

Projet : Réseaux et interconnexion

Filière : 5^{ème} Année Télécoms Réseaux et Systèmes Embarqués

Thème : Supervision d'un réseau avec NAGIOS



Réalisé par :

SALIOU Mohamadou

NIKIEMA Roukiatou

MHIDI Abdelhak

Encadré par :

M. SAIDI Abdelali

Remerciements

Avant tout propos nous tenons à remercier Dieu tout puissant qui nous a donné la patience, la volonté, le courage d'aller jusqu'au bout de notre travail.

Nous tenons évidemment à remercier, Mr Saidi Abdelali, qui est notre Professeur actuel à l'IGA, pour sa patience et le partage de son expertise au quotidien.

Résumé

La taille des réseaux ne cessant de grandir de jour en jour et l'importance de ceux-ci dans le monde de l'entreprise prenant une place prépondérante, le besoin de contrôler en temps réel leur qualité et leur état est rapidement devenu une priorité. C'est dans ce but qu'est apparu, il y a maintenant une vingtaine d'années, le concept de supervision de réseaux.

Nous présenterons dans ce rapport ce qu'est la supervision de réseaux ainsi qu'une implémentation sur une machine virtuelle.

Pour ce faire nous allons définir le concept et la notion de la supervision de réseaux. Nous allons aussi faire l'étude de Nagios qui est un outil de supervision. Enfin nous allons procéder à sa mise en œuvre.

Tables des Matières

Projet : Réseaux et interconnexion.....	1
Remerciements.....	2
Résumé.....	3
Tables des Matières.....	4
Introduction générale.....	5
Chapitre I: Notion de Supervision.....	6
I.1-Qu'est-ce-que c'est que la supervision ?.....	7
I.2-Comment fonctionne la supervision réseau ?.....	7
I.3-Les fonctions des logiciels de supervision réseau [1].....	10
I.4-Comment un outil de supervision réseau surveille-t-il le réseau ? [1].....	14
I.4.1 Protocole SNMP (Simple Network Management Protocol).....	14
I.4.2 Protocole WMI (Windows Management Instrumentation).....	15
Chapitre II: Etude Nagios.....	16
II.1- Présentation.....	17
II.1.1- Nagios [3].....	17
II.2- Architecture [2].....	17
II.3- Fonctionnalités [2].....	18
II.4-Détermination de l'état et du type d'état des hôtes.....	19
II.4.1- Détermination de l'état des hôtes et/ou des services du réseau.....	19
II.5- Plugins.....	20
Chapitre 3: Installation et configuration du serveur Nagios.....	21
1- Configuration de Nagios.....	22
Les Prérequis.....	22
Étapes d'installation de Nagios sur Ubuntu [4].....	22
Étape 1 : Mise à jour du système.....	22
Étape 2 : Installation des dépendances nécessaires.....	22
Étape 3 : Création d'un utilisateur et d'un groupe pour Nagios.....	24
Étape 4 : Téléchargement et installation de Nagios Core.....	24
Étape 5 : Installation de plugins Nagios.....	25
Étape 6 : Configuration de Nagios.....	25
Étape 7 : Vérification de l'installation et changement des droits utilisateurs....	28
Étape 8: Installation de NDO et NDO2DB.....	28
2- Monitoring Avec Nagios [5].....	33
2-1 Configuration pour le monitoring.....	33
2-2 Configuration du client NSclient sur windows [6].....	36
Conclusion général.....	41

Références.....	42
-----------------	----

Table des illustrations

Figure 1 : La supervision.....	8
Figure 2 : Fonctionnement de la supervision réseaux.....	9
Figure 3 : Cartographie avec nagios.....	13
Figure 4 : Supervision avec nagios.....	14
Figure 5 : Alerte avec nagios.....	15
Figure 6 : Architecture de Nagios.....	20
Figure 7 : Fonctionnalité.....	22
Figure 8 : Fichier nagios.cfg.....	38
Figure 9 : Redémarrage des services NSClients.....	42
Figure 10 : Interface Nagios.....	43
Figure 11 : Vue des machines supervisées.....	43
Figure 12 : Services Monitorés.....	44
Figure 13 : Etats des services Monitorés.....	45
Figure 14 : Vue en Diagramme des machines monitorées.....	45
Figure 15 : Fonctionnalités de monitoring.....	46
Figure 16 : Ensembles des services activés.....	46

Introduction générale

Les systèmes d'information sont tous différents par leur taille, leur nature, leur criticité. Ils ont cependant pour point commun d'être le théâtre d'incidents, à un moment ou à un autre. Un des rôles des administrateurs est justement de gérer cela. Ils doivent concevoir l'architecture du système d'information de telle manière qu'une panne ait un impact minimal sur le reste du système.

Les administrateurs ont un objectif clair : le maintien en production du système d'information. Cependant, tous les éléments ne sont pas logés à la même enseigne en ce qui concerne la criticité. Certaines parties sont vitales pour l'entreprise, comme les serveurs. Sans outil de supervision, il est quasi impossible pour un administrateur de garder en tête ces différents niveaux de criticité.

L'outil de supervision peut ainsi aider à mettre des priorités sur les interventions des administrateurs et leur permettre de se concentrer sur l'essentiel.

C'est pourquoi les administrateurs réseaux et systèmes 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. Il peut être aussi informé (par email, par SMS) en cas de problème.

C'est ainsi que le présent travail nous a été demandé : supervision d'un réseau avec nagios. Pour ce faire nous allons définir le concept et la notion de la supervision de réseaux. Nous allons aussi faire l'étude de Nagios qui est un outil de supervision. Enfin nous allons procéder à sa mise en œuvre.

Chapitre I: Notion de Supervision

I.1 - Qu'est-ce que c'est que la supervision ?



Figure. 1 : La supervision

La supervision réseau fait référence à la surveillance du bon fonctionnement des réseaux informatiques et des services informatiques connectés sur ces réseaux. L'analyse du réseau est un processus informatique critique dans lequel tous les composants de mise en réseau tels que les routeurs, les commutateurs, les pare-feu, les serveurs et les machines virtuelles sont analysés pour détecter les pannes et les performances et évalués en continu pour maintenir et optimiser leur disponibilité.

I.2-Comment fonctionne la supervision réseau ?

La supervision réseau adopte certains mécanismes tel que:

- Analysez l'essentiel

Les périphériques réseau défectueux ont un impact sur les performances du réseau. Cela peut être éliminé grâce à une détection précoce et c'est pourquoi l'analyse continue du réseau et des périphériques associés est essentielle.

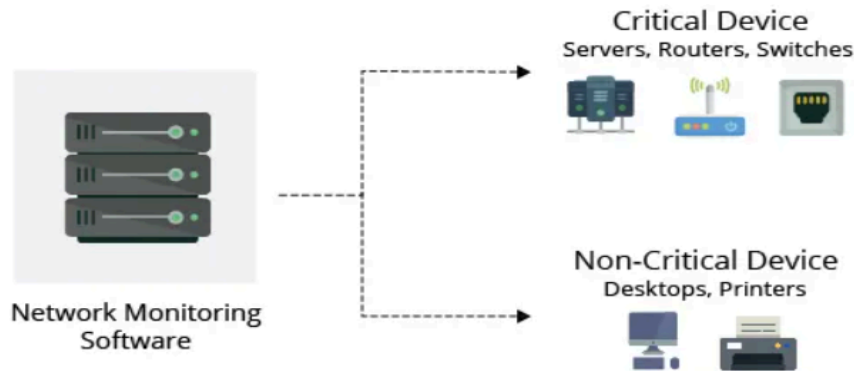


Figure 2 : Fonctionnement de la supervision réseaux

Dans une supervision réseau efficace, la première étape consiste à identifier les périphériques et les mesures de performances associées à contrôler. La deuxième étape consiste à déterminer l'intervalle d'analyse. Les périphériques tels que les ordinateurs de bureau et les imprimantes ne sont pas critiques et ne nécessitent pas de contrôle fréquent, tandis que les serveurs, les routeurs et les commutateurs effectuent des tâches critiques pour l'entreprise, mais ont en même temps des paramètres spécifiques qui peuvent être analysés de manière sélective.

- Optimiser l'intervalle d'analyse

L'intervalle d'analyse détermine la fréquence à laquelle les périphériques réseau et les mesures associées sont interrogés pour identifier les performances et l'état de disponibilité. La configuration d'intervalles d'analyse peut aider à alléger le système d'analyse du réseau et, à son tour, vos ressources. L'intervalle dépend du type de périphérique réseau ou du paramètre surveillé. L'état de disponibilité des appareils doit être contrôlé avec le plus petit intervalle de temps, de préférence toutes les minutes. Les statistiques du CPU et de la mémoire peuvent être contrôlées toutes les 5 minutes. L'intervalle d'analyse pour d'autres mesures telles que l'utilisation du disque peut être étendu et est suffisant s'il est interrogé toutes les 15 minutes. L'analyse de chaque appareil au moins de ces intervalles ne fera qu'ajouter une charge inutile au réseau et n'est pas tout à fait nécessaire.

- Choisir le bon protocole

Lors de l'analyse d'un réseau et de ses périphériques, une bonne pratique courante consiste à adopter un protocole de gestion de réseau sécurisé et ne consommant pas de bande passante pour minimiser son impact sur les performances du réseau. La plupart des périphériques réseau et des serveurs Linux prennent en charge SNMP (Simple Network Management Protocol) et les protocoles CLI et les périphériques Windows prennent en charge le protocole WMI. SNMP est l'un des protocoles largement acceptés pour gérer et analyser les éléments du réseau. La plupart des éléments du réseau sont fournis avec un network protocols to manage and monitor network elements. La plupart des éléments du réseau sont fournis avec un agent SNMP. Ils doivent simplement être activés et configurés pour communiquer avec le système de gestion de réseau (NMS). Autoriser l'accès en lecture-écriture SNMP donne un contrôle complet sur le périphérique. En utilisant SNMP, on peut remplacer la configuration entière de l'appareil.

Un système d'analyse du réseau aide l'administrateur à prendre en charge le réseau en définissant des privilèges de lecture/écriture SNMP et en restreignant le contrôle pour les autres utilisateurs.

- Fixer des seuils

Les temps d'arrêt du réseau peuvent coûter beaucoup d'argent. Dans la plupart des cas, l'utilisateur final signale un problème de réseau à l'équipe de gestion du réseau. La raison derrière cela est une mauvaise approche d'analyse proactive du réseau. Le principal défi d'analyse réseau en temps réel est d'identifier de manière proactive les goulots d'étranglement des performances. C'est là que les seuils jouent un rôle majeur dans le contrôle du réseau. Les limites de seuil varient d'un appareil à l'autre en fonction du cas d'utilisation professionnelle.

Remarque : Alerte instantanée basée sur des violations de seuil.

La configuration des seuils permet d'analyser de manière proactive les ressources et les services exécutés sur les serveurs et les périphériques réseau. Chaque appareil peut

avoir un intervalle ou une valeur seuil définie en fonction des préférences et des besoins de l'utilisateur. Un seuil à plusieurs niveaux peut aider à classer et à décomposer tout défaut rencontré. En utilisant des seuils, les alertes peuvent également être déclenchées avant que l'appareil ne tombe en panne ou n'atteigne un état critique.

La surveillance du réseau porte plus spécifiquement sur :

- la **qualité** (bande passante)
- la **sécurité** de la connexion Internet
- mais aussi, par extension, à l'état des services et matériels connectés : serveurs, imprimantes, postes de travail, etc.

La supervision réseau est l'un des 3 types de supervision informatique avec la **supervision système** (bas niveau), la **supervision applicative** et la **supervision Base de données** .

I.3-Les fonctions des logiciels de supervision réseau [1]

Nous avons abordé les bases de la mise en réseau, parlons maintenant des bases des systèmes de supervision réseau, ou NMS (Network Management Station).

Les systèmes de supervision réseau assurent cinq fonctions de base :

- Découvrir
- Cartographier
- Monitorer
- Alerter
- Rapporter

Remarque : Les NMS diffèrent dans les capacités qu'ils fournissent pour chacune de ces fonctions.

➤ **Découvrir** : Recherchez les périphériques sur votre réseau

La supervision réseau commence par le processus de découverte. En termes simples, si vous ne savez pas ce qu'il y a sur le réseau et de quelle manière il est connecté, vous ne pouvez pas le surveiller. Les NMS découvrent les périphériques sur le réseau - les routeurs, les commutateurs, les pare-feu, les serveurs, les imprimantes et bien plus encore.

Les NMS comprennent une bibliothèque de modèles de surveillance, qui définit la manière de surveiller un périphérique. Sur WhatsUp Gold, ces modèles sont appelés rôles de périphériques.

Les rôles de périphérique sont spécifiques au type et au fournisseur. Par exemple, ce que vous surveillez sur un routeur Cisco sera différent de ce que vous surveillez sur un serveur Dell.

Lorsqu'un logiciel de supervision réseau termine le processus de découverte, il attribue automatiquement un rôle de périphérique approprié à chaque périphérique découvert.

Les NMS diffèrent par leurs capacités de découverte. Tous les NMS découvrent les appareils sur le réseau. Cependant, tous ne découvrent pas comment les périphériques sont connectés au réseau. Par exemple, un NMS peut avoir identifié un serveur sur le réseau. Mais il ne saura pas à quel commutateur il est connecté.

Un NMS avec découverte de la couche 2/3 découvrira la connectivité de port à port entre les périphériques sur le réseau. Pour une supervision efficace du réseau, il ne suffit pas de savoir ce qui s'y trouve, il faut aussi comprendre comment il est connecté.

➤ Cartographier : Visualisez votre réseau

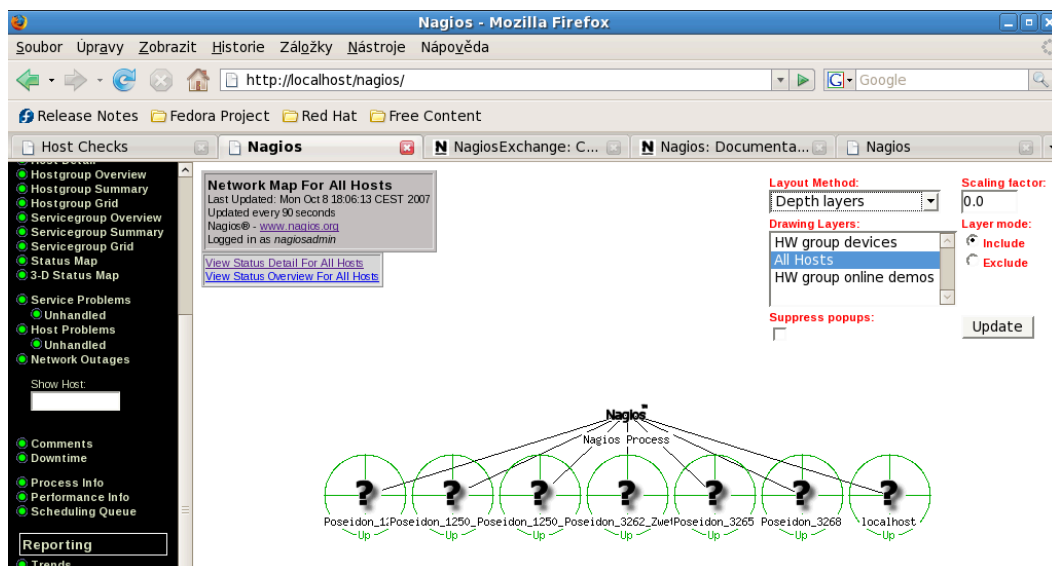


Figure 3 : Cartographie avec nagios

Les yeux d'un administrateur de réseau sont son outil de diagnostic le plus précieux. Leur capacité à visualiser leurs réseaux peut leur faire gagner des heures, voire des jours, dans la résolution des problèmes de réseau.

Malheureusement, les armoires de câblage du réseau deviennent complexes et désordonnées. Cela limite la capacité de l'administrateur réseau à visualiser le réseau et entrave la résolution des problèmes.

Les logiciels de supervision réseau génèrent des cartes réseau. Les cartes de réseau constituent un puissant outil de première intervention qui permet aux administrateurs de visualiser leurs réseaux. Elles fournissent une représentation propre et ordonnée de l'armoire de câblage. Les cartes de réseau affichent les dispositifs et leur état à jour.

De nombreux NMS nécessitent une quantité importante de traitement manuel pour créer une carte du réseau. Certains se contentent de fournir un outil de dessin et

s'appuient sur les connaissances de l'administrateur réseau pour cartographier l'infrastructure.

- **Superviser** : gardez un œil sur votre réseau

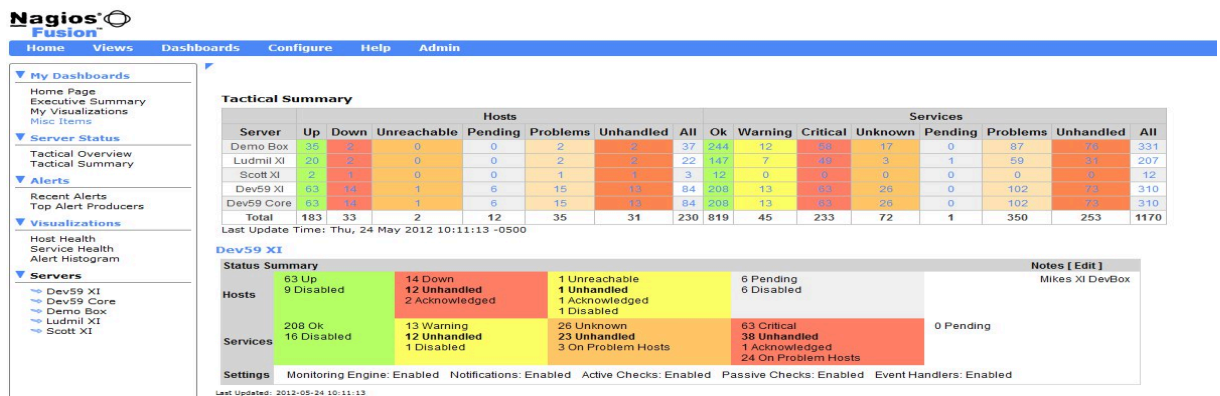


Figure 4 : Supervision avec nagios

Comme nous l'avons dit, les systèmes de supervision réseau fournissent des rôles de périphériques clés en main qui définissent ce qu'il faut superviser. Les administrateurs réseau peuvent modifier les rôles des périphériques ou en créer de nouveaux à partir de zéro. Les NMS exposent les administrateurs réseau à un large choix de moniteurs.

Pour commencer, les administrateurs réseau veulent superviser les « 5 grands » pour tout périphérique sur le réseau. Cela inclut la disponibilité et la latence du Ping, ainsi que l'utilisation du CPU, de la mémoire, du disque et de l'interface.

La plupart des outils de supervision réseau proposent des moniteurs pour d'autres composants matériels, comme les ventilateurs et les alimentations d'un commutateur, et surveillent même la température dans une armoire de câblage. Ils peuvent également surveiller les services réseau tels que HTTP, TCP/IP et FTP.

- **Alerter** : Recevez une notification en cas de panne des périphériques

Date: January 1, 2011 11:06:41 AM GMT+09:00
From: Nagios Monitoring <nagios@frank4dd.com>
Subject: **Nagios: PROBLEM Host dbserver1 (linux-servers) is DOWN**
To: support@frank4dd.com
Cc: acctmgr@frank4dd.com , public@frank4dd.com

Nagios Monitoring System Notification

Notification Type:	PROBLEM
Host Status:	DOWN
Hostname:	dbserver1
Hostalias:	vm20 on vhosting34 server group
IP Address:	70.85.16.87
Hostgroup:	linux-servers
Event Time:	Sat Jan 1 11:06:41 JST 2011
Event Data:	CRITICAL - Host Unreachable (70.85.16.87)

Generated by Nagios, the OpenSource monitoring solution at Frank4DD Systems, Inc.

Figure 5 : Alerte avec nagios

Les alertes basées sur des seuils permettent aux administrateurs réseau de réagir aux problèmes avant qu'ils n'aient un impact sur les utilisateurs, les applications ou l'entreprise. Par exemple, le NMS est configuré pour émettre une alerte lorsque l'utilisation du CPU d'un routeur dépasse 80 %. Cela permet à l'administrateur réseau d'enquêter de manière proactive et de réagir avant que le routeur ne tombe en panne.

Les mesures de performance telles que l'utilisation du CPU, de la mémoire et des interfaces fluctuent au cours de la journée. Elles peuvent dépasser les seuils pendant quelques secondes ou minutes pendant les périodes d'utilisation maximale. Les administrateurs de réseau ne veulent pas être dérangés par ces petits problèmes. Pour éviter cela, les alertes NMS sont configurées avec un élément temporel. Par exemple, si l'utilisation du CPU dépasse 80 % pendant plus de 10 minutes, une alerte est émise.

I.4-Comment un outil de supervision réseau surveille-t-il le réseau ? [1]

Les logiciels de supervision réseau interrogent les périphériques et les serveurs du réseau pour obtenir des données sur les performances à l'aide de protocoles standard tels que :

- SNMP, protocole de gestion de réseau simple
- WMI, Windows Management Instrumentation
- Et SSH, Secure Shell pour serveur Unix et Linux

Les deux protocoles de supervision les plus utilisés sont SNMP et WMI. Ils fournissent aux administrateurs réseau des milliers de moniteurs pour évaluer l'état de santé de leurs réseaux et des périphériques qui s'y trouvent.

I.4.1 Protocole SNMP (Simple Network Management Protocol)

SNMP est un protocole standard qui permet de collecter des données à partir de presque tous les périphériques connectés au réseau, à savoir : les routeurs, les commutateurs, les contrôleurs de réseau local sans fil, les points d'accès sans fil, les serveurs, les imprimantes, etc.

SNMP fonctionne en interrogeant des « objets ». Un objet est un élément sur lequel un NMS collecte des informations. Par exemple, l'utilisation du CPU est un objet SNMP. L'interrogation de l'objet d'utilisation du CPU renvoie une valeur qu'un NMS utilise pour les alertes et les rapports.

Les objets interrogés par SNMP sont maintenus dans une base d'informations de gestion, ou MIB. Une MIB définit toutes les informations qui sont exposées par le dispositif managé. Par exemple, la MIB d'un routeur Cisco contient tous les objets, définis par Cisco, qui peuvent être utilisés pour surveiller ce routeur, tels que l'utilisation de l'unité centrale, l'utilisation de la mémoire et le statut de l'interface.

Les objets d'une MIB sont catalogués à l'aide d'un système de numérotation normalisé. Chaque objet possède son propre identifiant d'objet, ou OID, unique.

Certains NMS fournissent un navigateur de MIB. Un navigateur de MIB permet aux administrateurs réseau de naviguer dans une MIB pour trouver des objets supplémentaires qu'ils veulent surveiller sur un périphérique.

I.4.2 Protocole WMI (Windows Management Instrumentation)

WMI est l'implémentation Microsoft de Web-Based Enterprise Management, une initiative de l'industrie du logiciel visant à développer une norme d'accès aux informations de gestion dans l'entreprise.

Ce protocole crée une interface de système d'exploitation qui reçoit des informations de périphériques exécutant un agent WMI. WMI recueille des détails sur le système d'exploitation, des données matérielles ou logicielles, l'état et les propriétés des systèmes locaux ou distants, des informations sur la configuration et la sécurité, ainsi que sur les processus et les services. Il transmet ensuite tous ces détails au logiciel de gestion du réseau, qui en surveille la santé, les performances et la disponibilité.

Bien que WMI soit un protocole propriétaire pour les systèmes et applications basés sur Windows, il peut fonctionner avec SNMP et d'autres protocoles. Cependant, Microsoft a déprécié les commandes WMI dans Windows en faveur des cmdlets CIM, donc si vous utilisez PowerShell pour gérer WMI, vous devriez plutôt utiliser ces commandes.

Chapitre II: Etude Nagios

II.1- Présentation

II.1.1- Nagios [3]

Autrefois connu sous le nom de Netsaint, NAGIOS est un logiciel de surveillance qui permet à la fois la surveillance active et passive de serveurs, d'équipements et de services réseau. Il assure la surveillance continue des hôtes et des services définis, générant des alertes en cas de dysfonctionnement ou de rétablissement des systèmes. NAGIOS, un logiciel libre sous licence GPL, jouit d'une reconnaissance mondiale dans le domaine de la supervision et est largement adopté par de grands opérateurs.

Un logiciel libre, tel que NAGIOS, se caractérise par la permission d'utiliser, d'étudier, de modifier, de dupliquer et de diffuser le programme, aussi bien sur le plan technique que légal. Les figures clés associées à NAGIOS incluent Ethan Galstad, responsable du développement du daemon Nagios et des mises à jour des différentes versions, ainsi que Karl Deisschop, Subhendu Ghosh, Ton Voon et Stanley Hopcroft, qui ont contribué au développement des plugins associés.

II.2- Architecture [2]

L'architecture de Nagios peut se résumer à travers la figure ci-dessous

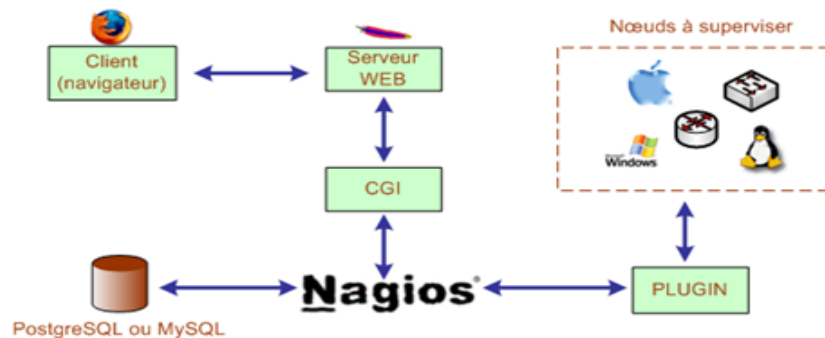


Figure 6 :Architecture de Nagios

Nagios est un programme modulaire composé de trois parties:

Le moteur de l'application qui est un ordonnanceur qui gère:

- L'ordonnancement et les dépendances des vérifications
- Les actions à entreprendre quand un hôte ou un service change d'état (alertes, escalades, corrections automatiques).

L'interface web, qui permet d'avoir une vue d'ensemble du système d'information

à travers des CGI. Les informations que présente l'interface web sont:

- Une vue d'ensemble sur l'état de tous les hôtes et services supervisés 3 travers Je cgi status.cgi.
- Une carte de tous les hôtes définis dans le réseau grâce au cgi statusmap.cgi
- Une interface WAP qui offre l'accès aux informations sur l'état du réseau via un téléphone portable compatible internet grâce au cgi statuswml.cgi
- Un aperçu de tous les hôtes du réseau en utilisant une modélisation 3D dans un langage VRML offert par le cgi statusvrJ.cgi .

Les plugins, qui sont des minis programmes que l'on peut compiler en fonction des besoins de supervision. Nagios exécute un plugin dès qu'il à besoin de connaître l'état d'un service ou d'un hôte et évalue le code de retour de ce plugin. L'avantage de cette architecture est qu'on peut contrôler tout ce que l'on veut à travers les plugins mais le revers est que nagios ne sait ce qu'on contrôle car il ne fait qu'interpréter les résultats.

II.3- Fonctionnalités [2]

Nagios fonctionne sur linux et dans le cas général pour la plupart des systèmes Unix.

Nagios offre les possibilités suivantes:

- La surveillance des services réseaux (SMTP, POP3, HTTP, NTP, PING)
- La surveillance des ressources des hôtes (charge du processeur, utilisation des disques,etc.)
- Le contrôle parallèle des services
- permet de définir la hiérarchie du réseau en utilisant des hôtes parents
- La capacité à définir des gestionnaires d'évènements permettant une résolution proactive des problèmes
- Permet la mise en œuvre d'une redondance des serveurs de supervision
- Une interface web permettant de voir l'état courant du réseau, l'historique des notifications et des problèmes, le fichier journal, etc.

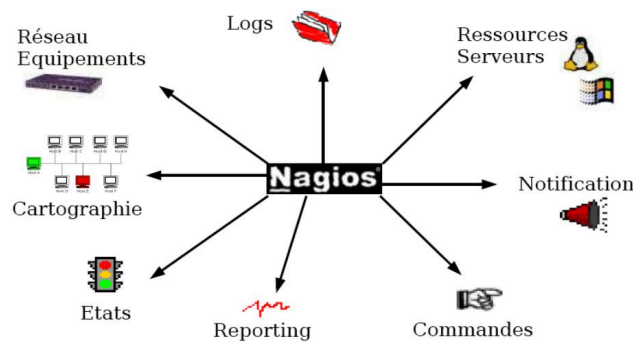


Figure 7 : Fonctionnalité

II.4-Détermination de l'état et du type d'état des hôtes

L'état courant des services et des hôtes est déterminé par deux composants: l'état du service ou de l'hôte (OK, WARNING, UP, DOWN) et le type d'état (HARD ou SOFT) dans lequel il se trouve.

II.4.1- Détermination de l'état des hôtes et/ou des services du réseau

Pour déterminer l'état de l'hôte ou du service, nagios évalue le code de retour des plugins. Nagios distingue quatre types d'états pour les services et trois pour les hôtes.

- ❖ Les états que peuvent avoir un hôte sont:
 - UP: il est en état de répondre ;
 - DOWN: indisponible;
 - UNREACHABLE: état non connu.
- ❖ Les états des services sont :
 - OK: tout va bien
 - WARNING: quelque chose commence à mal aller
 - CRITICAL: la situation du service est très grave et nécessite une intervention immédiate.
 - UNKNOWN: la commande de vérification n'a pas pu obtenir les informations

II.5- Plugins

Il existe de nombreux plugins pour Nagios et nous allons présenter quelques uns dans un tableau :

Nom du Plugin	Fonctionnalités
check_http	Surveillance des services HTTP
check_disk	Surveillance de l'espace disque
check_ping	Surveillance de la connectivité par ping
check_ssh	Vérification de la disponibilité SSH
check_mysql	Surveillance des bases de données
check_snmp	Surveillance des dispositifs SNMP
check_mail	Surveillance des boîtes aux lettres
check_dns	Vérification de la résolution DNS
check_load	Surveillance de la charge du système
check_users	Surveillance du nombre d'utilisateurs connectés
check_tcp	Surveillance de la connectivité TCP
check_udp	Surveillance de la connectivité UDP
check_ssl_cert	Vérification de la validité des certificats SSL

Chapitre 3: Installation et configuration du serveur Nagios

1- Configuration de Nagios

Les Prérequis

- ❖ **Système d'exploitation** : Debian 11 installé et mis à jour.
- ❖ **Accès root ou sudo** : S'assurer d'avoir un accès administratif pour installer des logiciels et exécuter des commandes en tant qu'administrateur.

Étapes d'installation de Nagios sur Ubuntu [4]

Étape 1 : Mise à jour du système

```
Unset  
sudo apt update  
sudo apt upgrade
```

Étape 2 : Installation des dépendances nécessaires

Pour vérifier si le package existe dans le dépôt.

Exemple:

```
Unset  
apt-cache search php-mysql
```

Installation de packages des dépendance nagios

```
Unset  
sudo apt install wget apache2 php openssl perl make gcc libc6 libgd-dev  
  
sudo apt install mailutils  
sudo apt install bsd-mailx  
sudo apt install build-essential
```

Serveur Web (apache) et PHP

Unset

```
sudo apt-get install apache2  
sudo apt-get install php php-mysql  
sudo apt-get install php-pear php-ldap php-snmp php-gd
```

Mariadb-server

Unset

```
sudo apt install libmariadb-dev
```

RRDTool

Unset

```
sudo apt-get install rrdtool  
sudo apt install librrds-perl
```

Perl

Unset

```
sudo apt-get install libconfig-inifiles-perl libcrypt-des-perl libdigest-hmac-perl  
sudo apt-get install libdigest-perl libgd-gd2-perl
```

SNMP

Unset

```
sudo apt-get install snmp snmpd libnet-snmp-perl libsnmp-perl
```

Les librairies GD

Unset

```
sudo apt-get install libgd-dev libpng-dev  
sudo apt-get install dnsutils fping
```

SSH

Unset

```
sudo apt-get install openssh-server
```

Étape 3 : Création d'un utilisateur et d'un groupe pour Nagios

Unset

```
sudo useradd -m -s /bin/bash nagios  
sudo groupadd nagcmd  
sudo usermod -a -G nagcmd nagios  
sudo usermod -a -G nagcmd www-data
```

A présent, on se délogue et on se connecte avec le compte nagios

Étape 4 : Téléchargement et installation de Nagios Core

On se place dans un répertoire de travail le répertoire home par exemple:

Unset

```
su - nagios  
sudo mkdir download  
cd download
```

On télécharge nagios depuis le navigateur : Téléchargement de Nagios par ce lien

<https://www.nagios.org/downloads/>

On décompresse le fichier zip téléchargé

Unset

```
sudo cp /home/saliouvm/Téléchargements/nagios-4.5.0.tar.gz  
/home/nagios/download/  
sudo tar -zxvf nagios-4.5.0.tar.gz  
cd nagios-4.5.0
```

```
sudo ./configure --with-httpd-conf=/etc/apache2/sites-enabled
```

Ensuite on compile et installe Nagios

```
Unset  
make all  
sudo make install  
sudo make install-init  
sudo make install-commandmode  
sudo make install-config  
sudo make install-webconf
```

Etape 5 : Installation de plugins Nagios

On se replace dans le répertoire download avec "cd .."

Puis on télécharger le plugins Nagios par ce lien <https://www.nagios.org/downloads/> :
sur le navigateur

```
Unset  
sudo cp/home/saliouvm/Téléchargements/nagios-plugins-2.4.8.tar.gz  
/home/nagios/download/  
sudo tar xvzf nagios-plugins-2.4.8.tar.gz  
cd nagios-plugins-2.4.8  
sudo ./configure --with-nagios-user=nagios --with-nagios-group=nagcmd  
--with-openssl=/usr/bin/openssl  
sudo make all  
sudo make install
```

Étape 6 : Configuration de Nagios

A- Configuration du fichier "Contacts.cfg": les informations de contact pour les notifications.

Ce fichier est utilisé pour définir les contacts auxquels Nagios envoie des notifications. Pour le modifier avec `sudo nano`, on suit ces étapes :

1. Ouvrez un terminal.

On Tape la commande suivante pour ouvrir le fichier `contacts.cfg` avec l'éditeur `nano` :

Unset

```
sudo nano /usr/local/nagios/etc/objects/contacts.cfg
```

Une fois dans le fichier, on doit avoir ceci

Unset

```
define contact {  
  
    contact_name      mycontact  
    alias              Mon Contact  
    email              mon@email.com  
}
```

2. Modifiez ces lignes selon vos besoins. Voici ce que font ces paramètres :
 - `contact_name` : Nom du contact (doit être unique). =nagiosadmin
 - `alias` : Nom convivial pour le contact.
 - `email` : Adresse e-mail à laquelle les notifications seront envoyées.=ton adresse email
3. On ajoute ou modifie les contacts selon vos besoins, en veillant à respecter la syntaxe propre à Nagios.
4. Une fois les modifications effectuées, on appuie sur `Ctrl + X` pour enregistrer le fichier, puis sur `Enter` pour confirmer.
5. Enfin, pour quitter l'éditeur, appuyez sur `Ctrl + X`.
On redémarre

Unset

```
sudo systemctl restart nagios
```

B- On vérifie les commandes.

Unset

```
sudo nano /usr/local/nagios/etc/objects/commands.cfg
```

On doit avoir Ceci:

Unset

```
define command {  
  
    command_name    notify-host-by-email  
    command_line    /usr/bin/printf "%b" "***** Nagios ***>  
}
```

NB: cette partie n'est pas forcément nécessaire

Configurons maintenant l'accès Web de Nagios

Mettre comme mot de passe : nagios

C- Création d'un mot de passe pour l'utilisateur admin de Nagios

Unset

```
sudo htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin
```

user = nagiosadmin; passwd = nagios

D- On édite le fichier httpd.conf comme suite

Unset

```
sudo nano /etc/apache2/httpd.conf
```

On Colle ce script

Unset

```
ScriptAlias /nagios/cgi-bin /usr/local/nagios/sbin
<Directory "/usr/local/nagios/sbin">
Options ExecCGI
AllowOverride None
Order allow,deny
Allow from all
AuthName "Nagios Access"
AuthType Basic
AuthUserFile /usr/local/nagios/etc/htpasswd.users
Require valid-user
</Directory>
Alias /nagios /usr/local/nagios/share
<Directory "/usr/local/nagios/share">
Options None
AllowOverride None
Order allow,deny
Allow from all
AuthName "Nagios Access"
AuthType Basic
AuthUserFile /usr/local/nagios/etc/htpasswd.users
Require valid-user
</Directory>
```

E- On redémarre le serveur apache

Unset

```
sudo a2enmod cgi
sudo systemctl restart apache2
sudo systemctl start nagios
sudo systemctl enable nagios
```

Étape 7 : Vérification de l'installation et changement des droits utilisateurs

On ouvre le navigateur et on accède à <http://localhost/nagios>. On se connecte en utilisant les identifiants `nagiosadmin` qu'on a précédemment créés.

Unset

```
sudo chown -R nagios:nagios /usr/local/nagios
sudo chmod -R 775 /usr/local/nagios
sudo chown -R nagios:www-data /usr/local/nagios/etc
sudo chmod -R 775 /usr/local/nagios/etc
sudo chown -R nagios:www-data /usr/local/nagios/share
sudo chmod -R 775 /usr/local/nagios/share
```

Étape 8: Installation de NDO et NDO2DB

Unset

```
cd ..
sudo wget
<http://prdownloads.sourceforge.net/sourceforge/nagios/ndoutils-2.0.0.tar.gz>
sudo tar xvzf ndoutils-2.0.0.tar.gz
cd ndoutils-2.0.0
```

On lance la configuration automatiquement.

Unset

```
sudo ./configure --prefix=/usr/local/nagios/ --enable-mysql --disable-pgsql \\\
--with-ndo2db-user=nagios --with-ndo2db-group=nagcmd
sudo make
sudo make all
```

Unset

```
sudo cp ./src/ndomod-3x.o /usr/local/nagios/bin/ndomod.o
sudo cp ./src/ndo2db-3x /usr/local/nagios/bin/ndo2db
sudo cp ./config/ndo2db.cfg-sample /usr/local/nagios/etc/ndo2db.cfg
sudo cp ./config/ndomod.cfg-sample /usr/local/nagios/etc/ndomod.cfg
sudo chmod 775 /usr/local/nagios/bin/ndo*
sudo chown nagios:nagios /usr/local/nagios/bin/ndo*
```

On Crée ensuite un daemon ndo2db:

Unset

```
sudo nano /etc/init.d/ndo2db
```

On copier-coller ce qui suit :

Unset

```
#!/bin/sh
#
#
# chkconfig: 345 99 01
# description: Nagios to mysql
#
# Author : Gaëtan Lucas
# Realase : 07/02/08
# Version : 0.1 b
# File : ndo2db
# Description: Starts and stops the Ndo2db daemon
# used to provide network services status in a database.
#
status_ndo ()
{
if ps -p $NdoPID > /dev/null 2>&1; then
return 0
else
return 1
fi
return 1
}
printstatus_ndo()
{
if status_ndo $1 $2; then
echo "ndo (pid $NdoPID) is running..."
else
echo "ndo is not running"
fi
}
killproc_ndo ()
{
```

```

echo "kill $2 $NdoPID"
kill $2 $NdoPID
}
pid_ndo ()
{
if test ! -f $NdoRunFile; then
echo "No lock file found in $NdoRunFile"
echo -n " checking runing process..."
NdoPID=`ps h -C ndo2db -o pid`
if [ -z "$NdoPID" ]; then
echo " No ndo2db process found"
exit 1
else
echo " found process pid: $NdoPID"
echo -n " reinit $NdoRunFile ..."
touch $NdoRunFile
chown $NdoUser:$NdoGroup $NdoRunFile
echo "$NdoPID" > $NdoRunFile
echo " done"
fi
fi
NdoPID=`head $NdoRunFile`
}
#Source function library
# Solaris doesn't have an rc.d directory, so do a test first
if [ -f /etc/rc.d/init.d/functions ]; then
./etc/rc.d/init.d/functions
elif [ -f /etc/init.d/functions ]; then
./etc/init.d/functions
fi
prefix=/usr/local/nagios
exec_prefix=${prefix}
NdoBin=${exec_prefix}/bin/ndo2db
NdoCfgFile=${prefix}/etc/ndo2db.cfg
NdoRunFile=${prefix}/var/ndo2db.run
NdoLockDir=/var/lock/subsys
NdoLockFile=ndo2db.lock

```

```

NdoUser=nagios
NdoGroup=nagios

#Check that ndo exists.
if [ ! -f $NdoBin ]; then
echo "Executable file $NdoBin not found. Exiting."
exit 1
fi
# Check that ndo.cfg exists.
if [ ! -f $NdoCfgFile ]; then
echo "Configuration file $NdoCfgFile not found. Exiting."
exit 1
fi
# See how we were called.
case "$1" in
start)
echo -n "Starting ndo:"
touch $NdoRunFile

chown $NdoUser:$NdoGroup $NdoRunFile
$NdoBin -c $NdoCfgFile
if [ -d $NdoLockDir ]; then
touch $NdoLockDir/$NdoLockFile;
fi
ps h -C ndo2db -o pid > $NdoRunFile
if [ $? -eq 0 ]; then
echo " done."
exit 0
else
echo " failed."
$0 stop
exit 1
fi
;;
stop)
echo -n "Stopping ndo: "
pid_ndo

```

```

killproc_ndo
# now we have to wait for ndo to exit and remove its
# own NdoRunFile, otherwise a following "start" could
# happen, and then the exiting ndo will remove the
# new NdoRunFile, allowing multiple ndo daemons
# to (sooner or later) run
# echo -n 'Waiting for ndo to exit .'
for i in 1 2 3 4 5 6 7 8 9 10 ; do
if status_ndo > /dev/null; then
echo -n '.'
sleep 1
else
break
fi
done
if status_ndo > /dev/null; then
echo
echo 'Warning - ndo did not exit in a timely manner'
else
echo 'done.'
fi
rm -f $NdoRunFile $NdoLockDir/$NdoLockFile
;;
status)
pid_ndo
printstatus_ndo ndo
;;
restart)
$0 stop
$0 start
;;
*)
echo "Usage: ndo {start|stop|restart|status}"
exit 1
;;
esac
# End of this script

```

On enregistre pour valider. On Ajoute ensuite le daemon au démarrage

Unset

```
sudo update-rc.d ndo2db defaults  
sudo chmod +x /etc/init.d/ndo2db
```

Voilà le daemon ndo2db est maintenant près.

2- Monitoring Avec Nagios [5]

2-1 Configuration pour le monitoring

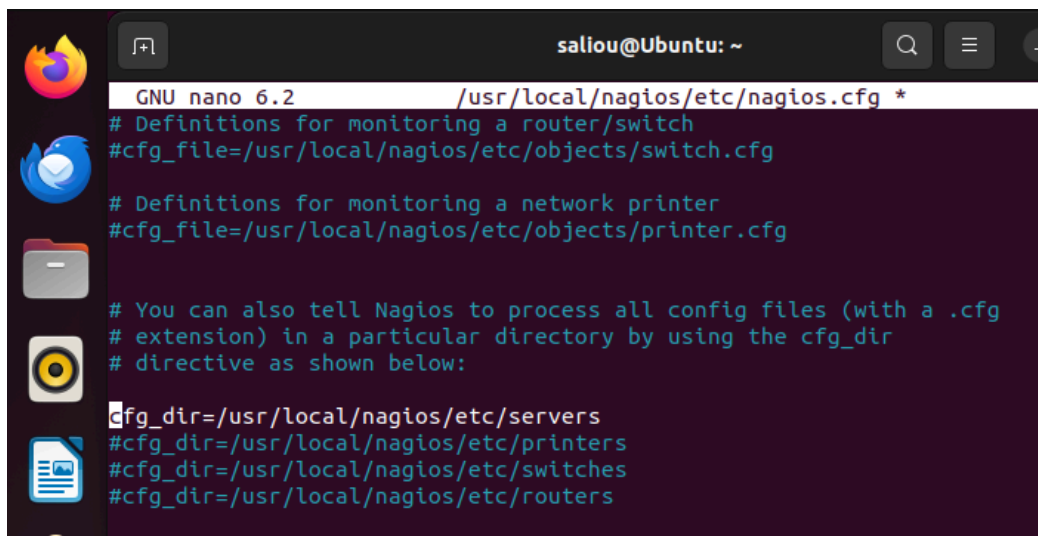
1- Aller dans le fichier : "/usr/local/nagios/etc/nagios.cfg"

Taper la commande:

Unset

```
sudo nano /usr/local/nagios/etc/nagios.cfg
```

Ensuite décommenter la ligne suivante comme le montre la figure ci-dessous.



```
GNU nano 6.2 /usr/local/nagios/etc/nagios.cfg *
# Definitions for monitoring a router/switch
#cfg_file=/usr/local/nagios/etc/objects/switch.cfg

# Definitions for monitoring a network printer
#cfg_file=/usr/local/nagios/etc/objects/printer.cfg

# You can also tell Nagios to process all config files (with a .cfg
# extension) in a particular directory by using the cfg_dir
# directive as shown below:

cfg_dir=/usr/local/nagios/etc/servers
#cfg_dir=/usr/local/nagios/etc/printers
#cfg_dir=/usr/local/nagios/etc/switches
#cfg_dir=/usr/local/nagios/etc/routers
```

Figure 8 : Fichier nagios.cfg

2- Créer un fichier servers comme suite.

Unset
`sudo mkdir -p /usr/local/nagios/etc/servers`

3- Définir une adresse mail pour recevoir les notifications.

Unset
`sudo nano /usr/local/nagios/etc/objects/contacts.cfg`

4- Activer les modules d'apache2

Unset
`sudo a2enmod rewrite`
`sudo a2enmod cgi`

5- Activer la virtualisation the nagios

Unset

```
sudo ln -s /etc/apache2/sites-available/nagios.config  
/etc/apache2/sites-enabled
```

6- Redémarrage des services

Unset

```
sudo service apache2 restart  
sudo service nagios start
```

8- Faire une mise à jour du système

Unset

```
sudo apt update  
sudo service apache2 restart  
sudo service nagios start
```

9-Modification du fichier de nagios

accéder au fichier: **nagios**

Unset

```
sudo nano /etc/init.d/nagios
```

Ajouter ce qui suit dedans

Unset

```
DESC="Nagios"  
NAME=nagios  
DAEMON=/usr/local/nagios/bin/$NAME  
DAEMON_ARGS=".d /usr/local/nagios/etc/nagios.cfg"  
PIDFILE=/usr/local/nagios/var/$NAME.lock
```

10- Rendre ce fichier exécutable et démarrer nagios

Unset

```
sudo chmod +x /etc/init.d/nagios  
sudo service apache2 restart  
sudo service nagios start
```

11- Création d'un fichier host

```
Unset
cd /usr/local/nagios/etc/servers
sudo nano hosts.cfg
```

On colle ce qui suit dedans:

```
Unset
define host{
    use                linux-server
    host_name          laptop_windows
    alias              My Windows Server
    address            192.168.11.106
    max_check_attempts 5
    check_period       24x7
    notification_interval 30
    notification_period 24x7
}
define host{
    use                linux-server
    host_name          Iphone
    alias              My Iphone
    address            192.168.11.105
    max_check_attempts 5
    check_period       24x7
    notification_interval 30
    notification_period 24x7
}
```

nous avons ajouté deux host dans la partie serveur à monitorer, le laptop windows et un appareil portable Iphone.

On redémarre nagios

Unset

```
sudo service nagios restart
```

12- Dans windows on vérifie l'adresse ip via CMD

Unset

```
ipconfig
```

2-2 Configuration du client NSClient sur windows [6]

1- Monitoring windows de windows

Installer NSClient++ Nagios core Agent sur windows : <https://nsclient.org/>

2. Configuration de Nagios
on édite le fichier nagios.cfg

Unset

```
sudo nano /usr/local/nagios/etc/nagios.cfg
```

décommenter la ligne:

Unset

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

Modifier mettre l'adresse IP du serveur nagios :

Unset

```
define host{
    use          windows-server ; Inherit default values from a Windows server
    template (make sure you keep this line!)
    host_name    winserver
    alias        My Windows Server
    address      192.168.11.106
}
```

Redémarrage du système:

Unset

```
sudo systemctl restart nagios.service
```

3. Modifier la configuration pour activer les modules suivants

Sur votre windows aller dans: C:\Program Files\NSClient++\nsclient

Modifier ce fichier nsclient dans la bloc note en tant qu'administrateur.

remplacer ces paramètres qui suivent :

Unset

```
CheckExternalScripts = 1
```

```
CheckHelpers = 1
```

```
CheckEventLog = 1
```

```
CheckNSCP = 1
```

```
CheckDisk = 1
```

```
CheckSystem = 1
```

Puis aller dans les services windows et redémarrer les service : NSClient++ Monitoring...

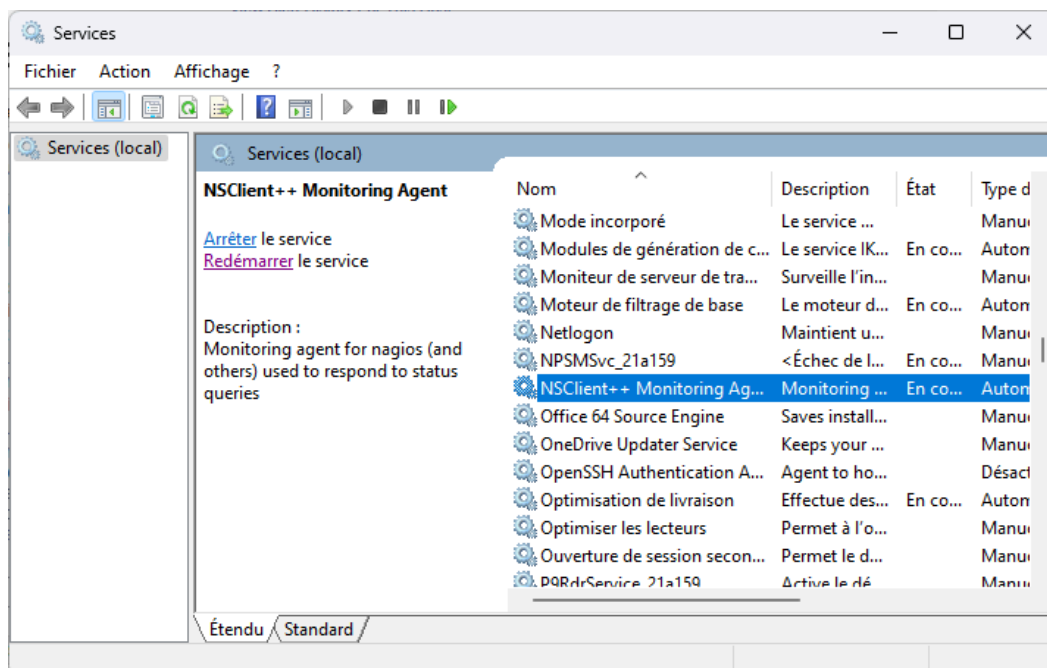


Figure 9 : Redémarrage des services NSClients

Puis sous ubuntu redémarrer nagios:

Unset

```
sudo systemctl restart nagios.service
```

2-3 Monitoring des hosts dans l'interface web nagios

1- Aller dans nagios web : `http://Ip_address/nagios` accéder avec vos informations d'identification déjà créées plus haut.

Aller dans "view Status overview "

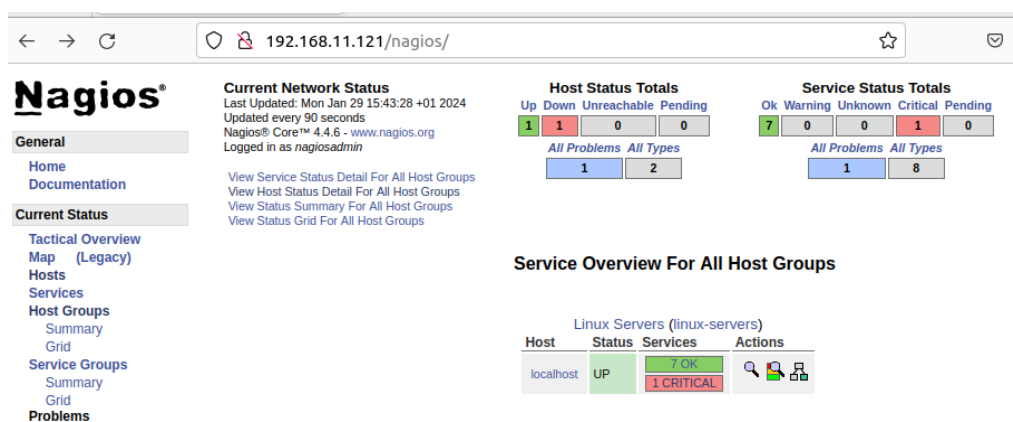


Figure 10 : Interface Nagios

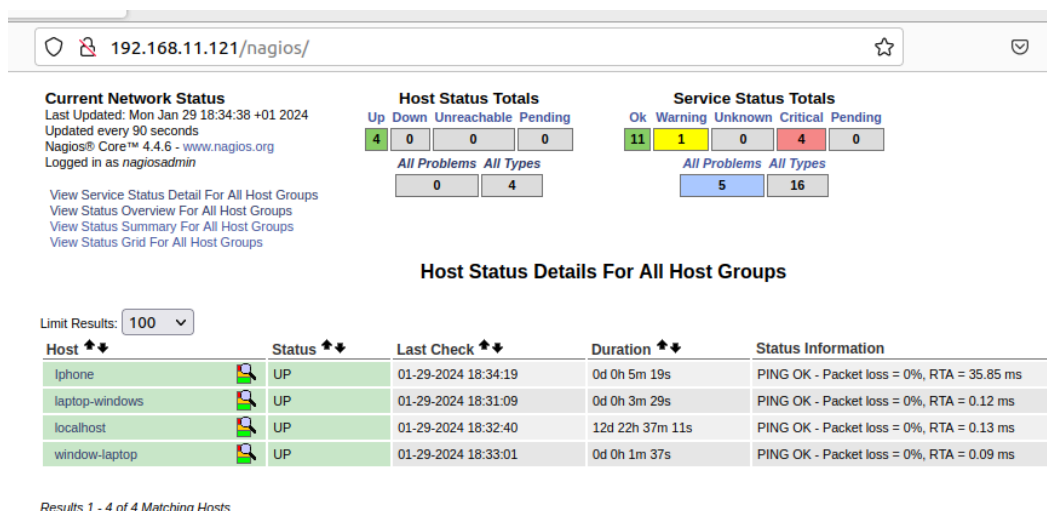


Figure 11 : Vue des machines supervisées

Les différents host sont monté en up maintenant nous pouvons consulter les services monitorés

Limit Results: 1000

Host	Service	Status	Last Check	Duration	Attempt	Status Information
localhost	Current Load	OK	01-29-2024 18:32:20	12d 22h 35m 57s	1/4	OK - load average: 0.66, 0.66, 0.46
	Current Users	OK	01-29-2024 18:32:24	12d 22h 35m 18s	1/4	USERS OK - 2 users currently logged in
	HTTP	OK	01-29-2024 18:33:48	12d 22h 34m 42s	1/4	HTTP OK: HTTP/1.1 200 OK - 10978 bytes in 0.003 second response time
	PING	OK	01-29-2024 18:31:05	12d 22h 34m 3s	1/4	PING OK - Packet loss = 0%, RTA = 0.09 ms
	Root Partition	OK	01-29-2024 18:32:58	12d 22h 38m 27s	1/4	DISK OK - free space: / 6596 MiB (27.78% inode=80%):
	SSH	OK	01-29-2024 18:35:13	0d 2h 26m 42s	1/4	SSH OK - OpenSSH_8.9p1 Ubuntu-3ubuntu0.6 (protocol 2.0)
	Swap Usage	OK	01-29-2024 18:31:00	12d 22h 37m 12s	1/4	SWAP OK - 79% free (2143 MB out of 2739 MB)
window-laptop	Total Processes	OK	01-29-2024 18:31:05	12d 22h 36m 34s	1/4	PROCS OK: 53 processes with STATE = RSZDT
	C:\ Drive Space	WARNING	01-29-2024 18:27:00	0d 0h 28m 54s	3/3	c: - total: 115.23 Gb - used: 102.14 Gb (89%) - free 13.09 Gb (11%)
	CPU Load	OK	01-29-2024 18:28:25	0d 0h 27m 29s	1/3	CPU Load 35% (5 min average)
	Explorer	OK	01-29-2024 18:28:01	0d 1h 16m 5s	1/3	Explorer.EXE: Running
	Memory Usage	CRITICAL	01-29-2024 18:31:13	0d 0h 4m 41s	3/3	connect to address 192.168.11.121 and port 12489: Connection refused
	NSClient++ Version	CRITICAL	01-29-2024 18:32:38	0d 0h 3m 16s	1/3	connect to address 192.168.11.121 and port 12489: Connection refused
	PING	CRITICAL	01-29-2024 18:26:04	0d 1h 19m 50s	3/3	PING CRITICAL - Packet loss = 100%
	Uptime	OK	01-29-2024 18:27:28	0d 0h 28m 26s	1/3	System Uptime - 0 day(s) 6 hour(s) 35 minute(s)
	W3SVC	CRITICAL	01-29-2024 18:29:26	0d 0h 6m 28s	3/3	connect to address 192.168.11.121 and port 12489: Connection refused

Figure 12 : Services Monitorés

Cette figure montre les services activés et en cours de monitoring.

Nous avons comme services:

- la CPU de la machine windows : la machine windows à consommer 35% de la CPU en 5 min
- L'explorateur de fichier : En cours d'utilisation
- L'espace mémoire du disque C : 102,14 Gb utiliser soit 89% et 13,09 Gb libre soit 11% de l'espace disque C.

Cependant le reste des services requiert des configuration supplémentaires des autorisations de connexion dont le windows defender empêche la connexion.

Quelques minute après on a ce résultat:

Limit Results: 100 ▼

Host	Service	Status	Last Check	Duration	Attempt	Status Information
localhost	Current Load	OK	01-29-2024 19:22:20	12d 23h 24m 48s	1/4	OK - load average: 1.87, 1.24, 1.04
	Current Users	OK	01-29-2024 19:22:24	12d 23h 24m 9s	1/4	USERS OK - 2 users currently logged in
	HTTP	OK	01-29-2024 19:22:30	12d 23h 23m 33s	1/4	HTTP OK: HTTP/1.1 200 OK - 10978 bytes in 0.001 second response time
	PING	OK	01-29-2024 19:23:43	12d 23h 22m 54s	1/4	PING OK - Packet loss = 0%, RTA = 0.07 ms
	Root Partition	OK	01-29-2024 19:20:36	12d 23h 27m 18s	1/4	DISK OK - free space: / 6593 MiB (27.76% inode=80%):
	SSH	OK	01-29-2024 19:21:51	0d 3h 15m 33s	1/4	SSH OK - OpenSSH_8.9p1 Ubuntu-3ubuntu0.6 (protocol 2.0)
	Swap Usage	OK	01-29-2024 19:21:51	12d 23h 26m 3s	1/4	SWAP OK - 76% free (2073 MB out of 2739 MB)
windows-laptop	Total Processes	OK	01-29-2024 19:24:11	12d 23h 25m 25s	1/4	PROCS OK: 51 processes with STATE = RSZDT
	C:\ Drive Space	WARNING	01-29-2024 19:23:04	0d 0h 1m 41s	3/3	c: - total: 115.23 Gb - used: 101.33 Gb (88%) - free 13.90 Gb (12%)
	CPU Load	OK	01-29-2024 19:22:56	0d 0h 0m 37s+	1/3	CPU Load 44% (5 min average)
	Explorer	PENDING	N/A	0d 0h 0m 37s+	1/3	Service check scheduled for Mon Jan 29 19:24:49 +01 2024
	Memory Usage	WARNING	01-29-2024 19:23:39	0d 0h 1m 6s	3/3	Memory usage: total:10982.90 MB - used: 8795.99 MB (80%) - free: 2186.91 MB (20%)
	NSClient++ Version	OK	01-29-2024 19:21:32	0d 0h 0m 37s+	1/3	NSClient++ 0.6.0.1 2023-07-30
	PING	CRITICAL	01-29-2024 19:23:24	0d 0h 1m 21s	3/3	PING CRITICAL - Packet loss = 100%
	Uptime	PENDING	N/A	0d 0h 0m 37s+	1/3	Service check scheduled for Mon Jan 29 19:25:17 +01 2024
	W3SVC	UNKNOWN	01-29-2024 19:22:07	0d 0h 2m 38s	3/3	Failed to open service W3SVC: 424: Le service spécifié n'existe pas en tant que service installé.

Figure 13 : Etats des services Monitorés

Certains services ont été activés et on obtient des informations sur l'état de santé de chaque service.

Avec cette image nous pouvons voir l'ensemble des machines en monitoring.

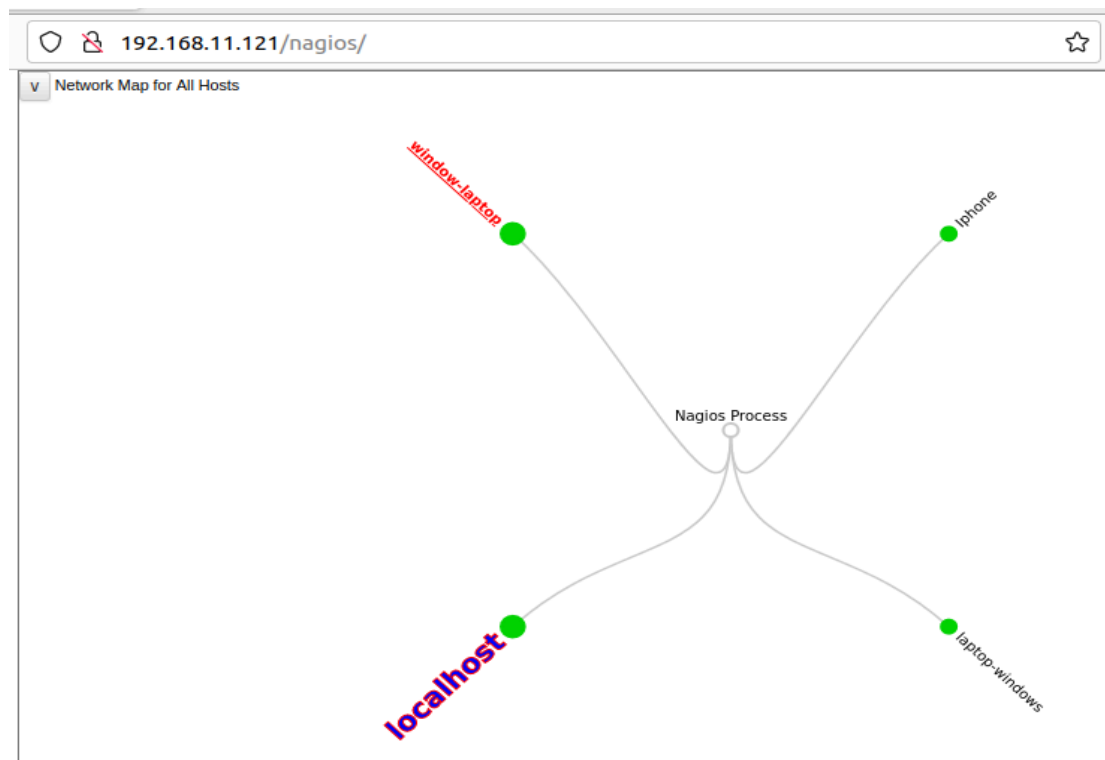


Figure 14 : Vue en Diagramme des machines monitorées

Sous l'onglet reports voici le résultat obtenu, en vert les hosts en bon état santé et en rouge les services en mauvais état de santé.

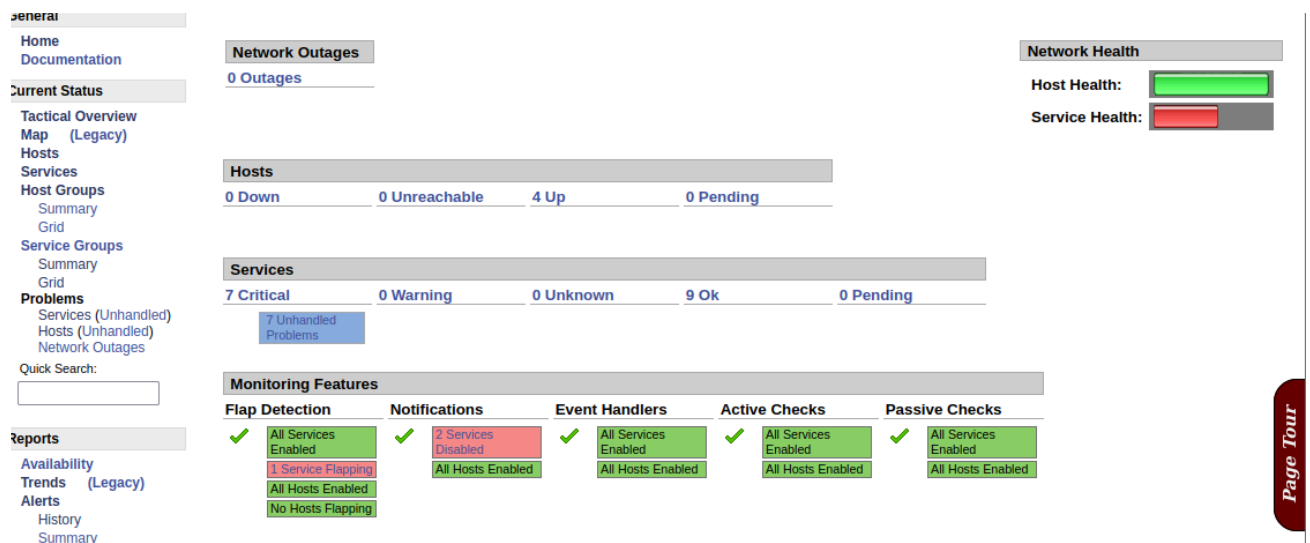


Figure 15 : Fonctionnalités de monitoring

Voici une vue sur l'ensemble des services activés en fonction des appareils monitorés.

192.168.11.121/nagios/							
Host	Service	Last Check	Next Check	Type	Active Checks	Actions	
localhost	Swap Usage	01-29-2024 18:51:00	01-29-2024 18:56:00	Normal	ENABLED	✖	🕒
localhost	Total Processes	01-29-2024 18:51:05	01-29-2024 18:56:05	Normal	ENABLED	✖	🕒
localhost	PING	01-29-2024 18:51:05	01-29-2024 18:56:05	Normal	ENABLED	✖	🕒
window-laptop	PING	01-29-2024 18:46:08	01-29-2024 18:56:08	Normal	ENABLED	✖	🕒
laptop-windows		01-29-2024 18:51:09	01-29-2024 18:56:09	Normal	ENABLED	✖	🕒
window-laptop	C:\ Drive Space	01-29-2024 18:47:00	01-29-2024 18:57:00	Normal	ENABLED	✖	🕒
localhost	Current Load	01-29-2024 18:52:20	01-29-2024 18:57:20	Normal	ENABLED	✖	🕒
localhost	Current Users	01-29-2024 18:52:24	01-29-2024 18:57:24	Normal	ENABLED	✖	🕒
localhost		01-29-2024 18:52:40	01-29-2024 18:57:40	Normal	ENABLED	✖	🕒
localhost	Root Partition	01-29-2024 18:52:58	01-29-2024 18:57:58	Normal	ENABLED	✖	🕒
window-laptop		01-29-2024 18:53:25	01-29-2024 18:58:25	Normal	ENABLED	✖	🕒
localhost	HTTP	01-29-2024 18:53:48	01-29-2024 18:58:48	Normal	ENABLED	✖	🕒
Iphone		01-29-2024 18:53:49	01-29-2024 18:58:49	Normal	ENABLED	✖	🕒
window-laptop	W3SVC	01-29-2024 18:49:26	01-29-2024 18:59:26	Normal	ENABLED	✖	🕒
localhost	SSH	01-29-2024 18:55:13	01-29-2024 19:00:13	Normal	ENABLED	✖	🕒
window-laptop	Memory Usage	01-29-2024 18:51:13	01-29-2024 19:01:13	Normal	ENABLED	✖	🕒
window-laptop	Uptime	01-29-2024 18:51:28	01-29-2024 19:01:28	Normal	ENABLED	✖	🕒
window-laptop	Explorer	01-29-2024 18:52:01	01-29-2024 19:02:01	Normal	ENABLED	✖	🕒
window-laptop	CPU Load	01-29-2024 18:52:25	01-29-2024 19:02:25	Normal	ENABLED	✖	🕒
window-laptop	NSClient++ Version	01-29-2024 18:52:38	01-29-2024 19:02:38	Normal	ENABLED	✖	🕒

Figure 16 : Ensembles des services activés

Conclusion général

Quelle que soit la qualité, le dispositif de sécurité ne peut pas protéger de façon optimale un réseau s'il n'est pas correctement supervisé.

En effet, la sécurité d'un système informatique ne se résume pas qu'au piratage. Elle correspond à un vaste domaine qui englobe beaucoup de notions. Ainsi, la sécurité d'un réseau repose d'une part sur l'architecture et son adéquation aux besoins des composants qui le constituent, mais aussi sur l'administration et la supervision, continue et efficace de ces équipements.

La supervision du réseaux, doit prendre une part très importante au sein de l'administration d'un parc informatique, il aide à anticiper les pannes et réagir rapidement tout en donnant une meilleure disponibilité et une meilleure qualité de service. La supervision vous permet aussi dans un temps différé d'avoir une vision synthétique de la vie de votre parc informatique car elle vous permettra par exemple de mieux calibrer vos lignes ou au contraire restreindre l'utilisation de celles-ci lorsqu'elles sont polluées.

Au cours de la réalisation du monitoring avec nagios nous avons rencontré beaucoup de difficultés, notamment au niveau du redémarrage de nagios suite aux erreurs de configurations, il fallait à chaque fois vérifier les logs pour corriger les erreurs, de plus au niveau de la configuration réseaux il a fallu toucher au fichier de configuration réseaux d'ubuntu et de modifier l'accès de l'interface au réseau WiFi de l'appareil hôte.

Dans l'ensemble, nous avons monitorer la machine hôte windows, de deux manières puis nous avons aussi monitoré un téléphone portable Iphone.

Références

- [1] : <https://www.whatsupgold.com/fr/logiciel-de-supervision-reseau>
- [2]:[https://www.memoireonline.com/04/12/5604/m_Monitoring-dune-infrastruc-ture-informatique-sur-base-d'outils-libres 22.html](https://www.memoireonline.com/04/12/5604/m_Monitoring-dune-infrastruc-ture-informatique-sur-base-d'outils-libres-22.html)
- [3] : <https://fr.wikipedia.org/wiki/Nagios>
- [4] : <https://fr.linux-console.net/?p=22061>
- [5] :
https://www.youtube.com/watch?v=6T_RCywnLB8&ab_channel=TutorialSchools
- [6] : <http://noc.checs.net/nagios/docs/monitoring-windows.html>