République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Benyoucef BENKHEDDA- Alger1

Faculté des Sciences

Département d'Informatique

Mémoire de Licence

En Informatique

Spécialité *: Ingénierie des Systèmes d'Information et du Logiciels*

Thème

Étude et mise en œuvre d'une solution centrale de supervision des plateformes Informatiques

---

Encadré par :

- Mr. IMERZOUKENE ZOUBIR

Réalisé par :

- Mr. BELKESSA Samy
- Mr. CHIKHI Mohamed Amine

2022/2023

Remerciements

Nous remercions Tout d'abord ALLAH de nous avoir donné la santé, la force et la détermination afin de pouvoir accomplir ce projet.

Nous exprimons notre extrême gratitude à notre encadrant « Mr. Imerzoukene Zoubir », de nous avoir accompagné, guidé et conseillé tout au long de ce projet.

Nous le remercions aussi pour sa patience, sa disponibilité et sa bienveillance durant notre travail.

Nos sincères remercîments également aux membres du jury qui ont eu l'amabilité d'examiner et d'évaluer notre travail, mais aussi de l'enrichir par leurs suggestions.

Ce projet est le fruit de trois années de travail et d'apprentissage durant lesquelles plusieurs professeurs nous ont enseignés, et nous tenons à tous les remercier pour leurs pédagogies, leurs soutiens et leurs encouragements durant nos études.

Et pour finir, nous remercions toutes les personnes qui ont contribués de prés ou de loin a l'élaboration de ce projet.

Dédicaces

Je dédie ce travail a tous ceux qui me sont chers

A ma Mère

« L'être le plus cher de ma vie, a qui deux lignes de texte ne suffiraient pas pour lui dire à quel point je l'aime. Merci pour tout Mama. »

A mon Père

« Pour son amour, ses sacrifices, sa patience, son dévouement et ses encouragements »

A Mon Frère

« Mon mentor, celui qui me protège, m'oriente et me guide dans ma vie. »

A ma Tante

« Ma deuxième Mère, pour son amour, ses enseignements et ses sacrifices. »

A mon binôme Mohamed

« Mon compagnon de route, merci pour ton soutien, ta patience, ta passion et tes idées brillantes, j'ai été honoré d'avoir pu partager cette expérience inoubliable avec toi. »

BELKESSA Samy.

Je dédie ce modeste travail a

A Mes chers Parents

« Qui ont toujours été à mes côtés pour m'encourager, me motiver et m'aider dans le besoin. Votre amour inconditionnel, votre soutien constant et vos sacrifices ont joué un rôle essentiel dans la personne que je suis devenu aujourd'hui. »

A mon frère et ma sœur

« Mes compagnons de route, vos encouragements et votre présence ont renforcé ma détermination.»

A ma merveilleuse amie

« Tu es ma source de soutien, de bonheur et de motivation. »

A mon binôme Samy

« Son soutien moral, sa collaboration et a patience ont été inestimables tout au long de ce projet. Cette expérience ne serait pas la même sans lui. »

« Et à toute personne m'ayant fait part de son savoir. »

CHIKHI Mohamed Amine.

Résumé

Le service de supervision des plateformes représente le garant pour les composants serveurs et baie de stockage au sein de la Direction de l'Ingénierie Technique et Production de La Banque d'Algérie.

Pour ce faire, il doit assurer la gestion des plateformes, de prendre en charge la maintenance préventive et curative et de fournir les services nécessaires au bon fonctionnement des applications.

Cette fonction de supervision est actuellement assurée de façon classique en se basant essentiellement sur les outils fournis par les constructeurs des équipements (Dell, HP, IBM, Cisco…) ainsi que l'exploitation des fichiers logs générés par les différentes solutions hébergées sur ces plateformes (OS, BD, Serveur Web, Messagerie, Services Applicatifs, …).

La multitude et la diversité des constructeurs et des éditeurs rendent cette façon de supervision compliquée et moins efficace.

Notre projet consiste à simplifier et améliorer les taches de supervision en réalisant une étude pour la mise en place d'une solution centrale de supervision. Cette dernière est construite autour du logiciel Nagios Core.

Notre solution vient donc s'inscrire dans le cadre de la supervision informatique.

Mots clés : supervision, réseau, Nagios Core, . . .

Abstract

The platform monitoring service represents the guarantor for server components and storage bays within the Technical Engineering and Production Directorate of the Bank of Algeria.

To do so, it must ensure platform management, take care of preventive and corrective maintenance, and provide the necessary services for the proper functioning of applications.

This monitoring function is currently carried out in a conventional manner, mainly based on tools provided by equipment manufacturers (Dell, HP, IBM, Cisco...) as well as the analysis of log files generated by various solutions hosted on these platforms (OS, DB, Web Server, Messaging, Application Services, etc.).

The multitude and diversity of manufacturers and publishers make this monitoring method complicated and less effective.

Our project aims to simplify and improve the monitoring tasks by conducting a study for the implementation of a central monitoring solution. This solution is built around Nagios Core

software.

Therefore, our solution falls within the scope of IT monitoring. Our solution fits within the framework of computer supervision.

Key words: monitoring, network, Nagios Core, . . .

الملخص

خدمة مراقبة المنصات تمثل ضامنًا لمكونات الخوادم ووحدات التخزين داخل إدارة الهندسة التقنية والإنتاج في بنك الجزائر.

للقيام بذلك، يجب عليها ضمان إدارة المنصات والاهتمام بالصيانة الوقائية والتصحيحية وتوفير الخدمات اللازمة لسليم تشغيل التطبيقات.

تتم تنفيذ هذه وظيفة المراقبة حاليًا بطريقة تقليدية، بناءً على الأدوات التي يوفرها مصنعو المعدات (Dell، HP، IBM، Cisco...) بالإضافة إلى تحليل سجلات الملفات التي تولدها الحلول المختلفة المستضافة على هذه المنصات (نظام التشغيل، قاعدة البيانات، خادم الويب، البريد الإلكتروني، الخدمات التطبيقية، إلخ).

تجعل تعدد وتنوع الشركات المصنعة والناشرين هذه الطريقة المعقدة وأقل فعالية.

يهدف مشروعنا إلى تبسيط وتحسين مهام المراقبة من خلال إجراء دراسة لتنفيذ حل مراقبة مركزي. يتم بناء هذا الحل حول برنامج Nagios Core.

بالتالي، تندرج حلولنا ضمن نطاق مراقبة تقنية المعلومات.

الكلمات الرئيسية: المراقبة، الشبكة، Nagios Core، . . .

Table des matières

Liste des figures

Liste des tableaux

Liste des abréviations

IHM	Interface homme machine
SNMP	Simple Network Management Protocol
MIB	Management information base
IPMI	Intelligent Platform Management Interface
BMC	Baseboard Management Controller
NRPE	Nagios Remote Plugin Executor
SMTP	Simple Mail Transfer Protocol
HTT¨P	Hypertext Transfer Protocol
PHP	Hypertext Preprocessor
UML	Unified Modeling Language
OS	Operating System
IP	Internet Protocol

Introduction générale

De nos jours, les entreprises sont de plus en plus dépendantes de leur infrastructure informatique pour leurs opérations quotidiennes. Les parcs informatiques des entreprises peuvent comprendre plusieurs dizaines, voire plusieurs centaines d'équipements. Afin d'assurer la fiabilité et l'efficacité de ces systèmes, il est essentiel de garantir leur disponibilité et leur performance en tout temps, et de minimiser les risques de défaillances, de pannes et de coupures. [1]

De ce fait, les administrateurs systèmes/réseaux font appel à des logiciels de surveillance et de supervision pour vérifier l'état de l'ensemble des systèmes informatiques en temps réel sous leurs responsabilités. Mais aussi pour être alerter automatiquement (par email, par SMS) en cas de problème. Cependant, dans certaines entreprises, les logiciels de supervision ne sont pas centralisés, et chaque constructeur dispose d'un logiciel spécifique. Cette situation peut entraîner des problèmes de compatibilité et une surcharge de travail pour les administrateurs. [2]

Grace aux logiciels de supervision, de nombreux composants des machines du réseau de l'entreprise, peuvent être surveiller : la consommation processeur, la consommation de mémoire RAM, ou encore le niveau de stockage du ou des disques durs présents dans ces machines.

Donc, l'objectif principal de ce projet consiste en la mise en place d'un outil centrale qui permet de superviser les équipements d'un réseau informatique localement ou à distance, quelle que soit leur marque, leur modèle, ou leur système d'exploitation.

Dans ce cadre, le présent rapport s'articule autour de 3 chapitres structurés comme suit :

- Le premier chapitre intitulé « Contexte général » décrit l'organisme d'accueil, et présente aussi une étude de l'existant.
- Le deuxième chapitre nommé « Analyse et conception » se rapporte à la modélisation de la solution de supervision à l'aide du langage UML.
- Le troisième chapitre qui s'intitule « Réalisation » est quant à lui consacré à l'implémentation de la solution centrale de supervision.

Chapitre 1

1. Etude de l'existant et état de l'art

1.1. Introduction

Dans le but de comprendre le contexte et l'importance de notre projet, nous avons dédié un chapitre entier pour définir son cadre général.

Ce chapitre présentera en premier lieu l'entreprise d'accueil, suivi par une étude de l'existant qui nous conduit à cerner la problématique de notre sujet et par conséquent, décrire la solution proposée. Vu la multitude de logiciels s'inscrivant dans ce contexte, une étude de choix sera présentée à la fin de ce chapitre.

1.2. Présentation de l'organisme d'accueil

La Banque centrale d'Algérie, appelée aussi Banque d'Algérie a été créée le 13 décembre 1962 par la loi numéro 62-144 votée par l'Assemblée constituante. [3]

Elle définit, applique et supervise la politique monétaire et de crédit du pays, et a pour mission de maintenir les conditions les plus favorables à un développement ordonné de l'économie. [3]

Le rôle principal de la Banque d'Algérie est l'émission et l'annulation de la monnaie, et elle est aussi chargé de la gestion des réserves de change, de la régulation du marché des changes ainsi que de la supervision du système bancaire et financier. [3]

Elle est dirigée par un gouverneur nommé par le président de la République pour un mandat de six ans renouvelables une fois. [3]

La Banque d'Algérie s'organise autour de plusieurs Directions Générales, mais nous nous intéresserons seulement à la Direction de l'Ingénierie Technique et Production faisant partie de la Direction Générale des Moyens et des Systèmes de Paiement. Une version de l'organigramme se focalisant sur notre périmètre d'étude est illustrée comme suit :

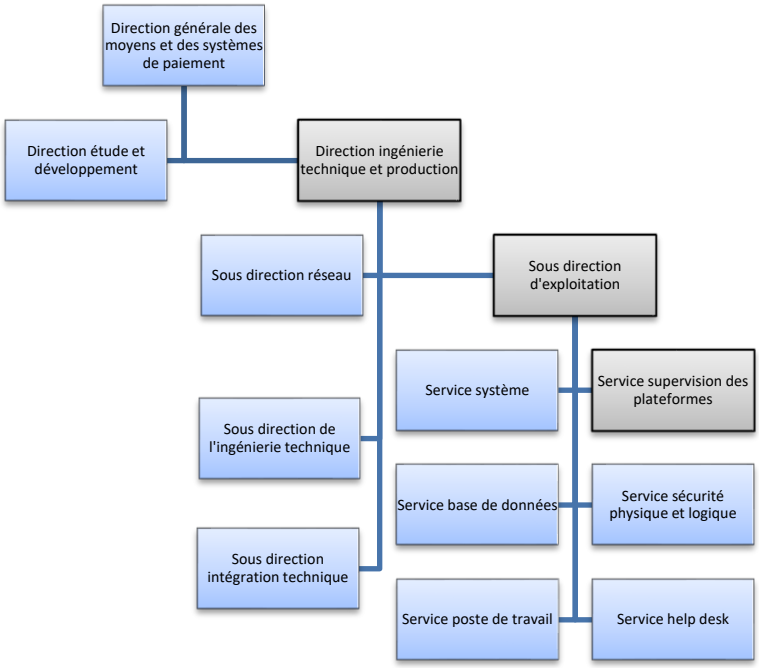

Figure 1.1- Organigramme de la Banque d'Algérie

Les sections en gris de l'organigramme montrent la partie de l'entreprise ou on a effectué notre projet.

1.3. Etude de l'existant

1.3.1. Description de l'existant

Le parc informatique de la Banque d'Algérie est composé d'une centaine de machines réparties sur plusieurs sites géographiques. Le nombre de ces machines ne cesse d'augmenter suite aux différentes opérations visant à moderniser davantage le système bancaire.

On distingue 3 types d'équipements :

- **Serveurs :** L'entreprise dispose d'environ 400 serveurs de différents constructeurs Dell, HP et IBM. Ces serveurs appartiennent à différentes gamme (Entrée, Moyenne, Haute) et sont de plusieurs générations (ancienne, nouvelle).
- **Baies de stockage :** il existe une dizaine de baie de stockage. De même, ces dernières appartenant à plusieurs constructeurs, de différentes gammes et différentes générations.
- **Robots de sauvegardes :** Même chose pour les robots ou librairie de sauvegarde.

Les systèmes d'exploitation installés sur le réseau de la Banque d'Algérie sont majoritairement Microsoft Windows sous différentes versions et éditions. Nous trouvons également des plateformes fonctionnant sous le système Linux dont la distribution RedHat est la plus utilisée.

En vue de l'hétérogénéité de ces systèmes d'exploitation, il est alors essentiel de superviser ces deux plateformes pour obtenir une vue complète et cohérente de l'ensemble du système. Windows et Linux offrent des fonctionnalités et des services différents, et chacun possède ses propres métriques, journaux système et paramètres spécifiques.

La supervision des machines Windows permet d'analyser des éléments tels que les performances du processeur, l'utilisation de la mémoire et les journaux d'événements, etc.

Le schéma suivant présente un exemple d'une supervision de machines Windows :

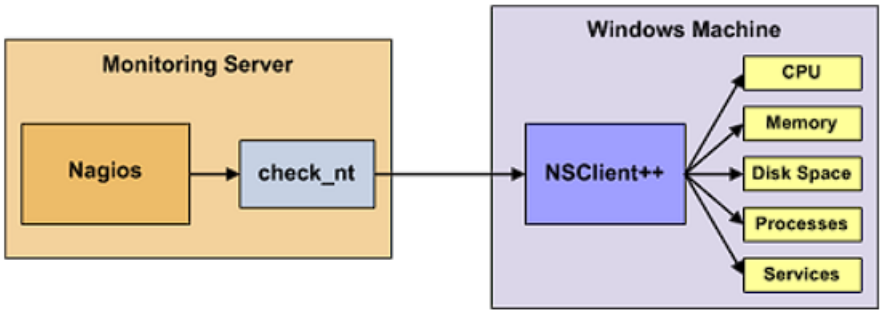

Figure 1.2- Exemple de supervision Windows

Tandis que **la supervision des machines Linux** s'intéresse aux aspects tels que l'utilisation des ressources et les journaux système, etc. En incluant ces deux aspects, on obtient une vision globale de l'état et du fonctionnement de l'ensemble du système informatique de l'entreprise.

Le schéma suivant présente un exemple d'une supervision d'une machine sous linux.

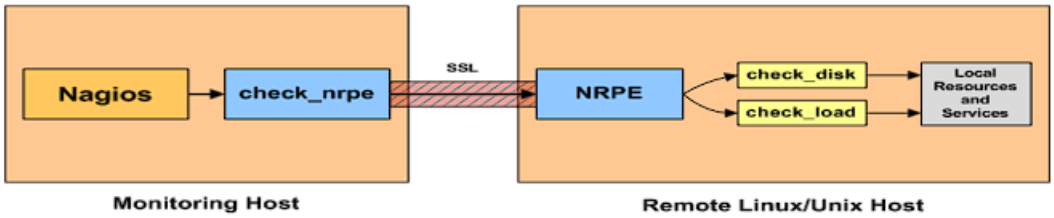

Figure 1.3- Exemple de supervision Linux

La supervision des deux systèmes d'exploitation permet d'optimiser les performances de manière spécifique à chaque plateforme, de détecter rapidement les problèmes et les incidents survenant sur les deux plateformes, et elle est essentielle pour garantir la sécurité et assurer la conformité aux politiques et réglementations en vigueur.

Pour la gestion et la surveillance de leurs plateformes informatiques, la Banque d'Algérie utilise différents logiciels de supervision fournis avec les équipements tels que

« Dell Open Manage System Administrator », « EMC Unisphere » et « HP System Management Home Page ».

En plus, cette supervision est renforcée par l'exploitation des fonctionnalités offertes par l'interface IPMI (Intelligent Platform Management Interface) et dont l'appellation diffère selon le constructeur (IDRAC : pour Dell, ILO : pour HP et IMM : pour IBM ». Il s'agit d'une interface normalisée utilisée pour la gestion du matériel à travers des messages. Son composant principal est une puce matérielle appelée Baseboard Management Controller (BMC) ou Management Controller (MC). [4]

Le contrôleur BMC fournit plusieurs interfaces qui permettent de surveiller l'état de santé du matériel système. Ces interfaces incluent des canaux utilisateur, des éléments de surveillance tels que la température, la tension, la vitesse des ventilateurs, les erreurs de bus, et d'autres éléments similaires. Il permet également d'effectuer des actions manuelles de récupération telles que les réinitialisations système en local ou à distance, les opérations de mise sous/hors tension. De plus, il permet d'établir une connexion sans intervention du système d'exploitation pour détecter des conditions anormales ou hors plage, afin de les examiner ultérieurement et de créer des alertes en conséquence. [4]

1.3.2. Critique de l'existant

Les logiciels déjà utilisés permettent uniquement une supervision individuelle des machines ce qui entraine une surcharge de travail pour l'administrateur vue le nombre important des serveurs à superviser avec une forte probabilité d'oubli. Ce qui rend cette méthode fastidieuse, compliquée et inefficace.

L'objectif de ce projet est donc de trouver une solution centrale pouvant prendre en charge n'importe quel équipement quel que soit son type ou son fabricant. De cette façon le superviseur disposera d'une seule interface pour détecter, interpréter et corriger n'importe quel problème survenant sur n'importe quelle machine du réseau.

1.3.3. Solution proposée

Après avoir étudié l'existant, et diagnostiquer les problèmes rencontrés par l'entreprise, nous avons conclu que la meilleure solution consiste à mettre en place une solution centrale de supervision des plateformes informatique, qui pourra grâce à ses fonctionnalités surveiller l'état des différents serveurs et leurs services respectifs, anticiper les pannes, voir même alerter et notifier l'administrateur pour réagir le plus rapidement possible.

1.4. Etude des solutions présentes sur le marché

Aujourd'hui, de nombreuses solutions de supervision sont disponibles. Certaines surveillent l'état intégrale du réseau en temps réel et ont une vue globale du fonctionnement de ce dernier, d'autres supervisent des domaines plus spécifiques du réseau de l'entreprise. [1]

Ces solutions sont généralement réparties en deux familles, les offres éditeurs et les offres libres.

1.4.1. Les offres éditeurs

Conscientes que le marché de la supervision est en plein essor, les entreprises investissent de plus en plus dans des logiciels permettant une meilleure gestion du réseau. [1]

Parmi ces logiciels, on peut citer « Nagios XI », « HP openview » qui sont des solutions qui supervisent des serveurs, des applications, des sites web, etc. Ou encore « Candle PathWAI » qui se penche principalement sur la supervision des applications.

Le point commun entre ces solutions est leur cout très élevé.

1.4.2. Les offres libres

Il existe aussi des logiciels de supervision libres et professionnels, comme « Cacti » ou encore « Prometheus », mais les plus répandues sont sans doute « Zabbix » et « Nagios Core » qui est la version libre (communautaires) de « Nagios XI ».

L'avantage de ces logiciels est leurs gratuités, la disponibilité du code source et la possibilité de le modifier, ainsi que la forte communauté présente sur les forums de ces logiciels. [1]

1.4.3. Choix du logiciel

Pour ce qui est des solutions commerciales, le cout de leurs mises en place est trop important pour que nous puissions envisager l'implémentation de l'une d'entre elles.

On s'est alors dirigé vers les logiciels libres, et parmi les plus utilisés on trouve « Zabbix » et « Nagios Core ». Et pour choisir entre les deux solutions, nous les avons comparés (voir tableau ci-dessous). [1] [2]

	Avantages	**Inconvénients**
Zabbix	• Solution complète et multiplateforme. • Interface vaste mais claire. • Configuration simple.	• L'agent de Zabbix communique les informations en clair, donc nécessité de les sécuriser. • Communauté limitée. • Peu d'interfaçage avec d'autres solutions

		commerciales.
Nagios Core	• Solution complète, modulaire et peut être étendu grâce aux plugins. • Reconnu auprès des entreprises. • Très grande communauté.	• Configuration complexe. • Interface pas très ergonomique, et peu intuitive.

Tableau 1.1- Tableau comparatif

Les deux solutions peuvent satisfaire les besoins de l'entreprise, mais nous avons estimé que « Nagios Core » serait plus adapté pour notre projet en raison de sa modularité. En effet, grâce à ses plugins, Nagios peut être adapté à n'importe quel environnement. [1]

Tout au long de ce rapport nous utiliserons les deux appellations « Nagios » et « Nagios Core » de façon interchangeable.

1.5. Conclusion

Dans ce premier chapitre, nous avons en premier présenté l'organisme d'accueil, ensuite déduit la problématique suite à l'étude de l'existant et sa critique. Et pour finir, nous avons proposé une solution et choisit le logiciel Nagios pour l'implémenter.

Chapitre 2

2. Analyse et conception

2.1. Introduction

La phase d'analyse et conception occupe une place centrale dans le processus de développement d'un projet, que ce soit dans le domaine de l'informatique, de l'ingénierie ou d'autres secteurs. Elles permettent de comprendre les besoins des utilisateurs, d'identifier les problèmes, de proposer des solutions et de concevoir une architecture globale qui servira de base pour la mise en œuvre du projet. Une analyse et une conception solides garantissent un développement efficace et une solution adaptée aux attentes des utilisateurs finaux.

2.2. Description générale de la solution

2.2.1. La supervision

La supervision informatique est un processus essentiel qui implique la surveillance et la gestion continues des systèmes informatiques et des réseaux d'une organisation. Elle vise à assurer leur bon fonctionnement, leur performance optimale et leur sécurité en détectant les problèmes potentiels, en collectant des données pertinentes et en fournissant des alertes en temps réel a l'administrateur. [1] [2]

2.2.2. Nagios

Présentation

Nagios Core est un logiciel de surveillance de système et de réseau Open Source. Il surveille les hôtes et les services spécifié par l'administrateur, et alerte ce dernier en cas détection de problème, ou de correction de panne dans le système. Il peut superviser différents systèmes d'exploitation et divers périphériques réseau. [5]

Fonctionnalités

Parmi les nombreuses fonctionnalités offertes par Nagios, voici quelques-unes des plus couramment utilisées [5] :

- Surveillance des services réseau (SMTP, HTTP, PING, etc.), et des ressources de l'hôte (charge du processeur, utilisation du disque, etc.).
- Notifications de contact lorsque des problèmes de service ou d'hôte surviennent et sont résolus.
- Une interface Web pour afficher l'état actuel du réseau, l'historique des notifications et des problèmes.
- Cartographie du réseau supervisé, et génération de rapports.

Plugins

Nagios s'appuie sur des programmes externes appelés « plugins » qui sont des exécutables ou des scripts compilés (scripts Perl, scripts shell, Python, PHP, Ruby, etc.) pour vérifier l'état des hôtes et des services du réseau. [6]

Il existe des centaines de plugins disponibles, et il est également possible de créer ses propres plugins pour répondre à des besoins spécifiques. Parmi les principaux on trouve [1] :

- **check_http :** Vérifie la présence d'un serveur web.
- **check_load :** Vérifie la charge CPU locale.
- **check_snmp :** Envoie une requête SNMP (passée en argument) à un hôte.
- **check_users :** Compte le nombre d'utilisateurs sur la machine locale.

La relation entre le noyau de Nagios et les plugins est assurée par les fichiers de configuration, ainsi que par le code de retour renvoyé par chaque plugin. Cette relation est synthétisée dans le tableau suivant [1] :

Code retour	Statut du Service	Description du Statut
0	OK	Tout va bien
1	Warning	Le seuil d'alerte est dépassé
2	Critical	Le service a un problème
3	Unknown	Impossible de connaître l'état du service

Tableau 2.1- Signification des codes de retours

Fichiers de configurations

Nagios s'appuie sur différents fichiers textes de configuration pour construire son infrastructure de supervision. Les plus importants sont [1] :

- **Nagios.cfg :** est le fichier de configuration principal de Nagios. Il contient la liste des autres fichiers de configuration et comprend l'ensemble des directives globales de fonctionnement.
- **Commands.cfg :** contient les définitions des commandes externes, telles que celles qui seront utiles pour la remontée d'alerte.

- **Hosts.cfg :** définit les différents hôtes du réseau à superviser. A chaque hôte est associé son nom, son adresse IP, le test à effectuer par défaut pour caractériser l'état de l'hôte, etc.
- **Services.cfg :** associe à chaque hôte ou à chaque groupe d'hôtes l'ensemble des services qui doivent être vérifiés.
- **Contacts.cfg :** déclare les contacts à prévenir en cas d'incident et définit les paramètres des alertes (fréquences des notifications, moyens pour contacter ces personnes, plages horaires d'envoi des alertes...).

2.3. Spécifications des besoins

2.3.1. Identifications des acteurs

Un acteur est une entité externe qui interagit avec le système. Il peut représenter un utilisateur, un système tiers ou un composant matériel. Les acteurs sont utilisés pour définir les rôles et les responsabilités dans le système. [7]

Pour notre système, nous avons identifié les acteurs suivants :

Administrateur de supervision : L'administrateur système est responsable de la configuration et de la gestion globale du système de supervision Nagios Core. Il peut créer, modifier et supprimer des hôtes, des services, des notifications, des plugins, etc. Il a accès à toutes les fonctionnalités du système.

Administrateur spécialisé : Cet acteur représente les utilisateurs qui consultent les informations de surveillance fournies par Nagios Core. Ils peuvent afficher les statuts, les alertes et les rapports générés par le système. Ils n'ont généralement pas les privilèges d'administration.

2.3.2. Les besoins fonctionnels

Acteur	**Besoins fonctionnels**
Administrateur de supervision	-Configurer le système de supervision. -Ajouter, modifier ou supprimer des hôtes/services. -Configurer les notifications et générer des rapports. -Surveiller l'état global du système. -s'authentifier.
Administrateur spécialisé	-Afficher les statuts des hôtes et des services surveillés.

	-Recevoir les alertes et les notifications, et consulter les rapports. -s'authentifier.

Tableau 2.2- Les besoins fonctionnels

2.3.3. Diagramme des cas d'utilisations

Un diagramme de cas d'utilisation est un diagramme qui permet de modéliser les besoins de l'utilisateur en identifiant les principales fonctions du système et en décrivant les interactions qui permettent aux participants d'atteindre leurs objectifs tout en l'utilisant. [7]

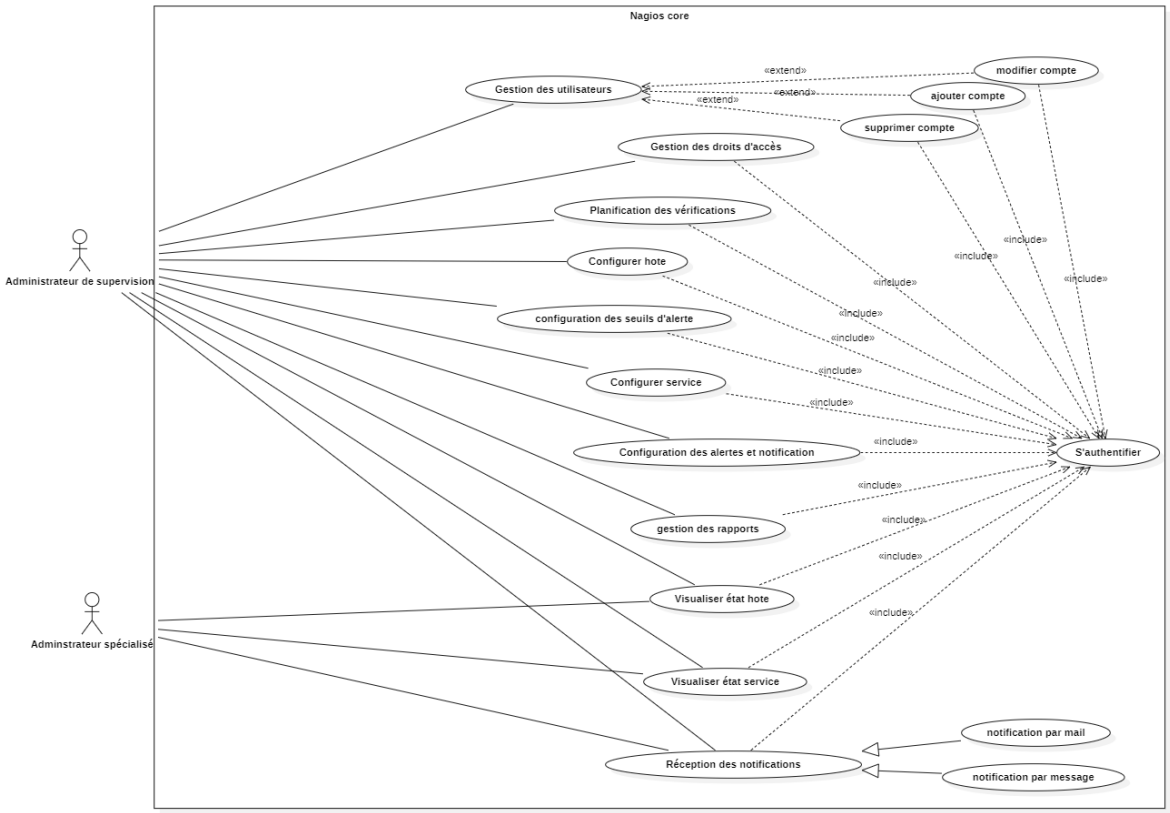

Figure 2.1- Diagramme des cas d'utilisation du système

Description textuelle des cas d'utilisation :

Cas d'utilisation	• Configurer hôte.
Acteur	• Administrateur de supervision.
Objectif	• Permettre à l'administrateur système de configurer les paramètres et les détails d'un hôte spécifique dans le système de

	supervision Nagios Core, afin de pouvoir surveiller son état et sa disponibilité.
Pré condition	• L'administrateur système doit être authentifié
Scénario nominal	1. L'administrateur système accède aux fichiers de configuration de Nagios Core. 2. L'administrateur système saisit les informations nécessaires pour définir un nouvel hôte, telles que l'adresse IP, le nom d'hôte, la description, les seuils de performances, etc. 3. L'administrateur système affecte l'hôte à un groupe d'hôtes pour une gestion efficace. 4. L'administrateur système vérifie les paramètres de configuration de l'hôte nouvellement créé et les enregistre.
Scénario alternatif	• Si les informations de l'hôte sont incorrectes ou manquantes lors de la configuration, l'administrateur système peut recevoir un message d'erreur et devra corriger les informations avant de pouvoir enregistrer la configuration. • Si l'hôte que l'administrateur souhaite configurer est déjà présent dans le système, il peut choisir de mettre à jour les informations existantes plutôt que de créer un nouvel hôte.
Post condition	• Le nouvel hôte est configuré avec les paramètres définis et ajouté à la liste des hôtes surveillés dans Nagios Core.

Tableau 2.3- Description du cas "Configurer hôte"

Cas d'utilisation	• Configurer service
Acteur	• Administrateur de supervision.
Objectif	• Permettre à l'administrateur système de configurer les paramètres et les détails d'un service spécifique associé à un hôte dans le système de supervision Nagios Core, afin de pouvoir surveiller et détecter les problèmes liés à ce service.
Pré condition	• L'administrateur système doit être authentifié • L'hôte pour lequel le service sera configuré est déjà ajouté dans Nagios Core.
Scénario nominal	1. L'administrateur système accède aux fichiers de configuration de Nagios Core. 2. L'administrateur système sélectionne l'hôte pour lequel le service sera configuré. 3. L'administrateur système saisit les informations nécessaires pour définir un nouveau service, telles que le nom du service, la description, les seuils de performances, les scripts de surveillance, etc. 4. L'administrateur système vérifie les paramètres de configuration du nouveau service et les enregistre.
Scénario alternatif	• Si les paramètres de surveillance ou les seuils de performances spécifiés pour un service sont incorrects, l'administrateur système peut recevoir un message d'erreur et devra ajuster les paramètres avant de pouvoir enregistrer la configuration.
Post condition	• Le nouveau service est configuré avec les paramètres définis et ajouté à la liste des services surveillés pour l'hôte spécifié dans Nagios Core.

Tableau 2.4- Description du cas "Configurer service"

Cas d'utilisation	• Configuration des alertes et notification.
Acteur	• Administrateur de supervision.
Objectif	• Permettre à l'administrateur système de configurer et de gérer les notifications et les alertes dans le système de supervision Nagios Core, afin de recevoir des informations pertinentes en cas de défaillances ou d'événements critiques détectés sur les hôtes ou

	les services surveillés.
Pré condition	• L'administrateur système doit être authentifié • Serveur de messagerie doit être configuré (postfix, mailx) • Les configurations des hôtes, des services et des utilisateurs/groupes de notification sont déjà définies.
Scénario nominal	1. L'administrateur système accède aux fichiers de configuration des notifications de Nagios Core. 2. L'administrateur système visualise et modifie les configurations des utilisateurs ou groupes de notification existants, y compris les adresses e-mail, les numéros de téléphone, les méthodes de notification préférées, etc. 3. L'administrateur système définit les règles de planification pour les notifications, telles que les heures de maintenance où les alertes ne doivent pas être envoyées. 4. L'administrateur système configure les seuils de déclenchement des alertes en fonction des niveaux de gravité souhaités (par exemple, avertissement, erreur critique). 5. L'administrateur système sélectionne les utilisateurs ou groupes de notification à associer à chaque hôte ou service surveillé, afin de recevoir des alertes spécifiques. 6. L'administrateur système vérifie et teste les configurations de notification pour s'assurer qu'elles fonctionnent correctement. 7. En cas de modifications ou d'ajouts de configurations de notification, l'administrateur système enregistre les modifications dans le système.
Scénario alternatif	• Lors de l'envoi de la notification de test, une erreur de connexion au serveur de messagerie empêche l'envoi de la notification. • L'administrateur système vérifie les paramètres de connexion et corrige les problèmes de connectivité avant de réessayer l'envoi de la notification.
Post condition	• Les configurations de notification sont mises à jour dans Nagios Core, permettant la réception appropriée des alertes en fonction des paramètres définis. • Les administrateurs et les utilisateurs appropriés sont notifiés des défaillances ou des événements critiques sur les hôtes ou les services surveillés.

Tableau 2.5- Description du cas "Configuration des alertes et notifications"

2.4. Conception

2.4.1. Architecture de Nagios

L'architecture de Nagios repose sur un modèle client-serveur, où le serveur principal, appelé "Nagios Core", joue un rôle central dans la collecte et la gestion des informations de surveillance. Elle peut être décomposée en trois parties coopératives [1] :

1. **Nagios Core (le noyau)** : C'est le cœur du système et le composant central de l'architecture. Nagios Core est installé sur un serveur dédié et est responsable de la planification et de l'exécution des vérifications de l'état des hôtes et des services. Il traite également les alertes et génère des rapports sur l'état du système. Nagios Core utilise des plugins pour effectuer des vérifications spécifiques sur les hôtes et les services.
2. **Plugins** : Ils sont utilisés par Nagios Core pour recueillir des informations sur l'état des différents composants du système. Nagios Core est livré avec un ensemble de plugins de base, mais il est possible d'en créer de nouveaux pour répondre à des besoins spécifiques.
3. **Interface utilisateur** : Nagios propose une interface web appelée "Nagios Core Web Interface". Cette interface permet aux utilisateurs de visualiser l'état du système, les alertes, les rapports et de gérer la configuration de Nagios.

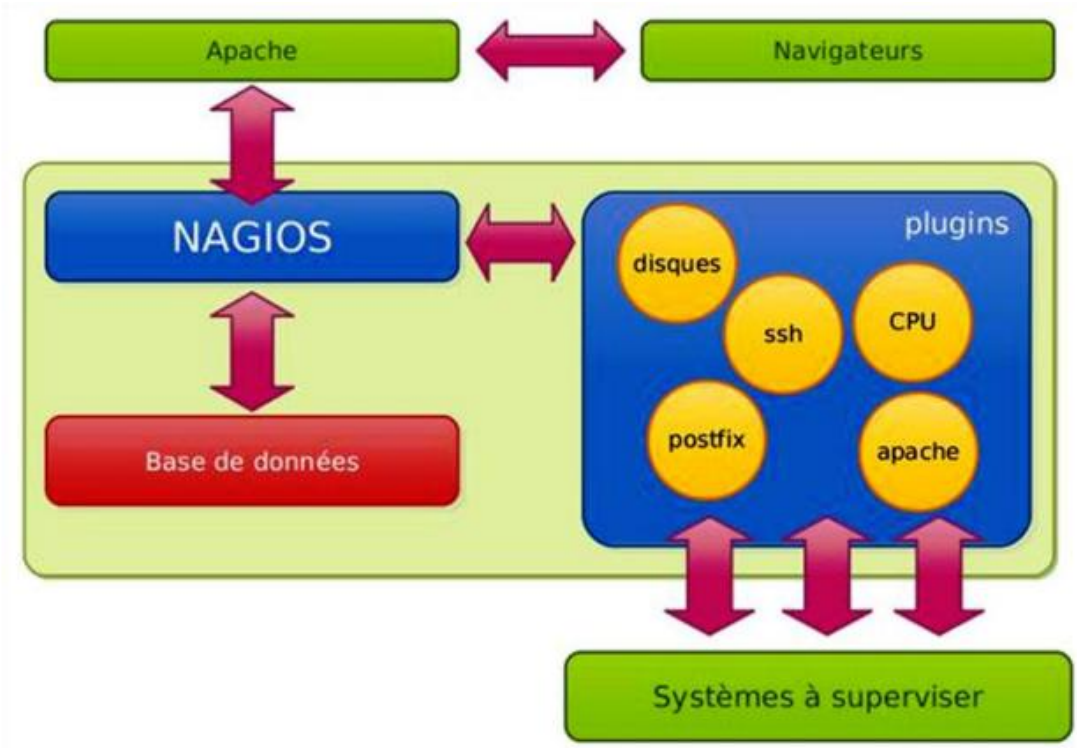

Figure 2.2- Architecture de Nagios

Pour la supervision des machines Windows et Linux, nous allons utiliser des logiciels appelés agent comme NSClient pour Windows, et NRPE pour Linux.

NSClient est un agent permettant de récupérer un nombre important d'informations à surveiller sur une machine Windows.

NSClient se base sur une architecture client/serveur (Figure 3.2). La partie cliente nommée check_nt, doit être disponible sur le serveur Nagios et on doit vérifier son existence parmi les plugins délivrés avec Nagios-plugins sinon l'installer. La partie serveur NSClient++ est à installer sur chacune des machines Windows à surveiller.

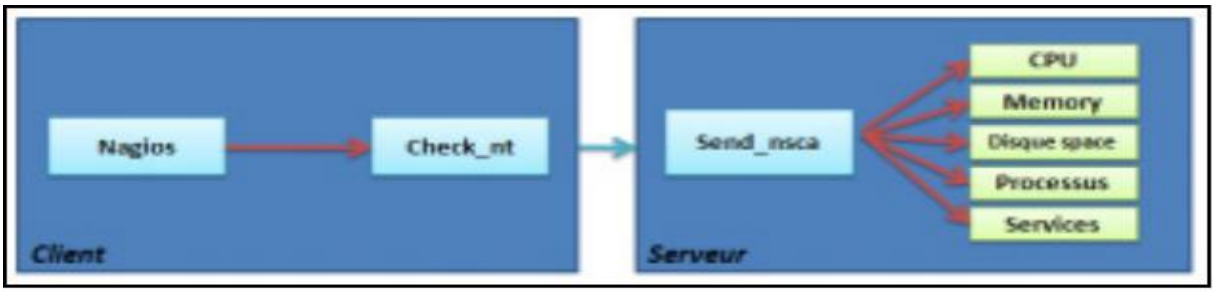

Figure 2.3- Architecture NSClient

NRPE (Nagios Remote Plugin Executor) est un agent de supervision qui vous permet de récupérer les informations à distance lors de la supervision d'un serveur Linux. Il a le grand avantage d'exécuter les commandes dans la machine à superviser ce qui permet ainsi de répartir les charges.

Il est livré avec un ensemble de commandes check définis par défaut dans son fichier de configuration et nécessite l'installation des plugins Nagios aussi.

NRPE se base sur une architecture client/serveur (Figure 3.3). Le plugin check_nrpe, doit être installé sur le serveur Nagios. NRPE est à installer sur chacune des machines Linux à surveiller.

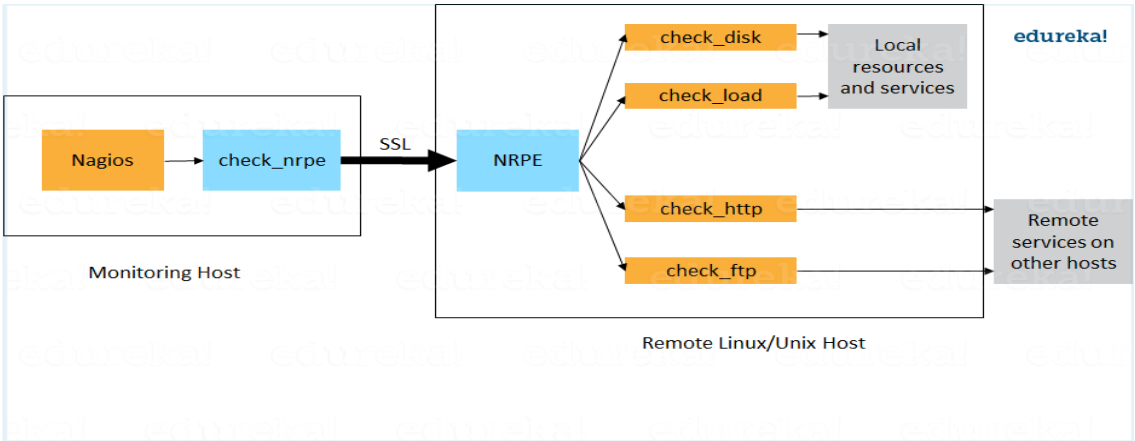

Figure 2.4- Architecture NRPE

Procédure de fonctionnement :

- Le serveur Nagios demande l'exécution d'un plugin sur la machine distante.
- Le daemon NRPE hébergé sur la machine distante, reçoit la requête d'exécution du plugin.
- Le plugin est exécuté sur la machine distante.
- Le daemon NRPE de la machine distante envoie le résultat du plugin au serveur Nagios.
- Le serveur Nagios interprète les résultats reçus.

2.4.2. Diagrammes de séquences

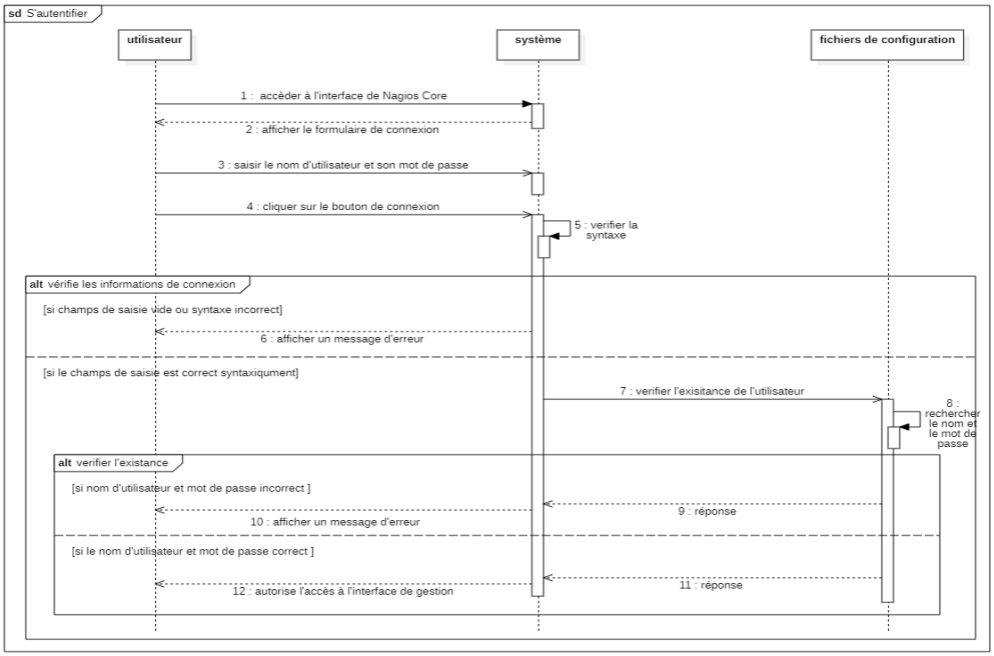

Figure 2.5- Diagramme de séquence du cas "S'authentifier"

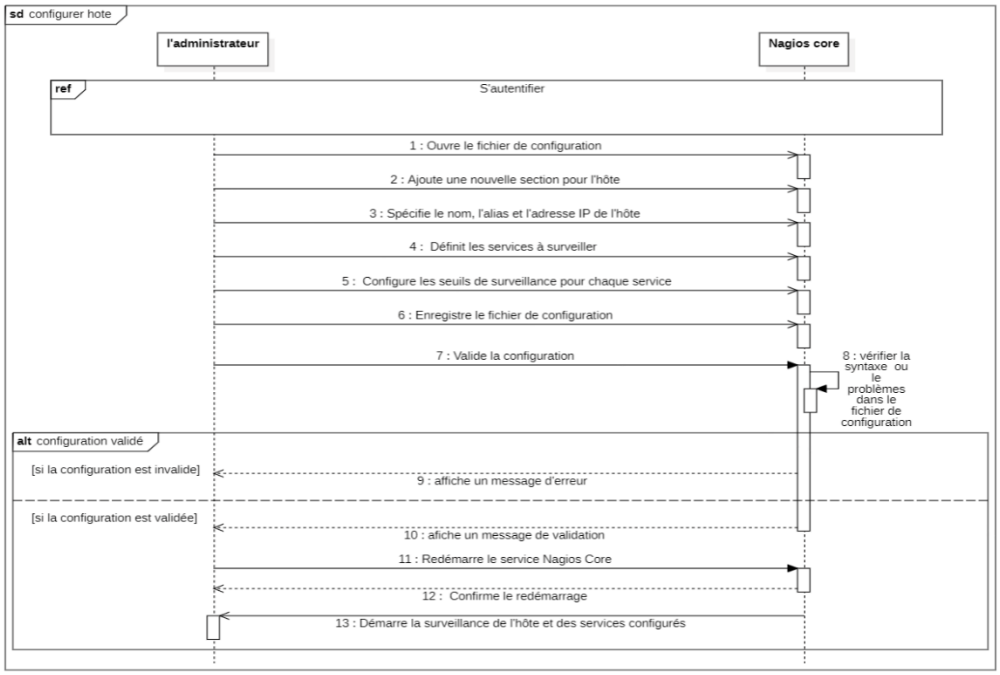

Figure 2.6- Diagramme de séquence du cas "Configurer hôte"

2.5. Conclusion

Dans ce chapitre, nous avons décrit la structure du système Nagios Core et spécifier les besoins, en utilisant les principaux diagrammes UML pour modéliser cette structure.

Le prochain chapitre présentera la mise en place de notre solution ainsi que ces principales interfaces.

Chapitre 3

3.Réalisation

3.1. Introduction

Après avoir présenté en détails la conception de notre solution, la dernière partie de ce rapport est quant à elle consacré à la phase réalisation et implémentation de cette dernière.

Avant d'intégrer la solution proposée dans le système de production de la Banque et afin d'éviter tout blocage ou perturbation de l'activité, il a été jugé plus judicieux d'implémenter la solution proposée en premier dans un environnement virtualisé de test dont le détail est donné par la suite.

Au sein de ce chapitre, nous allons présenter dans un premier lieu notre environnement de travail, ensuite la mise en place de Nagios, et enfin une présentation des interfaces de Nagios.

3.2. Environnements de mise en place

3.2.1. Environnement matériel

Lors de l'implémentation de la solution, nous avons utilisé comme environnement matériel deux machines avec les caractéristiques suivantes :

Ordinateur 1 :

Marque	Lenovo
Processeur	Intel(R) Core(TM) i7-8650U CPU @ 1.90GHz 2.11 GHz
Mémoire	16,0 Go
Système d'exploitation	Windows 11

Ordinateur 2 :

Marque	Lenovo
Processeur	AMD Ryzen 5 5600H with Radeon Graphics
Mémoire	16,0 Go
Système d'exploitation	Windows 11

3.2.2. Environnement logiciel

Grace au logiciel de virtualisation Oracle VM VirtualBox, nous avons installé sur nos machine physiques toutes les machines virtuelles nécessaires à l'implémentation du logiciel de supervision Nagios. Et les deux systèmes d'exploitation installés sur ces machines virtuelles sont : Linux Ubuntu, et Windows 10.

Figure 3.1- Logo Oracle VM VirtualBox

3.3. Mise en place de Nagios

La mise en place de Nagios se décompose en 4 grandes étapes :

1. L'installation de Nagios et de ces plugins.
2. La supervision des machines Windows
3. La supervision des machines Linux
4. La configuration des alertes et des notifications.

3.3.1. Installation de Nagios

Installation des Prérequis :

Nagios sera installé sur un OS « Linux Ubuntu ». Mais avant de l'installer, ce dernier doit satisfaire certains prérequis qui sont [8] :

- **Apache2 :** Un serveur web pour l'interface web de Nagios.
- **PHP :** Pour le serveur web.
- **Librairies GD :** Des librairies de développement.
- **gcc :** Compilateur.
- **Openssl.**

Installation de Nagios et des Plugins :

- Téléchargement des sources [8]

```
# cd /tmp

# wget -O nagioscore.tar.gz
https://github.com/NagiosEnterprises/nagioscore/archive/nagios-4.4.6.tar.gz

# tar xzf nagioscore.tar.gz
```

- Compilation [8]

```
# cd /tmp/nagioscore-nagios-4.4.6/

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

# sudo make all
```

- **Créer un utilisateur et un groupe** : Cela crée l'utilisateur et le groupe nagios. L'utilisateur www-data est également ajouté au groupe nagios. [8]

```
# sudo make install-groups-users

# sudo usermod -a -G nagios www-data
```

- **Installer les binaires** : Cette étape installe les fichiers binaires, les CGI et les fichiers HTML. [8]

```
# sudo make install
```

- **Installer Service / Daemon** : Cela installe les fichiers de service ou de démon et les configure également pour démarrer au démarrage. [8]

```
# sudo make install-daemoninit
```

- **Installer le mode de commande** : Ceci installe et configure le fichier de commande externe. [8]

```
# sudo make install-commandmode
```

- **Installer les fichiers de configuration** : Ceci installe les fichiers de configuration *SAMPLE*. Ceux-ci sont nécessaires car Nagios a besoin de certains fichiers de configuration pour lui permettre de démarrer. [8]

```
# sudo make install-config
```

- **Installer les fichiers de configuration Apache** : Cela installe les fichiers de configuration du serveur Web Apache et configure les paramètres Apache. [8]

```
# sudo make install-webconf

# sudo a2enmod rewrite

# sudo a2enmod cgi
```

- **Configurer le pare-feu** : On doit autoriser le trafic entrant du port 80 sur le pare-feu local afin de pouvoir accéder à l'interface Web de Nagios Core. [8]

```
# sudo ufw allow Apache

# sudo ufw reload
```

- **Créer un compte utilisateur nagiosadmin** : On doit créer un compte utilisateur Apache pour pouvoir nous connecter à Nagios. La commande suivante créera un compte appelé nagiosadmin et on devra fournir un mot de passe pour le compte. [8]

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

- **Démarrer le serveur Web Apache** : Il faut le redémarrer car il est déjà en cours d'exécution. [8]

```
# sudo systemctl restart apache2.service
```

- **Démarrer le Service/ Daemon** : Cette commande démarre Nagios Core. [8]

```
# sudo systemctl start nagios.service
```

- **Installation des plugins Nagios** : Nagios Core a besoin de plugins pour fonctionner correctement. Les étapes suivantes montreront l'installation des plugins Nagios. [8]

  - **Prérequis** : Certains packages doivent être installés. [8]

```
# sudo apt-get install -y autoconf gcc libc6 libmcrypt-dev make libssl-dev wget bc gawk dc build-essential snmp libnet-snmp-perl gettext
```

  - Téléchargement des sources. [8]

```
# cd /tmp

# wget --no-check-certificate -O nagios-plugins.tar.gz https://github.com/nagios-plugins/nagios-plugins/archive/release-2.3.3.tar.gz

# tar zxf nagios-plugins.tar.gz
```

  - Installation et Compilation. [8]

```
# cd /tmp/nagios-plugins-release-2.3.3/

# sudo ./tools/setup

# sudo ./configure

# sudo make
```

- **Test de Nagios** : Nagios est maintenant en cours d'exécution, pour le confirmer, nous devons nous connecter à l'interface Web de Nagios.
  On pointe notre navigateur Web vers l'adresse IP de notre serveur Nagios Core, par exemple [8] :

```
http://192.168.1.10/nagios
```

On sera invité à entrer un nom d'utilisateur et un mot de passe. Le nom d'utilisateur est nagiosadmin (créé précédemment) et le mot de passe est celui que nous avons fourni précédemment. Une fois connecté, l'interface de Nagios s'affichera.

3.3.2. La supervision des machines Windows

Pour la supervision des machines Windows, il existe deux méthodes, la première en installant un logiciel appelé agent sur la machine supervisé, et la deuxième sans agent en utilisant le protocole snmp.

Avec Agent (NSClient++) :

Pour la supervision des serveurs Windows, on va installer l'agent NSClient++ sur la machine distante, mais aussi vérifier que le plugin « check_nt » est parmi les plugins installé de Nagios pour que ces derniers puissent communiquer ensemble pour pouvoir superviser l'état de la machine mais aussi l'état de ces services.

- **Configuration coté client :**
  - On commence d'abord par télécharger l'exécutable de l'agent NSClient++ sur le site « http://nsclient.com/download/ ».
  - Ensuite, on installe ce dernier en suivant les étapes suivantes :
    - Sélectionner l'outil de supervision : on choisit Generic.

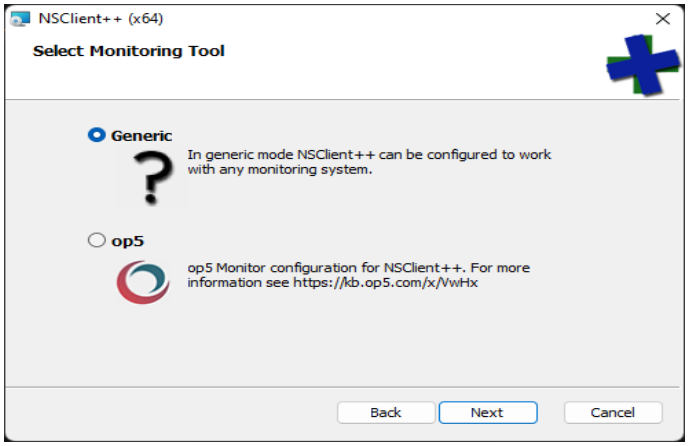

Figure 3.2- Etape 1, Installation NSClient++

    - Choisir le type de configuration : on choisit Typical.

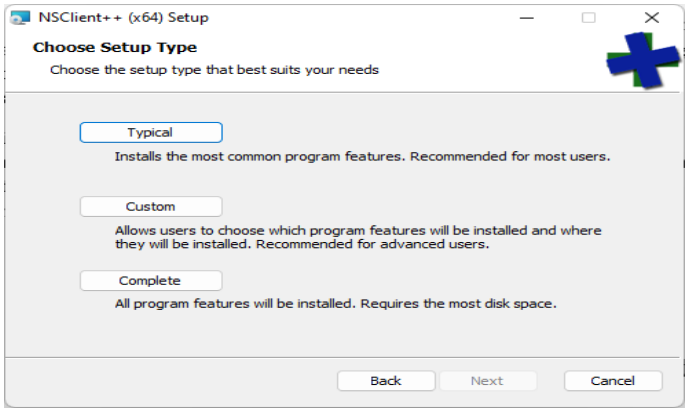

Figure 3.3- Etape 2, Installation NSClient++

    - Sur la fenêtre suivante, on introduit les adresses des hôtes autorisés (adresse de notre serveur Nagios), et le mot de passe qui sera utilisé pour se connecter à NSClient. Et cocher aussi les cases « Enable nsclient server (check_nt) » et « Enable Web server ». Et enfin, on clique sur installer.

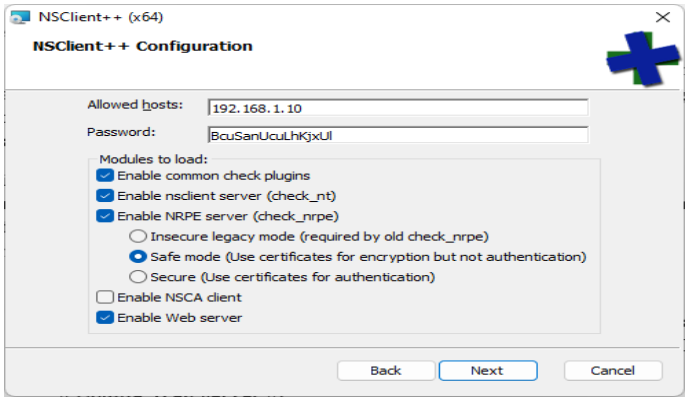

Figure 3.4- Etape 3, Installation NSClient++

- Maintenant que l'installation est achevée, on vérifie que le service « NSClient++ Monitoring Agent » peut interagir avec le bureau. Pour cela on se dirige vers la liste des services de Windows et on clique sur le service « NSClient++ Monitoring Agent ».
- Puis bouton droit et propriétés et on coche « Autoriser le service à interagir avec le bureau », puis on redémarre le service. [9]

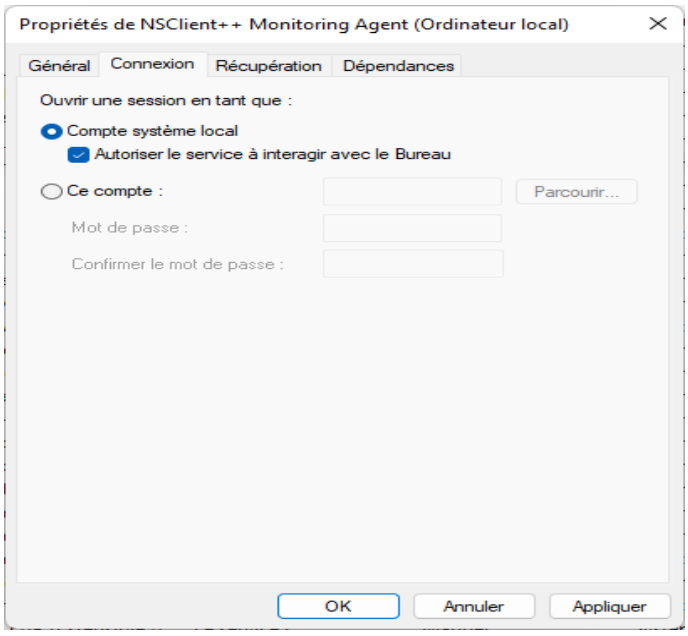

Figure 3.5- Autorisation interaction avec le bureau

- Après cela vient l'étape de configuration de NSClient++ via son interface web en activant les modules nécessaires à la supervision de la mémoire, de l'espace disque, ...etc. Qui par défaut ne le sont pas.
- D'abord, on se dirige vers le « panneau de configuration » → « Programmes et fonctionnalités » → « activer ou désactiver des fonctionnalités Windows » et on active « Internet Information Services » (voir la figure ci-dessous). [9]

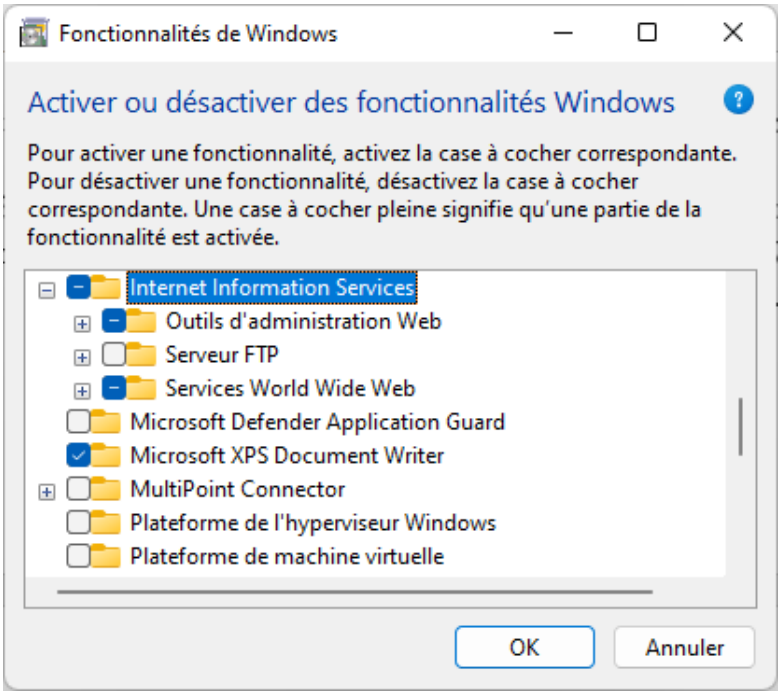

Figure 3.6- Activer Internet Information Service

- Et maintenant, pour activer les modules nécessaires à la supervision de la machine Windows il faut [9] :
  - Se connecter sur le serveur web à l'adresse : https://AdressePosteWindows:8443
  - Allez sur l'onglet module et cocher les modules nécessaires tel que : Check_disk, check_ping etc.

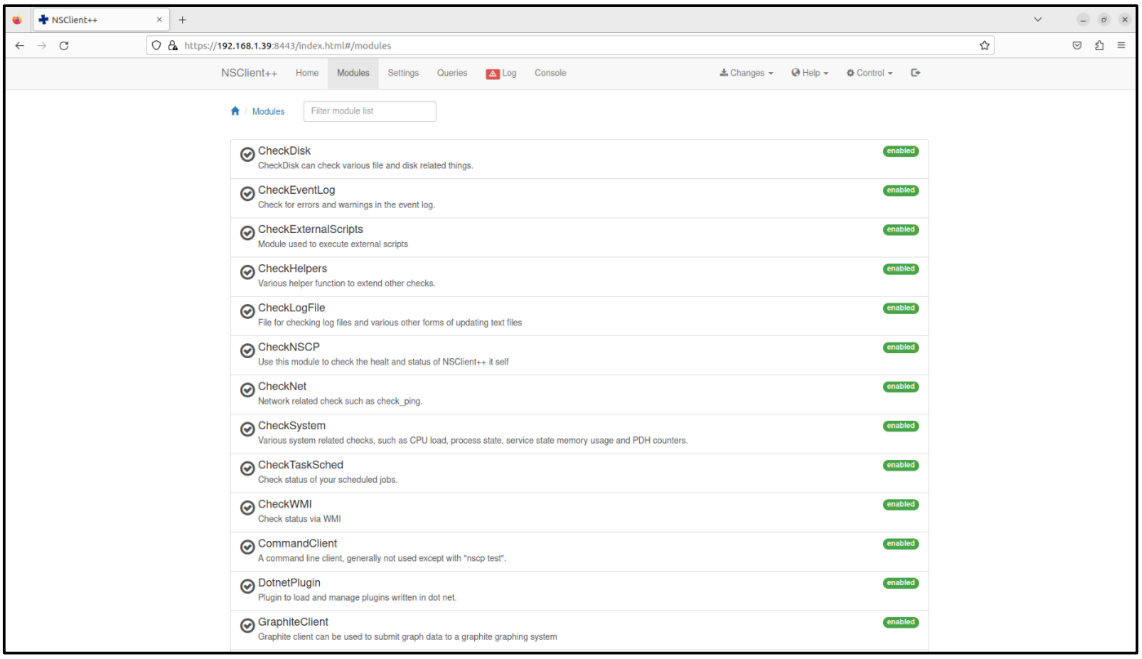

Figure 3.7- Module NSClient++

❖ **Configuration coté serveur :**

- On commence par éditer le fichier « **/usr/local/nagios/etc/nagios.cfg** » en décommentant la ligne **#cfg_file=/usr/local/nagios/etc/objects/windows.cfg.**
- Ensuite on définit l'hôte à superviser en modifiant le fichier « **/usr/local/nagios/etc/objects/windows.cfg** » de la manière suivante :
  - On met le « host_name » de la machine Windows qu'on souhaite superviser.
  - Mettre l'adresse IP du poste Windows à superviser (voir la figure ci-dessous).

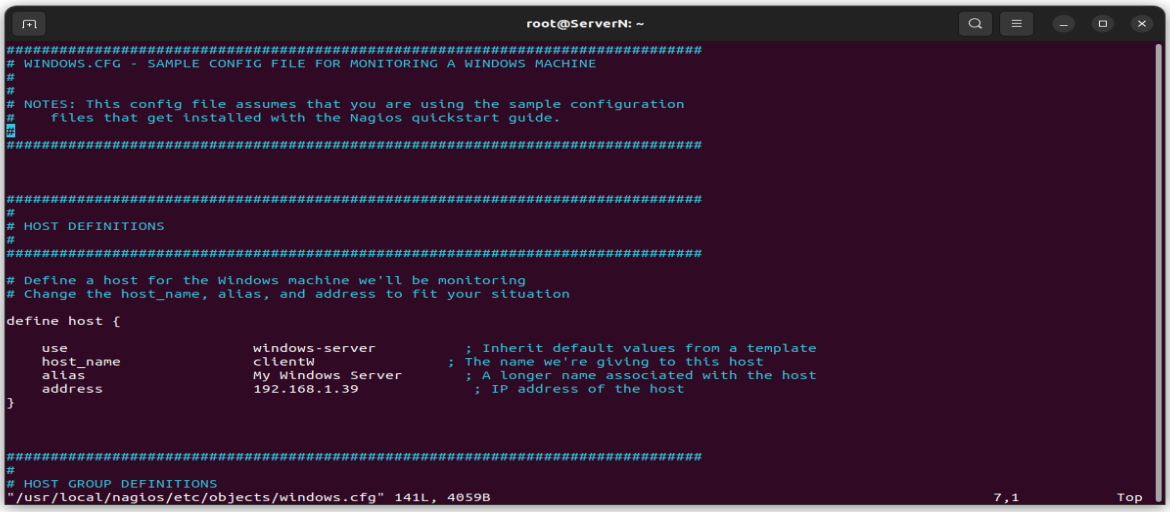

Figure 3.8- Définir hôte Windows

- Après cela, on vérifie que la configuration de Nagios est correcte en exécutant la commande suivante :

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

- Et pour finir, on relance les services de Nagios.

```
#systemctl restart nagios.service
```

Maintenant, Nagios pourra superviser les différents services de l'hôte Windows.

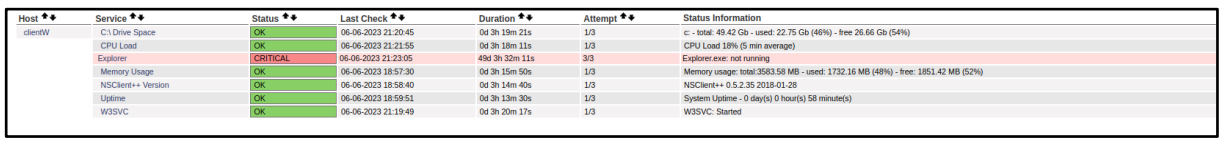

Figure 3.9- Hôte Windows ajouté

Sans Agent (Agentless) :

La deuxième méthode consiste à utiliser le protocole SNMP pour superviser nos hôtes Windows distants.

SNMP (Simple Network Management Protocol) : est un protocole de gestion de réseau largement utilisé pour superviser et gérer des dispositifs réseau. Il fournit une méthode standardisée pour la collecte d'informations et le contrôle de ces dispositifs au sein d'un réseau informatique. [2]

Le SNMP utilise une structure de données hiérarchique appelée Management Information Base (MIB) pour organiser les informations collectées des dispositifs gérés. La MIB définit les variables et les types de données que les dispositifs gérés peuvent fournir et que les gestionnaires peuvent récupérer. Les données contenues dans la MIB sont accessibles via des identifiants appelés Object Identifiers (OID). [2]

- **Configuration coté client :**
  - Dans un premier temps, on se dirige vers les paramètres Windows, dans la partie « Applications et fonctionnalités » → « Fonctionnalités facultatives » et on vérifie que le protocole SNMP est installé sur notre machine.

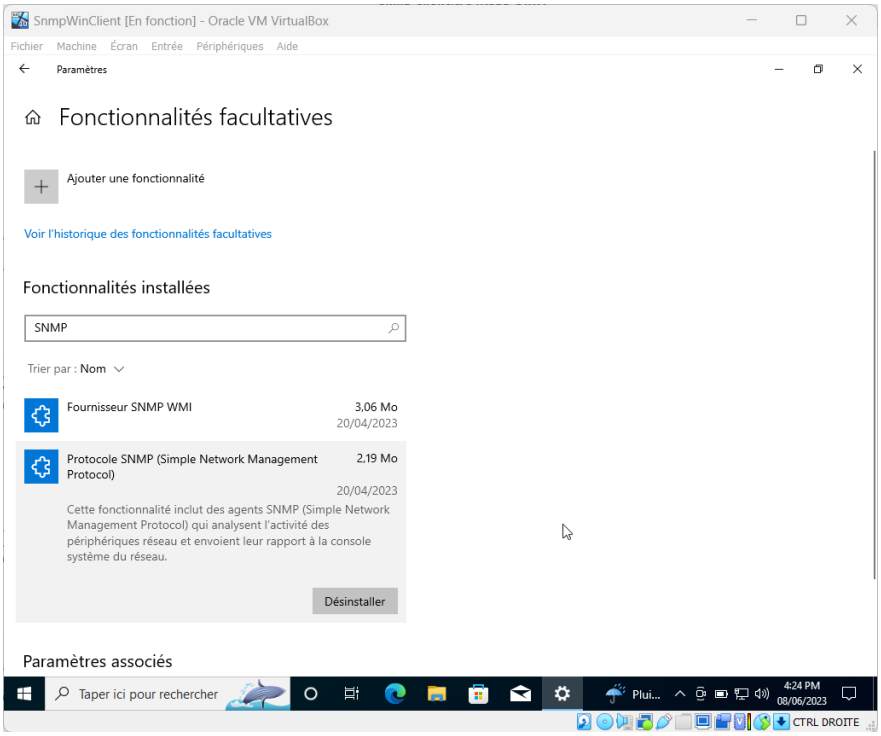

Figure 3.10- Installation Windows de SNMP

- Ensuite, on cherche dans la liste des services de Windows le service SNMP et on fait « clique droit » → « Propriétés ».

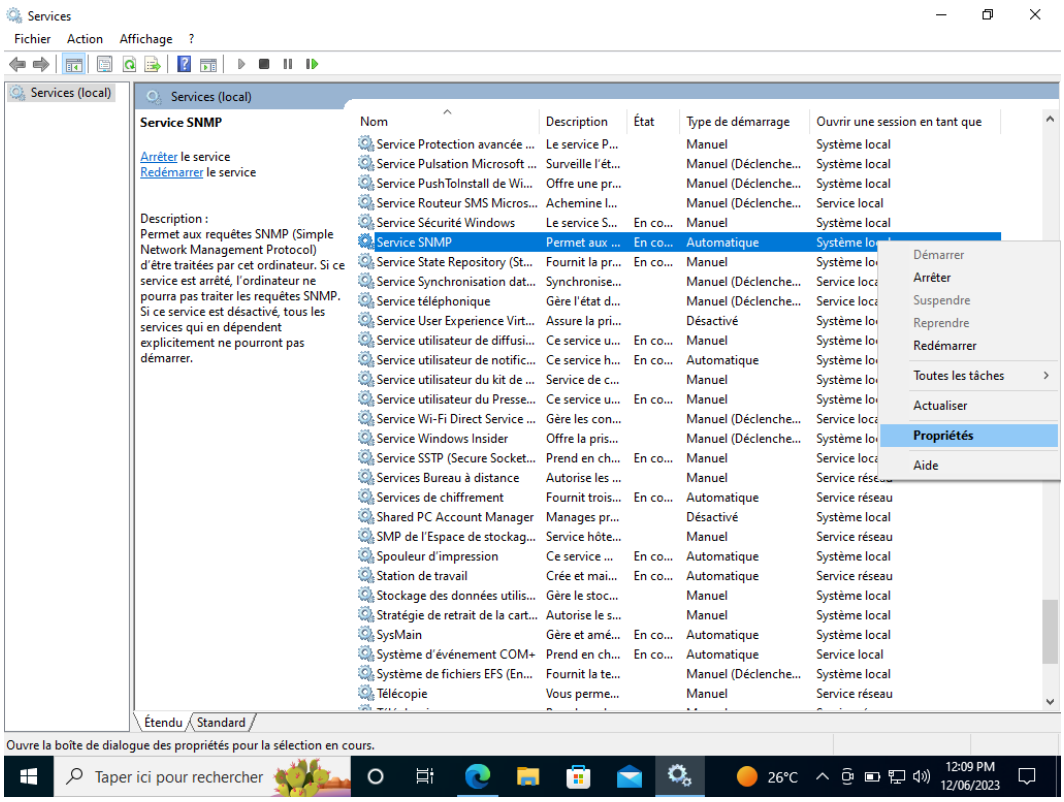

Figure 3.11- Accéder au service SNMP

- Après cela, on va dans la partie « Sécurité » pour ajouter une communauté dont le nom est « nagios » avec les droits de lecture et d'écriture. Et on ajoute aussi l'adresse IP de notre serveur Nagios dans la liste des hôtes autorisés à envoyer des paquets snmp a cette machine pour pouvoir la superviser.

Figure 3.12- Communauté SNMP

❖ Configuration coté serveur :

- On commence d'abord par installer SNMP grâce à la commande suivante :

```
#sudo apt install snmpd
```

- Ensuite, nous allons installer d'autres plugins snmp en plus de celui déjà présent par défaut qui est « check_snmp » pour pouvoir superviser plus de services. Pour cela on suit les étapes suivantes :
  - On clone un repository de github ou se trouve les plugins dont on aura besoin avec la commande :

```
#git clone https://github.com/techarkit/nagios.git
```

  - Ensuite, on se dirige vers le répertoire **/nagios/plugins**

```
# cd nagios

# cd plugins/
```

  - On change les permissions.

```
# chmod 777 *
```

  - Et pour finir, on copie tous les plugins snmp dans le répertoire **/usr/local/nagios/libexec/**

```
# cp check_snmp* /usr/local/nagios/libexec/
```

- La prochaine étape est de définir de nouvelles commandes pour les plugins qu'on vient d'installer en modifiant le fichier **/usr/local/nagios/etc/objects/commands.cfg** et le résultat est le suivant :

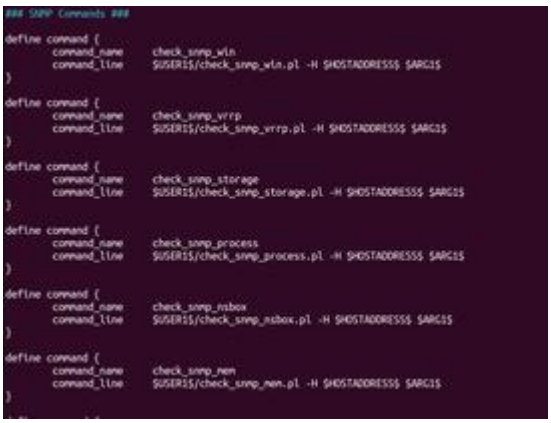

Figure 3.13- Commandes SNMP

- Maintenant, on va créer un fichier intitulé « **snmp-client.cfg** » dans le répertoire **/usr/local/nagios/etc/objects/** ou on va définir l'hôte qu'on va superviser et ses services.

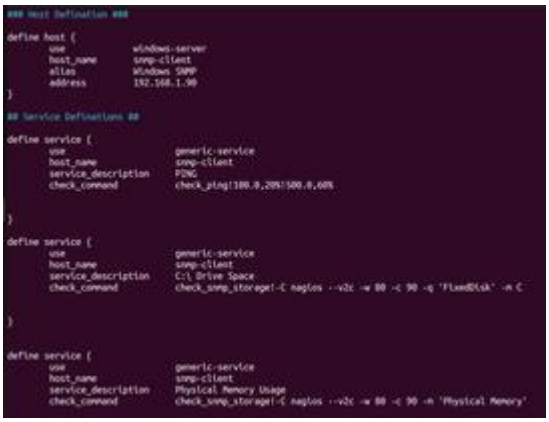

Figure 3.14- Définir Hôte SNMP

- Avant de finir, on ajoute la ligne « **cfg_file=/usr/local/nagios/etc/objects/snmp-client.cfg** » dans le fichier **/usr/local/nagios/etc/nagios.cfg**
- Pour la dernière étape, on vérifie que la configuration Nagios est correcte.

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

3.3.3. La supervision des machines Linux

Pour la supervision des serveurs Linux, nous allons installer l'agent NRPE sur la machine distante, et installer le plugin « check_nrpe » sur le serveur Nagios. [10]

❖ **Configuration coté client :**

- Installer les prérequis suivants :

```
# sudo apt-get update

# sudo apt-get install -y autoconf automake gcc libc6 libmcrypt-dev make libssl-dev wget openssl
```

- Installer le démon NRPE et les plugins Nagios, car NRPE a besoin des plugins pour fonctionner correctement.

```
# sudo apt-get install nagios-nrpe-server nagios-plugins -y
```

- Maintenant, on va modifier le fichier **/etc/nagios/nrpe.cfg** et ajouter l'adresse IP de notre serveur Nagios parmi les adresses des hôtes pouvant envoyer des requêtes a l'agent NRPE (voir figure ci-dessous).

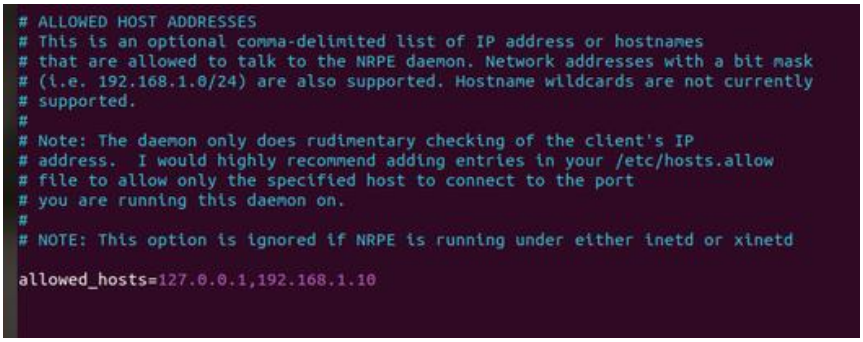

Figure 3.15- Modification nrpe.cfg

- Ensuite, on configure le parfeu, et on redémarre le service NRPE.

```
# sudo ufw allow 5666/tcp

# sudo systemctl nagios-nrpe-server.service
```

- Après cela, on retourne dans le fichier **/etc/nagios/nrpe.cfg** pour ajouter des commandes pour pouvoir superviser plusieurs services grâce aux plugins Nagios. Comme montrer sur la figure 3.16.

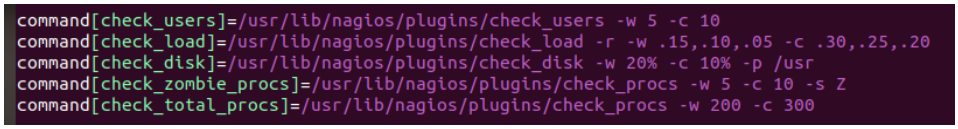

Figure 3.16- Commandes nrpe.cfg

❖ **Configuration coté serveur :**

- Tout d'abord, installer le plugin « check_nrpe » qui communiquera avec le démon NRPE installé sur la machine distante.

```
# cd /tmp/nrpe/

# ./configure

# make check_nrpe

# make install-plugin
```

- Ensuite, on modifie le fichier **/usr/local/nagios/etc/objects/commands.cfg** pour ajouter la commande « check-nrpe » qu'on va utiliser pour superviser les services de notre hôte (voir la figure ci-dessous).

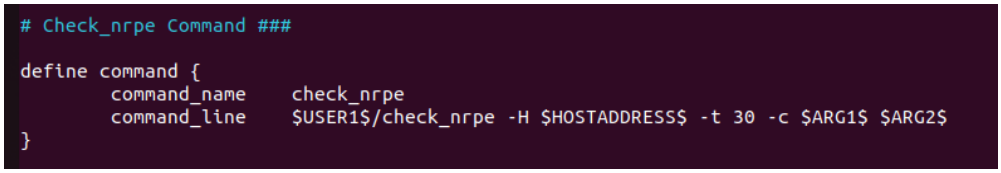

Figure 3.17- La commande check_nrpe

- Maintenant, on va créer un fichier intitulé « **linuxhost.cfg** » dans le répertoire **/usr/local/nagios/etc/objects/** ou on va définir l'hôte qu'on va superviser et ses services, comme le montre la figure 3.18.

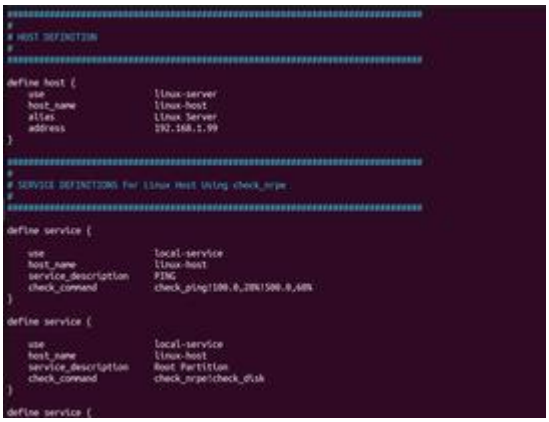

Figure 3.18- Définir hôte Linux

- Ensuite, on ajoute la ligne « **cfg_file=/usr/local/nagios/etc/objects/linuxhost.cfg** » dans le fichier **/usr/local/nagios/etc/nagios.cfg**

```
cfg_file=/usr/local/nagios/etc/objects/linuxhost.cfg
```

Figure 3.19- Modification nagios.cfg

- Et pour finir, on redémarre le service Nagios pour que les modifications prennent effet.

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

3.3.4. La configuration des alertes et des notifications

En plus d'être informé visuellement par l'interface web de Nagios, on peut configurer l'envoi de notification par mail ou par téléphone pour alerter d'un problème sur un hôte ou un service. Dans notre solution nous avons configuré l'envoi de notification par e-mail. [1]

❖ **Installation et configuration de Postfix :**

- Dans un premier lieu, nous avons besoin d'utiliser un serveur SMTP « Simple Mail Transfer Protocol » qui est un système de messagerie électronique qui permet d'acheminer les e-mails d'un expéditeur vers un destinataire en utilisant le protocole SMTP.
- On va utiliser aussi Postfix qui sert à l'envoi de notification vers notre serveur de messagerie.
- Pour installer Postfix, on exécute la commande suivante :

```
# sudo apt install postfix
```

- Ensuite, on passe à la configuration de postfix, et pour cela on va modifier le fichier **/etc/postfix/main.cf** de la manière suivant :
  - On renseigne dans la ligne « **relayhost** » l'adresse IP ou le nom DNS du serveur de messagerie SMTP utiliser pour router les courriers. Dans notre cas ça sera celui de Gmail qui est : **[smtp.gmail.com] : 587**
- Donc, Postfix va envoyer ces e-mails vers le serveur SMTP, et ce dernier les redirigera vers les utilisateurs qui doivent être notifier.

❖ **Configuration des utilisateurs à notifier :**

- Premièrement, on modifie le fichier **/usr/local/nagios/etc/objects/contacts.cfg** en ajoutant l'adresse mail, le nom d'utilisateur, mais aussi les périodes ou ce contact peut être notifier, sur quel hôte et quel service et pour quels statuts (voir figure ci-dessous). Et on peut aussi ajouter ce contact a un groupe.

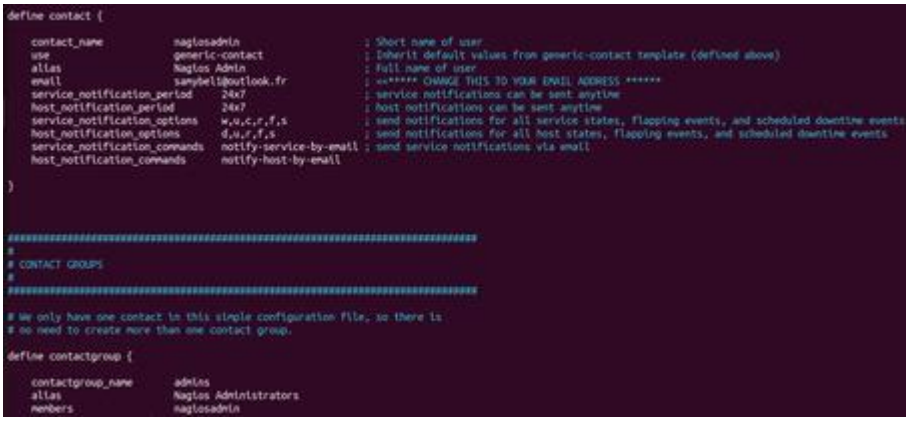

Figure 3.20- Définir Contact

- Ensuite, on modifie les fichiers de configurations des hôtes et des services en ajoutant une ligne « **contact** » ou « **contact_groups** » avec le nom des utilisateurs ou groupes d'utilisateurs à alerter en cas de problème concernant cet hôte ou ce service.
- Après ces modifications on vérifie que la configuration de Nagios est correcte et si c'est le cas, les utilisateurs recevront une notification par mail ayant la forme suivante :

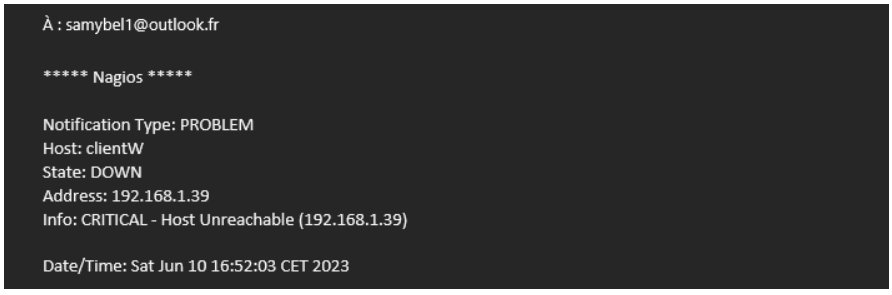

Figure 3.21- Exemple de notification

3.4.Présentations des interfaces Nagios

3.4.1. Interface d'authentification

Comme dit précédemment dans l'étape d'installation de Nagios, pour accéder à l'interface web de ce dernier il faut d'abord ouvrir un navigateur et écrire dans la barre de navigation « http://192.168.1.10/nagios. Une page d'authentification s'affiche demandant le nom d'utilisateur et le mot de passe comme l'indique la figure suivante.

Figure 3.22- Page d'authentification

3.4.2. Interface de supervision des hôtes

Cette interface nous permet d'accéder à nos hôtes et de constater leurs états.

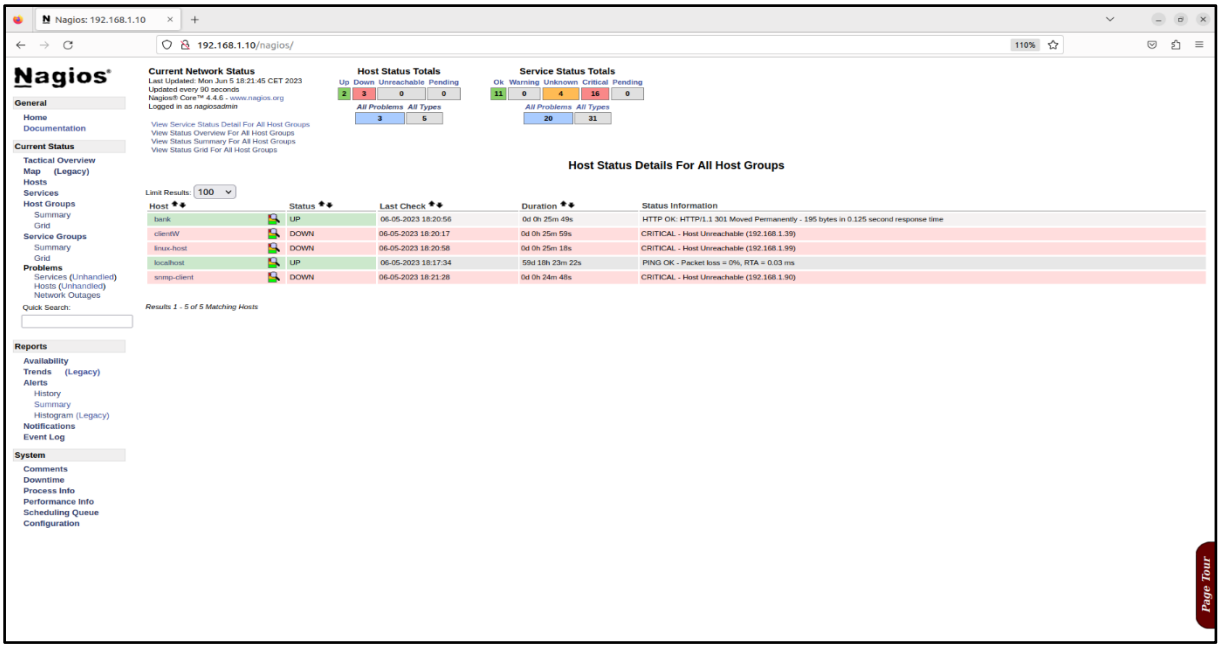

Figure 3.23- Interface de supervision des hôtes

3.4.3. Interface de supervision des services

Cette interface nous permet d'accéder à nos services et de constater leurs états.

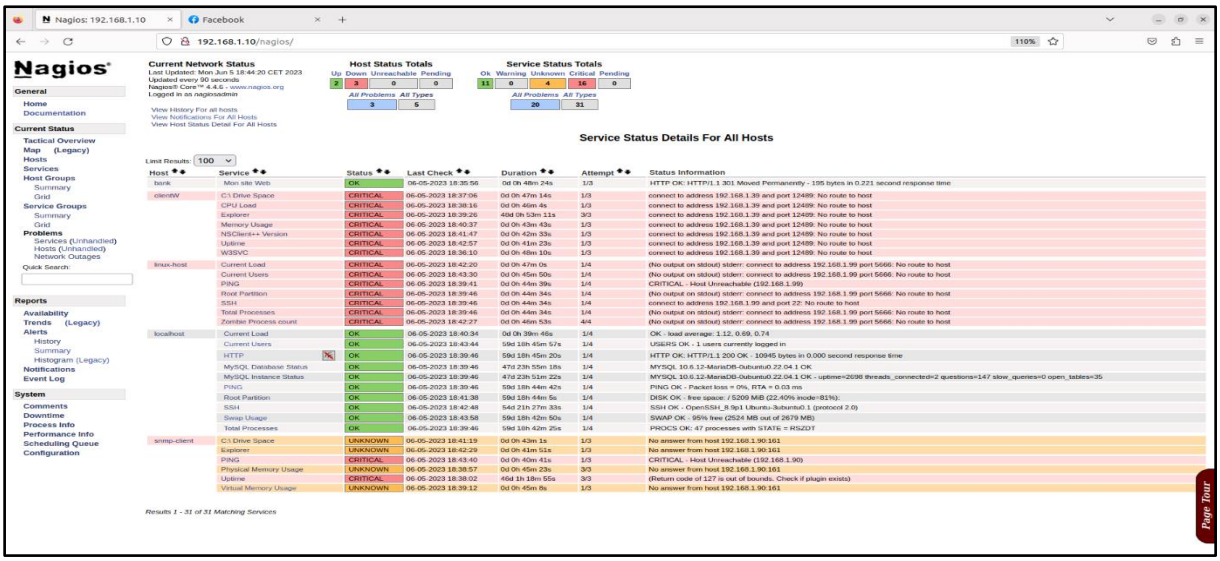

Figure 3.24- Interface de supervision des services

3.4.4. Interface des notifications

Cette interface nous montre l'historique des notifications envoyées aux contacts concernés avec le type de notification, le temps d'envoi, l'hôte et le service concerné ...etc.

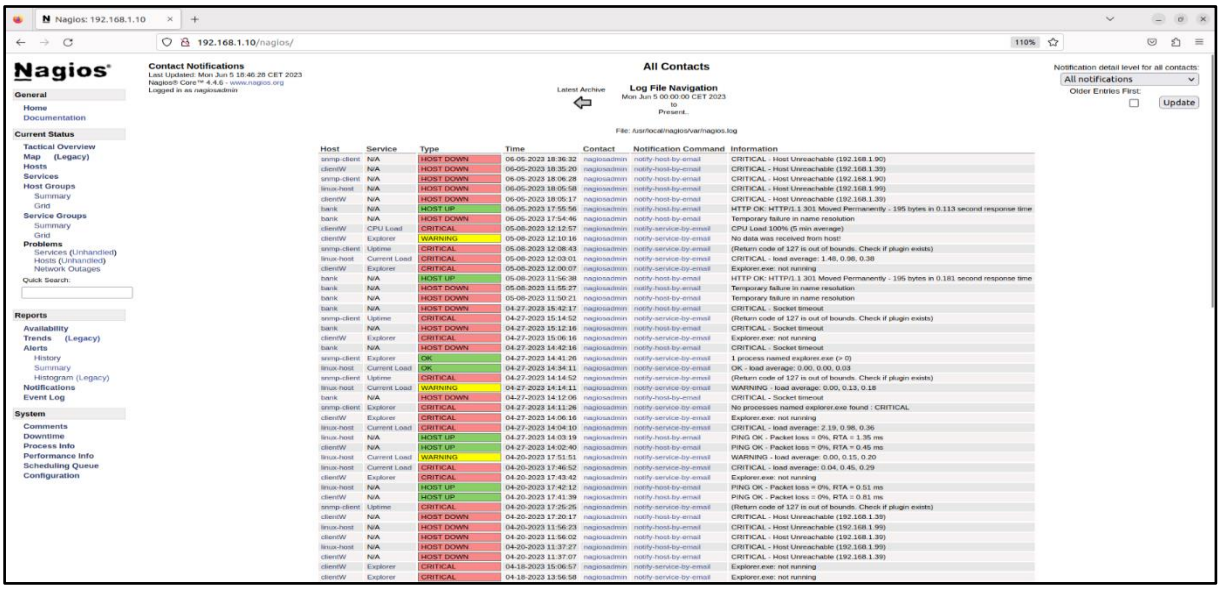

Figure 3.25- Interface de notification

3.5. Conclusion

Dans ce chapitre, nous avons décrit la mise en place de notre solution de supervision et avons aussi présentés les interfaces les plus importantes de celle-ci.

Conclusion générale et perspectives

Le domaine de la supervision est un des domaines les plus importants de l'administration systèmes et réseaux, et il a connu une évolution considérable au cours de ces dernières années. Ciblé sur ce secteur en particulier, l'objectif de note projet de fin d'étude est de mettre en œuvre une solution centrale de supervision des plateformes informatiques pour garantir la disponibilité, la performance et la fiabilité des systèmes.

Pour atteindre cet objectif, nous avons d'abord étudié tous l'existant en termes de matériels et de logiciels pour pouvoir choisir la solution la mieux adapté parmi les offres libres et éditeurs présentes sur le marché.

Deuxièmement, nous avons proposé la solution Nagios Core qui centralise la supervision des équipements, quels que soient leur marque, modèle ou système d'exploitation. Nous avons fait l'analyse et la conception de cette solution en utilisant des techniques de modélisation UML, ce qui nous a permis de planifier et de structurer efficacement la mise en œuvre.

Enfin, nous avons présenté l'environnement de travail, les outils utilisés, ainsi que l'implémentation et la mise en œuvre de notre solution.

L'un des éléments fondamentaux que nous envisageons d'ajouter à cette solution dans un avenir proche est l'intégration d'un outil complémentaire, comme Centreon. Cela permettrait de faciliter la configuration des équipements à superviser et la gestion globale du système, en affichant une interface web conviviale pour l'administrateur, qui sera un intermédiaire entre ce dernier et les fichiers de configuration de Nagios.

Bibliographie

[1] S. Othman, «Mise en place d'un système de supervision,» Tunis, 2011.

[2] K. BOUAOUD et S. ARABI, «La mise en place d'une solution de monitoring et,» 2019.

[3] Bank Of Algeria - DC., «Histoire de la Banque,» Bank Of Algeria, 2022. [En ligne]. Available: https://www.bank-of-algeria.dz/histoire-de-la-banque/. [Accès le 15 Juin 2023].

[4] IBM, «Présentation d'IPMI - Documentation IBM,» IBM, 28 Février 2021. [En ligne]. Available: https://www.ibm.com/docs/fr/power8?topic=power8-p8eih-p8eih-ipmi-overview-htm. [Accès le 15 Juin 2023].

[5] Nagios Enterprises, LLC., «About Nagios Core - Nagios Core Documentation,» Nagios, [En ligne]. Available: https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/4/en/about.html#whatis. [Accès le 5 Mars 2023].

[6] Nagios Enterprises, LLC., «Nagios Plugins - Nagios Documentation,» Nagios, [En ligne]. Available: https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/4/en/plugins.html. [Accès le 20 Mars 2023].

[7] N. Taibouni, «Génie Logiciel GL1,» 2021.

[8] Nagios Enterprises, LLC., «Quickstart Installation Guides - Nagios Core Documentation,» Nagios, [En ligne]. Available: https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/4/en/quickstart.html. [Accès le 5 Mars 2023].

[9] S. AREZKI ACHAB et A. AOUICHE, «MISE EN OEUVRE D'UNE SOLUTION DE SUPERVISION DU RESEAU INFORMATIQUE SOUS NAGIOS».

[10] Nagios Enterprises, LLC., «NRPE - How To Install NRPE v4 From Source,» 27 Aout 2022. [En ligne]. Available: https://support.nagios.com/kb/article.php?id=515. [Accès le 27 Avril 2023].