclient++.exe /install
nstray.exe
```

Ensuite il faut ouvrir la mmc **services.msc** et configurer le démarrage automatique du service et l'autoriser à interagir avec le bureau



Ensuite on va éditer le fichier **NSC.ini** pour configurer la connexion entre le serveur à monitorer et nagios. Dans ce fichier il faut décommenter tous les modules de la section **[MODULES]** à l'exception de **checkWMI.dll** et **RemoteConfiguration.dll**

```
[modules]
;# NSCLIENT++ MODULES
;# A list with DLLs to load at startup.
;  You will need to enable some of these for NSClient++ to work.
; ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! !
; *                                                               *
; * N O T I C E ! ! ! - Y O U   H A V E   T O   E D I T   T H I S *
; *                                                               *
; ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! !
FileLogger.dll
CheckSystem.dll
CheckDisk.dll
NSClientListener.dll
NRPEListener.dll
SysTray.dll
CheckEventLog.dll
CheckHelpers.dll
;CheckWMI.dll
;
; RemoteConfiguration IS AN EXTREM EARLY IDEA SO DONT USE FOR PRODUCTION ENVIROMNEMTS!
;RemoteConfiguration.dll
; NSCA Agent is a new beta module use with care!
NSCAAgent.dll
; LUA script module used to write your own "check deamon" (sort of) early beta.
LUAScript.dll
; Script to check external scripts and/or internal aliases, early beta.
CheckExternalScripts.dll
; Check other hosts through NRPE extreme beta and probably a bit dangerous! :)
NRPEClient.dll
; Extreamly early beta of a task-schedule checker
CheckTaskSched.dll
```

Ensuite il faut changer le **password** dans la section **[Settings]** pour que le client communique avec Nagios. On a entré le password pour nagios un peu plus haut, bien entendu il faut que ce soit le même.

```
;# PASSWORD
;  This is the password (-s)
access the daemon remotly.
password=Ton_Password
```

Ensuite il faut décommenter **allowed_hosts** option toujours dans la section **[Settings]**. Et il faut rajouter l'**adresse IP du serveur Nagios** avec lequel il va communiquer.

```
;# ALLOWED HOST ADDRESSES
;  This is a comma-delimited list of IP .
;  If leave this blank anyone can access
;  The syntax is host or ip/mask so 192.:
allowed_hosts=Adresse IP de Nagios
```

Ensuite il faut vérifier la ligne ou se configure le **port** sur lequel NSClient va communiquer par défaut c'est le **12489** (décommenter la ligne si elle est commentée et penser bien à l'ouvrir dans le pare-feu en TCP)

```
;# NSCLIENT PORT NUMBER
;  This is the port the NSClientListener.dll will listen to.
port=12489
```

Voilà la configuration de NSClient et Nagios est terminé donc maintenant on va démarrer NSClient :

```
nsclient++.exe /start
```

Maintenant on vérifie la configuration de nagios

```
/usr/nagios/bin/nagios -v /usr/ nagios/etc/nagios.cfg
```

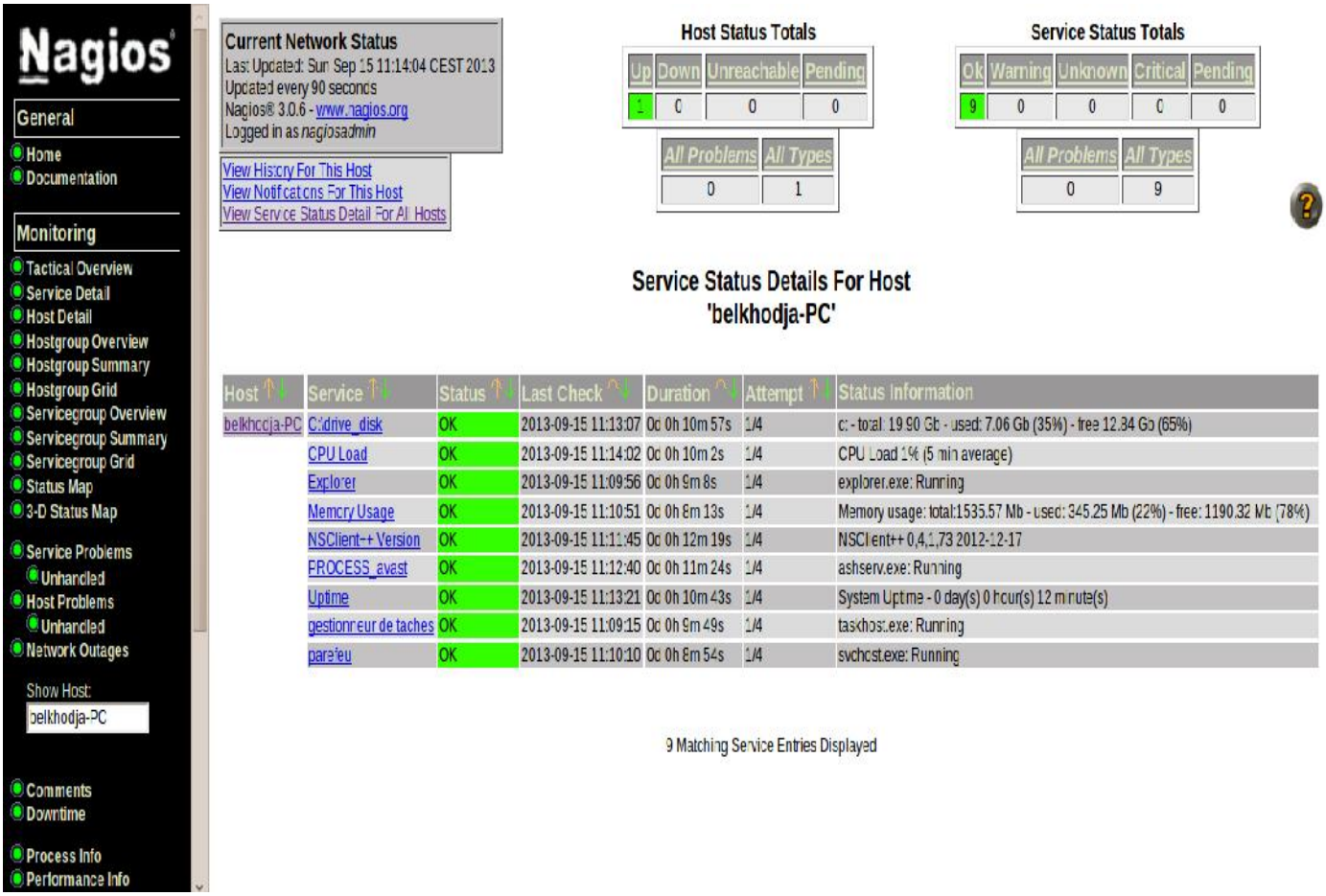


Figure IV.13 : Services détaillé pour une machines Windows

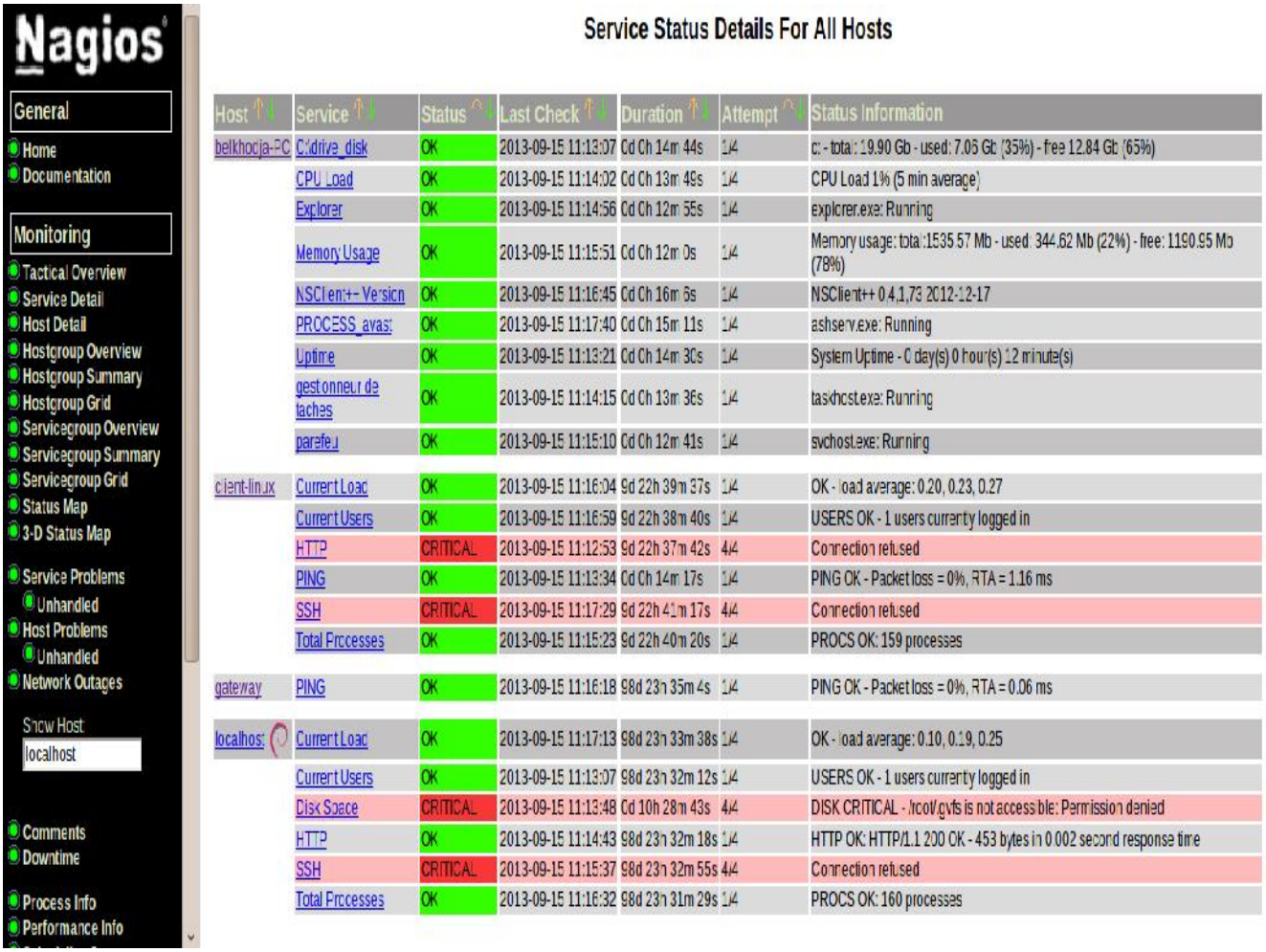


Figure IV.14 : Services détaillé pour tous les machines

IV.7 Conclusion

Avec les tests que nous pouvons conclure que Nagios est un outil qui fournit une analyse du trafic, le contrôle des liens, services de vérification et même de dispositifs qui prennent en charge SNMP avec Nagios. Malgré la complexité dans la mise en, pourrait déployer un système qui permet au gouvernement central pour contrôler l'ensemble du réseau et d'alerter la personne responsable pour les points de défaillance sont rapidement résolus.

Conclusion Générale

Conclusion générale

Nous sommes intéressées dans notre projet par un service importante pour un administrateur réseau notre travail a été consacré sur la notion de base de la supervision qui est devenue indispensable dans tout système d'information.

Il faut pouvoir surveiller de manière continu l'état des systèmes d'information afin d'éviter un arrêt de production de trop longue durée. C'est là ou la supervision intervient. Elle doit permettre d'anticiper les problèmes et de faire remonter des informations sur l'état des équipements. Donc nous avons donnés tous les étapes nécessaires de l'installation et de configuration d'un service de supervision Nagios.

Nagios est un logiciel qui fonctionne sous Linux et qui permet d'effectuer cette supervision.

Il utilise des plugins pour communiquer avec les machines hôtes et ainsi avoir une vue globale du réseau, avec les états des différentes machines.

De plus notre projet peut être développé par ceux qui veulent continuer ce travail pour rendre le système plus sécurisé et performant.

Bibliographie

Bibliographie

[1] www.trendmicro.fr/Virtualization

[2] http://doc.ubuntu-fr.org/virtualbox

[3] Thomas Vantroys supervision des réseaux Université de Lille I Laboratoire d'Informatique Fondamentale de Lille 2009-2010

[4] François Borderies, Olivier Chatel, Jean-Christophe Denis, Didier Reis, Administration Réseau,1 juillet 1993.

[5] youceuf NTCHIRIFOU Monitoring d'une infrastructure informatique sur base d'outils libre institut africain d'administration et d'études commerciale (IAEC)TOGO Master 2010

[6] LECORCHE Hubert - JEANDROZ Sylvain, SUPERVISION RESEAU AVEC NAGIOS

[7] M. Grégory Bernard, Présentation de l'outil d'administration de réseau Nagios, projet,octobre 2003,

[8] www.nagios.org/download/

[9] www.guellec.fr/ressources/articles/nagios.php

[10] http://doc.ubuntu-fr.org/nagios

[11] igm .univ-mlv.fr

[12] www.reseaumaroc.com

[13] www.nicosphere.net/lunix

[14] http://lunixetleschoses.tuxfamily.org

[15]. http://www.guill.net

Table des illustrations

Liste des figures

Liste des tableaux

Liste des Acronymes

Liste des acronymes

C

CGI : Common Gate Interface

H

HTTP: Hyper Texte Transfert Protocol

M

MIB: Management Information Base

MRTG: Multi Router Traffic Grapher

N

NSCA: : Nagios Service Check Acceptor

NRPE: Nagios Remote Plugin Execut

O

OID: Object Identifier

OVOW: OpenView Opération for Windows

S

SNMP: Simple Network Management Protocol

T

TCP: Transmission Control Protocol

U

UDP: User Datagram Protocol

V

VM: virtuelle machine

ملخص

الهدف من مشروعنا هو محاكاة الشبكة الافتراضية من خلال استخدام . على هذه الشبكة الافتراضية
للكشف عن العيوب في مختلف أجهزة هذه الشبكة بواسطة برنامج Nagios، SNMP
مما مكننا من تعميم هذا الحل على شبكة حقيقية تحتوي انظمة تشغيل مختلفة .

Résumé

L'objectif de notre projet et de simuler un réseau via la virtualisation en utilisant une solution existante .Sur ce réseau virtuel on a pu mètre en place une solution de supervision (SNMP,Nagios) permettant de détecter les pannes sur les différentes stations de se réseau virtuel qui nous aides a généraliser cette solution sur un réseau physique qui contient des architecture système différentes

Mots clés : Virualisation ,Supervision, Réseaux NAGIOS

Abstract

The objective of our project to simulate a network through virtualization using an existing solution. On this virtual network we could put a monitoring solution (SNMP, Nagios) for detecting faults on the various stations to virtual network t in order to generalize this solution to a physical network which contains a different system .
Keywords: Virualisation, Supervision, Networks NAGIOS