Université Assane SECK de Ziguinchor

UFR Sciences et Technologies

Département Informatique

Mémoire de fin d'études

Pour l'obtention du diplôme de Master

Mention : Informatique

Spécialité : Génie Logiciel

Sujet :

Sécurité et Supervision de réseaux

Présenté et soutenu par : M. Souleymane MARENA

Le samedi 13/08/2022

Sous la direction de :

Monsieur Youssou FAYE — Maître de Conférences à UASZ

Membres du jury :

Dr. Ousmane DIALLO	Maître de conférences	Président	UASZ
Dr. Youssou FAYE	Maître de conférences	Encadrant	UASZ
Dr. Elhadji Malick NDOYE	Maître assistant	Rapporteur	UASZ
Dr. Ibrahima DIOP	Maître de conférences	Examinateur	UASZ

Année universitaire 2020-2021

Remerciements

*Louange à **Dieu**, le **tout puissant**, qui m'a permis de voir ce jour et de pouvoir réalisé ce modeste travail.*

Je voudrais tout d'abord adresser toute ma gratitude à mon encadreur, ***Monsieur Youssou FAYE*** pour sa patience, sa disponibilité et surtout ses judicieux conseils, qui ont contribué à alimenter ma réflexion. Mes sincères remerciements.

Je souhaite remercier les membres du jury, ***Monsieur Ousmane DIALLO***, ***Monsieur Elhadji Malick NDOYE*** et ***Monsieur Ibrahima DIOP***. Merci de m'avoir fait l'honneur d'être dans mon jury.

Je voudrais aussi remercier ***mes parents***, eux qui ont tout fait pour ma réussite, merci pour tout.

Enfin, je tiens à remercier toutes les personnes qui ont contribué au succès de ce travail et qui m'ont aidé à bien faire ce document.

Dédicaces

Je dédie cette mémoire :

A mes chers parents, pour tous leurs sacrifices, leur amour, leur tendresse, leur soutien et leurs prières tout au long de mes études. Ce modeste travail est le fruit de tous les sacrifices que vous avez déployés pour mon éducation et ma formation. Je vous aime beaucoup et j'implore le **tout-puissant** pour qu'il vous accorde une bonne santé, ainsi qu'une longue et heureuse vie.

A mes chères frères et sœurs, pour leurs encouragements permanents, pour leurs appuis, leurs soutiens et leurs amours. Puissent nos liens se consolider et se pérenniser encore plus par la grâce du d'**ALLAH**.

A toute ma famille pour leur soutien tout au long de mes études surtout lors de mon parcours universitaire, que ce travail soit l'accomplissement de vos vœux tant allégués, et le fuit de votre soutien infaillible. Merci d'être toujours là pour moi. Que le **Tout Puissant** vous garde et vous procure santé et bonheur.

A Tous mes amis, merci d'être présent dans ma vie. Que **DIEU** vous garde.

A mon défunt camarade de classe Mamour Diouf, qu'il repose en paix.

A Toute la deuxième promotion MPI, je vous souhaite de réussir pleinement dans la vie.

Résumé

Dans le monde de l'internet et des réseaux, la sécurité est très importante. C'est pourquoi en plus de mettre tous les mécanismes de sécurité pour une protection d'un réseau surtout pour de grande structure, pouvoir superviser le réseau est aussi très importante.

Elle nous permet de pouvoir surveillée des machines, des routeurs, des switchs, etc. Ainsi nous pouvons savoir pour un réseau, l'état de chaque équipement et leurs services à temps réel. La supervision est possible grâce à des outils ou logiciels qui facilitent la surveillance des équipements et des services. Ces outils de supervision ont des interfaces web pour visualiser ce que nous voulons superviser. C'est en ce sens que nous avons étudié des logiciels de supervision et ainsi que les protocoles utilisés par les outils pour leur faciliter les taches. Nous avons choisi par la suite de travailler avec Nagios, plus particulièrement Nagios XI, qui est l'un des outils de supervision les plus utilisé dans le marché de l'entreprise actuellement et est en même temps open source.

Nagios XI nous a permis de superviser notre réseau et peut superviser n'importe quel autre réseau d'entreprise. En plus, des services peuvent être ajoutés de manières internes avec plugins déjà intégrés lors de l'installation de Nagios XI ou externes en téléchargeant (ou créant) des plugins et les intégrés.

Abstract

In the world of the Internet and networks, security is very important. This is why, in addition to putting all the security mechanisms in place to protect a network, especially for large structures, being able to monitor the network is also very important.

It allows us to monitor machines, routers, switches. Thus, we can know for a network, the state of each equipment and their services in real time. Monitoring is possible thanks to tools or software that facilitate the monitoring of equipment and services. These monitoring tools have web interfaces to visualise what we want to monitor. It is in this sense that we have studied supervision software and the protocols used by the tools to facilitate their tasks. We then chose to work with Nagios, more specifically Nagios XI, which is one of the most widely used monitoring tools in the enterprise market today and is open source.

Nagios XI allowed us to monitor our network and can monitor any other corporate network. In addition, services can be added internally with plugins already built in when Nagios XI is installed or externally by downloading (or creating) plugins and building them in.

Table des matières

Liste des figures

Liste des tableaux

Liste des abréviations

SET: Secure Electronic Transaction

DoS: Denial of Service

DDoS: Distributed Denial of Service

AAA: Authentification, Authorization, Accounting

MFA: Multi-factor authentification

ACL: Access Control List

IDS: Intrusion Detection System

IPS: Intrusion Prevention System

NIDS: Network Intrusion Detection System

HIDS: Host Intrusion Detection System

HIPS: Host Intrusion Prevention System

NIPS: Network Intrusion Prevention System

CPU: Central Processing Unit (Processeur)

SNMP: Simple Network Management Protocol

USM: User based Security Model

DES: Data Encryption Standard

VACM: View based Access Control Model

MIB: Management Information Base

UDP: User Datagram Protocol

OID: Object Identifier

PDU: Protocol Data Unit

WMI: Windows Management Instrumentation

API: Application Programming Interface

DMTF: Distributed Management Task Force

WBEM: Web-Based Enterprise Management

CIM: Common Information Model

WS: Web Services

SOAP: Simple Object Access Protocol

XML: Extensible Markup Language

HTTP: Hypertext Transfer Protocol

HTTPS: HyperText Transfer Protocol Secure

MRTG: Multi Router Traffic Grapher

PHP: Hypertext Preprocessor

RRD: Round Robin Database

IPMI: Intelligent Platform Management Interface

NPCA: Nagios Cross-Platform Monitoring

SMTP: Simple Mail Transfer Protocol

POP: Post Office Protocol

ICMP: Internet Control Message Protocol

CGI: Common Gateway Interface

RO: Read Only

RW: Read Write

NRPE: Nagios Remote PluginExecutor

NSCA : *Nagios* Service Check Acceptor

Introduction générale

Actuellement, toutes les structures sont équipées d'un réseau local au minimum, et de réseaux de longues distances pour les plus importantes d'entre elles. Ces structures englobent plusieurs équipements et assurent la sécurité de ces équipements devient une obligation pour contrer d'éventuelles attaques des cybercriminels et être prévenu en cas de problème sur le réseau ou sur les équipements, afin d'éviter des catastrophes.

Les entreprises ont besoin d'avoir une vue en temps réel relative à la situation du réseau après avoir mis en œuvre tous les mécanismes de protection nécessaires. Ce qui pourra permettre une détection précoce de tout disfonctionnement relatif à l'état du matériel (terminaux et équipements intermédiaires), des liens, des services et protocoles.

Dans ce mémoire, nous nous sommes proposés d'étudier un réseau local et de mettre en place un dispositif nécessaire pour assurer la sécurité. C'est ainsi qu'après avoir étudié les fondamentaux de la sécurité, nous avons abordé le thème de la supervision de réseaux afin de voir comment avoir le contrôle sur un réseau d'entreprise. Notre objectif principal est de pouvoir contrôler le bon fonctionnement du matériel, des débits sur les liaisons réseaux, des protocoles et applications, contrôle sans lequel le réseau serait exposé à des défaillances qui ne seraient visibles qu'après avoir causé des dégâts. Ainsi nous nous sommes intéressés à l'étude de la supervision d'un réseau simple qui renferme beaucoup de fonctions et services. Grâce à des logiciels de monitoring, les anomalies peuvent être aussitôt prises en main. Ces logiciels vérifient l'état du réseau ainsi que des machines et autres équipements (routeurs, switchs, imprimantes, etc.) connectées et nous permet d'avoir une vue d'ensemble en temps réel de l'ensemble du réseau informatique. Il peut être aussi informé (par email, par SMS) en cas de problème. Dans ce sillage, nous avons d'abord étudié les généralités de la sécurité informatique qui est la base de la supervision, ensuite une étude théorique de supervision suivi d'une étude comparative des solutions de supervision. Enfin nous avons utilisé Nagios une solution de supervision pour contrôler : le matériel, les liaisons, les protocoles et services.

Ainsi, le présent document est structuré en quatre chapitres :

Dans un premier chapitre intitulé « généralités sur la sécurité », présente les aspects généraux de la sécurité afin de mieux comprendre les mécanismes basiques de la supervision.

Le deuxième chapitre concerne « l'étude théorique de la supervision », dans ce chapitre nous allons voir la supervision informatique en générale puis particulièrement la supervision de réseaux.

Le troisième chapitre intitulé « logiciels de supervision », dans lequel l'accent est mis sur le fonctionnement des logiciels de supervision et les protocoles utilisés. Puis nous allons comparer les logiciels de supervision en vue d'en choisir le mieux adapté.

Et dans le quatrième et dernier chapitre « supervision avec Nagios », au sein de ce dernier, nous avons présenté l'outil de supervision Nagios XI avant de l'utiliser pour superviser un réseau, faire des tests, ajoutés des services supplémentaires en intégrant de nouveaux greffons (plugins déjà intégrés ou téléchargeables) et même pouvoir implémenter un plugin pour superviser un nouveau service.

CHAPITRE I : GENERALITES SUR LA SECURITE

Introduction

Le réseau d'information électronique connecté est devenu une partie intégrante de notre vie quotidienne. Les entreprises en tout genre utilisent ce réseau pour leur bon fonctionnement. Elles utilisent le réseau en recueillant, en traitant, en stockant et en partageant d'énormes quantités d'informations numériques. Comme de plus en plus d'informations numériques sont rassemblées et partagées, la protection de ces informations devient encore plus essentielle pour notre sécurité nationale et pour la stabilité économique.

C'est pour ces raisons que nous devons protéger nos informations. À titre personnel, nous devons protéger notre identité, nos données et nos périphériques informatiques. Au niveau de l'entreprise, tout le monde est responsable de la protection de la réputation, des données et des clients de l'entreprise. Au niveau national, la sécurité nationale, ainsi que la sécurité et le bien-être des citoyens sont en jeu.

I.1. Les services de la sécurité en informatique

A première vue, les défenseurs de la cybersécurité identifient les objectifs à protéger sur internet. Les objectifs identifiés constituent les principes fondateurs de la cybersécurité. Ces principes sont la confidentialité, l'authentification, l'intégrité, la disponibilité et la non répudiation. De ces principes les défenseurs de la cybersécurité consacrent leurs efforts à prendre des mesures pour assurer la protection des ressources sur internet. Mais aussi il faut assurer la protection des matériels qui peuvent fonctionner sans internet.

- La confidentialité : Consiste à empêcher la divulgation d'informations à des personnes, des ressources ou des processus non autorisés (garantir l'anonymat), seules les personnes autorisées devront consulter les données. Il faudra faire en sorte qu'au sein de l'entreprise, chaque personnel ai accès qu'aux données de son niveau, pas nécessaire d'avoir accès à toutes les données de l'entreprise.
  Parmi les méthodes permettant de garantir la confidentialité, il y a le cryptage des données, l'identifiant et le mot de passe liés au nom d'utilisateur…
- L'authentification : Être sûr de son origine, c'est la procédure qui consiste à vérifier l'identité d'une entité pour autoriser l'accès de cette entité à des ressources (systèmes, réseaux, applications…). En bref, elle protège à l'usurpation d'identité.

Il peut être sous plusieurs formes (mot de passe, code PIN, carte à puce, certificat électronique…).

- L'intégrité : Représente l'exactitude, la cohérence et la fiabilité des données pendant tout leur cycle de vie. Les données ne doivent pas être altérées durant le transfert ni être modifiées par des entités non autorisées. Les permissions de fichiers et le contrôle d'accès pour les utilisateurs peuvent empêcher l'accès non autorisé. Le contrôle des versions peut être utilisé pour empêcher des modifications accidentelles par des utilisateurs autorisés. Les sauvegardes doivent être disponibles pour restaurer les données corrompues et le hachage des sommes de contrôle peut permettre de vérifier l'intégrité des données pendant le transfert.

- La disponibilité : Elle garantit l'accès aux informations lorsque les utilisateurs autorisés en ont besoin. La maintenance des équipements, la réparation des matériels, la mise à jour des systèmes d'exploitation et des logiciels, et la création de sauvegardes permettent de garantir la disponibilité du réseau et des données pour les utilisateurs autorisés.
- La non répudiation : La non répudiation assure que l'émetteur du message ne pourra pas nier avoir émis le message dans le futur.

I.2. Risques, Menaces, Vulnérabilités et Attaques pour la sécurité

I.2.1. Risques

Définition : Probabilité plus ou moins grande de voir une menace informatique se transformer en événement réel entraînant une perte.

Les risques informatiques peuvent être d'origine naturelle ou humaine, accidentelle ou intentionnelle. Le risque informatique se mesure à la fois par la probabilité d'occurrence d'une menace et par le montant de la perte consécutive à sa réalisation. De plus, la proximité d'un événement comportant un certain degré d'incertitude est prise en considération dans l'évaluation du risque informatique.

I.2.2. Menaces

Définition : Une menace est une cause potentielle nuisible, qui peut résulter en un dommage au système informatique.

Les menaces peuvent être divisés en deux groupes, les menaces internes et les menaces externes.

- **Les menaces internes :**

Les menaces internes sont également susceptibles d'entraîner des dégâts plus importants que ceux des menaces externes, car les utilisateurs internes disposent d'un accès direct au bâtiment et aux périphériques de l'infrastructure. Les employés connaissent également le réseau d'entreprise, ses ressources et ses données confidentielles, ainsi que les différents niveaux de privilèges des utilisateurs et des administrateurs.

- **Les menaces externes :**

Les menaces externes provenant des amateurs et des agresseurs expérimentés peuvent exploiter les vulnérabilités dans le réseau ou dans les périphériques informatiques, ou utiliser le piratage pour obtenir l'accès.

Il faut noter que les menaces peuvent provenir de plusieurs choses comme :

- Failles de sécurité ;
- Logiciels espions ;
- Courier indésirables ;
- Programmes malveillants…

I.2.3. Vulnérabilités

Définition : Les vulnérabilités de sécurité représentent un défaut (faiblesse dans le système) matériel ou logiciel, qui peut être exploitée par une menace.

Après avoir pris connaissance d'une vulnérabilité, les utilisateurs malveillants tentent de l'exploiter. L'utilisation d'un exploit (terme employé pour désigner un programme écrit utilisé pour exploiter une vulnérabilité connue) contre une vulnérabilité est considérée comme une attaque et l'objectif de l'attaque est d'obtenir l'accès à un système, aux données hébergées ou à une ressource spécifique.

- **Les vulnérabilités du matériel :**

Les vulnérabilités sont souvent causées par des défauts de conception du matériel. Les vulnérabilités du matériel sont spécifiques aux modèles d'appareils et sont généralement

exploitées pour des tentatives compromettantes. Tandis que les exploits sur le matériel sont plus fréquents dans les attaques très ciblées, la protection classique contre les malwares et une sécurité physique constituent une protection suffisante pour l'utilisateur ordinaire.

- **Les vulnérabilités des logiciels :**

Les vulnérabilités des logiciels sont généralement introduites par des erreurs dans le système d'exploitation ou dans le code d'application ; malgré tous les efforts des entreprises pour détecter et corriger les vulnérabilités des logiciels, il est fréquent que de nouvelles vulnérabilités se présentent. Microsoft, Apple et d'autres producteurs de système d'exploitation sortent des correctifs et des mises à jour quasiment tous les jours. Les mises à jour d'applications sont également fréquentes. Des applications comme les navigateurs Web, les applications mobiles et les serveurs Web sont souvent mis à jour par les entreprises ou les organisations responsables pour corriger les vulnérabilités détectées. L'objectif des mises à jour logicielles est de rester à jour et d'éviter l'exploitation des vulnérabilités.

La plupart des vulnérabilités de sécurité de logiciels font partie des catégories suivantes :

Débordement de tampon : Cette vulnérabilité se produit lorsque les données sont écrites au-delà des limites d'un tampon. Les tampons sont des zones de mémoire affectées à une application. En modifiant les données au-delà des limites d'une mémoire tampon, l'application accède à la mémoire allouée à d'autres processus. Cela peut provoquer une panne du système, une compromission des données ou permettre une élévation des privilèges.

Entrée non validée : Les programmes interagissent fréquemment avec l'entrée de données. Ces données entrant dans le programme pourraient avoir un contenu malveillant, conçu pour détraquer les activités du programme. Considérons un programme qui reçoit une image à traiter. Un utilisateur malveillant pourrait concevoir un fichier image avec des dimensions d'image non valides. Les dimensions trafiquées de manière malveillante peuvent forcer le programme à répartir les tampons de tailles incorrectes et imprévues.

Situation de concurrence : Cette vulnérabilité se produit lorsque la sortie d'un événement dépend de sorties commandées ou planifiées. Une situation de concurrence devient une source de vulnérabilité lorsque les événements nécessaires commandés ou planifiés ne se produisent pas dans l'ordre correct ou en temps voulu.

Failles dans les mesures de sécurité : Les données système et les données sensibles peuvent être protégées grâce à des techniques comme l'authentification, l'autorisation et le chiffrement. Les développeurs ne doivent pas tenter de créer leurs propres algorithmes de sécurité, car cela pourrait introduire des vulnérabilités. Il est fortement conseillé aux développeurs d'utiliser les bibliothèques de sécurité déjà créées, testées et vérifiées.

Problèmes de contrôle d'accès : Le contrôle d'accès est le processus de contrôle des affectations, de la gestion de l'accès physique à l'équipement dictant l'accès d'une personne à une ressource, notamment un fichier, et ce qu'il peut réaliser avec ce fichier, comme lire ou modifier celui-ci. De nombreuses vulnérabilités de sécurité sont créées par tout utilisation inappropriée des contrôles d'accès.

I.2.4. Attaques

Définition : Elles représentent les moyens d'exploiter une vulnérabilité. Il peut y avoir plusieurs attaques pour une même vulnérabilité mais toutes les vulnérabilités ne sont pas exploitables.

Il existe plusieurs types d'attaques comme les attaques physiques, les attaques d'accès et d'espionnage, les attaques intrusions, les attaques d'usurpation d'identité et les attaques par saturation.

- Les attaques physiques : C'est quand les locaux, les machines, ou les serveurs sont attaqués.
  Exemples : Vols de machines, vols de disque dur…
- Les attaques d'accès et d'espionnage : C'est lorsque l'agresseur tante d'espionner le réseau (le ***sniffing*** : l'écoute du réseau) ou de manipuler psychologiquement des personnes pour obtenir des informations confidentielles (*l'ingénierie social*).
- Les attaques intrusions : C'est quand un attaquant entre dans un système de manière illégale, comme un virus, un publiciel…
- Les attaques d'usurpation d'identité : C'est l'attaquant se fait passer pour quelqu'un qu'il n'est pas, il masque son identité et se passer pour une autre personne.
- Les attaques par saturation : Aussi appelés **attaques par déni de service,** ces attaques se font par saturation du réseau ou d'un système de façon à ce qu'il ne fonctionne plus.
  Il existe deux types, une attaque par déni de service (DoS) représente un type d'attaque réseau mais provient de la même source et une attaque par déni de service

distribué (DDoS) est similaire à une attaque par déni de service (attaque DoS), mais elle provient de sources multiples et coordonnées.

I.3. Solutions de sécurité

Tout système doit être protéger, et pour cela nous allons penser à des mesures avant une attaque (mesures de préventions), pendant une attaque pour limiter les dégâts et après une attaque pouvoir se relancer ainsi qu'à ne pas faire les mêmes erreurs à l'avenir.

I.3.1. Préventions

I.3.1.1. Politique de sécurité

Une politique de sécurité regroupe les différents objectifs de sécurité définis par l'entreprise. Elle comprend des règles de comportement à l'intention des utilisateurs et des administrateurs, et définit une configuration système requise. Ces objectifs, ces règles et ces exigences assurent ensemble la sécurité du réseau, des données et des systèmes informatiques d'une entreprise.

Une politique de sécurité exhaustive porte sur plusieurs points :

- Elle montre l'engagement de l'entreprise envers la sécurité.
- Elle définit les règles relatives au comportement attendu.
- Elle garantit la cohérence au niveau des opérations du système, de l'achat et de l'utilisation de composants matériels et logiciels, ainsi que de la maintenance.
- Elle définit les conséquences juridiques des infractions.
- Elle garantit au personnel de sécurité le soutien de la direction.

Les politiques de sécurité informent les utilisateurs, le personnel et les dirigeants des exigences de l'entreprise quant à la protection des ressources d'informations et technologiques. Une politique de sécurité spécifie également les mécanismes requis pour répondre aux exigences en matière de sécurité.

Pour une bonne application des politiques de sécurité, il faut recourir à une politique d'audit. Une politique d'audit crée un fichier journal de sécurité qui se compose généralement des éléments suivants :

- **Politiques d'identification et d'authentification** : elles spécifient les personnes autorisées à accéder aux ressources réseau et décrivent les procédures de vérification.

- **Politiques de mot de passe** : elles garantissent que les mots de passe remplissent les conditions minimales requises et sont changés régulièrement.

- **Règles de bon usage** : elles identifient les ressources réseau et l'utilisation considérées comme acceptables par l'entreprise. Elles peuvent également identifier les conséquences d'une infraction.

- **Politiques d'accès à distance** : elles indiquent la manière dont les utilisateurs distants peuvent accéder à un réseau, ainsi que les ressources accessibles à distance.

- **Politiques de maintenance du réseau** : elles spécifient les procédures de mise à jour des systèmes d'exploitation des appareils réseau et des applications.

- **Politiques de gestion des incidents** : elles décrivent la manière dont sont gérés les incidents liés à la sécurité.

N.B : La règle d'utilisation acceptable est l'une des composantes les plus courantes de la politique de sécurité. Cette règle définit les autorisations des utilisateurs au niveau des divers composants système. La règle d'utilisation acceptable doit être aussi explicite que possible pour éviter tout malentendu. Elle peut ainsi répertorier les sites web, groupes de discussion et autres applications gourmandes en bande passante auxquels les utilisateurs ne peuvent pas accéder à l'aide des ordinateurs ou du réseau de l'entreprise.

I.3.1.2. Contrôle d'accès

Le contrôle d'accès définit plusieurs dispositifs de protection conçus pour interdire les accès non autorisés à un ordinateur, un réseau, une base de données ou d'autres ressources de données. Le but du contrôle d'accès est d'assurer trois services : l'authentification, l'autorisation et la journalisation (**AAA** : Authentification, Authorization, Accounting).

- ***L'authentification*** vérifie l'identité d'un utilisateur afin d'empêcher tout accès non autorisé. Les utilisateurs prouvent leur identité par un élément qu'ils connaissent (comme un mot de passe), une chose qu'ils possèdent (comme un jeton ou une carte), un élément qui les caractérise (comme une empreinte digitale).
- ***Les services d'autorisation*** identifient les ressources auxquelles les utilisateurs peuvent accéder, ainsi que les opérations qu'ils peuvent effectuer. Pour ce faire, certains systèmes utilisent une liste de contrôle d'accès (ACL). Cette liste détermine si,

une fois authentifié, un utilisateur dispose de certains privilèges d'accès. L'autorisation permet également de contrôler les périodes au cours desquelles un utilisateur peut accéder à une ressource spécifique.

- ***La journalisation*** consiste à suivre les actions des utilisateurs : les éléments auxquels ils accèdent, le temps d'accès aux ressources, les modifications effectuées. Une banque, par exemple, opère ce type de contrôle pour chaque compte client. Un audit de ce système peut révéler l'heure et le montant de toutes les transactions, ainsi que l'employé ou le système responsable de leur exécution. Dans le domaine de la cybersécurité, les services de journalisation adoptent un fonctionnement identique. Le système effectue le suivi de chaque transaction de données et fournit des résultats d'audit. Un administrateur peut configurer des politiques informatiques, comme illustré à la figure 3, pour activer l'audit du système.

Il existe plusieurs types de contrôles d'accès dont les contrôles d'accès physiques, les contrôles d'accès logiques, les contrôles d'accès administratifs…

I.3.1.2.1. Les contrôles d'accès physiques

Les contrôles d'accès physiques sont les barrières mises en place pour empêcher tout contact direct avec les systèmes. L'objectif est d'empêcher des utilisateurs non autorisés d'accéder physiquement aux sites, aux équipements et aux autres ressources de l'entreprise.

Le contrôle d'accès physique détermine quels individus sont autorisés à entrer (ou sortir), où et quand ils peuvent entrer (ou sortir).

Voici quelques exemples de contrôles d'accès physiques :

- Des gardes ou agents de sécurité surveillent le site.
- Des clôtures protègent le périmètre.
- Des détecteurs de mouvement détectent les objets en mouvement.
- Des dispositifs antivols pour ordinateur portable protègent l'équipement portable.
- Des portes verrouillées empêchent tout accès non autorisé.
- Des systèmes d'accès par carte magnétique permettent d'accéder aux zones d'accès limité.
- Des chiens de garde protègent le site.

- Des caméras vidéo surveillent les installations en capturant et en enregistrant des images.
- Des alarmes détectent les intrusions.

I.3.1.2.2. Les contrôles d'accès Logiques

Les contrôles d'accès logiques désignent les solutions matérielles et logicielles utilisées pour gérer l'accès aux ressources et aux systèmes. Ces solutions technologiques englobent des outils et des protocoles utilisés par les systèmes informatiques pour l'identification, l'authentification, l'autorisation et la responsabilisation.

Voici quelques exemples de contrôles d'accès logiques :

- Le chiffrement est un processus qui consiste à convertir du texte en clair en texte crypté.
- Les cartes à puce disposent d'une micropuce intégrée.
- Un mot de passe est une chaîne de caractères protégée.
- La biométrie analyse les caractéristiques physiques d'un utilisateur.
- Les listes de contrôle d'accès (ACL) définissent le type de trafic autorisé sur un réseau.
- Les protocoles sont des ensembles de règles qui régissent l'échange de données entre des appareils.
- Les pares-feux bloquent le trafic indésirable.
- Les routeurs connectent au moins deux réseaux.
- Les systèmes de détection d'intrusion (IDS) surveillent les activités suspectes sur un réseau.
- Les niveaux de coupure définissent des seuils d'erreurs autorisés avant le déclenchement d'une alerte.

I.3.1.2.3. Les contrôles d'accès administratifs

Les contrôles d'accès administratifs sont des politiques et des procédures mises en place par les entreprises pour contrôler les accès non autorisés. Les contrôles administratifs se concentrent sur les pratiques personnelles et professionnelles.

Voici quelques exemples de contrôles d'accès administratifs :

- Les politiques sont des déclarations d'intention.
- Les procédures détaillent les étapes à suivre pour effectuer une activité.
- Les pratiques de recrutement décrivent les procédures suivies par une entreprise pour trouver des employés qualifiés.
- La vérification des antécédents est un processus de filtrage des employés qui porte sur les antécédents professionnels, l'historique de crédit et les antécédents criminels d'un candidat.
- La classification des données classe les données en fonction de leur niveau de sensibilité.
- Une formation à la sécurité sensibilise les employés aux politiques de sécurité en vigueur dans l'entreprise.
- Une évaluation permet de mesurer le rendement d'un employé.

I.3.1.3. Authentification multi-facteur

L'authentification multi-facteur ou authentification multiple (MFA : Multi-factor authentification en anglais) utilise au moins deux méthodes de vérification. Les facteurs sont un élément que vous connaissez et un autre élément en votre possession. Vous pouvez aller encore plus loin en ajoutant un élément qui vous définit, comme une lecture d'empreintes digitales.

L'authentification multi-facteur permet de réduire l'impact d'une usurpation d'identité en ligne, dans la mesure où le simple fait de connaître le mot de passe ne permettra pas au cybercriminel d'accéder aux informations de l'utilisateur.

I.3.1.4. La cryptographie

La cryptographie qui est une discipline de la cryptologie, elle comprend l'ensemble des méthodes de protection d'une information. Elle sert à garantir la confidentialité d'une information lors de communication ou de son stockage, en utilisant le chiffrement. Mais elle a également d'autres objectifs de sécurité, tels que l'intégrité et l'authenticité.

Il existe trois techniques de chiffrement, à savoir le chiffrement symétrique, le chiffrement asymétrique et les fonctions de hachages.

I.3.1.4.1. La cryptographie symétrique

L'objectif de la cryptographie symétrique est de chiffrer er de déchiffrer un message avec la même clé, appelée « clé secrète ». Le chiffrement symétrique est particulièrement rapide mais

nécessite que l'émetteur transmette la clé au destinataire par un canal sécurisé, mais aussi qu'ils sont les seuls à connaitre la clé.

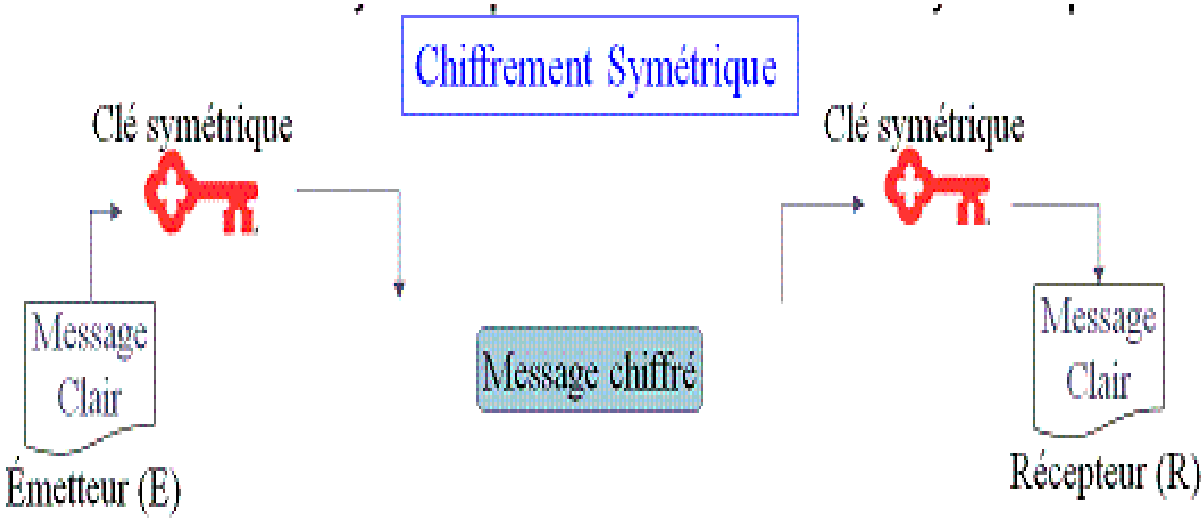


Figure 1: Chiffrement symétrique

Exemple d'utilisation :

SSH (Secure Shell) : Protocole pour le chiffrement d'un mode de communication terminal.

I.3.1.4.1.1. Avantage

L'avantage du chiffrement symétrique est qu'il facile à mettre en place et qu'il peut être réalisé en un clin d'œil.

I.3.1.4.1.2. Inconvénient

L'inconvénient est que la clé secrète doit être partagée avec le destinataire**.**

I.3.1.4.2. La cryptographie asymétrique

Son objectif est de chiffrer et déchiffrer un message avec une paire de clés (clé privée, clé publique) et que les émetteurs potentiels aient accès à la clé publique du destinataire. Mais L'émetteur n'a pas besoin d'envoyer une quelconque clé au destinataire. Dans ce cas, l'émetteur utilise la clé publique du destinataire pour chiffrer le message tandis que le destinataire utilise sa clé privée pour le déchiffrer.

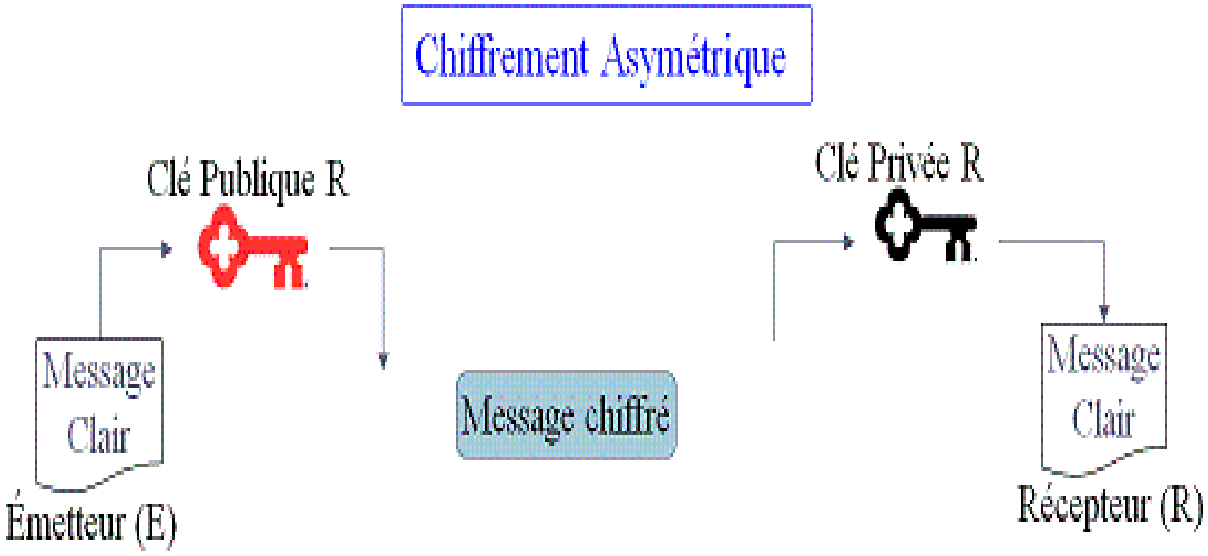


Figure 2: Chiffrement asymétrique

Exemple d'utilisation :

SET (Secure Electronic Transaction) : protocole pour le paiement sécurisé sur internet**.**

I.3.1.4.2.1. Avantages

L'avantage du chiffrement asymétrique est qu'il ne force pas l'utilisateur à communiquer des clés (secrètes) comme le fait le chiffrement symétrique, ce qui élimine la nécessité de distribuer des clés. Le chiffrement asymétrique prend en charge la signature numérique qui authentifie l'identité du destinataire. De même, il garantit que le message n'est pas altéré pendant son transit.

I.3.1.4.2.2. Inconvénients

L'inconvénient du chiffrement asymétrique est qu'il prend beaucoup de temps et qu'il nécessite beaucoup plus d'efforts. En outre, vous ne pouvez communiquer avec une autre personne que si elle a créé une paire de clés. Enfin, si vous perdez votre clé privée, vous la perdrez à jamais. La clé privée est irrécupérable.

I.3.1.4.3. Chiffrement hybride

Le chiffrement hybride résulte de la combinaison du chiffrement symétrique et du chiffrement asymétrique. Ici, une clé secrète est déterminée par une des deux parties souhaitant communiquer et celle-ci est envoyée chiffrée par un chiffrement asymétrique. Une fois connue des deux parties, celles-ci communiquent en chiffrant symétriquement leurs échanges.

Exemple d'utilisation :

Cette technique est notamment appliquée lorsque vous visitez un site dont l'adresse débute par « https ».

I.3.1.4.4. Les fonctions de hachage

La cryptologie permet justement de détecter si le message, ou l'information, a été involontairement modifié. Ainsi, une fonction de hachage permettra d'associer à un message, à un fichier ou à un répertoire, une empreinte unique calculable et vérifiable par tous. Cette empreinte est souvent matérialisée par une longue suite de chiffres et de lettres précédées du nom de l'algorithme utilisé, par exemple « SHA2 » ou « SHA256 ». Le hachage qui permet de garantir que le message est intègre, c'est-à-dire qu'il n'a pas été modifié.

Exemples d'utilisation :

- Pour sauvegarder vos photos sur votre espace d'hébergement (de type « cloud » par exemple) et vérifier que votre téléchargement s'est bien déroulé.
- Pour synchroniser vos dossiers et détecter ceux qu'il faut sauvegarder à nouveau et ceux qui n'ont pas été modifiés.

Il existe aussi des fonctions de hachage à clé qui permettent de rendre le calcul de l'empreinte différent en fonction de la clé utilisée. Avec celles-ci, pour calculer une empreinte, on utilise une clé secrète. Pour deux clés différentes l'empreinte obtenue sur un même message sera différente. Donc pour que l'émetteur et le destinataire calculent la même empreinte, ils doivent tous les deux utiliser la même clé.

Exemples d'utilisation :

- Votre service préféré reconnait votre mot de passe quand vous vous connectez.
- Vous voulez pouvoir détecter si quelqu'un modifie des documents sans vous le dire.

I.3.1.4.5. Certificat numérique

Au même titre que pour un document administratif ou un contrat sur support papier, le mécanisme de la signature numérique permet de vérifier qu'un message a bien été envoyé par le détenteur d'une clé publique. Ce procédé cryptographique permet à toute personne de s'assurer de l'identité de l'auteur d'un document et permet en plus d'assurer que celui-ci n'a pas été modifié.

Pour pouvoir signer, l'émetteur doit se munir d'une paire de clés :

- L’une, dite publique, qui peut être accessible à tous et en particulier au destinataire des messages qu’envoie l’émetteur ;
- L’autre, dite privée, qui ne doit être connue que l’émetteur.

En pratique, l’émetteur génère sa signature avec sa clé privée qui est connue par lui seul. N’importe quelle personne ayant accès à la clé publique d’Alice, dont Bob, peut vérifier la signature sans échanger de secret.

Exemples d’utilisation :

- Vous voulez garantir être l’émetteur d’un courriel.
- Vous voulez vous assurer qu’une information provient d’une source sûre.

I.3.2. Gestions d’impact

Il est important de comprendre que l’impact d’une faille est non seulement lié à son aspect technique, aux données volées, aux bases de données endommagées ou à l’atteinte à la propriété intellectuelle, mais également au préjudice pour la réputation de l’entreprise. La riposte à une violation de données est un processus très dynamique.

Voici quelques mesures importantes qu’une entreprise doit prendre lorsqu’une faille de sécurité est identifiée, selon l’avis de nombreux experts de la sécurité :

- Communiquez le problème. Les employés en interne doivent être informés du problème et appelés à agir. En dehors de l'entreprise, les clients doivent être informés par une communication directe et des annonces officielles. La communication crée la transparence, ce qui est crucial dans ce type de situation.
- Soyez sincère et responsable si l'entreprise est responsable.
- Fournissez des détails. Expliquez les raisons de la situation et ce qui a été compromis. Il est également prévu que l'entreprise prenne en charge les coûts des services de protection d'usurpation d'identité pour les clients concernés.
- Essayez de comprendre ce qui a causé la faille et l'a facilitée. Si nécessaire, embauchez des enquêteurs en informatique pour rechercher et étudier les détails.
- Appliquez ce qui a été appris au cours de l'enquête pour vous assurer que des failles similaires ne se produisent plus à l'avenir.

- Vérifiez que tous les systèmes sont sains, qu'aucune porte dérobée n'est installée et que rien d'autre n'a été compromis. Les agresseurs tenteront souvent de laisser une porte dérobée pour faciliter les failles futures. Assurez-vous que cela ne se produise pas.

- Formez les employés, les partenaires et les clients sur la méthode de prévenir des failles futures.

Conclusion

Même si, de nos jours, la majorité des entreprises prospères sont conscientes des problèmes de sécurité courants et ont déployé des efforts considérables pour les éviter, aucun système de sécurité n'est efficace à 100 %. Etant donné qu'une faille est susceptible de se produire si la valeur est importante, les entreprises et les organisations doivent également être disposées à limiter les dégâts. Nous allons dans la suite étudiée la supervision qui est aussi méthode de sécurité pour les systèmes informatiques.

CHAPITRE II : ETUDE THEORIQUE DE LA SUPERVISION

Introduction

Élément incontournable de la sécurité informatique, la supervision informatique permet de contrôler l'ensemble des infrastructures informatiques. Toujours avoir une aperçue sur tout le système est nécessaire pour une protection complète. Ce concept de surveillance regroupe tous les domaines afin d'offrir aux entreprises une sécurité optimale dans le cadre de la gestion des risques.

Dans ce chapitre, nous allons d'abord voir les systèmes de détections et de préventions d'intrusions dans le cadre de la sécurité d'un réseau ou hôte, ensuite parler de la supervision informatique en générale puis particulièrement de la supervision réseau et terminer ce chapitre par étudier quelques protocoles de supervision.

II.1. Systèmes de détection et de prévention d'intrusions

II.1.1. Les systèmes de détection d'intrusions (IDS)

Un système de détection d'intrusion est un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée (réseau, hôte).

Deux techniques de détection d'intrusion sont généralement mises en œuvre : la détection d'abus et la détection d'anomalie.

- La détection d'abus (misuse detection), aussi appelée détection de mauvaise utilisation, l'IDS analyse l'information recueillie et la compare avec une base de données de signatures d'attaques connues, et toute activité correspondante est considérée comme une attaque (avec différents niveaux de sévérité).
- La détection d'anomalie (anomaly detection), est une technique assez ancienne. L'idée principale est de modéliser durant ce qui est appelé le comportement "normal" d'un système, d'un programme ou même d'utilisateur en définissant une ligne de conduite, et de considérer ensuite comme suspect tout comportement inhabituel. La figure suivante représente le fonctionnement d'un IDS.

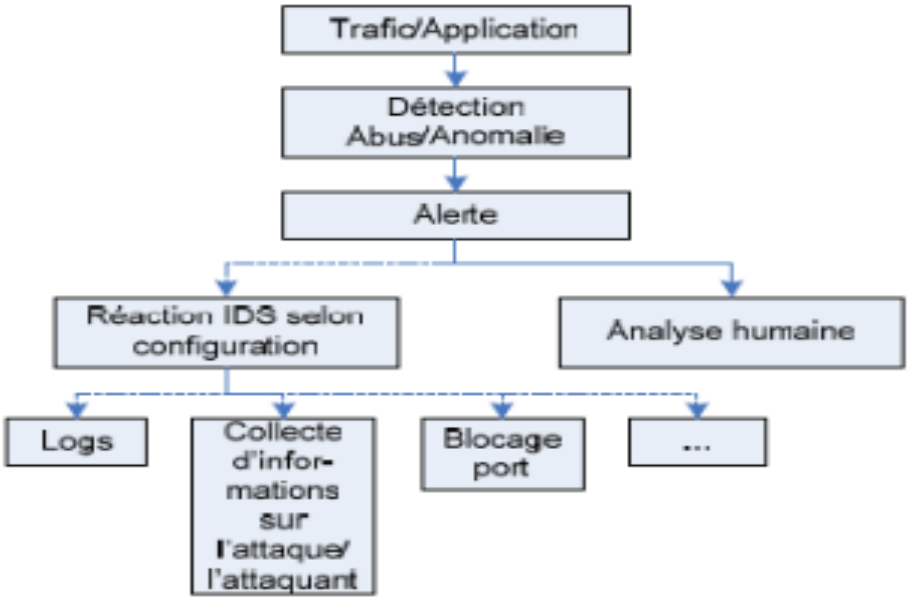


Figure 3: Fonctionnement d'un IDS

Il existe deux grandes types d'IDS : IDS réseaux (NIDS) et IDS hôte (HIDS).

II.1.1.1. La détection d'intrusion réseau (NIDS)

IDS réseau, appelé NIDS (Network-based Intrusion Detection System), est l'analyse et l'interprétation des paquets circulant sur ce réseau. Afin de repérer les paquets à contenu malicieux. Des détecteurs sont utilisés pour analyser le trafic et si nécessaire envoyer une alerte. Un IDS réseau travaille sur les trames réseau à tous les niveaux (couches réseau, transport, application). En plus, il est capable de détecter des paquets malveillants conçus pour outrepasser un pare-feu aux règles de filtrage trop laxistes, et de chercher des signes d'attaque à différents endroits sur le réseau.

Les IDS réseau ont des atouts, par exemple, les détecteurs peuvent être bien sécurisés puisqu'ils se contentent d'observer le trafic, les scans sont détectés plus facilement grâce aux signatures, etc. Cependant, les problèmes majeurs liés aux NIDS sont de conserver toujours une bande passante suffisante pour l'écoute de l'ensemble des paquets, et de bien positionner l'IDS pour qu'il soit efficace.

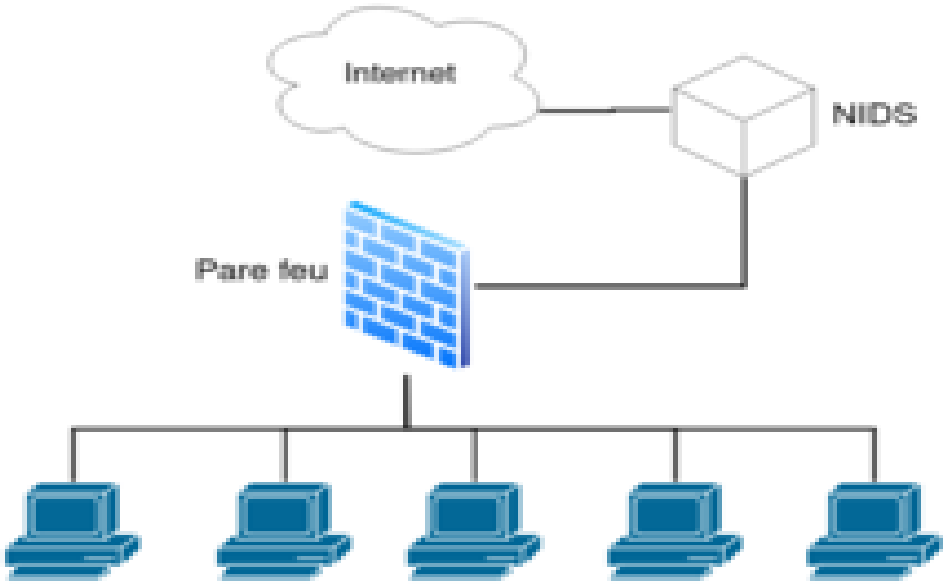


Figure 4: NIDS

II.1.1.2. La détection d'intrusion basée sur l'hôte (HIDS)

Les systèmes de détection d'intrusion basés sur l'hôte (HIDS, Host-based IDS), analysent exclusivement l'information concernant cet hôte. Comme ils n'ont pas à contrôler le trafic du réseau mais les activités d'un hôte, ils se montrent habituellement plus précis sur les variétés d'attaques. Ces IDS utilisent deux types de sources pour fournir une information sur l'activité : les logs et les traces d'audit du système d'exploitation.

Chacun a ses avantages : les traces d'audit sont plus précises, détaillées et fournissent une meilleure information. Les logs, qui ne fournissent que l'information essentielle, sont plus petits et peuvent être mieux analysés en raison de leur taille. Il n'existe pas de solution unique HIDS couvrant l'ensemble des besoins, mais les solutions existantes couvrent chacune un champ d'activité spécifique, comme l'analyse de logs système et applicatifs, la vérification de l'intégrité des systèmes de fichiers, l'analyse du trafic réseau en direction/provenance de l'hôte, le contrôle d'accès aux appels système, l'activité sur les ports réseau, etc. Les systèmes de détection d'intrusion basés sur l'hôte ont certains avantages : l'impact d'une attaque peut être constaté et permet une meilleure réaction.

Ils présentent néanmoins des inconvénients, parmi lesquels : les scans sont détectés avec moins de facilité, ils sont plus vulnérables aux attaques de type DoS, ils consomment beaucoup de ressources CPU, etc.

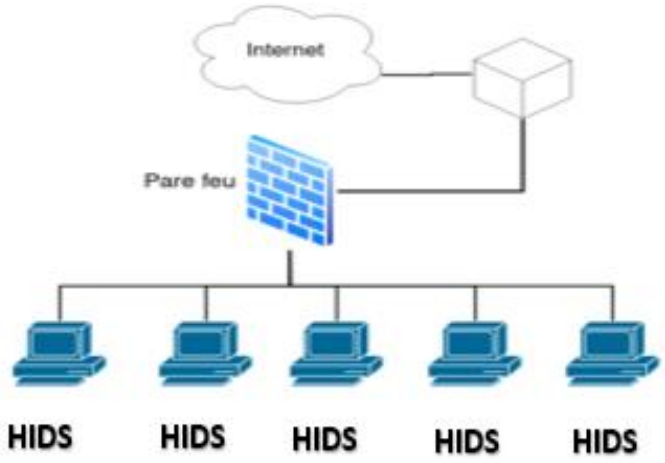


Figure 5: HIDS

II.1.2. Les systèmes de prévention d'intrusions (IPS)

Le principe de fonctionnement d'un IPS est symétrique à celui d'un IDS (IPS hôte et IPS réseau), ajoutant à cela l'analyse des contextes de connexion, l'automatisation d'analyse des logs et la coupure des connexions suspectes. Là où les systèmes de détection d'intrusion se contentent de donner l'alerte, les systèmes de prévention d'intrusion bloquent le trafic jugé dangereux.

Pour cela, avant toute action, une comparaison est faite avec un ensemble de règles. Si l'action est conforme à l'ensemble de règles, la permission de l'exécuter sera accordée et l'action sera exécutée. Si l'action est illégale (par exemple si le programme demande des données alors que cette action ne lui est pas permise), une alarme est donnée et le trafic sera bloqué. Dans la plupart des cas, les autres détecteurs du réseau en seront aussi informés dans le but d'empêcher les autres ordinateurs d'ouvrir ou d'exécuter des fichiers spécifiques. Le diagramme ci-après illustre le fonctionnement d'un IPS.

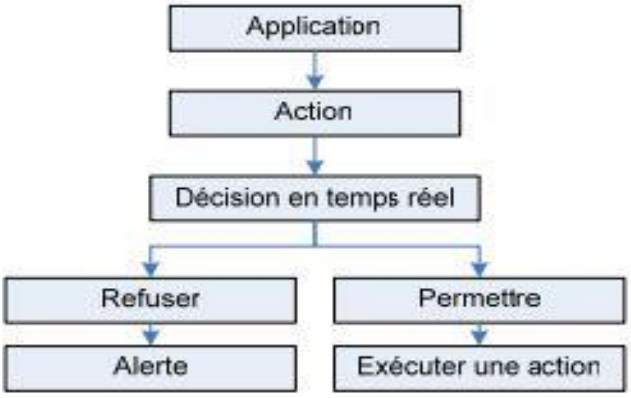


Figure 6: Fonctionnement d'un IPS

Comme pour les IDS, les IPS peuvent être orientés hôtes (Host IPS) ou réseaux (Network IPS).

II.1.2.1. La prévention d'intrusion basée hôte (HIPS)

Un IPS basé hôte est un agent du système ou un agent installé sur le système bloquant les comportements anormaux tels que la lecture ou l'écriture de fichiers protégés, l'accès à des ports non autorisés, une tentative de débordement de pile, un accès à certaines zones de la base de registres. En effet un HIPS analyse exclusivement l'information concernant cet hôte pour le protéger des comportements dangereux. Les HIPS sont en général placés sur des machines sensibles, susceptibles de subir des attaques et possédant des données importantes pour l'entreprise par exemple les serveurs.

Remarque : Les HIDS et les HIPS ont les mêmes positions.

II.1.2.2. La prévention d'intrusion basée réseau (NIPS)

Le rôle d'un IPS basé réseau est d'analyser les paquets circulant dans le réseau. La principale différence entre un NIDS et un NIPS tient principalement en 2 caractéristiques : le positionnement en coupure sur le réseau du NIPS et non plus seulement en écoute comme pour le NIDS et la possibilité de bloquer immédiatement les intrusions et ce quel que soit le type de protocole de transport utilisé et sans reconfiguration d'un équipement tierce. Ce qui induit que le NIPS est constitué d'une technique de filtrage de paquets et de moyens de blocage. Le NIPS analyse l'intégralité des paquets, depuis les couches réseaux jusqu'au niveau applicatif, et de manière furtif (pas d'adresse IP).

Les IPS permettent de stopper des attaques cependant les principales limites et contraintes des IPS à ce jour semblent être leur mise en place délicate, leur administration rebutante, la possibilité de bloquer tout le réseau en cas de fausse alerte.

Remarque : Les NIPS se placent aux mêmes endroits que les NIDS.

II.1.3. La différence entre IDS et IPS

La principale différence entre l'IDS et l'IPS est l'action prise lorsqu'un incident potentiel a été détecté :

- Les systèmes de détection des intrusions ne sont pas conçus pour bloquer les attaques. Ils se contentent de surveiller le réseau et d'envoyer des alertes aux administrateurs si une menace potentielle est détectée.
- Tandis que les systèmes de prévention des intrusions contrôlent l'accès à un réseau informatique et le protègent contre les abus et les attaques. Ces systèmes sont conçus pour surveiller les données d'intrusion et prendre les mesures nécessaires pour éviter qu'une attaque ne se déclenche.

II.2. La supervision informatique

II.2.1. Définition

La supervision informatique (appelée aussi monitoring du système informatique) est une technique de surveillance, d'analyses et d'alertes permettant de pallier les problèmes liés à tous les niveaux de fonctionnement informatique d'une entreprise.

Le recours à la supervision informatique a un objectif bien précis : rendre l'entreprise plus performante et surtout, être proactive. Elle permet de détecter toute anomalie en temps réel, afin de prendre les mesures nécessaires.

II.2.2. Fonctionnalités

La supervision informatique par des moniteurs de supervision regroupent les fonctionnalités ci-après :

- **Supervision système** : c'est la vérification de la santé des ressources matérielles (la mémoire, le CPU, le disque dur, etc.).

- **Supervision réseau** : elle porte sur la surveillance de manière continue de la disponibilité des services en ligne, du fonctionnement du réseau, des débits et bande passante, de la sécurité, etc.
- **Cartographie** : présente la vue d'ensemble de l'architecture informatique surveillée.
- **Rapports d'activité (reporting)** : comme les tableaux de bord et les histogrammes.
- **Exécution de commandes** : qui sont des actions ou programmes lancés automatiquement.
- **Envoi d'alertes** : lanceur d'alerte sous forme sonore, par message, visuelle ou encore par e-mail.

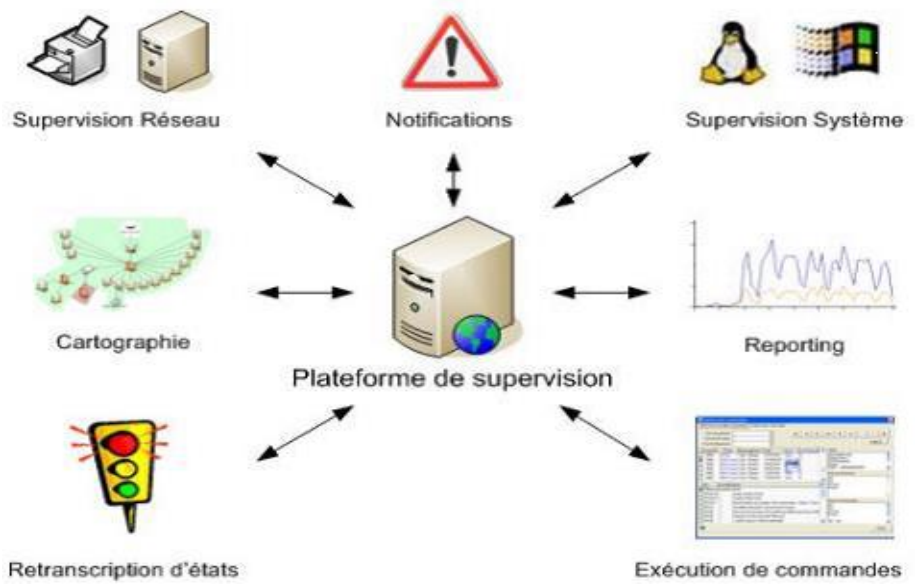


Figure 7: Fonctionnalités de la supervision

Il est à noter que ces fonctions fournies par les modules spécifiques qui composent le système de suivi produisent trois niveaux d'informations.

II.2.2.1. Informations sur les systèmes

Ce type de surveillance fournira des informations sur le fonctionnement du système, telles que l'utilisation du processeur, l'utilisation de la mémoire physique, l'espace libre sur le disque dur, l'état de la table de partition du disque, etc.

II.2.2.2. Informations sur les réseaux

Ce type de surveillance va permettre de diagnostiquer la disponibilité des équipements physiques connectés à un réseau. Les technologies employées pour ce type de supervision sont simples à utiliser et le niveau des informations retournées nous servent à savoir l'état de

nos équipements. Les équipements cibles sont : les commutateurs, les routeurs, les serveurs, les imprimantes, etc.

II.2.2.3. Informations sur les applications et services

On va disposer non seulement d'une visibilité sur l'équipement physique mais aussi sur les applications qui y sont exécutées et les informations renvoyées. Ses principaux axes sont : la disponibilité, le nombre d'utilisateurs, la cohérence des réponses aux interrogations et les performances de réponse aux requêtes.

II.2.3. Rôle de la supervision

Deux étapes sont importantes pour les administrateurs afin atteindre l'objectif de supervision souhaité, à savoir surveiller le système et assurer sa disponibilité même en cas d'anomalie.

- Essayez de prévenir et d'assurer un retour rapide en cas de problème (panne matérielle ou interruption de service) ;
- Automatiser les tâches de récupération des applications et des services en assurant des mécanismes de redondance en une durée d'intervention minimale.

II.3. La supervision réseau

II.3.1. Définition

Comme dit précédemment, la supervision réseau désigne l'ensemble des outils et ressources déployés afin de veiller à la surveillance des réseaux informatiques et des services.

Son objectif est de mettre en place une surveillance pour prévenir les interruptions de services, mais aussi de détecter les failles du réseau informatique afin d'éviter la détérioration des données et contrer les cyberattaques.

II.3.2. Principe

La supervision réseau peut être mise en œuvre sur la base d'analyse de résultats de commandes et de scripts locaux mais c'est surtout sur la base de protocoles standards. De nombreux logiciels existent et la communauté open source est particulièrement active dans le monitoring. Les logiciels permettent d'assister le technicien grâce à des interfaces de visualisations l'ensemble du réseau et à des alertes.

Des solutions logicielles proposant la supervision d'un réseau sont capables de vérifier l'état des équipements et des services à des intervalles de temps réguliers. Les données de résultats sont exploitables sous 3 formes différentes :

- Booléen (Le service est-il disponible ou non ?),
- Numérique (Quel est le temps de réponse de la machine ?)
- Qualitatif (Quel type d'erreur est renvoyé ?).

Les solutions de supervision permettent également de remplir des rapports d'activité selon la nature du service surveillé, comme des graphes d'utilisation réseau, ou encore des historiques de changement d'état sur le temps.

II.3.3. Méthodes de supervision

Deux grandes méthodes de supervision sont utilisées avec plusieurs variantes : les méthodes active et passive, détaillées dans les paragraphes suivants :

Supervision active :

La supervision active est la plus classique et la plus utilisée. Elle consiste en l'envoi de requêtes d'interrogation et de mesure par la plateforme de supervision. Elle a l'avantage d'être fiable : les vérifications se font de manière régulière et en mode question-réponse.

Cette méthode est composée de trois étapes :

- Le serveur envoie une requête vers la ressource supervisée.
- La ressource répond à la requête du serveur.
- Le serveur analyse l'information et détermine un état pour la ressource.

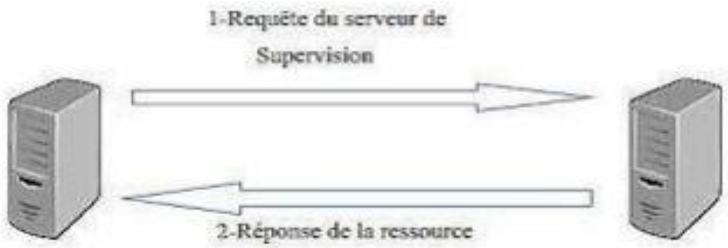


Figure 8: Supervision active

Le protocole le plus utilisé par les outils de supervision, SNMP utilise la méthode active.

Supervision passive :

La supervision passive l'est du point de vue du serveur de supervision : ce sont les ressources supervisées qui transmettent des alertes au serveur de supervision :

- La ressource supervisée vérifie son état et transmet de manière autonome le résultat au serveur de supervision.
- Le serveur de supervision reçoit l'alerte et la traite.

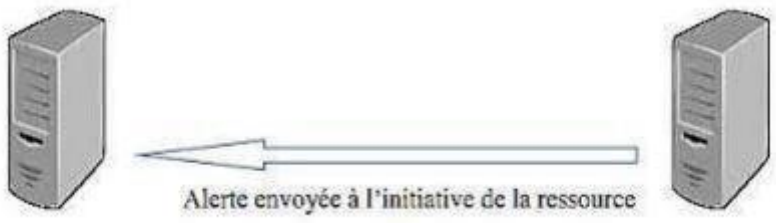


Figure 9: Supervision passive

Le protocole standardisé et privilégié pour la supervision passive est aussi SNMP avec le mécanisme de trappes.

II.4. Protocoles de supervision

Pour bien superviser, les systèmes de supervision utilisent des protocoles. Nous allons étudier quelques protocoles de supervision.

II.4.1. Protocole SNMP

SNMP qui signifie « Simple Network Management Protocol », qui veut dire protocole simple de gestion de réseau en français.

Le protocole SNMP est utilisé par la grande majorité des solutions de supervision. C'est un protocole de communication qui permet aux administrateurs réseau de gérer les équipements du réseau, de superviser et de diagnostiquer des problèmes de services du réseau, mais aussi de superviser un système d'exploitation, etc.

Pour cela, deux principes sont utilisés afin de récolter des informations :

- Requête du serveur vers l'équipement : supervision active.
- Alertes envoyées spontanément de l'équipement vers le serveur (traps) : supervision passive.

II.4.1.1. Les différentes versions du SNMP

Il existe actuellement 3 versions différentes du protocole SNMP :

- SNMP v1 : première version standard mais très pauvre au niveau de la sécurité.
- SNMP v2 : avec une amélioration de la sécurité mais jamais unifiée.
- SNMP v3 : de nouveau standard avec une grosse évolution au niveau de la sécurité avec 2 concepts, USM (User based Security Model) pour utiliser le système nom d'utilisateur et un mot de passe cryptés en DES (Data Encryption Standard), et VACM (View based Access Control Model) pour une restriction de lecture de la MIB.

II.4.1.2. Architecture SNMP

L'environnement de gestion SNMP est constitué de plusieurs composantes : La station de supervision (Manager), les éléments actifs du réseau, les variables MIB et des agents SNMP.

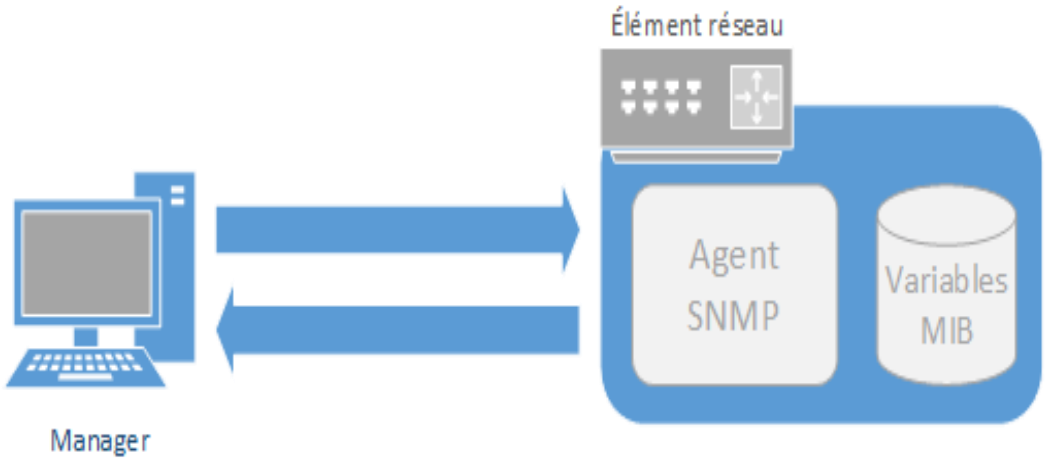


Figure 10: Architecture de SNMP

Les différentes composantes du protocole SNMP sont les suivantes :

- **Manager** : Il exécute les applications de gestion qui contrôlent les éléments réseaux. Physiquement, la station est un poste de travail. Le manager va aller récupérer les informations auprès des agents et les centraliser.
- **Elément du réseau** : Ce sont les équipements (Ex : Routeur, Switch, Poste de travail, imprimante, …) que l'on cherche à gérer. Chaque élément réseau est composé d'un Agent SNMP et d'une variable MIB.

- **Agent SNMP** : Chaque élément du réseau dispose d'un agent SNMP qui répond aux requêtes du manager. Ils vont chercher l'information requise dans la MIB et la retransmette ensuite au manager.
- **MIB** (Management Information Base) : C'est une collection d'objets représentant les caractéristiques du terminal administré.

On va voir de manière détaillée les composantes du protocole SNMP.

II.4.1.2.1. Le manager

Rappelons que le Manager se trouvera sur une machine d'administration (un poste de travail en général). Il reste un client avant tout, étant donné que c'est lui qui envoie les différentes requêtes aux agents. Il devra disposer d'une fonction serveur, car il doit également rester à l'écoute des alertes que les différents équipements sont susceptibles d'émettre à tout moment. Le Manager dispose d'un serveur qui reste à l'écoute sur le port UDP 162 ainsi que d'éventuels signaux d'alarme appelés des ***traps***.

II.4.1.2.2. L'agent SNMP

L'agent est un programme qui fait partie de l'élément actif du réseau. L'activation de cet agent permet de recueillir la base de données d'informations et la rend disponible aux interrogations. Les principales fonctions d'un agent SNMP :

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

Par ailleurs même si la principale fonction de l'agent est de rester à l'écoute des éventuelles requêtes du Manager et y répondre s'il y est autorisé, il doit également être capable d'alerter le manager en cas de problème, s'il a été configuré.

II.4.1.2.3. MIB

La MIB (Management Information base) est la base de données des informations de gestion maintenue par l'agent, auprès de laquelle le manager va venir pour s'informer.

Deux MIB publics ont été normalisées : MIB I et MIB II (dite 1 et 2). Un fichier MIB est un document texte écrit en langage ASN.1 (Abstract Syntax Notation 1) qui décrit les variables, les tables et les alarmes gérées au sein d'une MIB.

La MIB est une structure arborescente dont chaque nœud est défini par un nombre ou OID (Object Identifier). Cette OID est très utile car il permet d'accéder à une information grâce à la suite de tous les index.

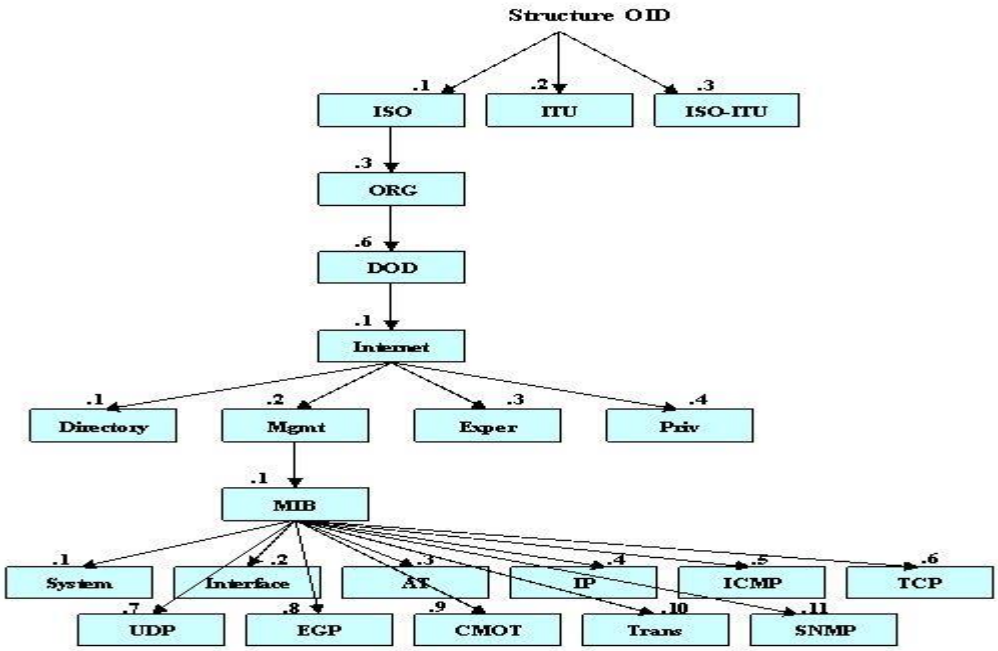


Figure 11: Exemple de structure d'un MIB

Pour accéder aux variables souhaitées, on utilisera l'OID (Object Identification) qui désigne l'emplacement de la variable à consulter dans la MIB.

II.4.1.3. Les requêtes SNMP

Le mécanisme de base du protocole SNMP est constitué d'échanges de type requête/réponse appelé PDU (Protocol Data Unit).

Il existe quatre types de requêtes SNMP : GetRequest, GetNextRequest, GetBulk, SetRequest.

- La requête GetRequest qui recherche une variable sur un agent ;
- La requête GetNextRequest qui recherche la variable suivante ;
- La requête GetBulk qui recherche un ensemble de variables regroupées ;
- La requête SetRequest qui change la valeur d'une variable sur un agent.

Les réponses de SNMP :

À la suite de requêtes, l'agent répond toujours par *GetResponse*. Toutefois si la variable demandée n'est pas disponible, le *GetResponse* sera accompagné d'une erreur *noSuchObject*.

Les alertes (Traps) :

Les alertes sont envoyées quand un événement non attendu se produit sur l'agent. Celui-ci en informe la station de supervision via une trap. Donc une notification est envoyée vers son manager pour signaler un événement, un changement d'état ou un défaut. L'agent n'attend pas d'acquittement de la part du manager.

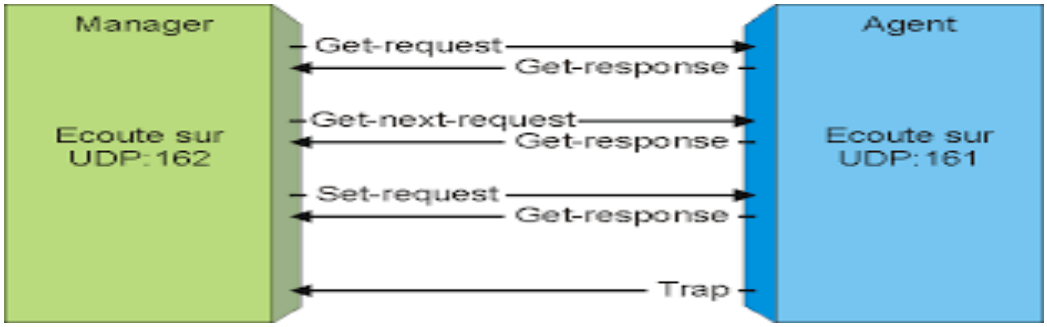


Figure 12: Protocole SNMP : Les échanges entre le manager et l'agent SNMP

II.4.2. WMI

II.4.2.1. Présentation WMI

Le WMI (Windows Management Instrumentation) est un système de gestion des éléments logiques et physiques d'une machine munie d'un système d'exploitation Windows. Ce système de gestion interne au système d'exploitation est responsable de la surveillance et du contrôle de toutes des ressources du système. Cet outil est très utile pour les administrateurs réseau car il s'agit d'une API (Application Programming Interface) qui effectue toutes des tâches d'administration.

WMI est le résultat du projet du groupe DMTF (Distributed Management Task Force) dont Microsoft fait partie et de l'initiative WBEM (Web-Based Enterprise Management). De ce plan de normalisation est né le modèle CIM (Common Information Model), qui est un modèle orienté objet dont le but est de fournir une gestion cohérente et unifiée pour tous les éléments gérés. Par conséquent, WMI est une implémentation du modèle CIM.

II.4.2.2. Architecture WMI

L'architecture WMI est structurée en 3 parties :

- Les ressources gérées (WMI Providers) ;
- L'infrastructure WMI (WMI Core Service) ;

- Les consommateurs (WMI Consumer).

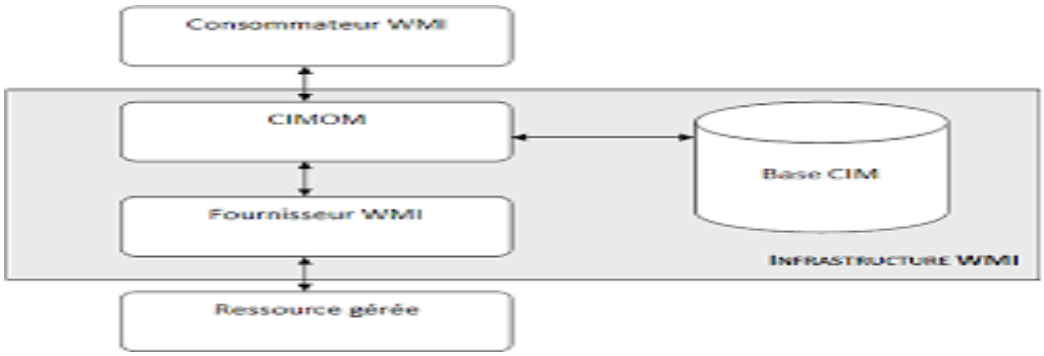


Figure 13: Architecture WMI

Si un administrateur tente d'accéder à un composant logique ou physique pour le gérer, par script ou une application de gestion. Par l'intermédiaire de Windows Management API, la requête est transmise au CIM Object Manager (connu sous le nom de CIMON). C'est ce dernier qui détermine si l'information est dans le conteneur WMI (Base CIM, WMI repository ou CIM repository, Cette base est une arborescence de classe représentant des familles d'éléments logiques ou physiques) ou si elle est fournie par un provider (ressource gérée), puis le WMI lui transmet la requête. Pour finir, la réponse est transmise au CIMON, puis au Windows Management API qui transmet à son tour la réponse à l'administrateur.

II.4.2.3. Requête WMI

Le WQL (Windows Query Language) est une implémentation Microsoft du CQL (CIM Query Language) dédiée au WMI. Par conséquent, nous pouvons agir sur les objets d'un système par requête.

Exemple : Select * FROM Win32_Service, pour accéder à la liste des services.

On peut également exprimer des conditions et des jointures (bonne pratique SQL) :

Select * FROM Win32_Service WHERE State='Stopped'

On peut aussi sélectionner les propriétés à récupérer sur les instances :

Select Name, FreeSpace FROM Win32_LogicalDisk WHERE DeviceID='c :'

II.4.3. WS-Management

II.4.3.1. Présentation de WS-Management

Le WS-Mangement (Web Services for Management) est une spécification du DMTF qui est basé sur SOAP (Simple Object Access Protocol) définissant un protocole de communication pour la gestion des serveurs, périphériques, applications et services Web. Ainsi, Ce protocole peut être utilisé pour la supervision et la gestion des équipements. Le WS-Management a été publié dans sa version finale (1.0).

SOAP est un protocole de transfert de messages qui utilise XML (Extensible Markup Language) et définit un ensemble de règles pour construire la structure d'échange de messages. Il est particulièrement utile pour les dialogues demande-réponse.

II.4.3.2. Mécanismes d'échanges de messages SOAP

La transmission des messages du protocole SOAP se fait en mode client-serveur, en utilisant le protocole HTTP pour la transmission du contenue des messages en format XML. La figure suivante explique le mécanisme.

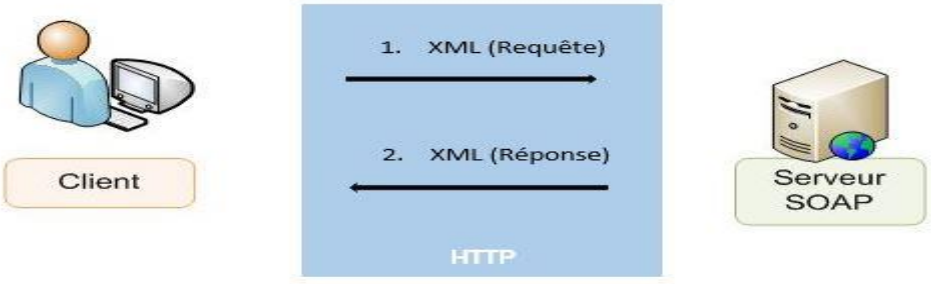


Figure 14: Mécanismes d'échanges de messages SOAP

Conclusion

La supervision est très importante pour le bon fonctionnement des systèmes informatiques et permet de réagir rapidement en cas de problèmes ou pannes. Dans ce qui suit, nous allons étudier quelques logiciels de supervision, voir même les plus utilisés, les comparer et choisir le mieux pour la suite du travail.

CHAPITRE III : LOGICIELS DE SUPERVISION

Introduction

Dans ce présent chapitre, nous allons présenter des outils de supervision réseau disponible en open source, pour voir comment fonctionne chaque logiciel et ce qu'il permet de superviser. Puis nous allons les comparer et terminer par choisir un à notre convenance.

Nous étudierons des logiciels comme suit : d'une part les logiciels de suivi graphique et d'autre part les logiciels à tableaux de bord.

III.1. Outils de supervision graphiques et statistiques

Ces logiciels fonctionnent tous sur le même principe : collecter régulièrement les données de supervision sur des systèmes et des équipements en appelant un agent préinstallé ou en activant le protocole SNMP, stocker ces données dans une base de données, produire des représentations graphiques temporelles et rassembler l'ensemble de ces informations sur un site web.

III.1.1. MRTG (Multi Router Traffic Grapher)

III.1.1.1. Présentation

MRTG est un logiciel dédié à la supervision réseau. Il permet d'obtenir toute une série de données statistiques sur des équipements *(tels que routeurs, serveurs, ou systèmes)* sous forme de représentations graphiques. Il va pour cela chercher des informations directement sur les interfaces des machines du réseau via le protocole SNMP *(Simple Network Management Protocol).*

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.

A travers une page web, il génère des pages html contenant des images au format PNG qui représentent graphiquement l'état en temps réel de la ressource surveillée. 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 quel 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.1.1.2. Les fonctionnalités

Nous allons citer quelques fonctionnalités de MRTG :

- Permet de surveiller des systèmes, des routeurs, des commutateurs, serveurs, etc….
- Fonctionne sur les systèmes Windows, Linux, Unix, Mac OS ….
- Obtient ses données via un SNMP agent.
- Collecte généralement des données toutes les cinq minutes (il peut être configuré pour collecter des données moins fréquemment).
- Crée un HTML page par cible comportant des graphiques (GIF ou PNG images).
- Les résultats sont représentés en fonction du temps dans des graphiques de jour, de semaine, de mois et d'année.
- Peut également envoyer des e-mails d'alerte si les cibles ont des valeurs supérieures à un certain seuil.

III.1.1.3. Architecture de MRTG

Le principe est simple : un script Perl recherche les données sur les équipements à surveiller via le protocole SNMP et envoi celles-ci à un programme C qui va les stocker et générer les graphiques.

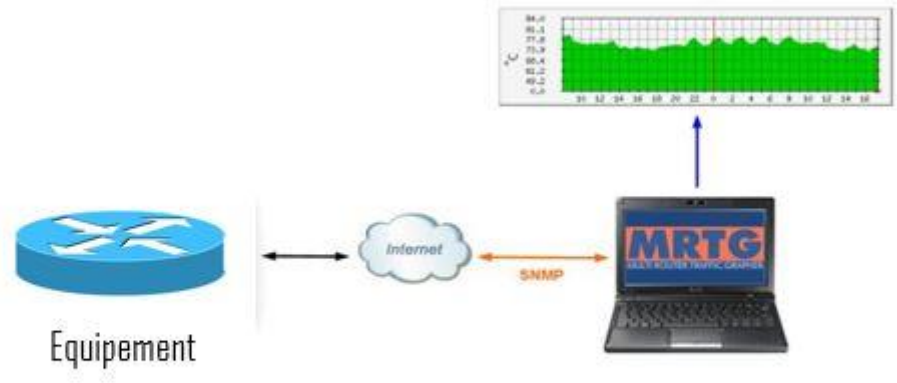


Figure 15: Architecture de MRTG

III.1.1.4. Les avantages et les inconvénients

III.1.1.4.1. Les avantages

MRTG possède de nombreux avantages dont :

- MRTG est un logiciel gratuit.
- MRTG est un outil multi plateforme (Linux, Unix, Windows).
- 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. De plus on peut même employer un programme externe pour recueillir les données qui doivent être contrôlées via MRTG. Il est possible de contrôler plus de 50 liens réseaux à partir d'une machine UNIX ou LINUX.
- Sa configuration se fait par l'intermédiaire d'un fichier de configuration, ce qui permet un control total de ses fonctionnalités.

III.1.1.4.2. Les inconvénients

Voici des inconvénients de MRTG :

- Passe trop de temps à créer des pages HTML.
- Trop orienté SNMP.
- Graphiques à deux courbes.

III.1.2. Cacti

III.1.2.1. Présentation

Cacti est un logiciel libre de supervision réseau basé sur la puissance de stockage de données RRDTool, qui peut être installé sur un système d'exploitation Linux ou Windows. Il est considéré comme le successeur de MRTG (Multi Router Traffic Grapher) et également comme une interface d'utilisation de RRDTool.

Il présente les statistiques du réseau sous forme de graphiques faciles à comprendre en utilisant le protocole SNMP et encore grâce à des scripts. Les données sont récoltées auprès des différents agents SNMP grâce à un script PHP. Pour de meilleures performances, un exécutable nommé cactid peut également effectuer les interrogations.

Mais contrairement à MRTG qui régénère l'ensemble des graphiques toutes les 5 minutes, Cacti génère les images dynamiquement à l'affichage à partir des fichiers de données RRDTool.

III.1.2.2. Les fonctionnalités

Cacti a plusieurs fonctionnalités dont :

- Fonctionne sous différentes plateformes dont Linux et Microsoft Windows.
- Permet la supervision de système.
- Surveillance des équipements réseaux (routeurs, commutateurs, imprimantes …).
- Basé sur RRDTool pour le système graphique et la conservation des données.
- Permet de récupérer les données à grapher en SNMP ou grâce à des scripts librement réalisables.
- Configurable grâce à une interface web sécurisée très conviviale.
- Graphiques totalement personnalisables avec un système de modèles exportables en XML.

III.1.2.3. Architecture de Cacti

Cacti fonctionne en collectant des données de performances sur les différents équipements surveillés, stocker ces données dans des bases, générer des graphes et les visualiser grâce à une interface web.

Collecter des données :

A intervalle donné (5 minutes par défaut), Cacti va collecter des valeurs ou mesurer des temps de réponse grâce à son ordonnanceur intégré. Il existe plusieurs types d'ordonnanceurs, du plus simple écrit en PHP au plus performant écrit en C. Cacti interroge les hôtes principalement par l'intermédiaire du protocole SNMP. Une majorité d'équipements réseaux et informatiques proposent cette fonctionnalité mais si ce n'est pas le cas, Cacti peut aussi interroger via des scripts étendant grandement les possibilités.

Stocker les données :

Le grand principe de RRDTool est de stocker les valeurs dans des bases de données tournantes à taille fixe, appelées RRD (Round Robin Database). On ne conserve que les dernières valeurs, ensuite ces valeurs sont moyennées pour fournir une autre base sur une période plus longue, et ainsi de suite.

Générer des graphes :

S'appuyant sur RRDTool, Cacti fournit une représentation graphique de ces valeurs et de leur évolution dans le temps. Les graphes sont générés en temps réel et l'on peut zoomer ou changer l'échelle de temps.

Une interface de visualisation :

Cacti permet aux utilisateurs de consulter les graphes à travers une interface web écrite en PHP. Mais elle permet aussi d'effectuer très simplement toute la configuration de l'outil.

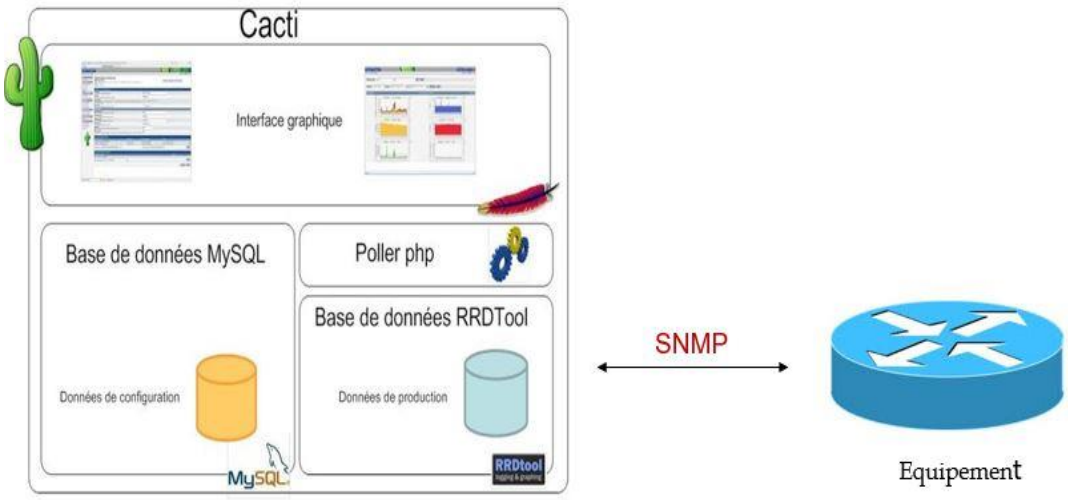


Figure 16: Architecture de Cacti

III.1.2.4. Les avantages et les inconvénients

III.1.2.4.1. Les avantages

Ses avantages sont :

- Facilité d'installation.
- Facilité de configuration.
- Affichage clair des graphs sur plusieurs périodes.
- Peut-être amélioré grâce à des plugins.
- Gestion des utilisateurs
- Grosse communauté.

III.1.2.4.2. Les inconvénients

Il a aussi des limites :

- Limité de base.
- Peut mettre un certain temps à générer les graphs.
- Pas de gestion d'alertes.

III.1.3. Ganglia

III.1.3.1. Présentation

Ganglia est un système de surveillance distribué et évolutif pour les systèmes de calcul haute performance tels que les clusters et les grilles. Il est basé sur une conception hiérarchique destinée aux fédérations de clusters. Il s'appuie sur des technologies largement utilisées telles

que XML pour la représentation des données, XDR pour le transport compact et portable des données, et RRDtool pour le stockage et la visualisation des données. Il utilise des structures de données et des algorithmes soigneusement conçus pour obtenir des frais généraux par nœud très faibles et une forte concurrence. L'implémentation est robuste, a été portée sur un ensemble étendu de systèmes d'exploitation et d'architectures de processeurs, et est actuellement utilisée sur des milliers de clusters dans le monde. Elle est actuellement utilisée sur des milliers de clusters dans le monde entier. Elle a été utilisée pour relier des clusters sur des campus universitaires et dans le monde entier et peut évoluer pour gérer des clusters de 2000 nœuds. De plus, il a été porté sur un grand nombre de plateformes (Unix propriétaires, Linux, Windows, etc.).

III.1.3.2. Les fonctionnalités

Ganglia permet de :

- Superviser des machines (PC, serveurs) en groupe.
- Configurer des seuils d'alerte.
- Faire des analyses corrélatives.
- Regrouper des alertes.
- Conserver des événements historiques de l'appareil.
- Surveiller les caractéristiques du matériel.

III.1.3.3. Architecture de Ganglia

Ganglia fonctionne suivant un mécanisme qui commence sur chaque nœud surveiller (point de surveillance). Chaque nœud exécute un démon gmond qui envoie les données vers le démon gmond sur le nœud maître du cluster. Un démon gmetad sur la console de supervision de la grille collecte les informations de chaque nœud maître, met à jour des bases RRD et crée des résumés au format XML. Enfin, une application web écrite en PHP rassemble les informations et crée les graphiques à la demande (gweb).

Il est possible d'ajouter des métriques (données) par la commande en ligne gmetric. On peut donc écrire des scripts pour étendre les possibilités de Ganglia.

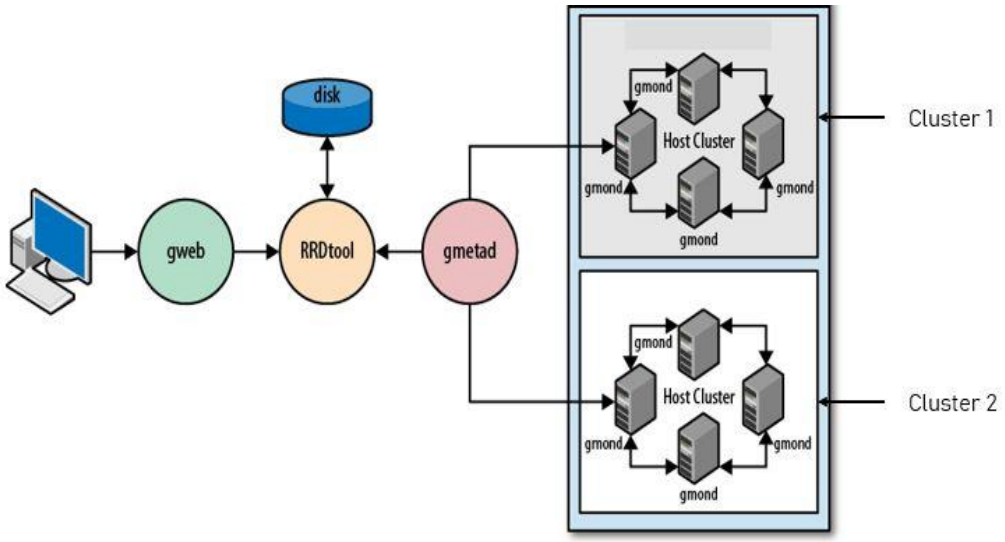


Figure 17: Architecture de Ganglia

III.1.3.4. Les avantages et les inconvénients

III.1.3.4.1. Les avantages

Voici des avantages de l'outil Ganglia :

- Solution gratuite.
- Aperçue de l'ensemble des clusters.
- Disposer des informations en quasi temps réel.
- Regroupement de la supervision.
- Gestion des alertes.

III.1.3.4.2. Les inconvénients

Parmi ces inconvénients :

- Trop orienté machine.
- Pas de système de notification intégré.

III.2. Outils de supervision avec tableau de bord

Ces logiciels ont pour fonctions de vérifier la disponibilité des services et des ressources, réagir aux alertes en notifiant l'administrateur ou en redémarrant des services, synthétiser l'état du système d'information sur une page web. Ces logiciels permettent aussi de visualiser des graphiques générés à partir des données obtenues.

III.2.1. Zabbix

III.2.1.1. Présentation

Zabbix est un logiciel de surveillance de réseau open source et dont la première version voit le jour en 2001. Il nous permet de surveiller l'état de divers services réseau, serveurs, postes de travail et autres matériels (routeurs, pare-feu, imprimantes, etc.). Zabbix fournit des vues graphiques (générées par RRDtool) et des alarmes de seuil.

Il peut être décomposé en 3 parties indépendantes : serveur de données, interface de gestion et serveur de traitement. Chacun d'eux peut être disposé sur des machines différentes pour répartir la charge et optimiser les performances. L'agent ZABBIX peut également être installé sur des hôtes Linux et Windows pour obtenir des informations statistiques telles que la charge CPU, l'utilisation du réseau, l'espace disque etc. Le logiciel utilise principalement le protocole SNMP mais supporte également le protocole IPMI (Intelligent Platform Management Interface ou L'Interface de gestion intelligente de matériel).

III.2.1.2. Les fonctionnalités

Zabbix offre de nombreuses possibilités à l'administrateur réseau pour faciliter ses tâches et assurer le bon fonctionnement du réseau :

- Interface web flexible.
- Vue globale des équipements à superviser.
- Configuration facile (ajout des équipements à superviser, sélection des déclencheurs d'alarmes, etc.).
- Notification d'alerte par e-mail, sms etc.
- Supervision répartie sur une administration web centralisée.
- Agent local hautes performances (sur les systèmes Linux, Windows, Solaris etc.).
- Supervision sans agent.
- Rapports (synthèse des alarmes déclenchées).
- Journal d'audit.

III.2.1.3. Architecture de Zabbix

Zabbix se compose de plusieurs composants logiciels majeurs (dont 3 principaux), dont les responsabilités et leurs fonctionnements sont décrites ci-dessous.

- Le serveur Zabbix est le composant central auquel les agents envoient leur disponibilité, les informations d'intégrité et les statistiques. Le serveur est le

référentiel central dans lequel toutes les données de configuration, statistiques et données opérationnelles sont stockées.

- Stockage des données : Toutes les informations de configuration ainsi que les données collectées par Zabbix sont stockées dans une base de données.
- L'interface Web est fournie pour permettre un accès facile à Zabbix de n'importe où et de n'importe quelle plate-forme. L'interface fait partie du serveur Zabbix et fonctionne généralement (mais pas nécessairement) sur la même machine physique que celle qui exécute le serveur.
- Le Proxy Zabbix peut collecter des données de performance et de disponibilité au nom du serveur Zabbix. Un proxy est un composant facultatif du déploiement de Zabbix. Cependant, il peut être très bénéfique de distribuer la charge d'un seul serveur Zabbix.
- Les Agents Zabbix sont déployés sur des cibles de surveillance pour superviser activement les ressources locales et les applications, et envoyer les données collectées au serveur Zabbix.

Ce qui suit est la représentation du principe de fonctionnement de Zabbix (son architecture).

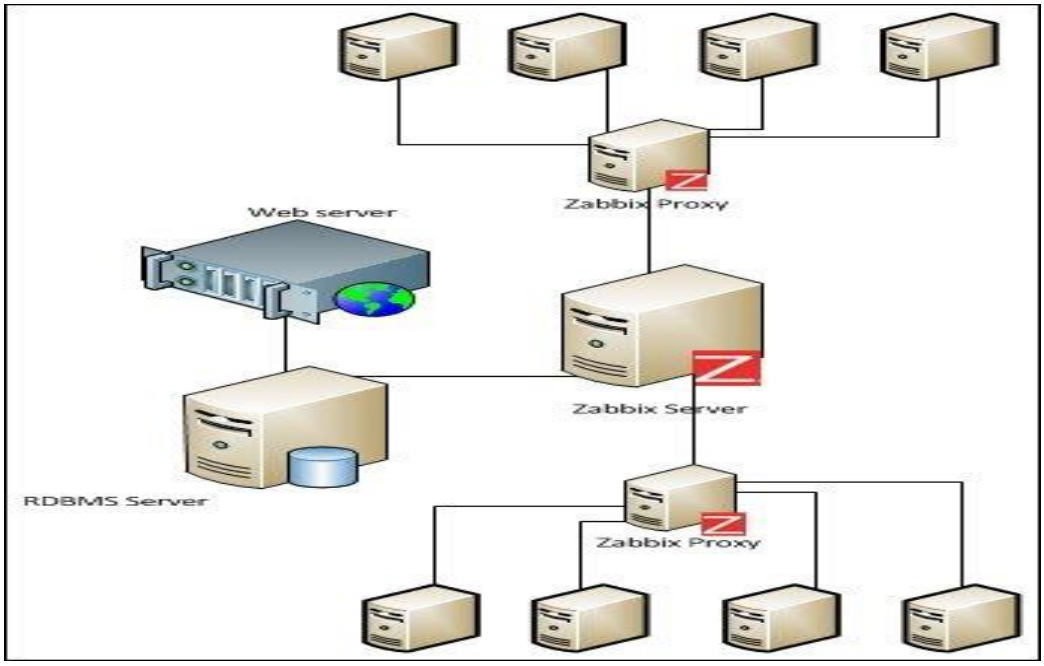


Figure 18: Architecture de Zabbix

III.2.1.4. Les avantages et les inconvénients

III.2.1.4.1. Les avantages

Voici quelques avantages de l'outil de supervision Zabbix :

- Solution Open Source.
- Facilité d'installation.
- Génération facile des graphs.
- Facilité de consultation des graphs en fonction du temps.
- Affichage clair des erreurs sur le Dashboard.

III.2.1.4.2. Les inconvénients

Parmi les inconvénients de Zabbix on distingue :

- Chaque machine à superviser doit disposer du client Zabbix.
- Limité au ping sans le client.
- Problème de configuration sur le switch.

III.2.2. Nagios

III.2.2.1. Présentation

Nagios, qui est une évolution de Netsaint, est un logiciel de supervision réseau permettant la surveillance réseau et système conçu pour fonctionner sous un système d'exploitation Linux mais peut fonctionner sur les autres systèmes comme Windows, Mac OS, etc. La surveillance est assurée grâce au protocole SNMP mais aussi des agents comme NSCLIENT, NPCA et autres.

Cet outil propose de superviser des machines, des équipements et leurs services via des plugins indépendants, chacun responsable d'un test particulier. Nagios récupère les informations fournies par les services de surveillance et les analyse. Si le résultat de cette analyse fait remonter un problème, les services de surveillance le signal et peuvent envoyer des avertissements à l'administrateur par courrier électronique, SMS, etc.

III.2.2.2. Les fonctionnalités

Voici les principales possibilités offertes par Nagios :

- Superviser des ressources machines (processeur, disques durs, mémoire, les fichiers de log, . . .) ;
- Superviser des services : SMTP, POP, HTTP, ICMP, SNMP… ;
- La supervision des équipements réseaux (routeurs, commutateurs, imprimantes, etc.)
- Superviser des données comme la température, la luminosité, l'humidité par des sondes ;

- Possibilité de définir des gestionnaires d'événement, qui s'exécutent pour une résolution pro-active des problèmes ;
- Envoi d'alertes sous plusieurs formes (affichage sur l'interface, email, SMS...) vers des groupes de contact, avec une possibilité d'escalade ;
- Historisation des événements et données, qui peuvent servir pour l'élaboration de rapport ;
- Interface web pour suivre l'état du réseau, son évolution, ses problèmes ;
- Définition de plages horaires de surveillance ;
- Niveau de hiérarchie des équipements permettant de distinguer un serveur en panne et un serveur injoignable ;
- Support pour l'implémentation de serveurs de supervision redondants et distribués.
- La détermination à distance et de manière automatique l'état des objets et les ressources nécessaires au bon fonctionnement du système grâce à ses plugins.
- Les plugins sont écrits dans les langages de programmation les plus adaptés à leur tâche (Bash, C++, Python, Perl, PHP, C#, etc.).

Toutes ces fonctionnalités sont assurées grâce à la gestion de manière centralisée autour de Nagios. Illustré dans la figure si après :

Figure 19: Les fonctionnalités de Nagios

III.2.2.3. Architecture de Nagios

Nagios fonctionne par un principe qui est basée sur le paradigme serveur-agent. Plus précisément, un serveur sert de point central pour la collecte des informations tandis que les autres machines du réseau exécutent un agent chargé de renvoyer les informations au serveur.

L'architecture globale de Nagios est composée principalement de 3 parties :

- Un noyau qui est le cœur du serveur Nagios, chargé de contrôler quand et dans quel ordre les contrôles des services sont effectués. C'est le principe de répartition des contrôles au mieux dans le temps qui nous évite la surcharge du serveur et des machines à surveiller.
- Des exécutants (ou plugins) dont un grand nombre est fourni de base, responsables de l'exécution des contrôles et tests sur des machines distantes ou locales et du renvoie des résultats au noyau du serveur Nagios. C'est possible de télécharger et même de créer de nouveaux plugins.
- Une interface graphique accessible par le web et conçu pour rendre plus exploitable les résultats. Elle est basée sur les CGI (Common Gateway Interface) fournis par défaut lors de l'installation de Nagios qui interprètent les réponses des plugins pour les présenter dans l'interface.

  Cette interface sert à afficher de manière claire et concise une vue d'ensemble du système d'information et l'état des services surveillés, de générer des rapports et de visualiser l'historique. D'une manière générale avoir la possibilité de détecter en un simple coup d'œil, les services ou hôtes ayant besoin d'une intervention de leur administrateur.

N.B. : Il est possible de coupler Nagios à une base de données (comme MySQL, …) lorsque le nombre d'objets à superviser devient conséquent.

La figure suivante modélise l'architecture de Nagios, illustrant son principe de fonctionnement.

Figure 20: Architecture de Nagios

III.2.2.4. Les avantages et les inconvénients

Les principaux avantages et les inconvénients de Nagios sont :

III.2.2.4.1. Les avantages

Les principaux avantages de Nagios sont :

- Disponible en open source.
- Surveillance des services réseaux (SMTP, POP, HTTP, PING, etc.).
- Surveillance des ressources des équipements (serveur, routeur, etc.) comme la charge du processeur, des informations sur l'utilisation des disques durs, les processus en cours.
- Très puissant et modulaire.
- Peut-être associé à un autre outil (Centreon par exemple).
- Interface web, pour voir l'état actuel du réseau, notification et historique des problèmes, fichiers log, etc.
- Surveillance des données environnementales comme par exemple la température.
- Système simple de plugins permettant aux utilisateurs de développer facilement leurs propres vérifications de services.
- Beaucoup de documentations sur le web.

III.2.2.4.2. Les inconvénients

Le principal inconvénient de Nagios est la configuration complexe des différents types de serveurs et d'objets. Par conséquent, il est recommandé de lire le manuel d'instructions et de regarder le tutoriel sur le site officiel de Nagios surtout si vous n'utilisez pas le mode de configuration graphique.

III.2.3. Monit

III.2.3.1. Présentation

Monit est un outil de supervision open source destiné à superviser une machine et les services réseaux accessibles depuis cette machine (supervision système). Disponible dans la plupart des systèmes d'exploitation mais pas toute gratuite.

III.2.3.2. Les fonctionnalités

Les fonctionnalités de l'outil Monit sont de :

- Désactiver/activer la surveillance d'un service.

- Surveiller la disponibilité des processus applicatifs et remonter une alerte si ces derniers ne répondent plus.
- Superviser les services tournant sur une machine donnée (CPU, espace disque…).
- Redémarrer les processus indisponibles ou autre action similaire en cas de détection d'une anomalie.

III.2.3.3. Architecture de Monit

Monit est fait pour superviser les services tournant sur une machine donnée et agir en cas de problème (mail à un administrateur, redémarrage d'un service planté, arrêt en cas de surcharge, etc.) Monit peut également faire des contrôles d'intégrité de fichiers (pour recharger un service après modification de la configuration ou signaler une intrusion).

III.2.3.4. Les avantages et les inconvénients

III.2.3.4.1. Les avantages

Les avantages sont :

- Petit, très simple et efficace.
- Surveiller des processus locaux.
- Redémarrer des services si nécessaire.
- Contrôle de tous les services.

III.2.3.4.2. Les inconvénients

Deux inconvénients majeurs :

- Tout fonctionne sur une seule machine.
- La solution complète n'est pas libre.

III.3. Comparaison des logiciels et choix de l'outil

III.3.1. Comparaison des logiciels

- Graphiques et statistiques :

Logiciel	MRTG	Cacti	Ganglia
Cout	Disponible en version gratuit	Disponible en version gratuit	Disponible en version gratuit

Plateformes	Unix, Linux, Windows, etc.	Linux et Windows	Unix propriétaires, Linux, Windows, etc.
Protocole utilisé	SNMP	SNMP	Pas de protocole
Supervision (système, services et équipements)	▪ Système ; ▪ Routeurs, serveurs, commutateurs, etc.	▪ Système ; ▪ Routeurs, commutateurs, imprimantes, etc.	▪ Système ; ▪ Serveurs.

Tableau 1: comparaisons entre MRTG, Cacti et Ganglia

- Tableaux de bord :

Logiciel	**Zabbix**	**Nagios**	**Monit**
Cout	Disponible en version gratuit	Disponible en version gratuit	Disponible en version gratuit
Plateformes	Linux, Windows.	Linux, Windows, Mac OS, etc.	Linux, Windows, Mac OS, etc.
Protocole utilisé	SNMP, autres.	SNMP, autres	Pas de protocole
Supervision (système, services et équipements)	▪ Systèmes ; ▪ Routeurs, commutateurs, Imprimante, … ; ▪ Services (SMTP, POP, HTTP, …).	▪ Systèmes ; ▪ Routeurs, commutateurs, serveurs, … ; Services (HTTP, ICMP, LDAP, …).	▪ Système.
Flexibilité	Oui	Oui	Non
Mode de configuration	Interface web	Interface web et sur un terminal	Interface web

Tableau 2: comparaisons entre Zabbix, Nagios et Monit

III.3.2. Choix de l'outil

Comme nous voulons un logiciel plus adapter à notre travail, nous avons donc choisi les logiciels de supervision avec tableaux de bord car ils nous permettent de vérifier la disponibilité des services et des ressources, réagir aux alertes en notifiant l'administrateur ou

en redémarrant des services, synthétiser l'état du système d'information sur une page web. Ces logiciels permettent aussi de créer des graphiques avec les données obtenues. Disons tout ce dont on a besoin pour la bonne supervision d'un réseau.

Sur les trois logiciels avec tableaux de bord étudiés, on n'a décidé de ne pas choisir Monit parce qu'il se limite à la supervision système et nous voulons faire de la supervision réseau. Aussi Zabbix est un bon logiciel de supervision mais a un problème de configuration sur le switch. Donc notre choix s'est porté sur Nagios qui est un bon logiciel de supervision réseau.

En effet, Nagios est une solution très performante qui a d'énormes avantages dont sa totale modularité facilitée par les plugins pour résoudre un grand nombre de problèmes et sa capacité à gérer un grand nombre de machines et d'équipements. En plus, il fait partie des outils de supervisons les plus utilisés dans le marché de l'informatique et pour terminer l'outil Nagios a beaucoup de documentations sur le web.

Conclusion

Les logiciels de supervision réseau sont à la base du bon fonctionnement d'une architecture réseau, permettant de savoir l'état des équipements et machines, et permet aussi de réagir rapidement en cas de problèmes ou pannes. Après avoir effectué le choix de l'outil de supervision open source Nagios, nous allons l'installer et passer à la supervision d'un réseau qui sera défini dans le chapitre suivant.

CHAPITRE IV : SUPERVISION AVEC NAGIOS

Introduction

Dans ce dernier chapitre, nous allons passer à la supervision d'un réseau local en utilisant l'un des meilleurs outils dans ce domaine qui est Nagios, plus particulièrement Nagios XI. Nous allons présenter dans un premier temps l'outil en générale, puis son architecture, ensuite le réseau de déploiement (réseau à superviser), après passer à l'installation du logiciel, faire des tests et on termine par montrer comment ajouter de nouveaux services.

IV.1. Présentation de Nagios XI

Nagios XI dont Ethan Galstad pour le développement du daemon Nagios et les mises à jour des versions et Karl Debisschop, Subhendu Ghosh, Ton Voon e' Stanley Hopcroft pour le développement des plugins, est un logiciel libre qui permet de superviser des systèmes d'exploitation (Linux, Windows, Mac OS) et également des équipements réseaux (commutateurs, routeurs, imprimantes, …), des terminaux, et des services et protocoles réseaux. Il permet entre autres la surveillance des services réseaux tels que : SMTP, HTTP, FTP, SSH, etc., la surveillance des ressources machines telles que la charge de processeur, l'utilisation de l'espace disque, de la mémoire, etc. Nagios dispose d'une interface web optionnelle permettant de visualiser l'état actuelle du réseau, les notifications et les fichiers journaux. Il permet de concevoir de simples greffons (plugins) permettant aux utilisateurs de développer leurs propres vérificateurs de services. Il dispose de notifications par mail ou sms lorsqu'un problème survient sur un service ou une machine.

Il est utilisé par de nombreuses entreprises, dont il fait l'objet de contribution et recherche très actives. Disponible en version d'essais, en version d'utilisation gratuite pour une durée limitée et en version entreprise avec une licence. Cet outil est conçu pour fonctionner sous un système d'exploitation Linux et sous la plupart des systèmes Unix mais peut fonctionner aussi sur Windows. Pour installer, il est recommandé d'avoir une machine avec les caractéristiques suivantes : une RAM au moins 2 GO, un processeur qui dépasse les 2 GHz et une espace disque libre d'au moins 40 GO.

IV.2. Architecture de Nagios XI

L'architecture de Nagios XI est la même que celle donnée dans le chapitre III (figure 20).

En résumé, l'architecture de Nagios est structurée comme suit :

- ***Les équipements à superviser :*** il peut être un ordinateur, un routeur, un commutateur avec un système d'exploitation (Windows, Linux, MAC-SO etc..) et peut héberger des services et intégrer des protocoles.
- ***L'élément moteur qui est le serveur Nagios*** : c'est un ordinateur avec et une interface web pour visualiser tout ce qu'il faut superviser.
- ***Les plugins*** : sont des éléments intermédiaires qui sont chargés de récupérer les informations sur chaque élément à superviser, et pour chaque service à superviser il y a un plugin spécifique. Le plugins ou greffon est un programme exécutable ou script (perl, shell, etc.) capable de fournir au moteur :
    A. Un code de retour :
        - => 0 = tout va bien (OK)
        - => 1 = avertissement (WARNING)
        - => 2 = alerte (CRITICAL)
        - => 3 = inconnu (UNKNOWN)
    B. Un court message descriptif
    C. En option, un greffon peut retourner des informations de performance permettant à Nagios de les interpréter pour tracer des graphiques.
- ***Le CGI*** : il convertit les informations récupérées sur les équipements en des données claires et explicites pour être visualisées sur un interface web.
- ***La base de données*** : peut être utilisée pour le stockage des données afin de libérer le serveur Nagios pour être plus performant.

IV.3. Fonctionnement de l'architecture de Nagios XI

Nagios repose sur des programmes externes appelés greffons (plugins). Il peut être assimilé à un planificateur de tâches qui exécute un greffon à intervalle régulier lorsqu'un service ou un host doit être surveiller.

Par exemple le serveur Nagios à travers le plugin check_http interroge un hôte pour connaitre l'état du service HTTP. Une fois la requête reçu, l'hôte transmet l'état du service HTTP à

Nagios avec toujours l'aide du plugin check_http. Puis c'est au tour du CGI de convertir l'information reçu en donnée claire pour être visualisée sur l'interface web.

IV.4. Interaction de Nagios avec différentes plateformes et services

L'interaction de Nagios se fait à travers des greffons qui peuvent fonctionner localement (directement sur la machine supervisée) ou à distance (au travers du réseau). L'exécution à distance des greffons par le biais d'autres serveurs de supervision Nagios utilisé en supervision distribuée qui sort du cadre de ce mémoire. Dans ce mémoire nous nous limitons aux agents d'exécution de tests tels que : NRPE, NSCA, NCPA, NSClient, etc...

IV.4.1. Avec OS Windows

Pour superviser une machine Windows, l'agent NSClient++ doit être installé sur la machine distante à superviser. Le schéma suivant présente les différents composants qui doivent être mis en place et leur interaction pour que la supervision soit opérationnelle.

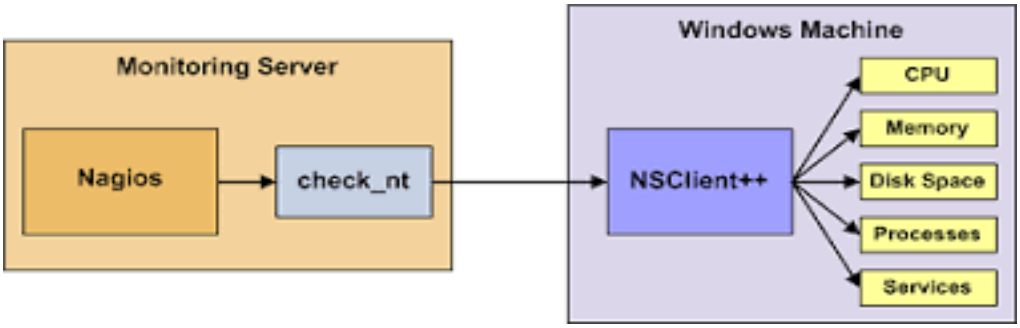


Figure 21: Architecture entre Nagios et machine Windows

La supervision Nagios via "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++) doit être installée sur chacune des machines Windows à surveiller.

IV.4.2. Avec OS Linux

Pour superviser une machine Linux, l'agent NRPE doit être installé sur la machine distante à superviser. Le schéma suivant présente les différents composants qui doivent être mis en place et leur interaction pour que la supervision soit opérationnelle.

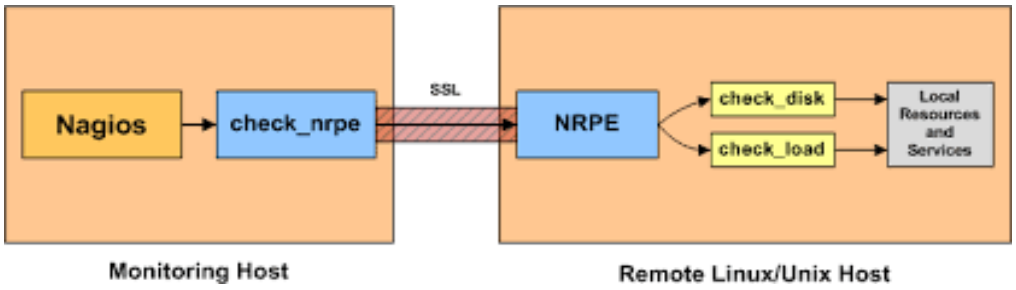


Figure 22: Architecture entre Nagios et machine Linux

Avec NRPE, la demande d'exécution d'un plugin actif est faite à l'initiative du serveur Nagios.

- Le serveur Nagios demande, via le client NRPE, l'exécution du plugin check_nrpe sur la machine Linux à superviser ;
- Le daemon NRPE hébergé sur la machine Linux à superviser, reçoit la requête d'exécution du plugin check_nrpe ;
- Le plugin check_nrpe est exécuté sur la machine Linux à superviser ;
- Le daemon NRPE de la machine Linux à superviser envoie le résultat du plugin check_nrpe au serveur Nagios ;
- Le serveur Nagios interprète les résultats retournés par le plugin check_nrpe.

IV.4.3. Avec Mac OS

L'agent NCPA peut être utilisé pour superviser une machine Mac mais aussi Linux et Windows. Il suffit juste de l'installer comme les autres agents sur la machine. Le schéma est suivant :

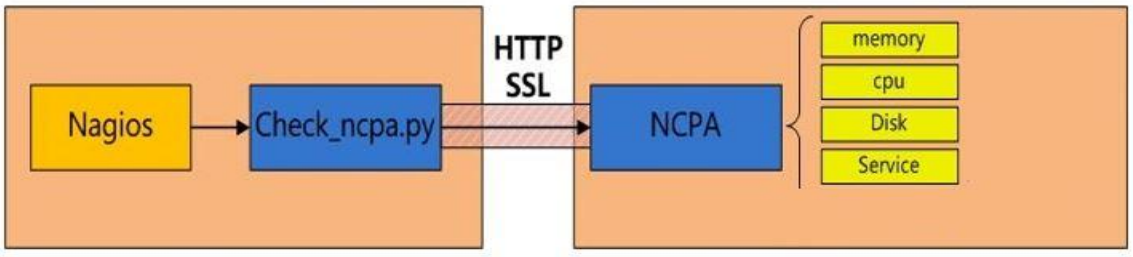


Figure 23: Architecture Nagios et machine (Windows ou Linux ou Mac)

Le serveur Nagios récupère les informations sur l'agent NCPA en utilisant de manière active le plugin check_ncpa.py.

IV.4.4. Avec un service

Pour monitorer les machines distantes (services et ressources), on doit modifier certains fichiers de configuration de Nagios. Par exemple si c'est un hôte, une entrée doit figurer dans le fichier “hosts.cfg” et si c’est un service dans “services.cfg”. Ainsi on crée un ensemble de fichiers de configurations en fonction de nos besoins, qui permettent de monitorer certains services et ressources d'une machine.

Les plugins fournis avec Nagios sont destinés à la supervision des services et ressources classiques du style (HTTP, FTP, CPU, etc.…). Pour les nouvelles applications, on doit développer ses propres greffons et de les faire exécutés soit par NRPE, soit par NSCA, ou autres. Le langage de développement peut être le C, perl, shell, etc....

IV.4.5. Avec un routeur ou un switch

Le principe de la supervision utilisé pour les OS est le même pour les autres équipements réseaux tels que les Routeurs, les Commutateurs, etc…. Nagios supporte nativement les routeurs qui utilisent le Simple Network Management Protocol (SNMP). On doit fournir l'adresse IP et les informations d'authentification des périphériques SNMP et Nagios se configure automatiquement pour fonctionner avec le routeur.

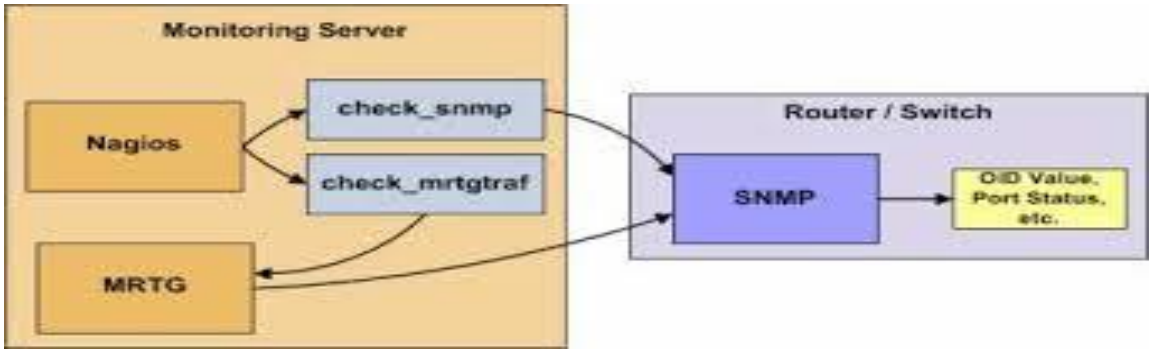


Figure 24: Architecture entre Nagios et un routeur (ou switch)

IV.5. Déploiement de Nagios : Application au réseau local

L’idée de départ, était de superviser un réseau d’entreprise à l’image de celui de l’UASZ en mettant en place une supervision derrière une architecture sécurisée implémentant un Firewall. Dans ce mémoire nous nous sommes limités à une supervision active où un Firewall n’est pas traversé et notre objectif a été d’avoir différents types d’hôtes, de services et de protocoles. Ainsi nous présentons une architecture avec différentes plateformes (Linux,

Windows, Mac OS etc…) et équipements (ordinateurs, switchs et routeurs etc..) utilisant commutation et routage.

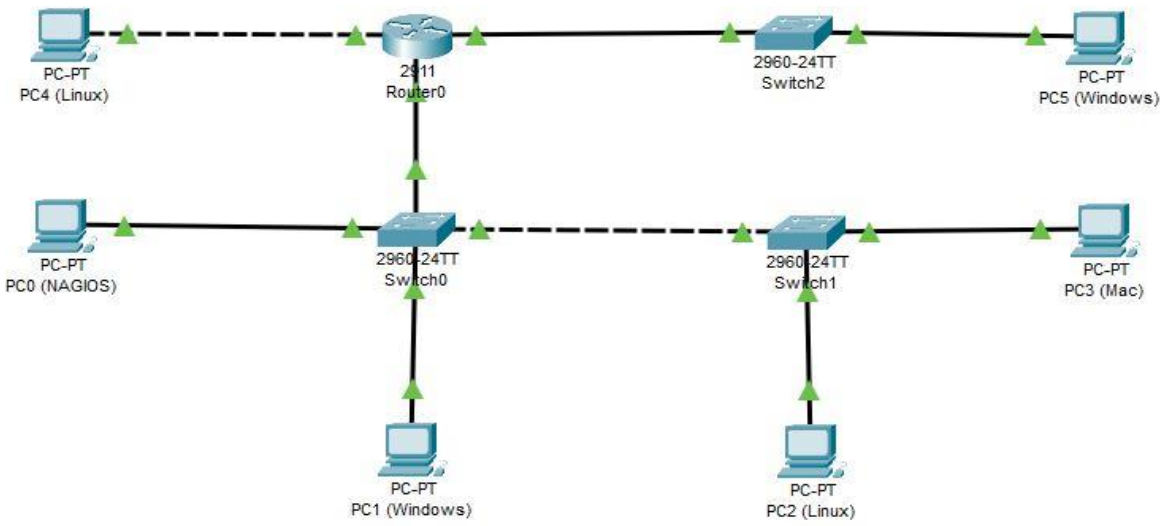


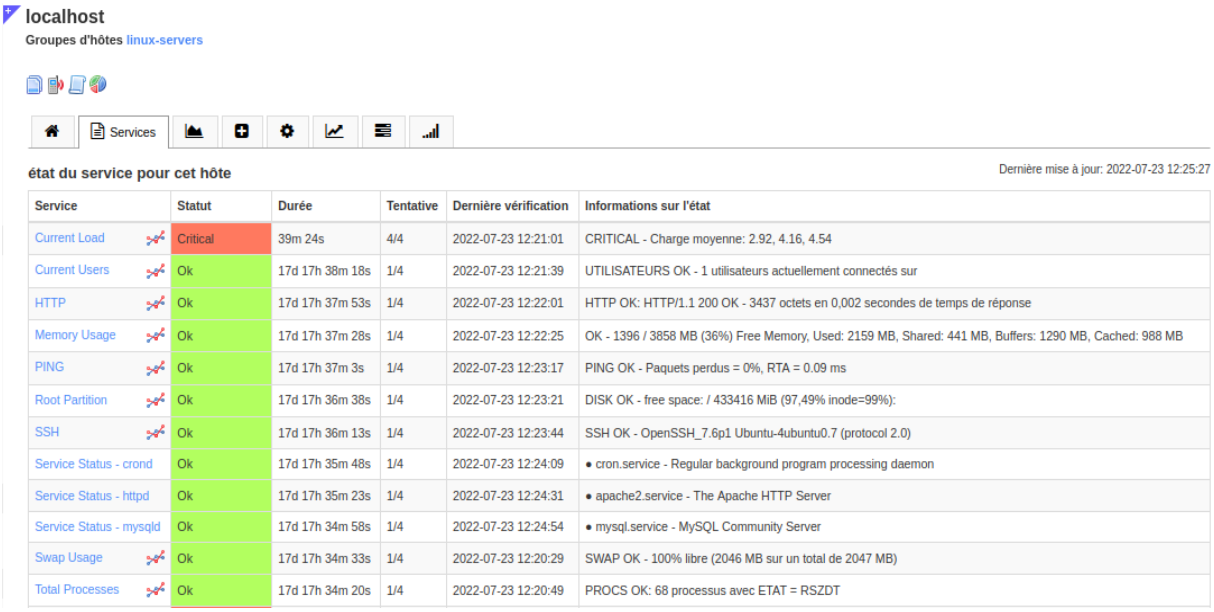
Figure 25: Architecture du réseau de déploiement

Sur la base de cette architecture, nous allons superviser :

- Des PCs Windows, Linux, Mac OS ;
- Des switchs et routeurs Cisco.

IV.6. Tests

IV.6.1. Supervision de services de la machine où est installé Nagios (localhost)



localhost

Groupes d'hôtes linux-servers

Services

état du service pour cet hôte

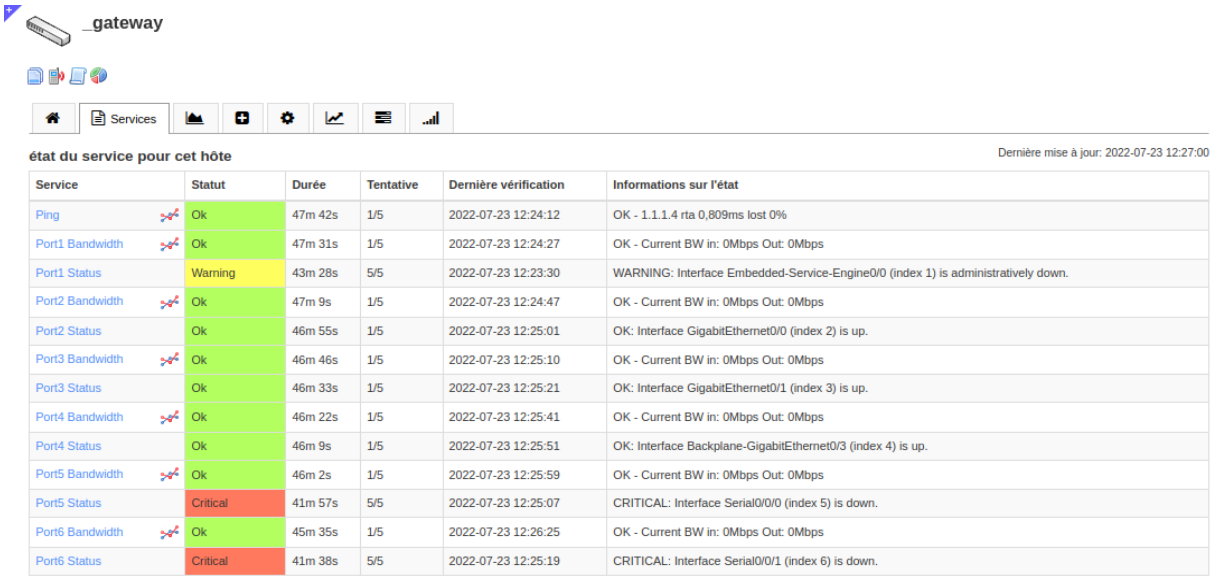
Dernière mise à jour: 2022-07-23 12:25:27

Service	Statut	Durée	Tentative	Dernière vérification	Informations sur l'état
Current Load	Critical	39m 24s	4/4	2022-07-23 12:21:01	CRITICAL - Charge moyenne: 2.92, 4.16, 4.54
Current Users	Ok	17d 17h 38m 18s	1/4	2022-07-23 12:21:39	UTILISATEURS OK - 1 utilisateurs actuellement connectés sur
HTTP	Ok	17d 17h 37m 53s	1/4	2022-07-23 12:22:01	HTTP OK: HTTP/1.1 200 OK - 3437 octets en 0,002 secondes de temps de réponse
Memory Usage	Ok	17d 17h 37m 28s	1/4	2022-07-23 12:22:25	OK - 1396 / 3858 MB (36%) Free Memory, Used: 2159 MB, Shared: 441 MB, Buffers: 1290 MB, Cached: 988 MB
PING	Ok	17d 17h 37m 3s	1/4	2022-07-23 12:23:17	PING OK - Paquets perdus = 0%, RTA = 0.09 ms
Root Partition	Ok	17d 17h 36m 38s	1/4	2022-07-23 12:23:21	DISK OK - free space: / 433416 MiB (97,49% inode=99%):
SSH	Ok	17d 17h 36m 13s	1/4	2022-07-23 12:23:44	SSH OK - OpenSSH_7.6p1 Ubuntu-4ubuntu0.7 (protocol 2.0)
Service Status - crond	Ok	17d 17h 35m 48s	1/4	2022-07-23 12:24:09	● cron.service - Regular background program processing daemon
Service Status - httpd	Ok	17d 17h 35m 23s	1/4	2022-07-23 12:24:31	● apache2.service - The Apache HTTP Server
Service Status - mysqld	Ok	17d 17h 34m 58s	1/4	2022-07-23 12:24:54	● mysql.service - MySQL Community Server
Swap Usage	Ok	17d 17h 34m 33s	1/4	2022-07-23 12:20:29	SWAP OK - 100% libre (2046 MB sur un total de 2047 MB)
Total Processes	Ok	17d 17h 34m 20s	1/4	2022-07-23 12:20:49	PROCS OK: 68 processus avec ETAT = RSZDT

Figure 26: Les services du localhost

On peut superviser l'état de l'hôte et des services : ping, HTTP, SSH, ….

IV.6.2. Supervision des services d'un routeur



_gateway

Services

état du service pour cet hôte

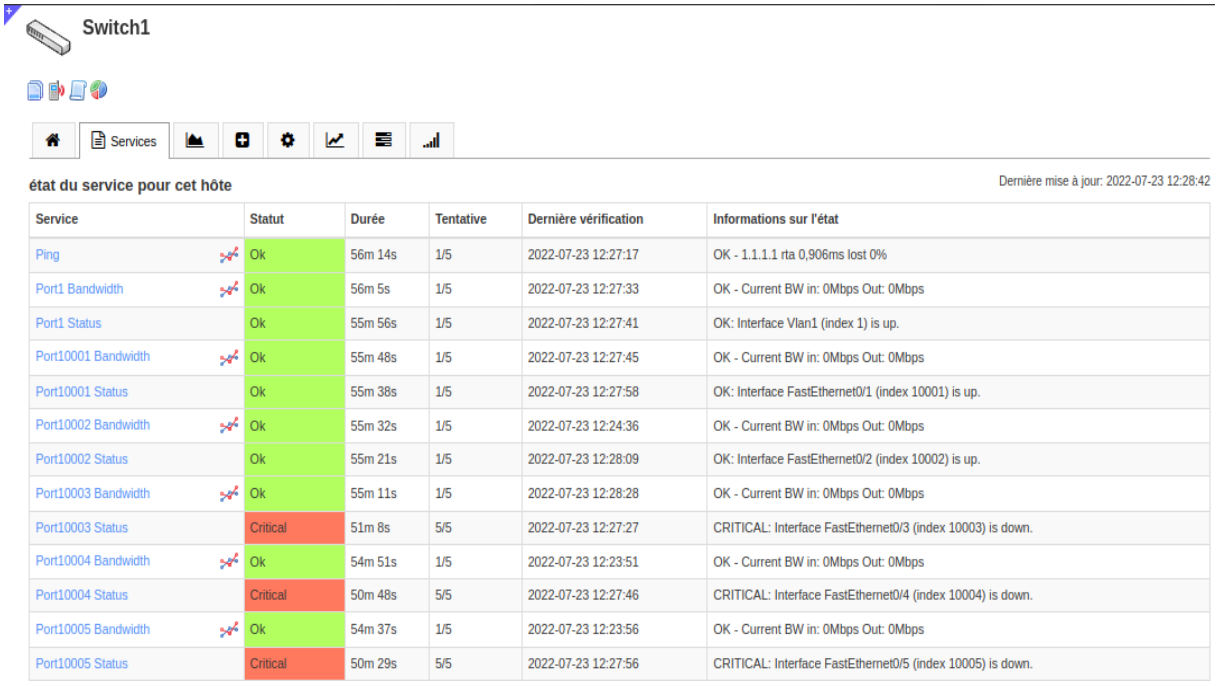
Dernière mise à jour: 2022-07-23 12:27:00

Service	Statut	Durée	Tentative	Dernière vérification	Informations sur l'état
Ping	Ok	47m 42s	1/5	2022-07-23 12:24:12	OK - 1.1.1.4 rta 0,809ms lost 0%
Port1 Bandwidth	Ok	47m 31s	1/5	2022-07-23 12:24:27	OK - Current BW in: 0Mbps Out: 0Mbps
Port1 Status	Warning	43m 28s	5/5	2022-07-23 12:23:30	WARNING: Interface Embedded-Service-Engine0/0 (index 1) is administratively down.
Port2 Bandwidth	Ok	47m 9s	1/5	2022-07-23 12:24:47	OK - Current BW in: 0Mbps Out: 0Mbps
Port2 Status	Ok	46m 55s	1/5	2022-07-23 12:25:01	OK: Interface GigabitEthernet0/0 (index 2) is up.
Port3 Bandwidth	Ok	46m 46s	1/5	2022-07-23 12:25:10	OK - Current BW in: 0Mbps Out: 0Mbps
Port3 Status	Ok	46m 33s	1/5	2022-07-23 12:25:21	OK: Interface GigabitEthernet0/1 (index 3) is up.
Port4 Bandwidth	Ok	46m 22s	1/5	2022-07-23 12:25:41	OK - Current BW in: 0Mbps Out: 0Mbps
Port4 Status	Ok	46m 9s	1/5	2022-07-23 12:25:51	OK: Interface Backplane-GigabitEthernet0/3 (index 4) is up.
Port5 Bandwidth	Ok	46m 2s	1/5	2022-07-23 12:25:59	OK - Current BW in: 0Mbps Out: 0Mbps
Port5 Status	Critical	41m 57s	5/5	2022-07-23 12:25:07	CRITICAL: Interface Serial0/0/0 (index 5) is down.
Port6 Bandwidth	Ok	45m 35s	1/5	2022-07-23 12:26:25	OK - Current BW in: 0Mbps Out: 0Mbps
Port6 Status	Critical	41m 38s	5/5	2022-07-23 12:25:19	CRITICAL: Interface Serial0/0/1 (index 6) is down.

Figure 27: supervision des services d'un routeur

On peut superviser l'état du routeur et les services comme le ping, le statut et la bande passante de chaque port.

IV.6.3. Supervision des services d'un switch



Switch1

Services

état du service pour cet hôte

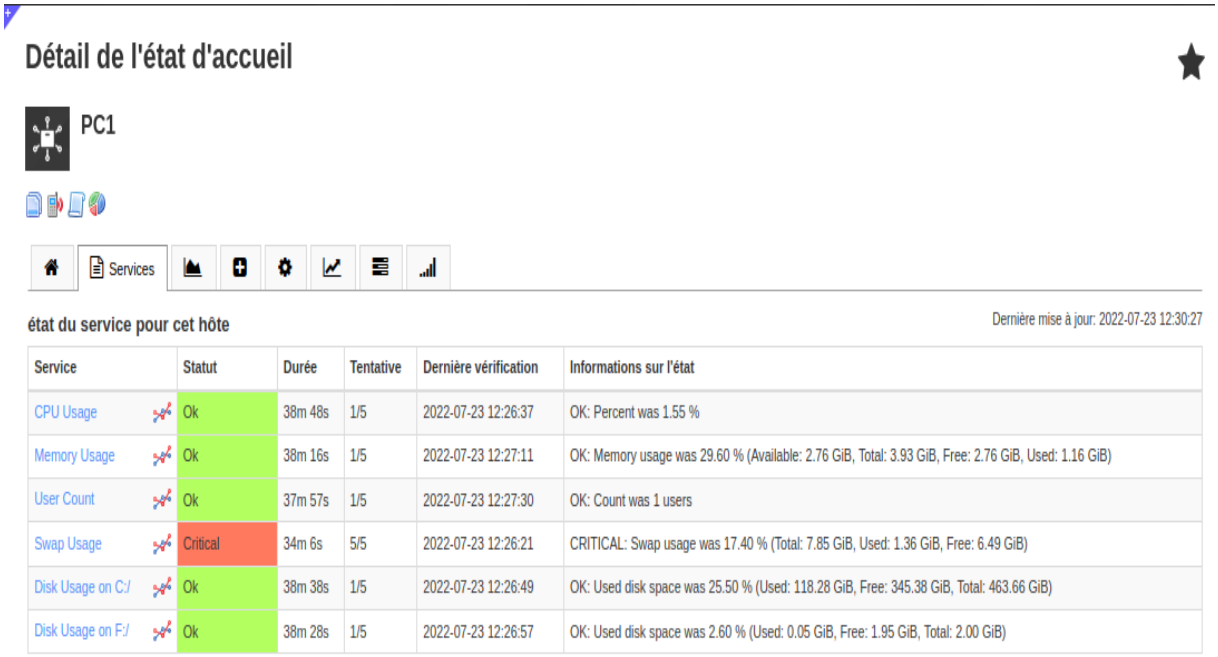
Dernière mise à jour: 2022-07-23 12:28:42

Service	Statut	Durée	Tentative	Dernière vérification	Informations sur l'état
Ping	Ok	56m 14s	1/5	2022-07-23 12:27:17	OK - 1.1.1.1 rta 0,906ms lost 0%
Port1 Bandwidth	Ok	56m 5s	1/5	2022-07-23 12:27:33	OK - Current BW in: 0Mbps Out: 0Mbps
Port1 Status	Ok	55m 56s	1/5	2022-07-23 12:27:41	OK: Interface Vlan1 (index 1) is up.
Port10001 Bandwidth	Ok	55m 48s	1/5	2022-07-23 12:27:45	OK - Current BW in: 0Mbps Out: 0Mbps
Port10001 Status	Ok	55m 38s	1/5	2022-07-23 12:27:58	OK: Interface FastEthernet0/1 (index 10001) is up.
Port10002 Bandwidth	Ok	55m 32s	1/5	2022-07-23 12:24:36	OK - Current BW in: 0Mbps Out: 0Mbps
Port10002 Status	Ok	55m 21s	1/5	2022-07-23 12:28:09	OK: Interface FastEthernet0/2 (index 10002) is up.
Port10003 Bandwidth	Ok	55m 11s	1/5	2022-07-23 12:28:28	OK - Current BW in: 0Mbps Out: 0Mbps
Port10003 Status	Critical	51m 8s	5/5	2022-07-23 12:27:27	CRITICAL: Interface FastEthernet0/3 (index 10003) is down.
Port10004 Bandwidth	Ok	54m 51s	1/5	2022-07-23 12:23:51	OK - Current BW in: 0Mbps Out: 0Mbps
Port10004 Status	Critical	50m 48s	5/5	2022-07-23 12:27:46	CRITICAL: Interface FastEthernet0/4 (index 10004) is down.
Port10005 Bandwidth	Ok	54m 37s	1/5	2022-07-23 12:23:56	OK - Current BW in: 0Mbps Out: 0Mbps
Port10005 Status	Critical	50m 29s	5/5	2022-07-23 12:27:56	CRITICAL: Interface FastEthernet0/5 (index 10005) is down.

Figure 28: supervision des services d'un switch

On peut aussi voir l'état du switch et les services comme le ping, le statut et la bande passante de chaque port.

IV.6.4. Supervision des services d'une machine



Détail de l'état d'accueil

PC1

Services

état du service pour cet hôte

Dernière mise à jour: 2022-07-23 12:30:27

Service	Statut	Durée	Tentative	Dernière vérification	Informations sur l'état
CPU Usage	Ok	38m 48s	1/5	2022-07-23 12:26:37	OK: Percent was 1.55 %
Memory Usage	Ok	38m 16s	1/5	2022-07-23 12:27:11	OK: Memory usage was 29.60 % (Available: 2.76 GiB, Total: 3.93 GiB, Free: 2.76 GiB, Used: 1.16 GiB)
User Count	Ok	37m 57s	1/5	2022-07-23 12:27:30	OK: Count was 1 users
Swap Usage	Critical	34m 6s	5/5	2022-07-23 12:26:21	CRITICAL: Swap usage was 17.40 % (Total: 7.85 GiB, Used: 1.36 GiB, Free: 6.49 GiB)
Disk Usage on C:/	Ok	38m 38s	1/5	2022-07-23 12:26:49	OK: Used disk space was 25.50 % (Used: 118.28 GiB, Free: 345.38 GiB, Total: 463.66 GiB)
Disk Usage on F:/	Ok	38m 28s	1/5	2022-07-23 12:26:57	OK: Used disk space was 2.60 % (Used: 0.05 GiB, Free: 1.95 GiB, Total: 2.00 GiB)

Figure 29: supervision des services d'une machine

On peut savoir l'état du PC, ainsi que le fonctionnement des services comme l'utilisation de la CPU, l'utilisation de la mémoire RAM, le nombre d'utilisateurs connectés, l'utilisation des disques, etc.

IV.7. Supervision de services supplémentaires

IV.7.1. Ajouter un nouveau service

Il est possible d'ajouter des services dont les plugins ne sont préinstallés sur Nagios mais disponible sur le site officiel des plugins de Nagios https://exchange.nagios.org/. L'ajout peut se faire directement sur l'interface web ou par commande sur le *terminal*.

Cela se passe ainsi par commande sur le terminal :

- On télécharge le plugin du service qu'on veut superviser sur https://exchange.nagios.org/ et extraire le fichier s'il est zippé.
  On va prendre comme exemple le plugin *countdown_to_date* qui permet de compter le nombre de jours à partir d'une date et d'avertir. Il peut être téléchargé en utilisant le lien suivant :
  https://exchange.nagios.org/directory/Plugins/Others/countdown_to_date/details.
  Extraire le fichier countdown_to_date.php.
- Ensuite il faut copier ou déplacer le fichier sur le répertoire */usr/local/nagios/libexec*, l'ensemble des plugins utilisables y sont.
- Exécuter le fichier sur le répertoire : on peut utiliser la commande *chmod +x :*
  Exemple:
  Chmod +x /usr/local/nagios/libexec/countdown_to_date.php
- Maintenant on va définir une nouvelle commande au niveau du fichier *commands.cfg* dans le répertoire */usr/local/nagios/etc* avec la commande : *nano /usr/local/nagios/etc/commands.cfg*.
  Exemple:
  On fait *nano/usr/local/nagios/etc/commands.cfg* et on y ajoute :

```
define command {
    command_name    countdown_to_date
    command_line    countdown_to_date.php --date $ARG1$ --warning $ARG2$ --
critical $ARG3$
}
```

- Pour terminer, on définit le nouveau service au niveau du fichier de configuration des services de l'hôte à superviser :

  Exemple : le nouveau service est configuré sur l'hôte localhost.

  On accède au fichier par : *nano /usr/local/nagios/etc/services/localhost.cfg*

  Puis on ajoute :

  define service {

  host_name localhost

  service_description Date Check

  use local-service

  check_command countdown_to_date!2017-01-19!60!30!

  register 1

  }
- Redémarrer Nagios par *systemctl restart Nagios* et le nouveau service est ajouté.

L'ajout d'un nouveau service par mode graphique c'est-à-dire sur l'interface web de Nagios sera donné en annexe.

IV.7.2. Ajouter un service dont le plugin n'existe pas

Il est possible aussi de vouloir ajouter un service dont le plugin n'existe pas encore. Dans ce cas, on peut créer notre propre plugin pour ce service.

- Des guides pour développer un nouveau plugin son disponible sur https://nagios-plugins.org/doc/guidelines.html ou Plugin Nagios en Perl (developpez.com).
- Une fois de plugin est développé, le fichier est ensuite copié sur le répertoire */usr/local/nagios/libexec* et puis l'exécuté.
- On définit la nouvelle commande dans : */usr/local/nagios/etc/commands.cfg*.
- On définit le nouveau service dans : */usr/local/nagios/etc/services/nom_de_lhote.cfg*
- Et on redémarre Nagios pour terminer.

Il est possible aussi d'utilisé le mode graphique pour intégrer de nouveaux plugins et services sur Nagios XI.

Conclusion

Nagios fait partie des logiciels de supervision réseau les plus performants et les plus utilisés sur le marché de l'entreprise. Elle permet entre autres d'avoir une vue globale du fonctionnement et des problèmes pouvant survenir sur un réseau mais aussi d'avoir des

indicateurs sur la performance de son architecture, en temps réel. Sa configuration est plus ou moins complexe en fonction du type de configuration (par modification manuelle des fichiers de configuration sur un terminal ou par l'assistance graphique sur l'interface web) utilisé. Nous avons voulu développer notre propre plugin mais par contrainte de temps, nous nous proposons de le faire à l'avenir.

Conclusion générale

L'objectif de notre projet était de superviser les équipements et les services de notre réseau. En effet une solution de supervision permet de diminuer le taux de diagnostic des pannes et de faciliter les tâches de maintenance tout en assurant la sécurité des équipements. Plus le nombre des équipements et des services informatiques augmentent plus les tâches de l'administrateur deviennent trop compliquées, surtout si les configurations sont faites par commandes, mais peuvent être plus facile en utilisant l'assistance de configuration que nous offre Nagios XI.

Notre travail consistait à mettre en place un outil de supervision de système et de réseau. Dans un premier lieu, nous avons pu étudier l'existant et dégager ses limites afin de fixer la solution retenue après avoir réalisé une étude comparative entre les différentes solutions open source existantes sur le marché. Dans la partie réalisation, nous avons mis en place l'outil Nagios XI, installer sur Ubuntu et nous avons configurer des machines, des routeurs et switchs. Ensuite nous avons pu ajouter des services supplémentaires.

- Les services supervisés :
  - Ping,
  - HTTP,
  - SSH,
  - L'utilisation de la CPU,
  - L'utilisation de la mémoire RAM,
  - L'utilisation du Swap,
  - Le nombre d'utilisateurs connectés pour chaque machine,
  - L'utilisation des disques,
  - Le statut des ports des switchs et routeurs,
  - La bande passante de chaque port des ports des switchs et routeurs.
  - Etc.
- Services supplémentaires ajoutés :
  - Countdown_to_date,
  - SSL_expiration (qui vérifie d'expiration du certificat ssl).

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

- La supervision des services de bases de données ;
- La supervision d'imprimante ;

- Le développement d’un plugin pour un nouveau service ou protocole ;
- La supervision distribuée ou passive derrière un Firewall ;
- Et autres suggestions.

Bibliographie et Webographie

[1] « Cybersecurity, Cisco Networking Academy », https://www.netacad.com/ (consulté entre Septembre 2020 et Avril 2021).

[2] « La sécurité informatique dans la petite entreprise : état de l'art et bonnes pratiques », édition 2009.

[3] « Cryptographie et Sécurité informatique », de Renaud Dumont édition 2009 – 2010.

[4] F. Cikala, R. Lataix, S. Marmeche, « Les IDS/IPS. Intrusion Detection/Prevention Systems », Présentation, 2005.

[5] Youssouf N'TCHIRIFOU, « Monitoring d'une infrastructure informatique sur base d'outils libres », 2010.

[6] Guillaume LEROY, « Gestion du déploiement d'une solution de supervision réseau multi-sites », 2017.

[7] « Protocole SNMP », Protocole SNMP - FRAMEIP.COM (consulté en Mai 2021).

[8] « Windows managements instrumentation », http://igm.univ-mlv.fr/~dr/XPOSE2006/duarte/architecture.html#fonctionnement (consulté en Mai 2021).

[9] « Windows managements instrumentation (WMI) », https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmi-architecture (consulté en Mai 2021).

[10] « Requête WMI », https://docs.microsoft.com/fr-fr/system-center/orchestrator/standard-activities/query-wmi?view=sc-orch-2019 (consulté en Mai 2021).

[11] « Multi Router Traffic Grapher », https://wikipfr.icu/wiki/Multi_Router_Traffic_Grapher (consulté en Juin 2021).

[12] « Monitoring d'une infrastructure informatique sur la base d'outils libres », https://www.memoireonline.com/04/12/5604/m_Monitoring-dune-infrastructure-informatique-sur-base-doutils-libres.html (consulté en Juin 2021).

[13] « Principe de base de la supervision », http://igm.univ-mlv.fr/~dr/XPOSE2010/supervision/index.html (consulté en Aout 2021).

[14] « Cacti », https://www.cacti.net/ (consulté en Mai 2021).

[15] « Supervision avec Cacti », https://open-source-guide.com/Solutions/Infrastructure/Supervision-et-la-metrologie/Cacti (consulté en Mai 2021).

[16] http://ganglia.sourceforge.net/(consulté en Juin 2021).

[17] « Supervision avec Ganglia » https://www.oreilly.com/library/view/monitoring-with-ganglia/9781449330637/ch01.html (consulté en Juin 2021).

[18] « Ganglia », https://www.logiciels.pro/logiciel-saas/ganglia/ (consulté en Juin 2021).

[19] « Zabbix », http://www.zabbix.com/(consulté en Juin 2021).

[20] « Zabbix documentation », http://www.zabbix.com/documentation/ (consulté en Juin 2021).

[21] « Monit », http://mmonit.com/monit/(consulté en Juin 2021).

[22] « Supervision avec Monit », https://connect.ed-diamond.com/GNU-Linux-Magazine/glmf-180/supervision-distribuee-avec-monit-et-puppet(consulté en Juin 2021).

[23] « Supervision avec Nagios », www.nagios.com (consulté entre Juin 2021 et Avril 2022).

[24] « Agent NSClient », Welcome to NSClient++ - NSClient++ (consulté en Avril 2022).

[25] « Agent NCPA », Getting Started · NCPA (nagios.org) (consulté en Avril 2022).

[26] « Nagios plugins », https://nagios-plugins.org/doc/guidelines.html (consulté en Mai 2022).

[27] « Nagios plugins », Plugin Nagios en Perl (developpez.com) (consulté en Mai 2022).

Annexes

Annexe A : installation du serveur Nagios

Dans notre cas nous avons installé Nagios XI sur un système Linux (Ubuntu) de 64 bits (disponible seulement en 64 bits). Il faudra au préalable Ubuntu 16, 18 ou 20. La procédure installation se fait en deux étapes.

Première partie :

- On commence par ouvrir le *terminal* et se mettre en mode *root*.
- Puis se mettre le répertoire tmp : *cd /tmp*
- Ensuite, on télécharge Nagios XI avec la commande : *wget https://assets.nagios.com/downloads/nagiosxi/xi-latest.tar.gz*
- Après on désippre le paquet téléchargé : *tar xzf xi-latest.tar.gz*
- On accède au répertoire nagiosxi : *cd nagiosxi*
- Maintenant le va faire son installation avec : *./fullinstall*

La première partie se termine lorsque le message « Installatin complete ! » s'afiche et que l'adresse d'accès à l'interface web de Nagios est donnée *http://<adresse_du_serveur/nagiosxi*.

```
Nagios XI Installation Complete!
---------------------------------

You can access the Nagios XI web interface by visiting:
    http://<server_address>/nagiosxi
```

Figure 30: Fin de l'installation du serveur Nagios

Deuxième partie :

On accède à la configuration d'accès à l'interface web via le lien : *http://<adresse_du_serveur/nagiosxi*.

- Etape 1 : première interface de Nagios XI permettant de commencer la configuration de l'interface web.

Figure 31: Interface de bienvenue de Nagios XI

- Etape 2 : définir les paramètres généraux et la licence.

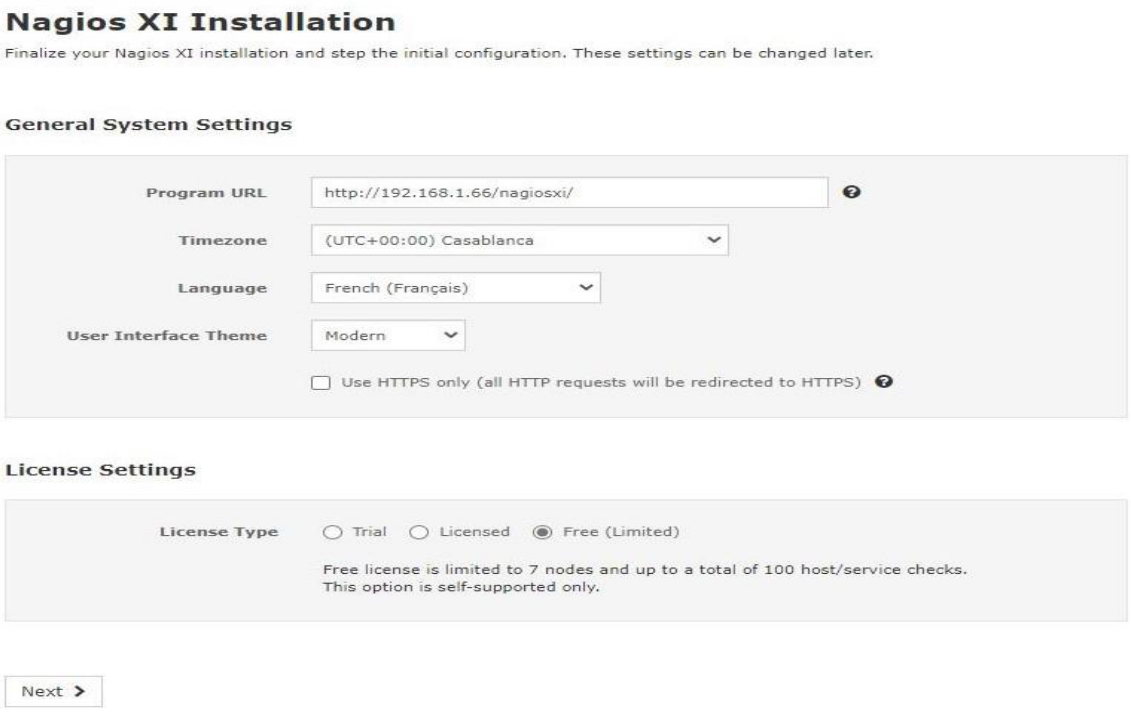


Figure 32: Configurations paramètres et licence

- Etape 3 : définir le nom d'utilisateur, le mot de passe, le nom d'administrateur et l'adresse mail.

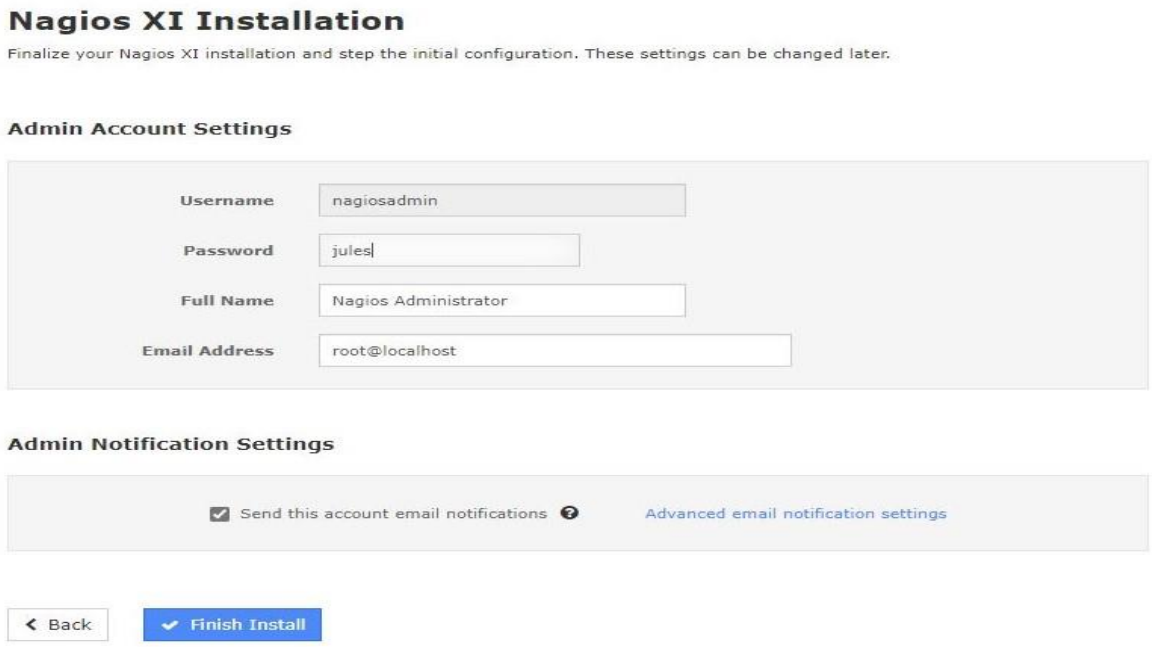


Figure 33: Configurations nom d'utilisateur, mot de passe et email

- Etape 4 : nom d'utilisateur et mot de passe pour accéder à l'interface web de Nagios.

Figure 34: Fin de la configuration de l'interface web

- Etape 5 : authentification (entrer le nom d'utilisateur et le mot de passe).

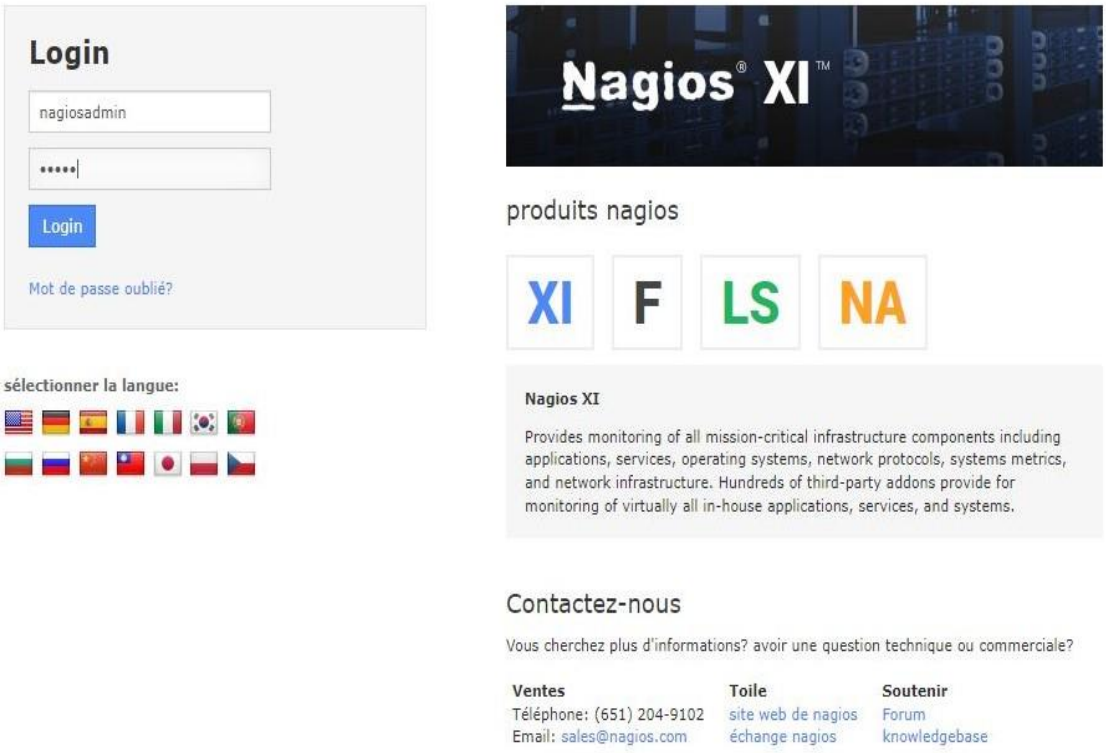


Figure 35: Interface d'authentification Nagios XI

- Etape 6 : lire et accepter les conditions de licence de Nagios.

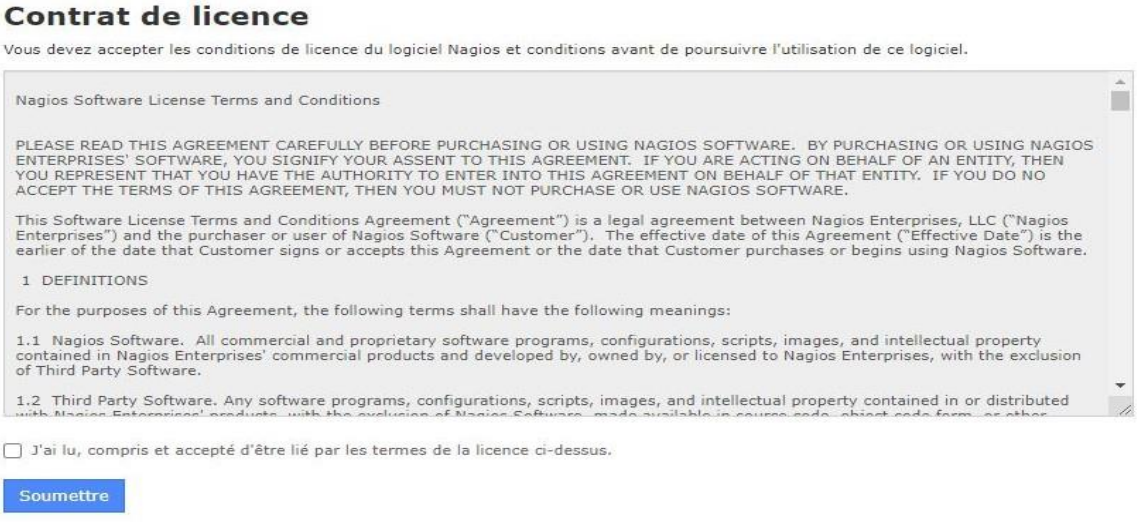


Figure 36: Contrat de licence

- Etape 7 : page d'accueil de Nagios XI.

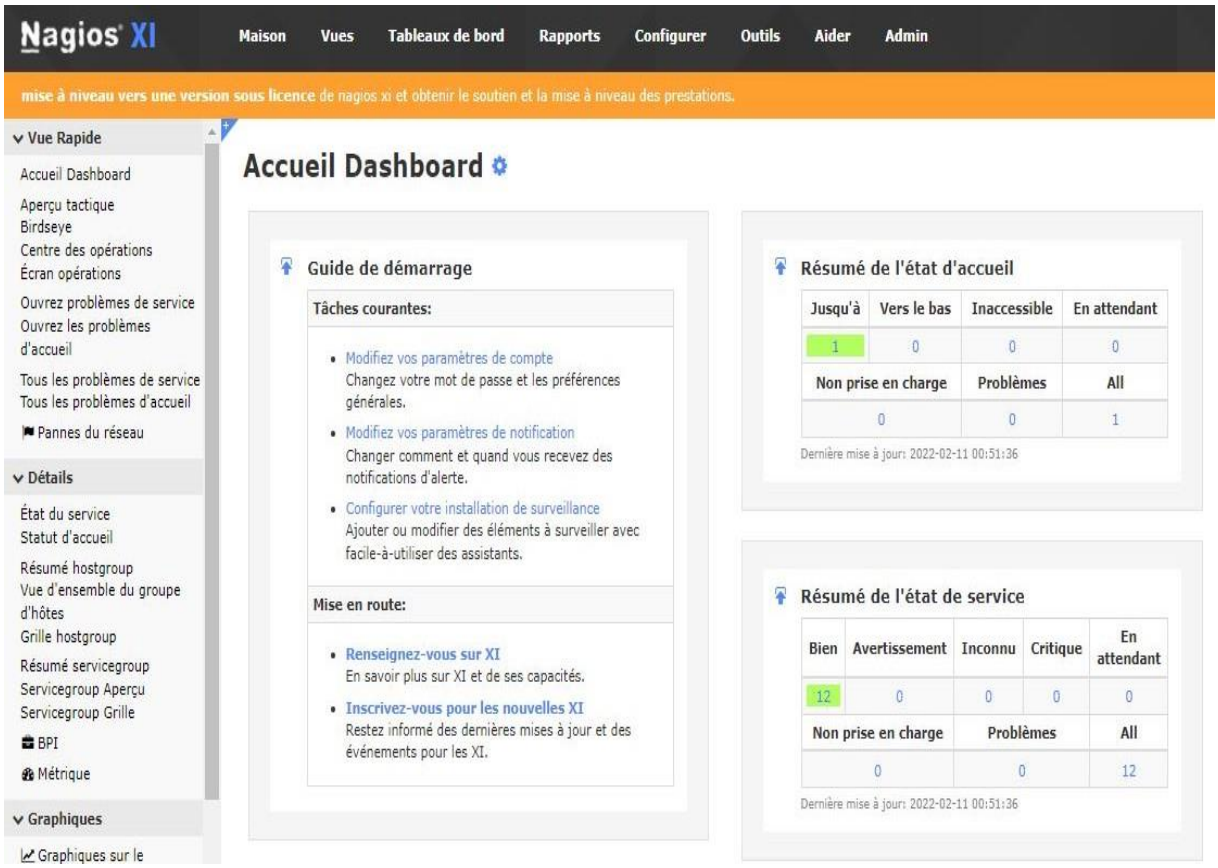


Figure 37: Interface d'accueil de Nagios XI

Annexe B : installation des clients sur les systèmes

Pour pouvoir surveiller les machines, nous installons d'abord un agent sur chaque machine que nous voulons surveiller, puis configurons Nagios. Ces agents ou clients utilisent les deux types de supervision possible à savoir la supervision active et la supervision passive.

- **NSClient + + pour une machine Windows** :

Avant de pouvoir surveiller les services privés sur les machines Windows, nous devons installer un agent sur ces machines. Nous avons choisi NSClient++ pour cela.

Pour installer NSClient++ sur, on télécharge la dernière version de NSClient++ selon le type de système d'exploitation depuis https://nsclient.org/download/. Une fois le téléchargement terminé, on passe à l'installation du logiciel :

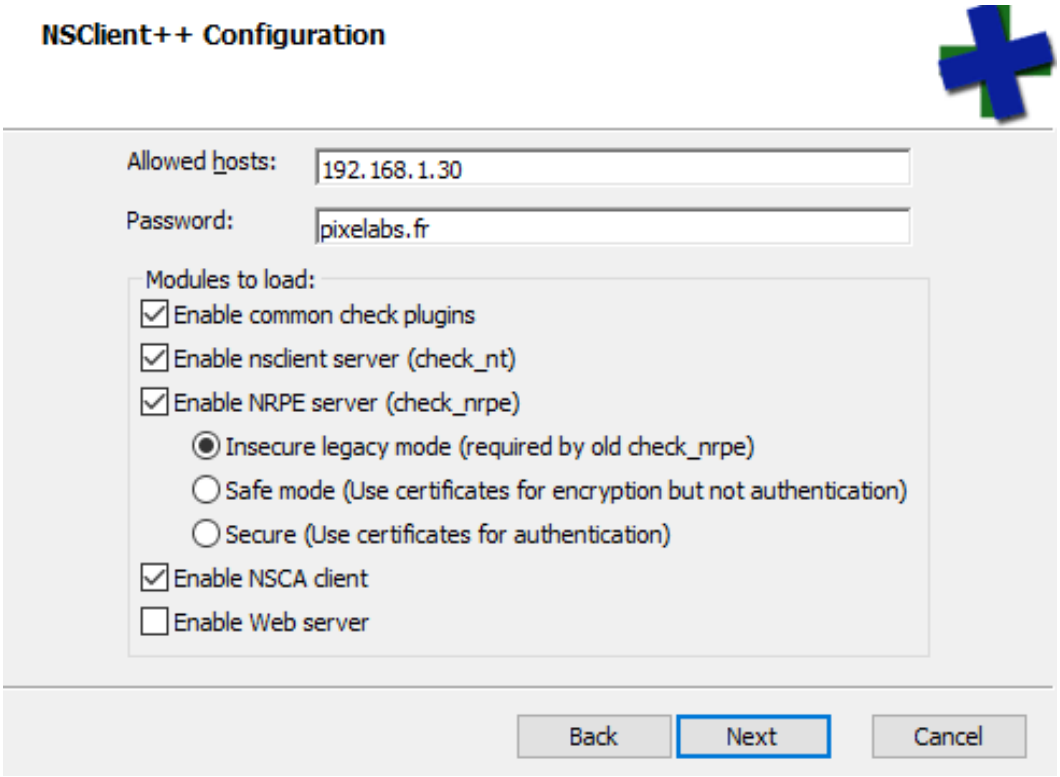


Figure 38: Fenêtre de configuration NSClient++

Important : on donne l'adresse IP de la machine ou est installé le serveur de Nagios et noter aussi que le mot de passe n'est pas obligatoire.

- **NRPE pour une machine Linux** :

NRPE (Nagios Remote Plugin Executor) est un agent de surveillance qui permet de récupérer des informations à distance lors de la surveillance de serveurs Linux/Unix.

L'installation se passera comme suit sur un *terminal* Ubuntu :

- D'abord mettre à jour les applications : *sudo apt update.*
- Télécharger et installer l'agent avec : *sudo apt install nagios-nrpe-server nagios-plugins.*
- On termine la configuration par donner l'adresse du serveur Nagios avec la commande : *sudo nano /etc/nagios/nrpe.cfg* (exemple : allowed_hosts=127.0.0.1, *192.168.1.100 avec 192.168.1.100 l'adresse du serveur Nagios*).

- **NCPA pour Windows, Linux, Mac OS et autres** :

NCPA (Nagios Cross Platform Agent) est un agent multiplateforme Nagios qui peut être installé sous Windows, Linux et Mac OS X. Le NCPA a pour but de simplifier et d'universaliser la supervision par agent à travers différents systèmes d'exploitation.

- Installation sous Windows :

Tout d'abord, il faut télécharger le programme d'installation de Windows sur Monitoring Agent · NCPA (nagios.org). Puis on va passer à l'installation du logiciel :

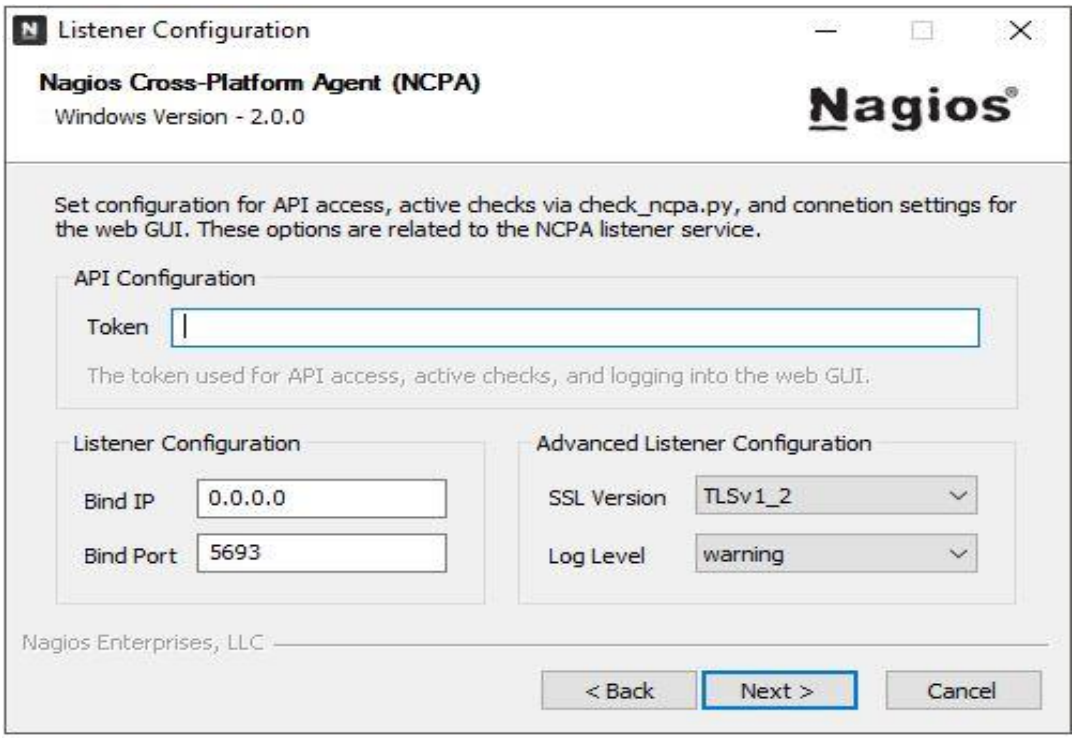


Figure 39: Fenêtre d'installation NCPA

Entrez le Token qui est comme un mot de passe et sera demander dans la configuration sur Nagios, laisser les autres paramètres par défaut. Puis poursuivre l'installation jusqu'à voir « **Finish** » pour terminer l'installation de l'agent NCPA.

- Installation Linux (Ubuntu) :

Pour Ubuntu, il faut exécuter la commande ci-après pour faire l'installation complète de NCPA : *dpkg -i /tmp/ncpa-<version and arch>.deb*.

- Installation Mac OS :

L'installation sur Mac nécessite des droits d'administrateur (root) et doit être exécutée à l'aide de la ligne de commande suivante : *sudo zsh /Volumes/NCPA-<version>/install.sh*.

Annexe C : activation de SNMP sur les équipements (routeur et switch)

L'activation de SNMP permettra à Nagios serveur de communiquer avec les équipements et de pouvoir récupéré les informations sur ceux. L'activation se fait de la manière suivante :

- On se connecte au *terminal* de l'équipement (switch ou routeur) par Telnet, SSH ou simplement via le câble console ;
- **Se mettre en mode privilégié** : *enable* ;
- Se mettre en mode configuration : *configure terminal ;*
- Activer la communauté public en lecture seule (RO: Read Only) : *snmp-server community public RO* ;
- Activer la communauté privé en lecture seule (RW: Read Write) : *snmp-server community private RW* ;
- Quitter le mode configuration : *exit* ;
- Enregistrer les nouvelles configurations : *write memory* ;

On termine par vérifier que les nouvelles configurations sont enregistrées : *show running-config*.

Annexe D : Comment configurer les équipements par interface et par commande

L'ajout des équipements sur Nagios XI peut se faire de deux manières :

- **Sur l'interface web de Nagios XI**
  - Ajout d'un PC :

Il faudra au préalable installer sur le PC un agent (exemple : NCPA) puis accéder à l'interface web de Nagios XI par http://adresse_du_serveur/nagiosxi et entrer son login et son mot de passe. Ensuite on accède à *configurer -> assistants de configuration*, et on recherche *NCPA* puis voici la suite :

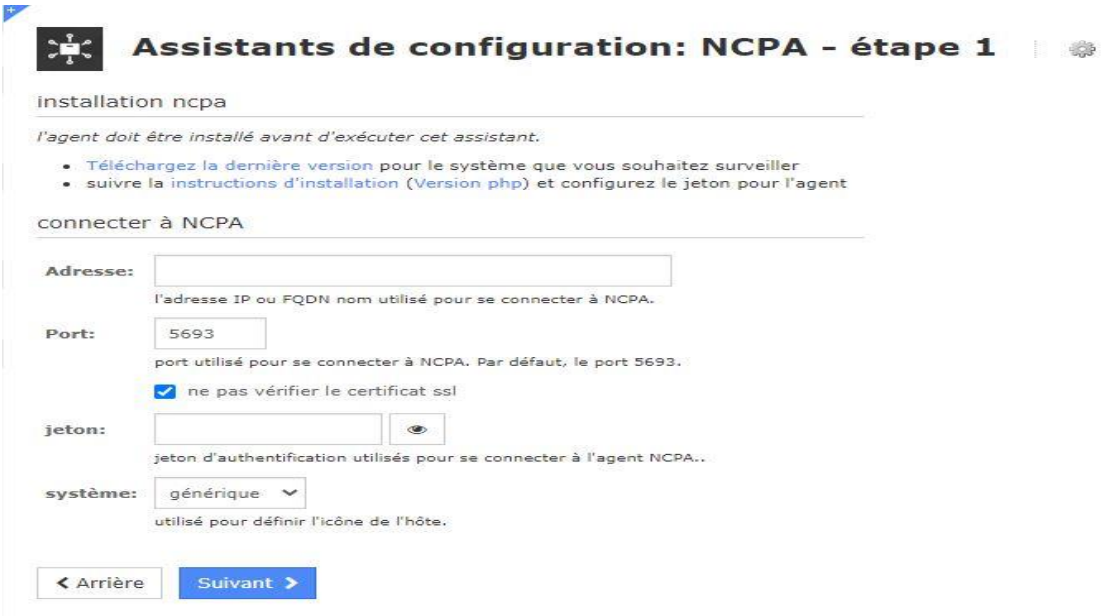


Figure 40: Configuration de l'ajout d'un PC avec l'assistance NCPA

Entrer *l'adresse IP* du PC et le *jeton* donné lors de l'installation de NCPA sur le PC, passer sur suivant pour voir les services à superviser, choisir ceux que nous voulons superviser puis faire suivant et terminer, ce qui termine la configuration du PC.

- Ajout d'un Routeur ou Switch

Si c'est un routeur ou un switch, il faut d'abord activer SNMP sur l'équipement. Ensuite accéder à l'interface de Nagios XI, passer à *configurer* puis *assistants de configuration*, rechercher *routeur* ou *switch* et passer à la configuration :

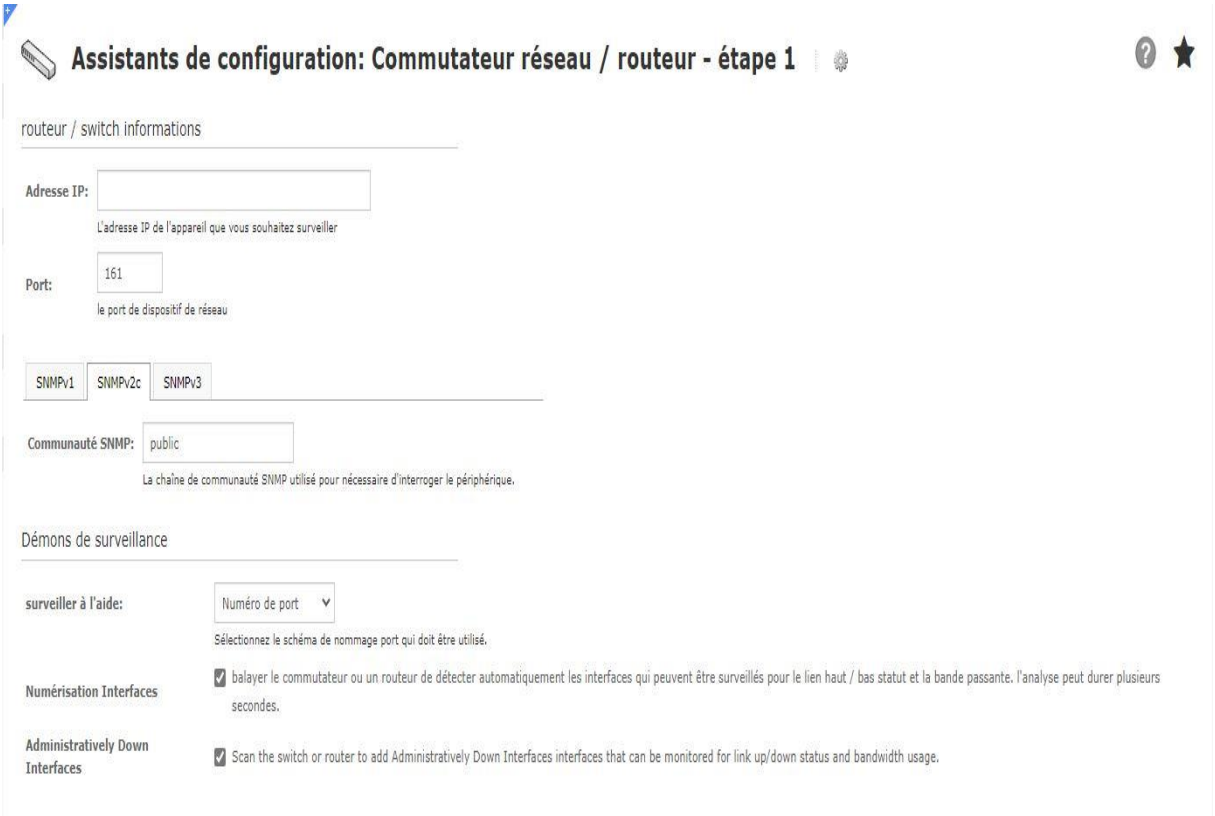


Figure 41: Configuration d'un switch ou routeur avec l'assistance SNMP

On entre *l'adresse IP* de l'équipement réseau et on passe à suivant. Ensuite on sélectionne les services à superviser sur chaque port, cliquer sur *suivant* puis *terminer* pour finir la configuration.

➢ **Par commande sur le terminal**

- Ajout d'un PC :

Toujours il faut installer un agent (exemple : NCPA) sur le PC puis ouvrir le *terminal*.

Définir un nouvel hôte pour PC en créant un nouveau fichier de configuration sur le répertoire /usr/local/nagios/etc/hosts/ : nano /usr/local/nagios/etc/hosts/PC1.cfg

define host {

host_name PC1

use xiwizard_ncpa_host

address 1.1.1.3

max_check_attempts 5

check_interval 5

check_period xi_timeperiod_24x7

contacts nagiosadmin

notification_interval 60

notification_period xi_timeperiod_24x7

_xiwizard ncpa

register 1

}

NB : On a utilisé le générique *xiwizard_ncpa_host* qui représente une manière simple de définir un hôte à partir hôte prédéfini par Nagios.

Définir les services pour cet hôte en créant aussi un nouveau fichier de configuration sur le répertoire /usr/local/nagios/etc/services/ : /usr//usr/local/nagios/etc/services/PC1.cfg

define service {

host_name PC1

service_description CPU Usage

use xiwizard_ncpa_service

check_command check_xi_ncpa!-t 'ab1' -P 5693 -M cpu/percent -w '$

max_check_attempts 5

```
    check_interval          5
    retry_interval          1
    check_period            xi_timeperiod_24x7
    notification_interval   60
    notification_period     xi_timeperiod_24x7
    contacts                nagiosadmin
    _xiwizard               ncpa
    register                1
}
define service {
    host_name               PC1
    service_description     Disk Usage on C:/
    use                     xiwizard_ncpa_service
    check_command           check_xi_ncpa!-t 'ab1' -P 5693  -M 'disk/logical/C$
    max_check_attempts      5
    check_interval          5
    retry_interval          1
    check_period            xi_timeperiod_24x7
    notification_interval   60
    notification_period     xi_timeperiod_24x7
    contacts                nagiosadmin
    _xiwizard               ncpa
    register                1
}
```

```
define service {
    host_name               PC1
    service_description     Disk Usage on F:/
    use                     xiwizard_ncpa_service
    check_command           check_xi_ncpa!-t 'ab1' -P 5693  -M 'disk/logical/F$
    max_check_attempts      5
    check_interval          5
    retry_interval          1
    check_period            xi_timeperiod_24x7
    notification_interval   60
    notification_period     xi_timeperiod_24x7
    contacts                nagiosadmin
    _xiwizard               ncpa
    register                1
}
define service {
    host_name               PC1
    service_description     Memory Usage
    use                     xiwizard_ncpa_service
    check_command           check_xi_ncpa!-t 'ab1' -P 5693 -M memory/virtual -$
    max_check_attempts      5
    check_interval          5
    retry_interval          1
    check_period            xi_timeperiod_24x7
```

notification_interval 60

notification_period xi_timeperiod_24x7

contacts nagiosadmin

_xiwizard ncpa

register 1

}

define service {

host_name PC1

service_description User Count

use xiwizard_ncpa_service

check_command check_xi_ncpa!-t 'ab1' -P 5693 -M user/count -w '2$

max_check_attempts 5

check_interval 5

retry_interval 1

check_period xi_timeperiod_24x7

notification_interval 60

contacts nagiosadmin

_xiwizard ncpa

register 1

}

NB : On a utilisé le générique *xiwizard_ncpa_service* qui représente une manière simple de définir des services à partir d'un service prédéfini par Nagios.

- Ajout d'un Routeur ou Switch

Installer SNMP sur l'équipement ensuite accéder au *terminal* dans la machine où est installé Nagios.

Définir un nouvel hôte pour le routeur ou switch en créant un nouveau fichier de configuration toujours sur le répertoire /usr/local/nagios/etc/hosts/ : nano /usr/local/nagios/etc/hosts/Routeur.cfg

```
define host {
   host_name            Routeur
   use                  xiwizard_switch_host
   address              1.1.1.4
   max_check_attempts   5
   check_interval       5
   check_period         xi_timeperiod_24x7
   contacts             nagiosadmin
   notification_interval  60
   notification_period    xi_timeperiod_24x7
   _xiwizard            switch
   register             1
}
```

NB : On a utilisé le générique *xiwizard_switch_host* qui représente une manière simple de définir un hôte de type routeur ou switch à partir hôte prédéfini par Nagios.

Définir les services de l'équipement sur le répertoire /usr/ : nano /usr/local/nagios/etc/services/Routeur.cfg

```
define service {
   host_name            Routeur
   service_description  Ping
   use                  xiwizard_switch_ping_service
   max_check_attempts   5
   check_interval       5
```

```
    retry_interval          1
    check_period            xi_timeperiod_24x7
    notification_interval   60
    notification_period     xi_timeperiod_24x7
    contacts                nagiosadmin
    _xiwizard               switch
    register                1
}
define service {
    host_name               Routeur
    service_description     Port1 Bandwidth
    use                     xiwizard_switch_port_bandwidth_service
    check_command           check_xi_service_mrtgtraf!1.1.1.4_1.rrd!5.00,5.00!$
    max_check_attempts      5
    check_interval          5
    retry_interval          1
    check_period            xi_timeperiod_24x7
    notification_interval   60
    notification_period     xi_timeperiod_24x7
    contacts                nagiosadmin
    _xiwizard               switch
    register                1
}
define service {
```

```
    host_name               Routeur
    service_description     Port1 Status
    use                     xiwizard_switch_port_status_service
    check_command           check_xi_service_ifoperstatus!public!1!-v 2 -p 161
    max_check_attempts      5
    check_interval          5
    retry_interval          1
    check_period            xi_timeperiod_24x7
    notification_interval   60
    notification_period     xi_timeperiod_24x7
    contacts                nagiosadmin
    _xiwizard               switch
    _xiwizard               switch
    register                1
}
define service {
    host_name               Routeur
    service_description     Port2 Bandwidth
    use                     xiwizard_switch_port_bandwidth_service
    check_command           check_xi_service_mrtgtraf!1.1.1.4_2.rrd!50.00,50.0$
    max_check_attempts      5
    check_interval          5
    retry_interval          1
    check_period            xi_timeperiod_24x7
```

```
    notification_interval    60
    notification_period      xi_timeperiod_24x7
    contacts                 nagiosadmin
    _xiwizard                switch
    register                 1
}
define service {
    host_name                Routeur
    service_description      Port2 Status
    use                      xiwizard_switch_port_status_service
    check_command            check_xi_service_ifoperstatus!public!2!-v 2 -p 161
    max_check_attempts       5
    check_interval           5
    retry_interval           1
    check_period             xi_timeperiod_24x7
    notification_interval    60
    notification_period      xi_timeperiod_24x7
    contacts                 nagiosadmin
    _xiwizard                switch
    register                 1
}
```

NB : On a utilisé les génériques *xiwizard_switch_ping_service* pour le service ping, *xiwizard_switch_port_bandwidth_service* pour connaitre la bande passante des ports supervisés et *xiwizard_switch_port_status_service* pour le statut des ports supervisés.

Annexe E : Comment ajouter un nouveau service via interface web de Nagios XI

Il est plus facile d'ajouter un nouveau service sur un hôte en utilisant l'interface web de Nagios XI. Via son interface web on peut aussi trouver et installer de nouveaux plugins, définir les commandes et les utiliser dans nos services.

D'abord, on localise et télécharge notre plugin sur https://exchange.nagios.org/.

On va reprendre l'exemple précédant avec le plugin countdown_to_date, il peut être téléchargé sur https://exchange.nagios.org/directory/Plugins/Others/countdown_to_date/details et extraire le fichier principale countdown_to_date.php.

Maintenant on va installer le nouveau plugin dans Nagios XI :

- Aller dans *Admin* > *Manage plugins* puis importer le fichier en utilisant *Browser* puis cliquer sur *Upload Plugin* pour intégrer le nouveau plugin :

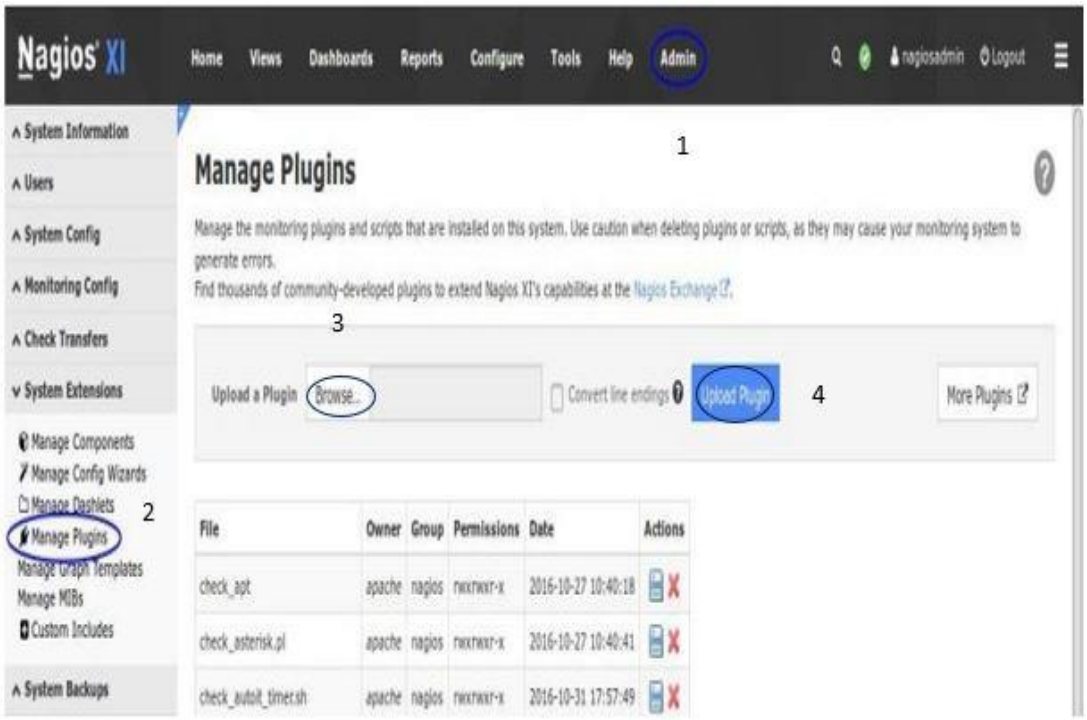


Figure 42: Intégration d'un nouveau plugin

Exemple : countdown_to_date.php.

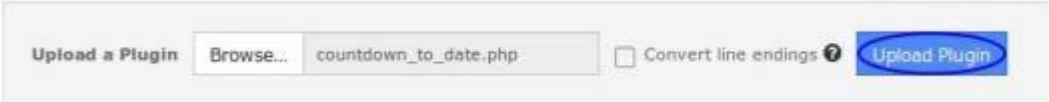


Figure 43: Exemple d'intégration plugin avec countdown_to_date.php

Une fois le plugin téléchargé, on aura un message similaire au suivant :

Figure 44: Message de succès de l'intégration du plugin

L'ensemble des plugins sont sur le répertoire */usr/local/nagios/libexec*, accessible qu'en tant qu'utilisateur *root*.

- La prochaine étape est de définir une nouvelle commande :

Dans l'interface web de Nagios XI, on va dans *Configure* > *Core Config Manager* > *Commands*.

Figure 45: Définir une nouvelle commande pour un nouveau plugin

- Et voici comment on définit la commande :

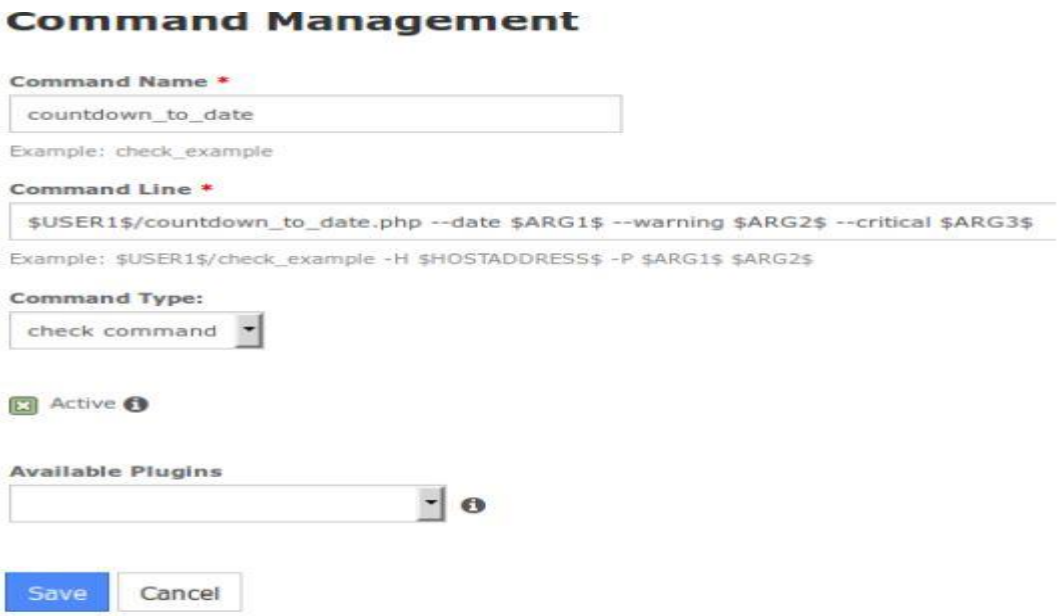


Figure 46: Configuration de la nouvelle commande

Après avoir cliqué sur **'*Save*'**, cliquer encore sur **'*Apply Configuration*'** pour valider les changements dans Nagios XI. Ainsi la nouvelle commande est définie.

- Maintenant on ajoute un nouveau service :

  On reste dans **'*Core Config Manager*'**, puis on va sur ***Monitoring*** **>** ***Services*** et on recherche l'hôte où le service sera ajouté (exemple : *localhost*). Il est plus facile de copier un service et de le modifier ensuite.

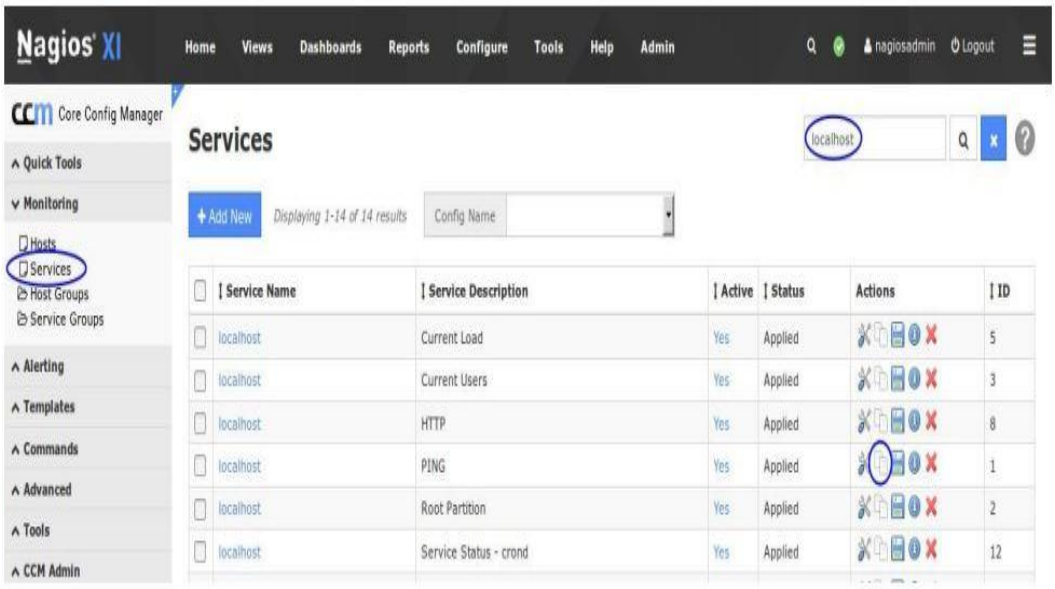


Figure 47: Ajout d'un nouveau service

On définit le nouveau service :

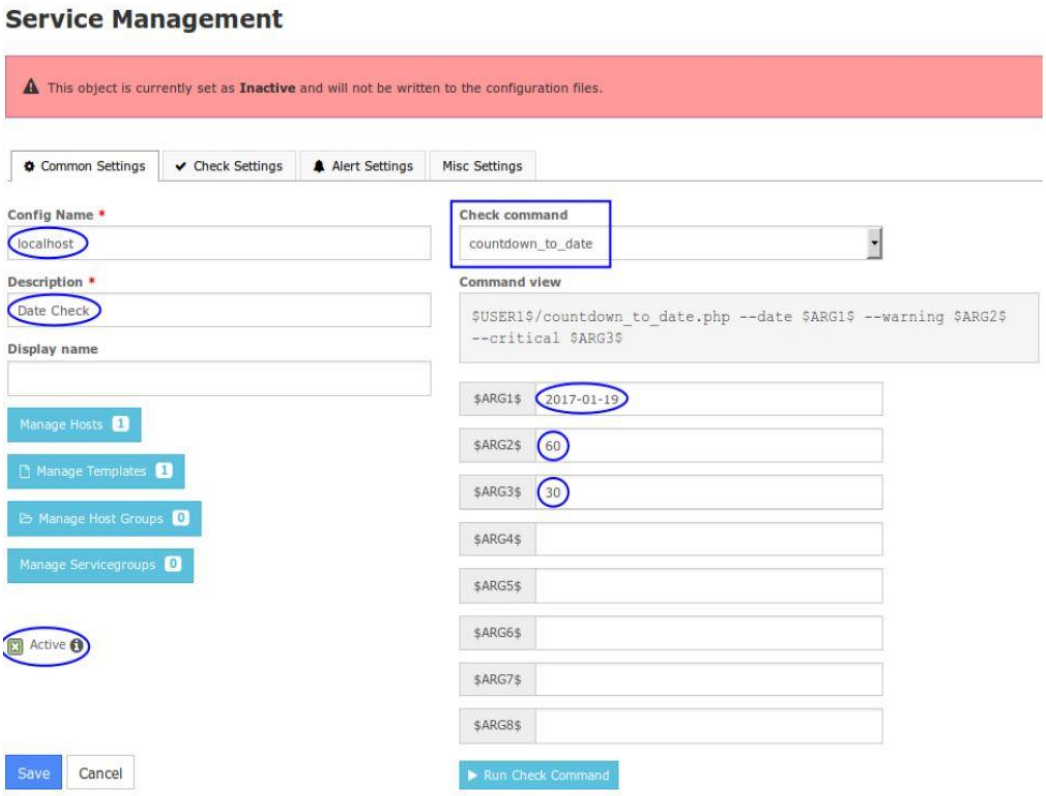


Figure 48: Configuration du nouveau service

Cliquer sur **'*Save*'** puis sur **'*Apply Configuration*'**.

- La dernière étape est de vérifier que le service est bien ajouté et qu'il fonctionne :

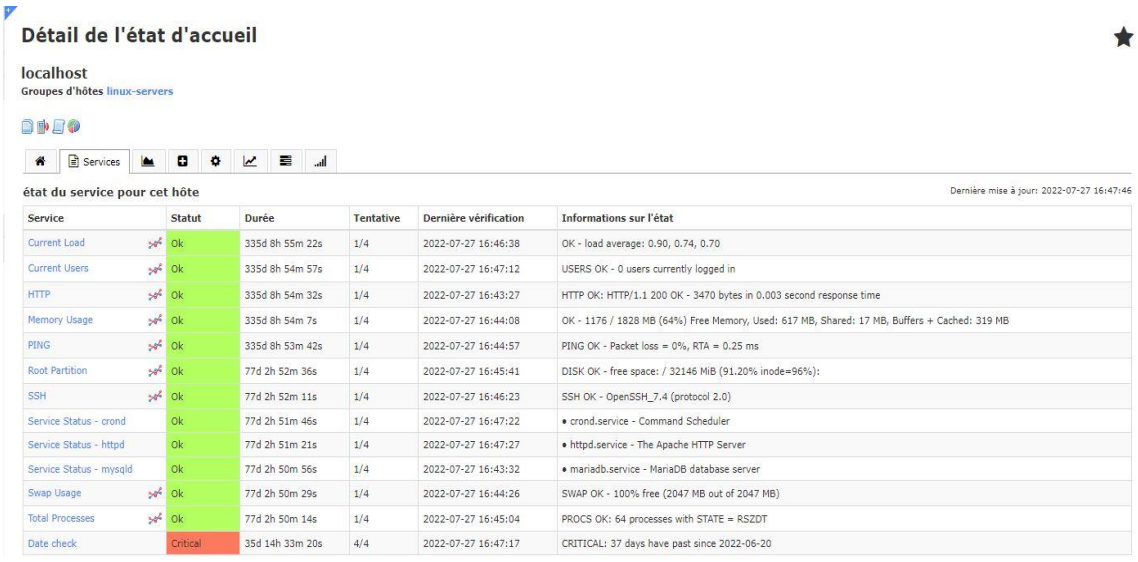


Figure 49: Vérification de l'ajout du nouveau service

Le service '*Date check'* est bien ajouté et fonctionne correctement.