

Sommaire

Introduction générale.....	1
Chapitre I : Présentation du cadre du projet.....	2
I. Présentation de la société.....	3
1. Services :	3
2. Architecture :	3
II. Etude de l'existant	5
3. Description de l'existant.....	5
4. Critique de l'existant	9
5. Solution proposée	10
6. Conclusion.....	10
Chapitre II :Etat de l'art	11
I. nécessité de la supervision.....	12
II. les fonctionnalités d'un système de surveillance.....	12
III. Domaine de supervisions.....	13
IV. solutions open source	13
V. solutions propriétaires	15
VI. choix de la solution de supervision	16
VII. Conclusion.....	17
Chapitre III : Spécification des besoins et architecture.....	18
I. Analyse des besoins :	19
1. Besoins Fonctionnels.....	19
1. Besoins non Fonctionnels.....	19
II. Architecture du projet.....	19
III. Conclusion	23
Chapitre IV: Mise en place du système de supervision.....	24
I. Environnements de mise en place	25
1. Environnement matériel	25
2. Environnement logiciel	26
II. Mise en place de Nagios/Cacti et les plugins	26
1. Pré-requis Nagios/Cacti.....	26
2. Installation de Nagios/Cacti	26

3.	Installation de NSClient	26
4.	Installation de NRPE	26
5.	Interface Nagios / Cacti	27
6.	Notification par mail	36
III.	Conclusion	36
	Conclusion générale	37
	Références netographiques	38
	Annexes	39

Liste des figures

Figure 1:organigramme générale de la Poste tunisienne	4
Figure 2:Schéma global du réseau informatique	5
Figure 3:synoptique de la liaison entre les différents composants du reseau postal	6
Figure 4:Synoptique d'interconnexion de différentes parties du réseau national	7
Figure 5:centralisation des locaux au direction generale de Siliana.....	8
Figure 6:reseau local du bureau de poste Bourouis.....	9
Figure 7:maquette de test sous GNS3.....	20
Figure 8:Emplacement de mise en place de Nagios dans le réseau de la poste.....	21
Figure 9:Architecture Nagios.....	22
Figure 10:synoptique de l'architecture générale de Cacti	23
Figure 11: synoptique générale de la structure du réseau du ONP	25
Figure 12:interface état d'une hôte linux sur Nagios.....	26
Figure 13:configuration de la carte réseau du serveur de supervision.....	27
Figure 14:interface d'authentification Nagios.....	27
Figure 15:interface d'authentification Cacti.....	28
Figure 16:page d'accueil de Nagios.....	29
Figure 17:page d'accueil de Cacti.....	29
Figure 18:liste des hôtes supervisés par Nagios.....	30
Figure 19:carte des hôtes supervisés par Nagios.....	31
Figure 20:liste des hôtes supervisés par Nagios avec visualisations des différents ports et services ..	31
Figure 21:etat de service pour une hôte Linux.....	32
Figure 22: les informations détaillés de la hôte BP_Sfax	32
Figure 23:interface Devices dans Cacti.....	33
Figure 24:interface d'ajout d'un routeur sur Cacti.....	33
Figure 25:interface d'ajout d'une hôte Linux sur Cacti	34
Figure 26: tracé de Traffic Fibre Optique de DRP_Beja.....	34
Figure 27:Graphes de différentes caractéristiques du Local host générés par Cacti.....	35
Figure 28:Fichiers Log générés par Cacti.....	35

Liste des tableaux

Tableau 1:avantages et inconvénients des solutions open source	13
Tableau 2:avantages et inconvénients des solutions propriétaires.....	15
Tableau 3:Comparaison entre différentes solutions de supervision	17

Introduction générale

De nos jours, les entreprises sont équipées au moins d'un réseau local, et dans d'autres cas on trouve aussi un réseau étendu(WAN) avec des parcs informatique qui englobent des multiples équipements, engendrés par des serveurs, des serveurs de traitements et des bases de données.

Vu que les réseaux informatiques deviennent de plus en plus grands et encombrée et repartis sur d'immenses territoires avec un nombre d'utilisation de plus en plus grand, les administrateurs réseaux ont besoin de superviser et bien contrôler les aspects de leurs réseaux afin de minimiser les anomalies.

D'où l'intérêt de notre projet qui consiste à mettre en place un système de supervision pour bien améliorer notre administration réseau de la poste tunisienne qui est reparti sur toute la république tunisienne, et la rend facile à gérer et aussi informer le responsable suite à l'envoi des notifications automatiquement par Email en cas de dysfonctionnement pour intervenir en mode proactif afin de minimiser l'indisponibilité des systèmes.

Le présent document comporte quatre chapitres :

Le premier chapitre «Présentation du cadre du projet».

Le second chapitre «Etat de l'art» consiste à présenter le concept de la supervision.

Le troisième chapitre «Spécification des besoins et architecture», est plus technique, il contient une spécifications des besoins et une description détaillée de l'architecture de la solution.

Dans la phase «Mise en place du système de supervision» on présente l'aspect pratique et la mise en place de la solution.

Enfin, le rapport de notre mémoire de mastère a été clôturé par une conclusion générale qui doit dresser la synthèse du travail.

Chapitre I : Présentation du cadre du projet

Dans ce chapitre on va se concentrer sur le cadre générale du projet et la présentation de l'entreprise accueillante et l'étude détaillée de l'existant

I. Présentation de la société

La poste tunisienne est la société responsable du service postal en Tunisie. Il exploite également des services bancaires en Tunisie. La société a été fondée en 1847 et a été admise à l'Universal Post Union en 1878. La poste tunisienne a ouvert la Caisse d'épargne nationale tunisienne en 1956[1]. La Poste Tunisienne assure des prestations économiques et sociales importantes qui sont conformes au Code de la Poste promulgué le 02 juin 1998. Son activité s'articule principalement autour de :

- Les prestations et les services nouveaux.
- L'exploitation et la fourniture de services financiers.
- La collecte, le transport et la distribution du courrier.

1. Services :

Aujourd'hui la poste Tunisienne offre plusieurs services à sa clientèle dont notamment :

- **Les services financiers** : chèques, mandats, épargne.
- **Le courrier postal.**

L'informatisation des services postaux a mené à des réseaux informatiques privés qui ont atteint un niveau de performance très appréciable et ne cessent pas s'accroître et de s'améliorer de jour en jour de afin d'offrir plus de services avec une meilleure qualité, fiabilité et plus d'ouverture vers le monde extérieur.

2. Architecture :

La figure1 représente d'une manière générale l'organigramme de la poste tunisienne et l'organisation des différents services et départements. Notre projet s'est déroulé au sein de centre informatique qui se situe à Tunis-Hached.

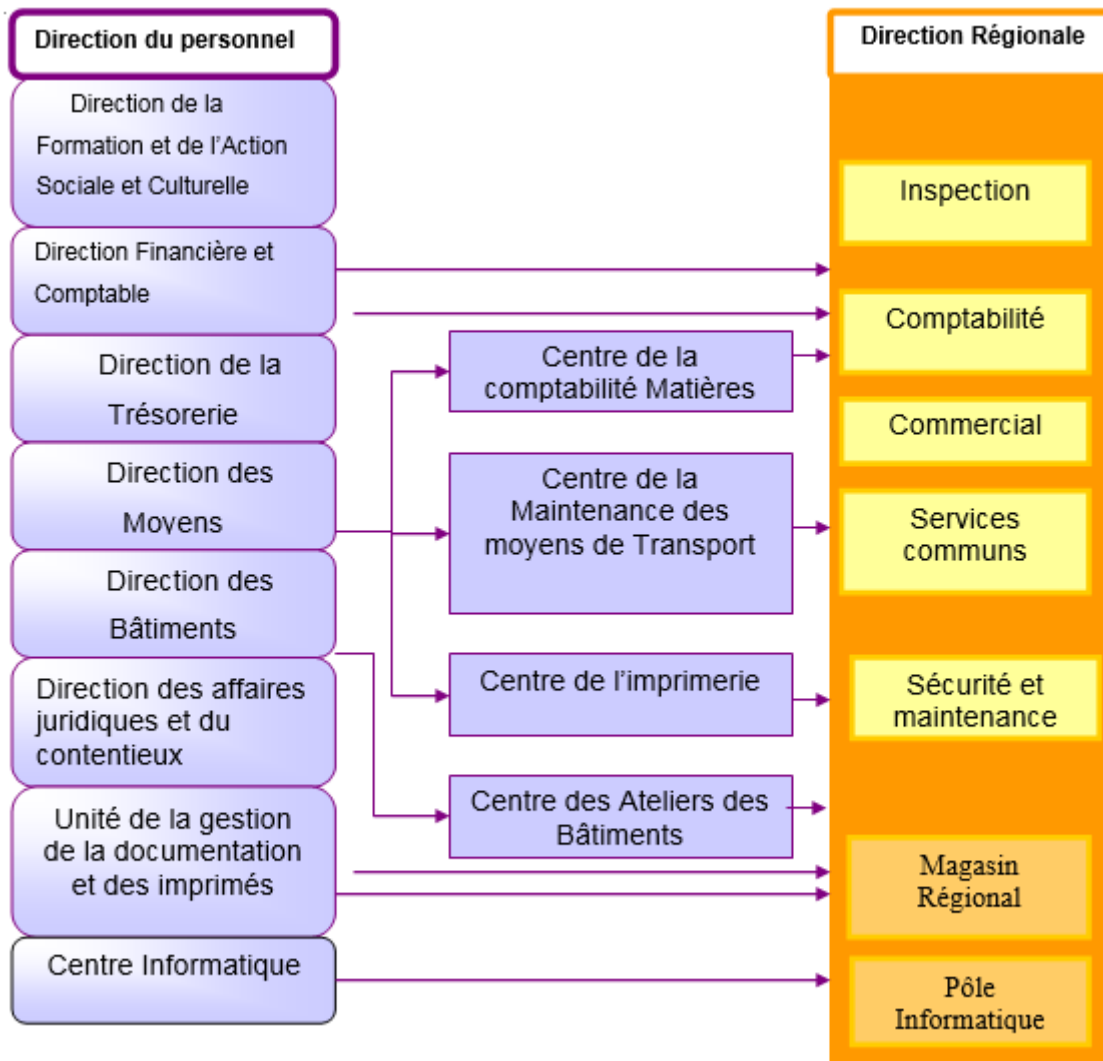


Figure 1:organigramme générale de la Poste tunisienne

Le centre informatique:

Est chargé de :

- L'exécution du chemin directeur de l'information et sa mise à jour, de même le développement de l'utilisation de l'informatique au niveau de différents services de l'ONP.
- L'exploitation et la maintenance des équipements et des programmes informatiques.
- La fixation de besoins en matière informatique et participation à l'élaboration des cahiers de charge des appels d'offres pour l'acquisition d'équipements informatiques.
- La participation à l'élaboration des programmes de formation et de recyclage.

- Le développement des programmes informatiques concernant les produits financiers.
- Le suivi et l'application des programmes de maintenance des équipements informatiques au niveau régional à travers les pôles régionaux.

II. Etude de l'existant

3. Description de l'existant

L'office national des postes possède un réseau informatique reparti sur tout le territoire tunisien (toutes les villes et les municipalités tunisiennes et même les zones rurales) qu'on peut le décomposer selon les services.

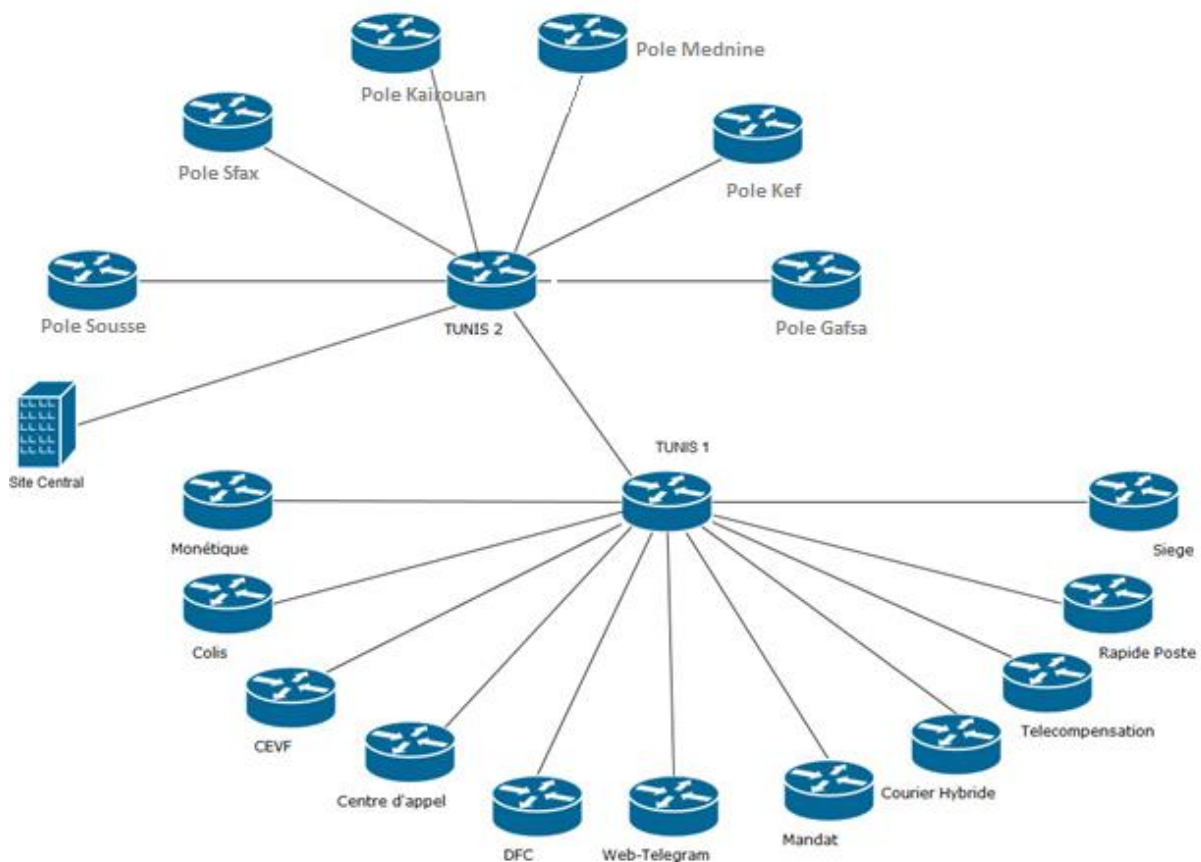


Figure 2: Schéma global du réseau informatique

Les réseaux principaux sont relatifs aux systèmes d'informations suivants :

- **Le système d'informations financier** qui gère les opérations financières. Il est fondé autour d'un réseau informatique décentralisé d'architecture à trois niveaux : Central, régional et local qui se communique les informations via des réseaux étendu et locaux.

- **Le système de gestion du courrier postal IPS (International Postal System)** : Permet la gestion, le contrôle et le suivi du courrier à l'échelle nationale et internationale. Il est bâti autour d'un réseau informatique décentralisé reliant d'une part, le siège par les agences via le réseau étendu et d'autre part, le siège par l'UPU à travers le réseau SITA.
- **Le système de gestion** : permet de gérer le budget, la comptabilité et les ressources humaines de la poste. L'architecture de ce système est centralisée et elle est en cours de migration vers une architecture décentralisée à trois niveaux : site central, recettes régionales et bureaux de postes.

Ce réseau comporte aussi des pôles régionaux qui sont répartis dans toute la république selon l'emplacement géographique des habitants et on trouve 8 pôles qui sont :

TUNIS-I, TUNIS-II, SOUSSE, KAIROUAN, KEF, GAFSA, SFAX, MEDNINE.

Chaque bureau de poste est doté d'un réseau local en étoile formé d'un serveur, des ordinateurs tournant les applications guichet, des modems, des routeurs, des serveurs optionnels ...

Comme montre la figure 3, un bureau de poste est lié à un pôle informatique et par son intermédiaire à la direction régionale pour l'application comptabilité.

Il est ensuite lié par l'intermédiaire du routeur du pôle aux différents sites centraux tels que le mandat électronique, la télécompensation, la comptabilité, rapide poste, centrale financière de Tunis-Hached ...

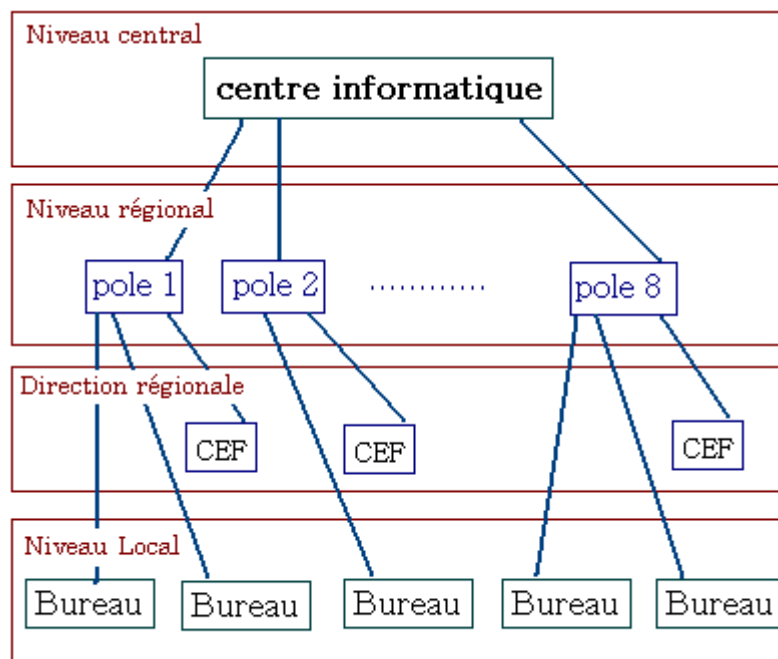


Figure 3: synoptique de la liaison entre les différents composants du réseau postal

Les routeurs repartis sur tous le territoire tunisien sont interconnectés entre eux par des liaisons ADSL et Sdsl sur le Backbone Tunisie Télécom.

Chaque bureau de poste a un routeur qui est relié à un pôle informatique à travers sa direction régionale. Tous les routeurs de réseaux sont connectés à la centrale informatique soit par une liaison directe ou indirecte (figure3).

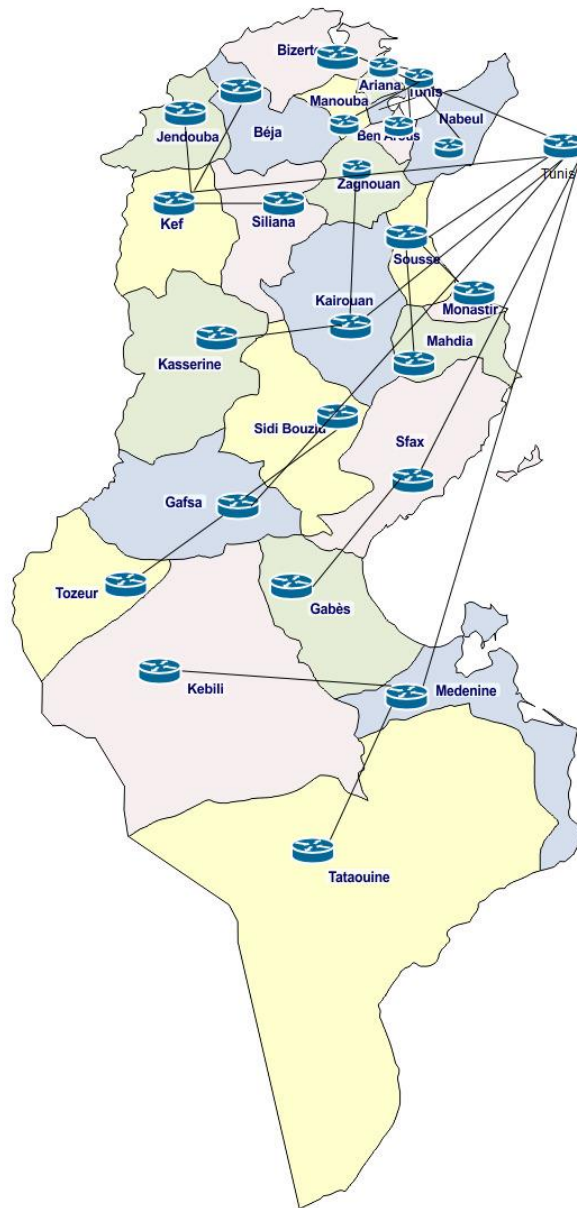


Figure 4:Synoptique d'interconnexion de différentes parties du réseau national

La figure5 suivante montre l'exemple du gouvernorat de Siliana pour montrer comment les réseaux locaux sont centralisés via la direction régional puis connectés au pôle informatique du kef.



Figure 5:centralisation des locaux au direction generale de Siliana

Au niveau local/bureau de poste, on trouve généralement :

- Un serveur avec système Windows server 2003
- Un Switch ou plusieurs administrable avec configuration du VLAN
- routeur Cisco.
- Les Pc des personelles sous le domaine par exemple D*** et authentifie par le matricule de l'agent.

- Des onduleurs pour l'armoire des réseaux branché avec câble USB au serveur pour la suivi de L'état de la batterie.
- Les imprimantes et DAB

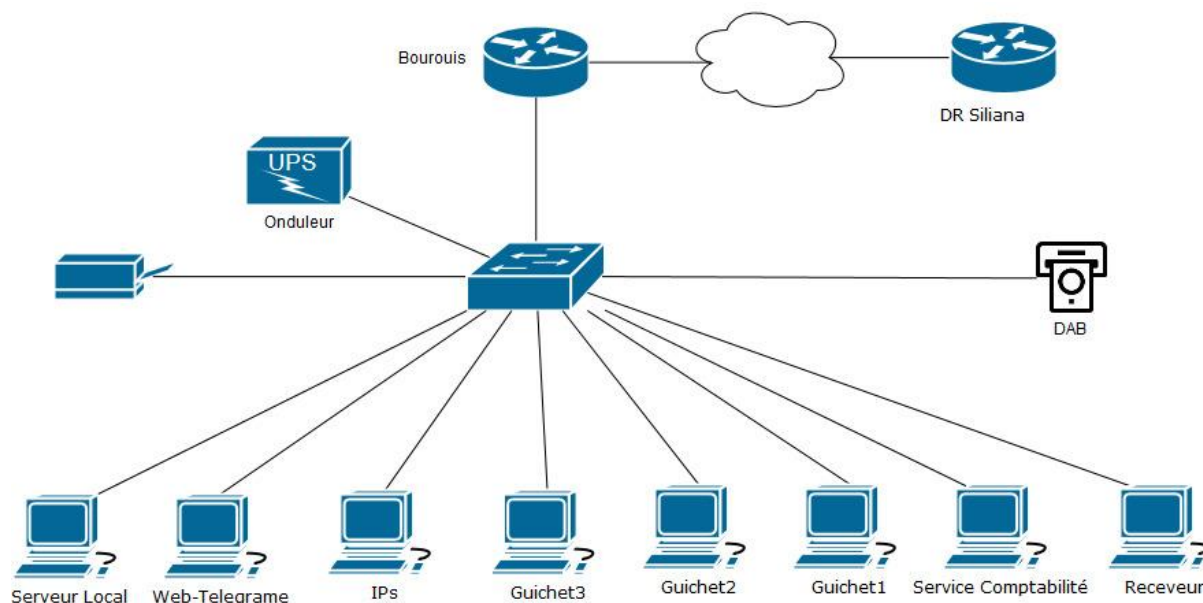


Figure 6: reseau local du bureau de poste Bourouis

Ce réseau ne cesse pas à s'étendre chaque jour et le nombre de ses composants augmente

4. Critique de l'existant

Ayant un très grand nombre de serveurs à gérer, les administrateurs centraux et régionaux sont incapables d'effectuer la vérification de leurs disponibilités (sont en ligne ou non), et la détermination de la qualité des services offerts, ni la détection de la défaillance des équipements (Etat mémoire, surcharge du disque, charge CPU ...), ni les surcharges temporaire des ressources. La seule méthode de détection ces anomalies est seulement par la réception des différentes plaintes et réclamations des utilisateurs dans les différents bureaux.

Ayant souci de sa réputation et visant la satisfaction et le confort de ses clients, la Poste Tunisienne veut à tout prix, éviter la confrontation à des clients mécontents d'où leur perte.

Pour cela, l'ONP travaille tous le temps pour offrir des services de haute qualité, en anticipant les pannes et éviter l'arrêt de ses services qui peuvent causer de graves conséquences sur le plan financière et organisationnelles

5. Solution proposée

La gestion des serveurs distants et la supervision des réseaux étant le plus grand souci des administrateurs, Et afin de pallier aux problèmes cités ci-dessus, la poste tunisienne m'a proposé de mettre en place un système de supervision réseau. Pour gérer le fonctionnement du réseau, d'analyser les données collectées et de définir des minimums d'alertes qui peuvent servir afin de déclencher des alertes lors de détection des problèmes.

Il s'agit d'une solution pour prévoir les pannes proposées en suivant le fonctionnement du système et en surveillant le statut des équipements, des différents services et d'offrir des informations supplémentaires voir mémoire disponible, charge CPU, espace disque, mémoire disponible, etc.

Un système de supervision offre à son utilisateur la possibilité de répondre rapidement aux alertes des pannes qui peuvent intervenir afin d'éviter un arrêt d'un service pour une longue durée.

6. Conclusion

Dans ce chapitre on a entamé de manière générale la structure de réseau informatique de la poste tunisienne, son architecture et ses problèmes et la solution pour l'améliorer.

Dans le chapitre suivant on va essayer de mieux expliquer la solution proposée.

Chapitre II :Etat de l'art

Dans ce chapitre on va commencer par la mise en point sur l'importance de la supervision et la définition d'un tel système de supervision, puis on va passer au domaine de surveillance suivi par une présentation des différentes solutions qui existent sur le marché, et on va finir par le choix de solution.

I. nécessité de la supervision

Dans nos jours, les réseaux informatiques relient tous, mais avant l'échange des données entre les hôtes, il faut savoir si ce lien peut être établi ou non.

Pour cela, il faut vérifier l'état de réseaux et des équipements pour y accéder et modifier les données.

On peut définir la supervision de réseaux comme l'exploitation de ressources réseaux adaptées afin d'avoir des informations sur l'utilisation et la condition de réseau et ses composants dans le but de garantir un bon niveau des services.

Afin d'atteindre cet objectif, on va mettre en place un système de surveillance avec des tâches bien déterminées.

II. les fonctionnalités d'un système de surveillance

Le but principal d'une mise en place d'un système de supervision réseau est la collection régulière des données nécessaires concernant l'état de ce dernier et de les étudier.

Une telle solution de supervision réseau doit être réactive en alertant l'administrateur en cas d'arrêt d'un tel composant de réseau.

En plus elle doit prévoir les dysfonctionnements probables et les cibler dès son apparition

Parmi les multiples fonctionnalités d'un système de surveillance réseau on peut citer :

- Supervisions des services réseaux: (HTTP, SMTP, ICMP, SNMP, LDAP POP3, NNTP, etc.).
- Supervision des services des équipements et systèmes (charge mémoire, CPU ...)
- Le contrôle distant automatisé des états des hôtes et des objets nécessaires au bon fonctionnement via les plugins
- Représentation claire et distinctes (couleurs) des états.
- Gestions des avertissements

- L'universalité afin de bien Contrôler n'importe quel processus des différents hôtes.

III. Domaine de supervisions

Le but de la supervision est le suivi du bon fonctionnement d'un système ou activité.

Les cibles de la surveillance peuvent être classées comme suit :

- infrastructure réseaux :

La supervision réseau porte sur la surveillance de manière continue de la disponibilité des services en ligne, du fonctionnement, des débits, de la sécurité mais aussi du contrôle des flux.

- Infrastructure Système

La supervision système porte principalement sur les trois types principaux de ressources système : le processeur, la mémoire, le stockage, les commutateurs, bases de données, les serveurs...

- Infrastructure applicative

La supervision des applications (ou supervision applicative) permet de connaître la disponibilité des machines en termes de services rendus en testant les applications hébergées par les serveurs.

Ce type de supervision est basé sur les flux de service en utilisant des tests d'où la validation fonctionnelle.

IV. solutions open source

Un logiciel Open Source est un programme informatique dont le code source est distribué sous une licence permettant à quiconque de lire, modifier ou redistribuer ce logiciel.

Le tableau suivant résume de façon générale les avantages et les inconvénients des solutions open source :

Avantages	inconvénients
<ul style="list-style-type: none"> - coût d'acquisition faible. - Développements additionnels peu coûteux et riches. - Respect des standards. - Indépendance des fournisseurs 	<ul style="list-style-type: none"> - Support difficile. - Prolifération des licences - Transparence

Tableau 1:avantages et inconvénients des solutions open source

Dans ce qui suit on va énumère quelques exemples des solutions de monitoring qui existe dans le marché.

- Monit :

Il s'agit d'une solution open source qui surveille non seulement un serveur, mais aussi elle a pour objectif d'anticiper les problèmes grâce à des mesures pris pour certain scenarios et l'automatisation de différentes réactions et redémarrage des services

- Ganglia :

C'est un outil open source destiné généralement à la supervision des systèmes en cluster.

Il utilise des structures de données et d'algorithmes soigneusement conçues pour atteindre de très faibles frais généraux par nœud et haute concurrence.

- Nagios

Nagios est une référence dans le domaine de supervisions des infrastructures informatique.

C'est vrai que l'installation et la configuration de Nagios est un peu compliqué, mais tous ca est négligeable devant sa richesse en terme de fonctionnalités qui sont intégrales par rapport aux autres solutions qui existe sur le marché.

Nagios prend en charge la surveillance de plusieurs hôtes et peut envoyer des alertes par email, pager (si vous utilisez encore cette technologie ancienne) ou la messagerie texte / SMS.

Comme l'argent, il peut également être configuré pour répondre automatiquement à des problèmes.

Nagios est un outil de surveillance réseau puissant qui aide à assurer que les systèmes critiques, les applications et les services sont toujours en marche. Il fournit des fonctionnalités telles que les alertes, gestion des événements et des rapports.

Nagios XI est la version de classe entreprise pré-configuré construit sur Nagios de base et soutenue par une société commerciale qui offre un soutien et des fonctionnalités supplémentaires telles que plus de plugins et de reporting avancé.

- Zabbix

Zabbix est un outil de surveillance riche en fonctionnalités.

Il a un grand soutien de visualisation y compris les vues définies par l'utilisateur, le zoom et la cartographie.

Il peut envoyer des alertes par e-mail, SMS ou un message instantané.

Il fournit également des alertes sonores, qui peuvent être utiles lorsque vous êtes physiquement près de la machine de surveillance.

- Cacti

Cacti est un logiciel libre de mesure de performances réseau et serveur basé sur la puissance de stockage de données de RRDTool. Il est souvent utilisé avec des logiciels de supervision (par exemple Nagios), mais il ne fait pas de supervision en tant que tel. Il ne fait pas de corrélation d'incidents ni d'alerte en cas d'incident (bien que des plugins existent, ce n'est pas son but premier).

V. solutions propriétaires

Bien évidemment est comme tout domaine, il y a en matière de surveillance informatique des solutions payantes qui ont des avantages et des inconvénients aussi comme montre le tableau suivant :

avantages	inconvénients
<ul style="list-style-type: none"> - Solutions globales et éprouvés - Périmètres techniques et fonctionnels étendus 	<ul style="list-style-type: none"> - Coût d'acquisition et de support - Incompatibilités entre fournisseur à choix d'un fournisseur unique - Développement additionnel restreint et coûteux

Tableau 2:avantages et inconvénients des solutions propriétaires

Parmi les solutions de supervision propriétaires, on cite à titre d'exemple :

- HP Open View

HP OpenView est l'ancien nom d'une famille de produits Hewlett Packard qui consistait de produits de réseau et de gestion des systèmes.

En 2007, HP OpenView a été rebaptisé HP BTO (Business Technology Optimization) Software quand il est devenu partie de la division HP Software. Les produits sont maintenant disponibles sous forme de produits HP, commercialisés par la division HP Software.

Logiciel HP OpenView fourni système à grande échelle et la gestion de réseau de l'infrastructure informatique d'une organisation. Il comprenait des modules optionnels de HP ainsi que des logiciels de gestion tiers, qui reliait dans un cadre commun et a communiqué avec un de l'autre.

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

- Big Brother

Superviseur simple de services fonctionnant sous Windows NT.

Il est efficace mais ne permet de superviser qu'un nombre restreint de services (http, pop, nntp, smtp et quelques autres).

De plus on ne peut lui ajouter de nouvelles fonctionnalités et il est incapable de remonter les alarmes autrement que graphiquement (pas d'envoi de mail ou de sms).

- PRTG

PRTG (*Paessler Router Traffic Grapher*) est un logiciel qui permet grâce à l'analyse de trames SNMP de créer des graphiques sur le trafic réseau. PRTG est aussi capable de faire du sniffing.

VI. choix de la solution de supervision

Il existe différents types d'outils de supervision ayant chacune leurs qualités et leurs défauts :

- Solutions propriétaires coûteuses
- Utilisation d'outils open source qui ont fait leurs preuves

Le choix d'une telle solution de supervision doit répondre beaucoup de critères afin de s'adapter avec le réseau cible qui est ce développe de temps en temps avec une diversité d'équipements variables.

Donc le choix des outils de supervision pour ce comparatif s'est fondé sur plusieurs facteurs :

- Totalement Open-source
- Encore supportés
- Permettent une génération de « graphs »
- Fonctionnent sur différents équipements (switchs, routeurs, serveurs, ...)
- Dispose d'une interface web
- Gère le SNMPv3
- Avertissent les administrateurs en cas de problèmes

On a synthétisé notre étude de choix par un tableau comparatifs sur les différents logiciels libres.

Logiciel	Open source	cartographie	interface web	SNMPv3	Avertissement
PRTG	Non et très couteux	non	Viewing	limité	oui
Zabbix	Oui	oui	oui	oui	oui
HP Open View	Non et très couteux	non	inconnu	inconnu	inconnu
Cacti	Oui	oui	oui	oui	oui
Nagios	Oui/free	oui	oui	supporté	oui

Tableau 3: Comparaison entre différentes solutions de supervision

VII. Conclusion

Dans ce chapitre on a entamé le cadre générale du projet et on a présenté la supervisions et l'architecture des différents réseaux de l'ONP pour atteindre la solution proposée afin d'entamer la partie conceptuelle.

Chapitre III :

Spécification des besoins et architecture

Dans le chapitre présent, on va commencer par la spécification des besoins et les fonctionnalités que notre application doit offrir aux différents utilisateurs puis on va passer la présentation de l'architecture du notre projet

I. Analyse des besoins :

L'objectif de notre travail consiste à mettre en place une solution de supervision du réseau de la poste tunisienne.

Cet outil doit être capable de superviser les équipements réseau et assure la gestion des alarmes en cas de problèmes pour aider les administrateurs à intervenir rapidement pour minimiser l'indisponibilité du système.

1. Besoins Fonctionnels

Les besoins fonctionnels sont :

- La gestion des utilisateurs : facilités d'ajout et de suppression des utilisateurs en assurant la confidentialité
- gestion des équipements a supervisé : facilités d'ajout et de suppression des nouvelles hôtes à superviser avec flexibilité de classification de ces derniers
- la solution doit assurer la sécurité en gérant les droits d'accès
- gestion des incidents en visualisant clairement les états et alertes et les enregistrer
- Gestion du trafic

1. Besoins non Fonctionnels

- espace de stockage des données suffisant
- la rapidité de réponse
- la facilité de maintenance

II. Architecture du projet

Comme on ne peut pas toujours travailler sur le réseau de la poste tunisienne directement chaque fois pour des raisons de sécurité et de disponibilité, on a utilisé une maquette réseau réalisée sur gns3.

On a cloné une partie du réseau qui représente la connexion entre le centre informatique (lieux de mise en place de notre solution) et quelque routeur placé dans des différentes places sur le territoire tunisien.

Le serveur contenant Nagios et Cacti est place dans le centre informatique, exactement dans le service maintenance réseau.

Il est connecté au LAN du service maintenance qui est relié au switch Edge siège à travers le routeur du service.

Le switch Edge est connecté directement avec le data centre, a un switch Core pour l'accès à l'internet et a un autre switch Edge qui rassemble tous les connexions avec les différents composants du réseau de l'ONP.

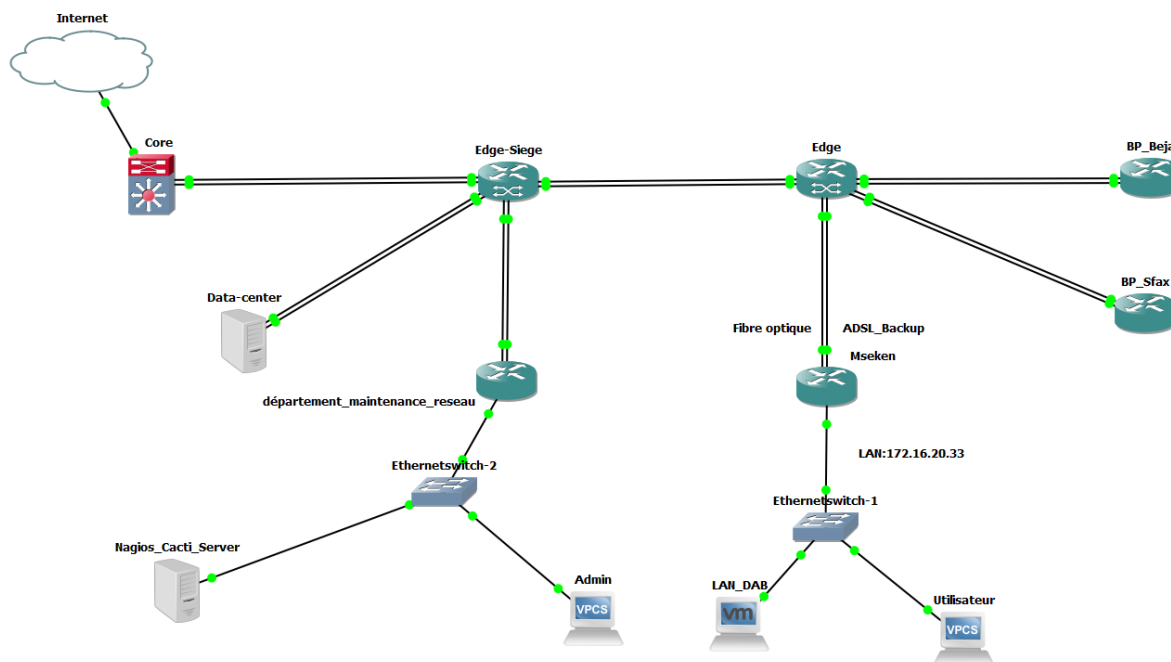


Figure 7:maquette de test sous GNS3

Dans ce qui suit on va définir et expliquer le rôle des différents composants mentionnés dans la figure7 :

Switch Core : il s'agit d'un switch de grande capacité généralement qui est placé dans le backbone, il sert comme une passerelle entre le réseau de la poste vers Internet.

Ils constituent le point d'agrégation final du réseau et permettent à plusieurs modules d'agrégation de fonctionner ensemble.

Switch Edge : c'est un switch situé au point de rencontre de deux réseaux. Ces dispositifs connectent les réseaux locaux d'un bureau de poste ou d'un département comme celui de la maintenance réseau mentionné dans la figure 7 aux réseaux des fournisseurs de services Internet (Tunisie Télécom)

Data-Center : c'est placé dans le même bâtiment de centre informatique à Tunis-Hached II comprend les différents serveurs (Mandats, Refonte ...) et les bases de données des différents services et leur backup, des alimentations redondantes ou de secours, des connexions de communication de données redondantes, des contrôles environnementaux (par exemple, la climatisation, la suppression des incendies) et divers dispositifs de sécurité.

Serveur Nagios/Cacti :

Il s'agit d'une machine qui tourne linux et qui englobe deux solution de supervision réseau ; Nagios et Cacti.

En générale, il est conseillé d'utiliser plusieurs machines distribuées dans le réseau pour éviter les blackouts complets, c.-à-d. on mais un serveur de supervision dans chaque réseau local qui remonte les informations au serveur situé au central informatique, mais dans notre projet on

va utiliser un seul serveur de supervision placé au département maintenance réseau afin de tester la solution.

L'emplacement du serveur est défini de façon qu'il ait la possibilité d'accéder à un maximum de composant réseaux de la poste tunisienne et manipulable directement par l'équipe de maintenance.

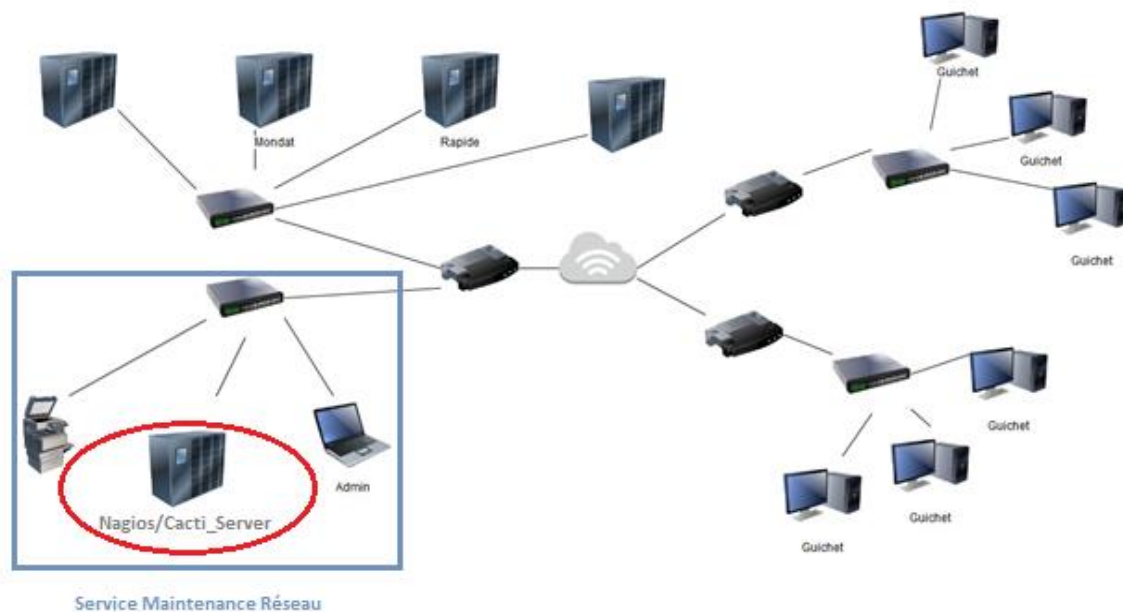


Figure 8: Emplacement de mise en place de Nagios dans le réseau de la poste

Parmi la fonctionnalité de Nagios on cite :

- Supervision des services réseaux (http, POP3, DAP, SMTP..), équipements et ressources systèmes (CPU, mémoire...) sous n'importe quel système d'exploitation
- Détermination des états des ressources de façon automatique et à distance (via SSH, SSL).
- Présentation cartographique et coloré de réseaux avec les états des différents services.
- Gestion des alertes
- Facilité de gestion des Plugins et leur adaptation (puisqu'ils sont écrits en Bash, C++, Python...).

Nagios a comme architecture serveur-agent.

Le serveur joue le rôle d'un point central qui collecte les informations des équipements surveillés ou il y a des agents installés.

On peut généralement décomposer cette architecture en trois grandes parties :

- Un noyau : qui représente le cœur du serveur Nagios, il est lancé sous forme de démon et collète et analyse les informations, et organise l'ordonnancement des vérifications, la réaction et la prévention.

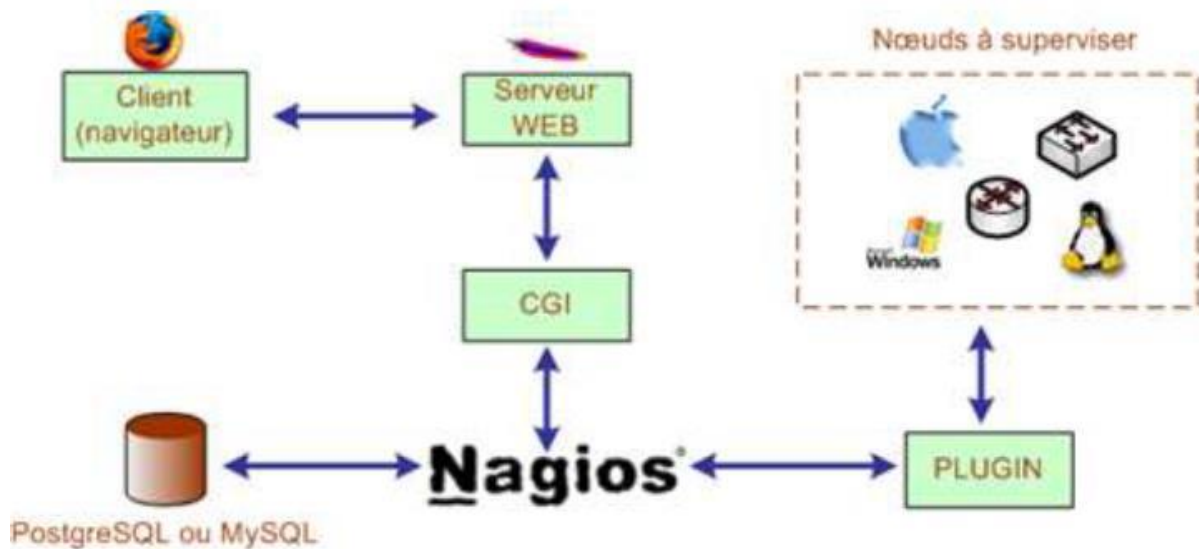


Figure 9:Architecture Nagios

- Les exécuteurs : ce sont les plugins qui sont responsable d'exécuter les tests et les contrôles sur les hôtes locaux ou distants et l'émission des résultats vers le noyau
 - IHM : il s'agit d'une interface graphique qu'on peut l'y accéder via le web
- Cette interface est fournie par défaut lors de l'installation du Nagios, elle représente les états des équipements du réseau surveillé.

Cacti est un outil de surveillance et de graphisme de réseau open-source, basé sur le Web, conçu comme une application frontale pour l'outil de journalisation de données open-source et standard de l'industrie RRDtool. Cacti permet à un utilisateur d'interroger des services à des 28 intervalles prédéterminés et de représenter graphiquement les données résultantes. Il est généralement utilisé pour représenter les données de séries chronologiques de métriques telles que la charge du processeur et l'utilisation de la bande passante du réseau. Une utilisation courante consiste à surveiller le trafic réseau en interrogeant un commutateur de réseau ou une interface de routeur via le protocole SNMP (Simple Network Management Protocol). Cacti fonctionne grâce à un serveur web équipé d'une base de données MySQL et du langage PHP. Il peut être considéré comme le successeur de MRTG et également comme une interface d'utilisation de RRDTool.

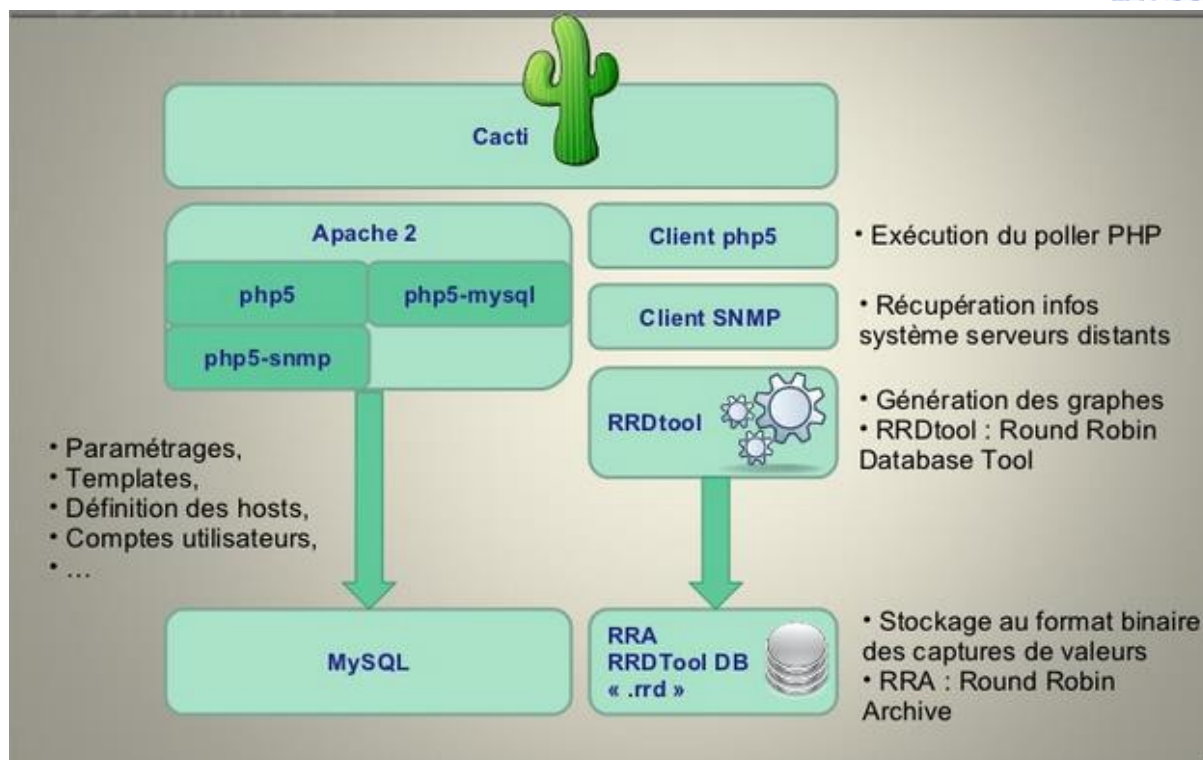


Figure 10:synoptique de l'architecture générale de Cacti

III. Conclusion

Dans ce chapitre on a présenté les compléments qu'on a choisis pour Nagios, il y'a ceux qui sont obligatoire comme les adons NRPE et NSClient, l'autre sont ajouter pour l'amélioration et la facilité d'utilisation et configuration de Nagios.

Dans le chapitre suivant on entamera le côté technique de notre projet et la mise en place de la solution.

Chapitre IV: Mise en place du système de supervision

Dans ce chapitre, on va commencer par la spécification de l'environnement de la mise en place de notre solution.

Puis on va entamer la mise en place du serveur Nagios _ Cacti

I. Environnements de mise en place

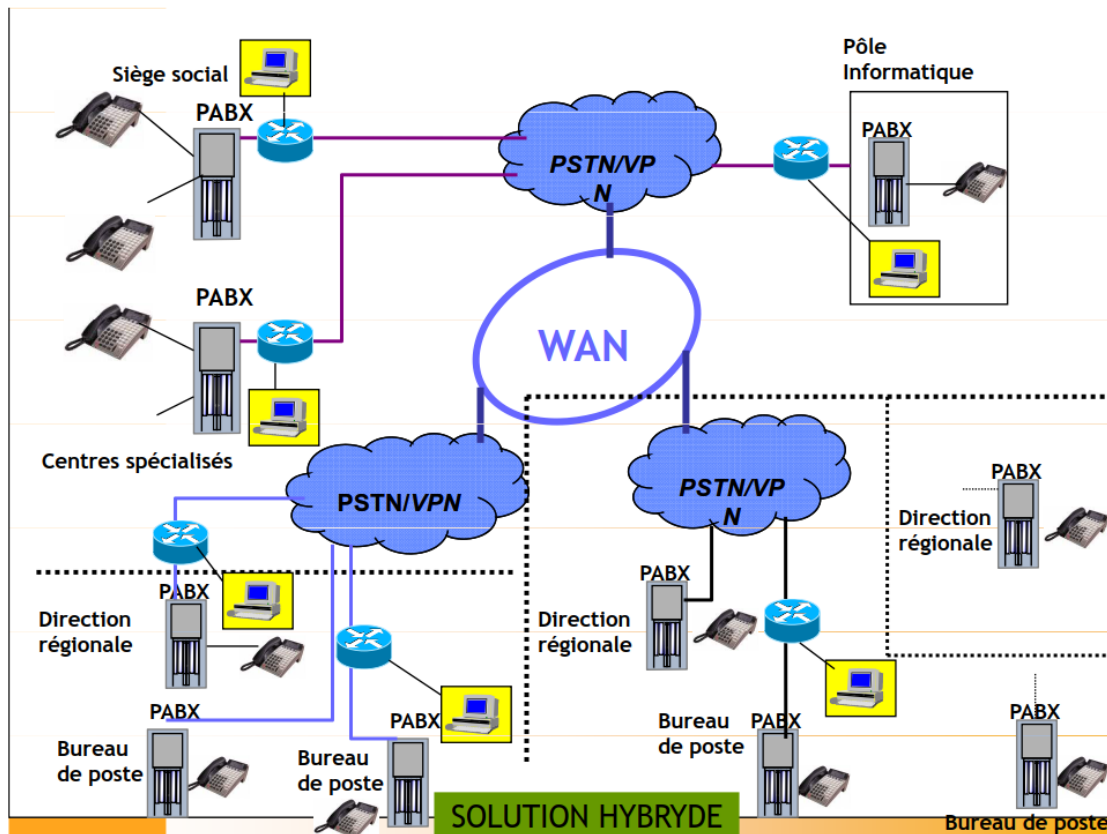


Figure 11: synoptique générale de la structure du réseau du ONP

La figure ci-dessus représente l'architecture simplifiée du réseau de la poste tunisienne en Tunisie dont ils ont besoin de la superviser.

Dans ce cas on a besoin d'une installation d'un serveur Nagios pour superviser tous ces ressources réseaux repartis sur toute la république tunisienne

1. Environnement matériel

- PC portable : TOSHIBA SATELLITE C855-139
- Processeur : i5-2450M CPU @ 2.50GHZ
- Mémoire : 8 Go

2. Environnement logiciel

On a installé le système d'exploitation Ubuntu sur ce serveur avec tous les outils nécessaires pour faire fonctionner notre solution.

Les outils installés sont les suivants :

- L'outil de supervision Nagios
- Nagios-plugins
- Cacti
- Le plugin NRPE pour la supervision des serveurs Linux.

II. Mise en place de Nagios/Cacti et les plugins

1. Pré-requis Nagios/Cacti

En plus que les plugins, Nagios à besoin de satisfaire certaines dépendances pour assurer la bonne installation.

Les prérequis à l'installation sont :

- Apache2, PHP5, MySQL
- bibliothèque Perl
- Les bibliothèques graphiques : GD, libgd libpng, libjpeg...
- Compilateur : gcc, gcc-gc++

2. Installation de Nagios/Cacti

Les étapes d'installation et de configuration de « Nagios4.1.1 », ses plugins « Nagios-plugins-2.1.1 » et « Cacti » seront détaillées dans l'annexe

Figure 12: interface état d'une hôte linux sur Nagios

3. Installation de NSClient

Pour superviser des hôtes Windows ; on a installé les plugins NSClient sur chaque hôte et vérifier la présence de la commande « check_nt ».

4. Installation de NRPE

Pour superviser des hôtes Linux ; on a installé les plugins NRPE sur chaque machine et vérifier la présence de la commande « check_nt ».

5. Interface Nagios / Cacti

Pour bien connecté le serveur au réseau de la poste tunisienne et affecter le test de la solution, on affecter à sa carte réseaux un adresse compris dans la plage de service maintenance comme montre la figure 13.

Obtenir une adresse IP automatiquement
 Utiliser l'adresse IP suivante :

Adresse IP :	192 . 168 . 52 . 25
Masque de sous-réseau :	255 . 255 . 255 . 0
Passerelle par défaut :	192 . 168 . 52 . 1

Figure 13: configuration de la carte réseau du serveur de supervision

La première étape à faire est l'authentification afin de bien sécuriser la solution.

Dès l'accès a Nagios ou Cacti via le navigateur on trouve directement une interface de saisie du login et mot d passe

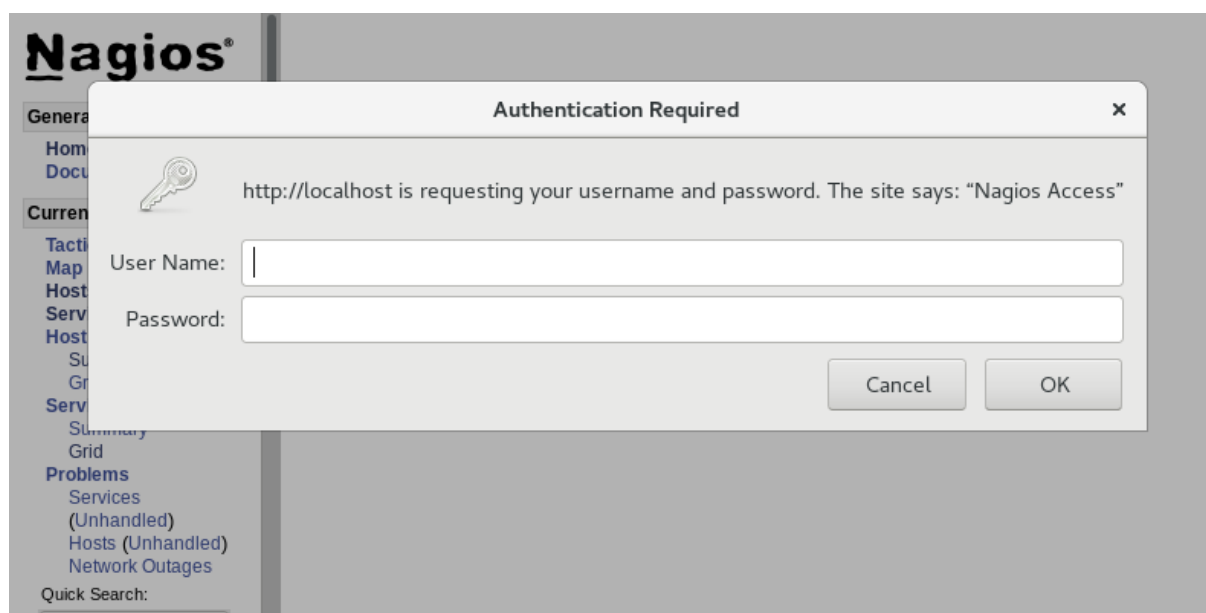


Figure 14: interface d'authentification Nagios



Figure 15:interface d'authentification Cacti

En accédant à la page d'accueil de Nagios on peut facile avoir une vue global sur notre solution.

Cette interface offre une facilité de navigation entre les différentes options de la solution puisque tout est noté et claire.

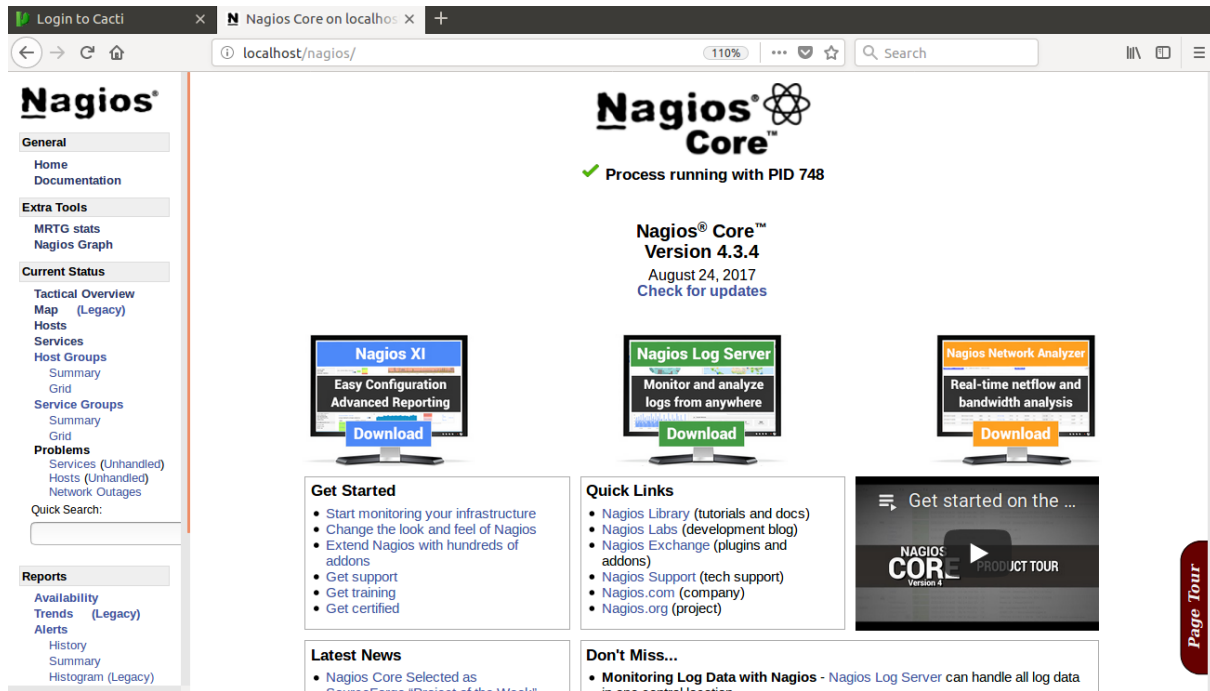


Figure 16:page d'accueil de Nagios

Même chose pour l'interface de Cacti, elle est aussi ergonomique est facile à manipuler (figure 17)

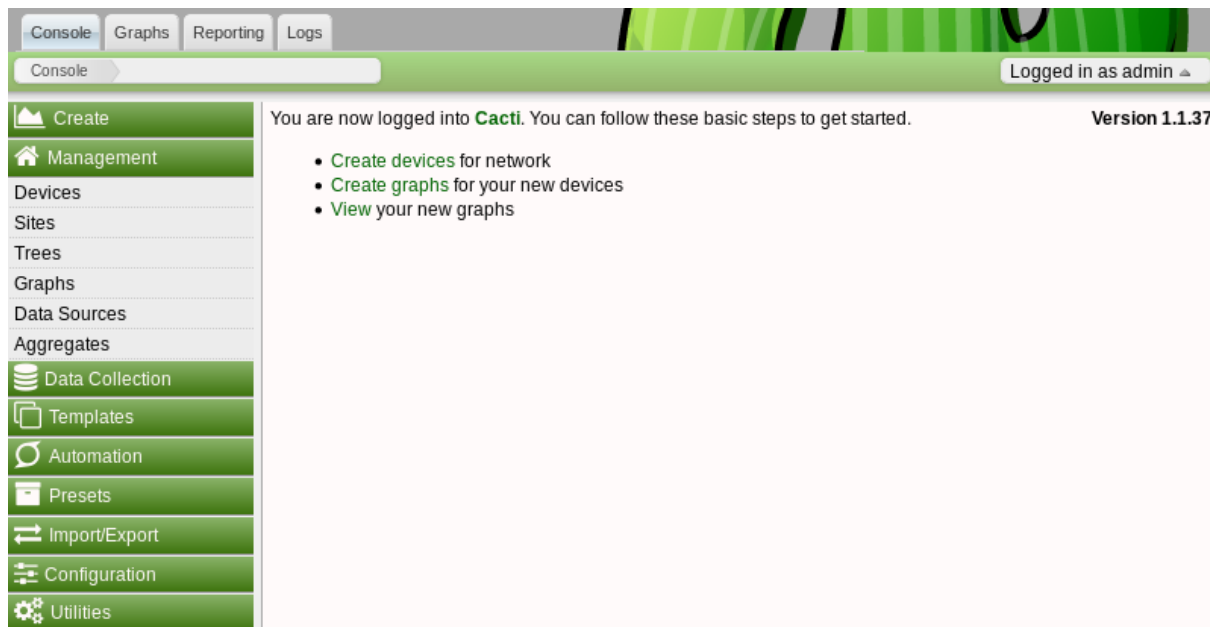


Figure 17:page d'accueil de Cacti

Nagios offre beaucoup d'options pour la surveillance du réseau, on peut les suivre de manières générale et globale avec l'option d'affichage en Map (figure19), ou sous forme d'une liste (figure18).

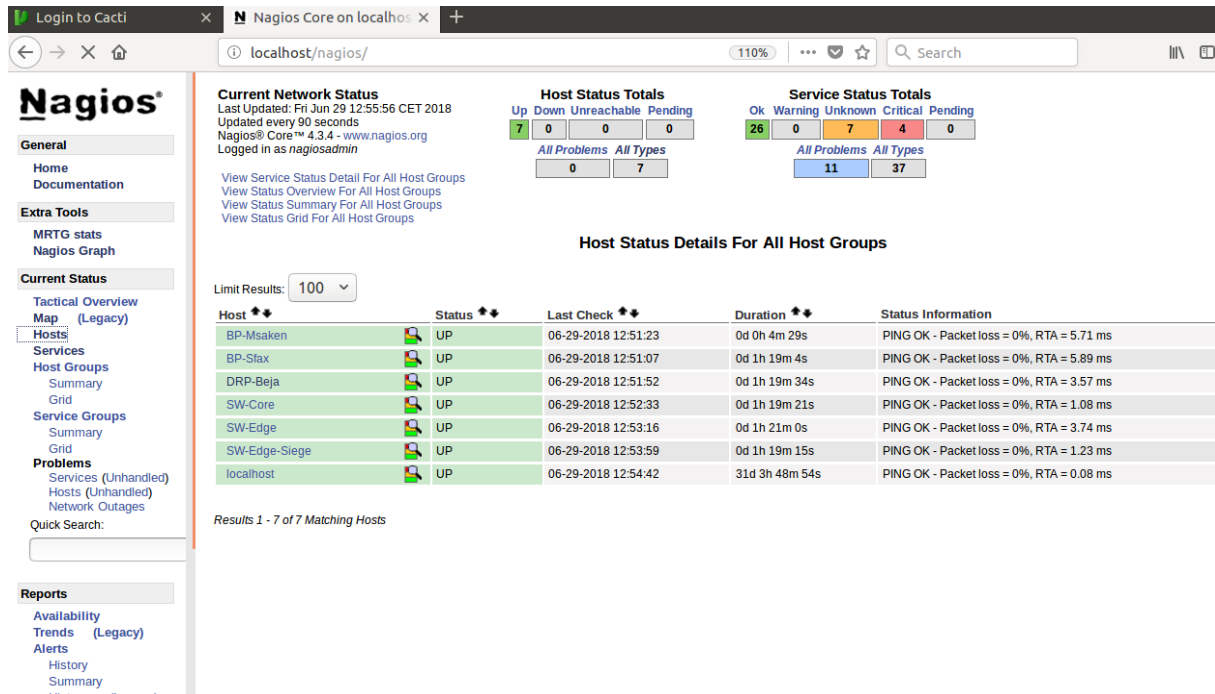


Figure 18: liste des hôtes supervisés par Nagios

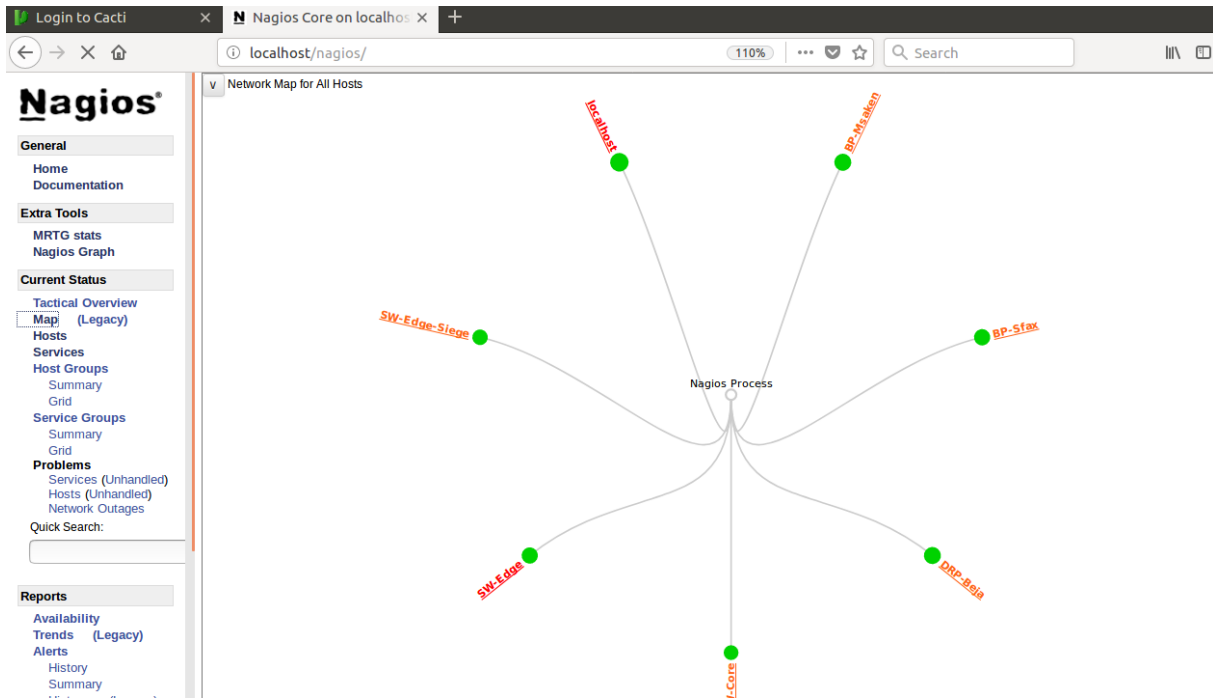


Figure 19: carte des hôtes supervisés par Nagios

En appuyant sur l'option « services », on peut avoir une vue globale des différents services des hôtes à superviser.

Comme montre la figure 20, chaque hôte est suivie par leurs services à Controller.

Host	Service	Status	Last Check	Duration	Attempt	Status Information
BP-Msaken	ADSL_Backup	OK	06-29-2018 12:51:57	0d 1h 13m 33s	1/3	ATM0/1/0:UP, ATM0/1/0-ads1:UP, ATM0/1/0-atm layer:UP, ATM0/1/0-aa15 layer:UP, ATM0/1/0-aa5 layer:UP, ATM0/1/0-0-atm subif:UP:6 UP: OK
	LAN	OK	06-29-2018 12:53:29	0d 1h 14m 1s	1/3	GigabitEthernet0/0:UP:1 UP: OK
	LAN_DAB	OK	06-29-2018 12:55:01	0d 1h 22m 29s	1/3	GigabitEthernet0/1:UP:1 UP: OK
	LS_MPLS	OK	06-29-2018 11:55:44	0d 1h 20m 57s	1/3	Ethernet0/0/0:UP:1 UP: OK
	PING	OK	06-29-2018 12:56:18	0d 1h 19m 34s	1/3	PING OK - Packet loss = 0%, RTA = 6.76 ms
	Uptime	UNKNOWN	06-29-2018 11:58:48	28d 17h 58m 6s	3/3	No OIDs specified
BP-Sfax	ADSL_Backup	OK	06-29-2018 12:52:10	0d 1h 13m 20s	1/3	ATM0/1/0-ads1:UP, ATM0/1/0-1-atm subif:UP, ATM0/1/0-0-aa15 layer:UP, ATM0/1/0-UP, ATM0/1/0.1-aa5 layer:UP, ATM0/1/0-atm layer:UP, ATM0/1/0.0-atm subif:UP, ATM0/1/0-aa15 layer:UP:8 UP: OK
	LAN	OK	06-29-2018 12:53:42	0d 1h 13m 48s	1/3	GigabitEthernet0/0/1:UP:1 UP: OK
	Liaison FO	OK	06-29-2018 12:55:14	0d 1h 12m 16s	1/3	GigabitEthernet0/0/0:UP, GigabitEthernet0/0.3248:UP, GigabitEthernet0/0.1223:UP:3 UP: OK
	PING	OK	06-29-2018 12:55:04	0d 1h 19m 57s	1/3	PING OK - Packet loss = 0%, RTA = 5.28 ms
	Uptime	UNKNOWN	06-29-2018 11:57:29	28d 17h 58m 6s	3/3	No OIDs specified
DRP-Beja	ADSL_Backup	OK	06-29-2018 11:51:01	0d 1h 15m 40s	1/3	ATM0/1/0-0-atm subif:UP, ATM0/1/0:UP, ATM0/1/0-ads1:UP, ATM0/1/0-0-aa15 layer:UP, ATM0/1/0-aa5 layer:UP, ATM0/1/0.1-aa5 layer:UP, ATM0/1/0-atm layer:UP, ATM0/1/0.1-atm subif:UP:8 UP: OK
	LAN	OK	06-29-2018 12:52:23	0d 1h 15m 7s	1/3	GigabitEthernet0/0/1:UP:1 UP: OK
	Liaison FO	OK	06-29-2018 12:53:55	0d 1h 13m 35s	1/3	GigabitEthernet0/0/0.123:UP, GigabitEthernet0/0.3190:UP, GigabitEthernet0/0/0:UP:3 UP: OK
	PING	OK	06-29-2018 12:52:17	0d 1h 19m 19s	1/3	PING OK - Packet loss = 0%, RTA = 3.84 ms
	Port Gi0/0/0 Usage	UNKNOWN	06-29-2018 11:56:10	28d 10h 45m 28s	3/3	check_mrtgtraf: Unable to open MRTG log file
	Uptime	UNKNOWN	06-29-2018 11:57:42	28d 17h 58m 5s	3/3	No OIDs specified
SW-Core	Connected to	OK	06-29-2018 11:51:14	0d 1h 15m 27s	1/3	GigabitEthernet7/37:UP:1 UP: OK
	PING	OK	06-29-2018 12:52:37	0d 1h 18m 54s	1/3	PING OK - Packet loss = 0%, RTA = 1.53 ms
	Uptime	UNKNOWN	06-29-2018 12:54:08	28d 17h 58m 5s	3/3	No OIDs specified
SW-Edge	FO_BTT	CRITICAL	06-29-2018 12:55:40	0d 1h 1m 50s	3/3	GigabitEthernet1/2/19:DOWN, GigabitEthernet1/2/14:UP, GigabitEthernet1/12:UP, GigabitEthernet1/2/15:DOWN, GigabitEthernet1/2/1:UP, GigabitEthernet1/2/11:DOWN, GigabitEthernet1/2/10:DOWN, GigabitEthernet1/2/16:DOWN, GigabitEthernet1/2/18:DOWN, GigabitEthernet1/2/13:UP, GigabitEthernet1/2/17:DOWN: 7 int NOK :

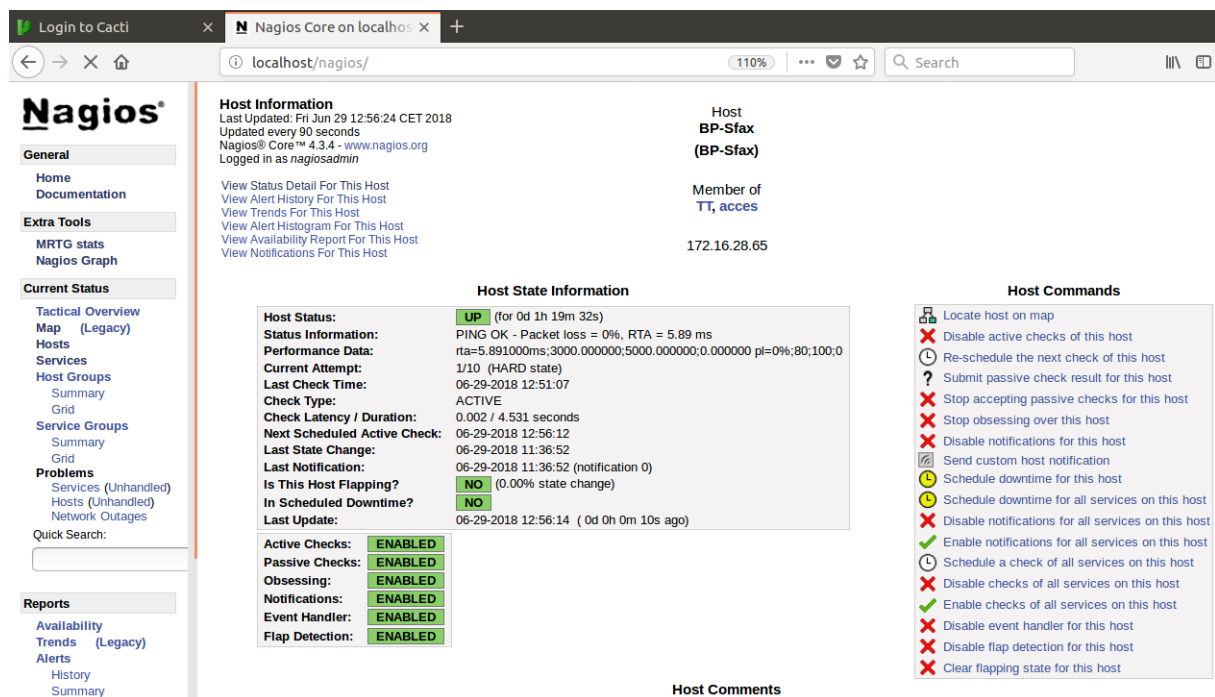
Figure 20: liste des hôtes supervisés par Nagios avec visualisations des différents ports et services

En cliquant sur une hôte on peut directement accéder aux services contrôlés avec plus de détails (figure21/22).

Limit Results: 100

Host	Service	Status	Last Check	Duration	Attempt	Status Information
localhost	Current Load	OK	06-23-2018 10:59:29	32d 8h 40m 18s	1/4	OK - load average: 0.04, 0.23, 0.20
	Current Users	OK	06-23-2018 11:00:07	32d 8h 39m 40s	1/4	USERS OK - 2 users currently logged in
	HTTP	WARNING	06-23-2018 10:55:44	32d 8h 39m 3s	4/4	HTTP WARNING: HTTP/1.1 403 Forbidden - 5179 bytes in 0.013 second response time
	PING	OK	06-23-2018 10:56:22	32d 8h 38m 25s	1/4	PING OK - Packet loss = 0%, RTA = 0.06 ms
	Root Partition	OK	06-23-2018 10:56:59	32d 8h 37m 48s	1/4	DISK OK - free space: / 3334 MB (40% inode=96%):
	SSH	OK	06-23-2018 10:57:37	32d 8h 37m 10s	1/4	SSH OK - OpenSSH_7.4 (protocol 2.0)
	Swap Usage	OK	06-23-2018 10:58:14	32d 8h 36m 33s	1/4	SWAP OK - 100% free (1022 MB out of 1023 MB)
	Total Processes	OK	06-23-2018 10:58:52	32d 8h 35m 55s	1/4	PROCS OK: 50 processes with STATE = RSZDT

Figure 21: etat de service pour une hôte Linux



The screenshot shows the Nagios Core web interface for host 'localhost/nagios/'. The main content area displays 'Host Information' for 'BP-Sfax (BP-Sfax)'. Key details include:

- Host Status:** UP (for 0d 1h 19m 32s)
- Status Information:** PING OK - Packet loss = 0%, RTA = 5.89 ms
- Performance Data:** rta=5.891000ms;3000.000000;5000.000000;0.000000 pl=0%;80;100;0
- Current Attempt:** 1/10 (HARD state)
- Last Check Time:** 06-29-2018 12:51:07
- Check Type:** ACTIVE
- Check Latency / Duration:** 0.002 / 4.531 seconds
- Next Scheduled Active Check:** 06-29-2018 12:56:12
- Last State Change:** 06-29-2018 11:36:52
- Last Notification:** 06-29-2018 11:36:52 (notification 0)
- Is This Host Flapping?:** NO (0.00% state change)
- In Scheduled Downtime?:** NO
- Last Update:** 06-29-2018 12:56:14 (0d 0h 0m 10s ago)

 Below this, there are sections for 'Host Commands' (e.g., 'Locate host on map', 'Disable active checks of this host') and 'Host Comments'. A left sidebar contains navigation menus for 'General', 'Extra Tools', 'Current Status', and 'Reports'.

Figure 22: les informations détaillées de la hôte BP_Sfax

L'interface « Devices » de Cacti offre presque les mêmes apparences que celle de Nagios.

Elle affiche tous les équipements à surveiller

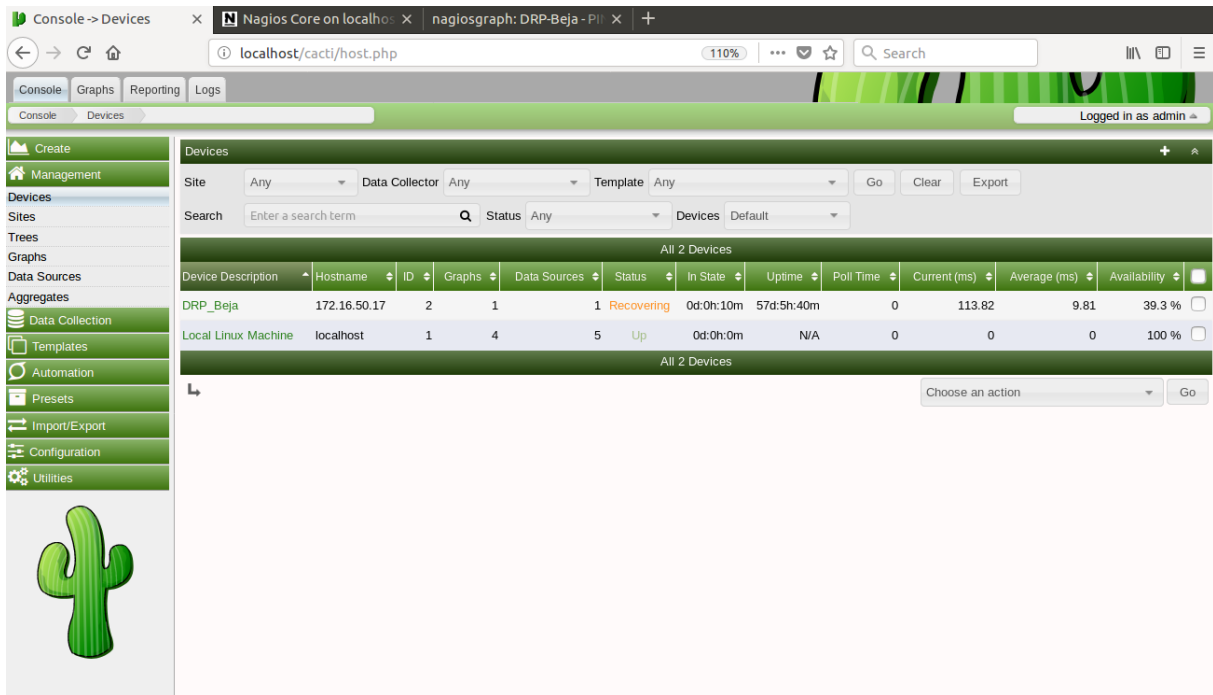


Figure 23: interface Devices dans Cacti

Les figures 24 et 25 montrent la manipulation et l'ajout de quelque hôte sur Cacti.

On peut constater que la manipulation de la solution est très simple mais efficace puisqu'elle donne la main à Controller différents paramètres

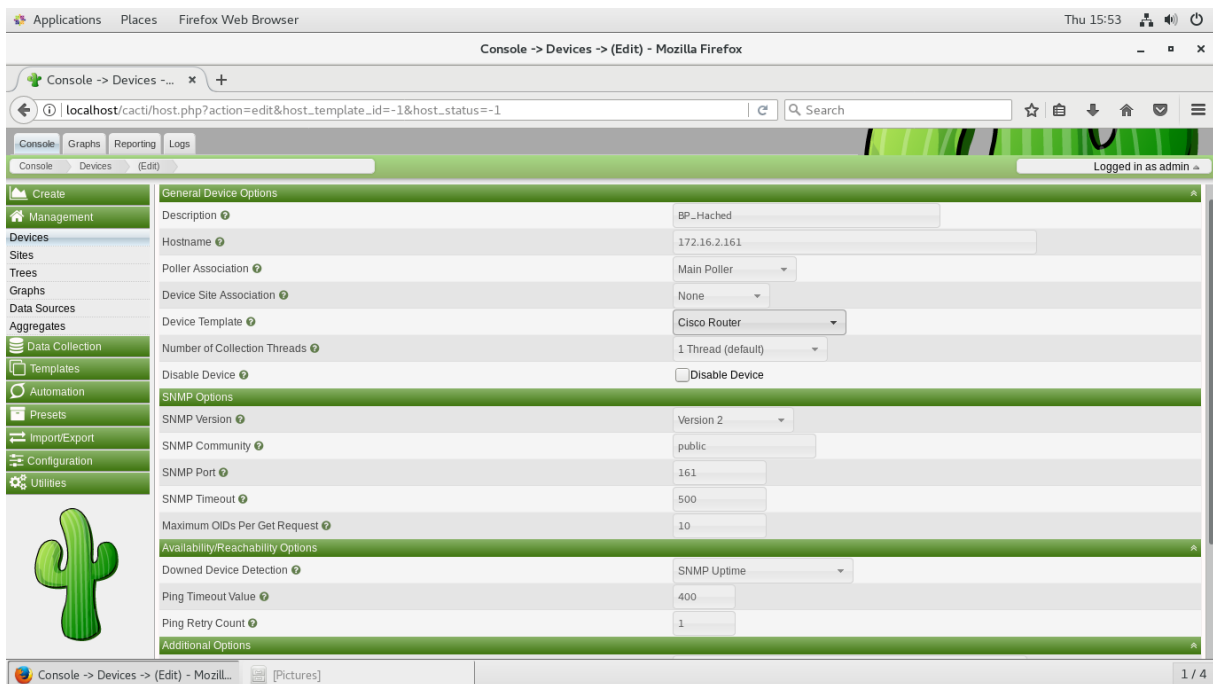


Figure 24: interface d'ajout d'un routeur sur Cacti

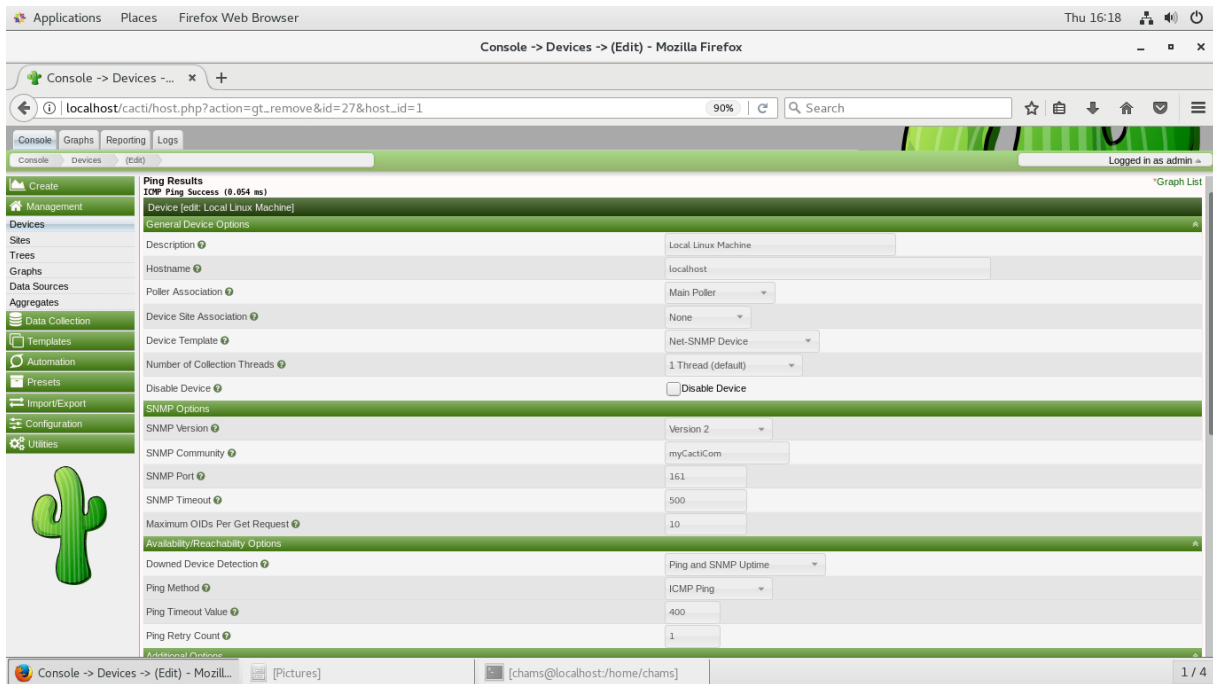


Figure 25: interface d'ajout d'une hôte Linux sur Cacti

Cacti aussi offre beaucoup d'option avec une représentation graphique du fonctionnement ou évolution d'état d'une hôte avec des graphes (figure26/27).

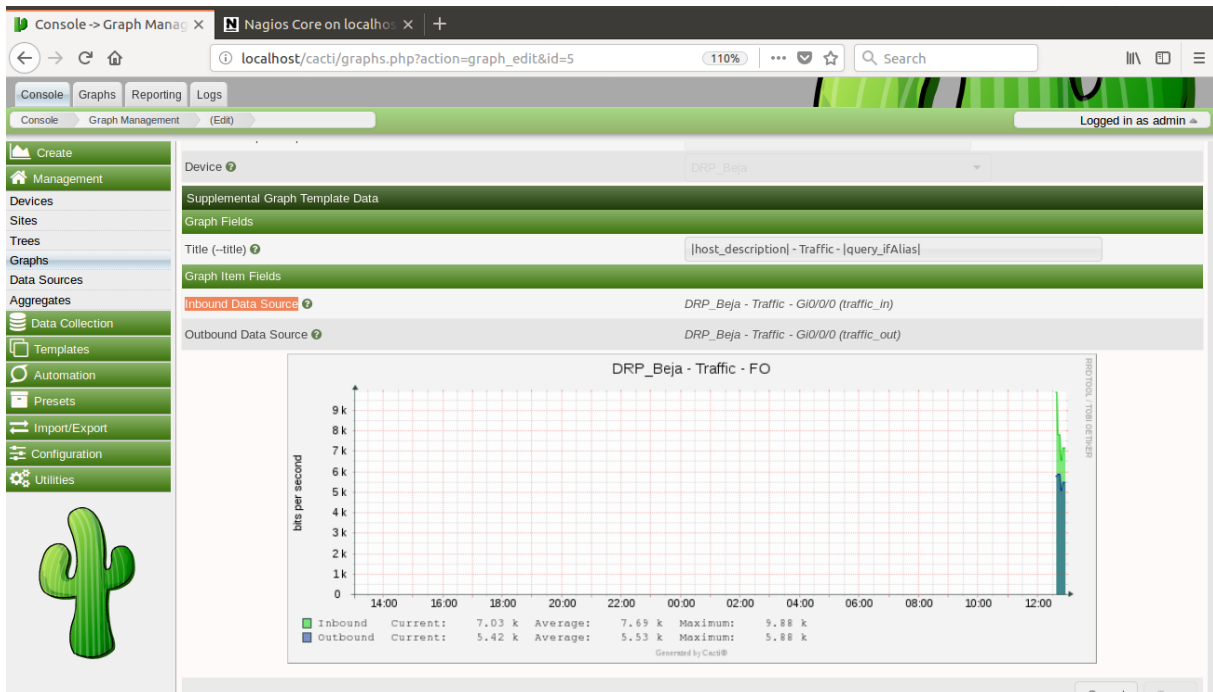


Figure 26: tracé de Traffic Fibre Optique de DRP_Beja

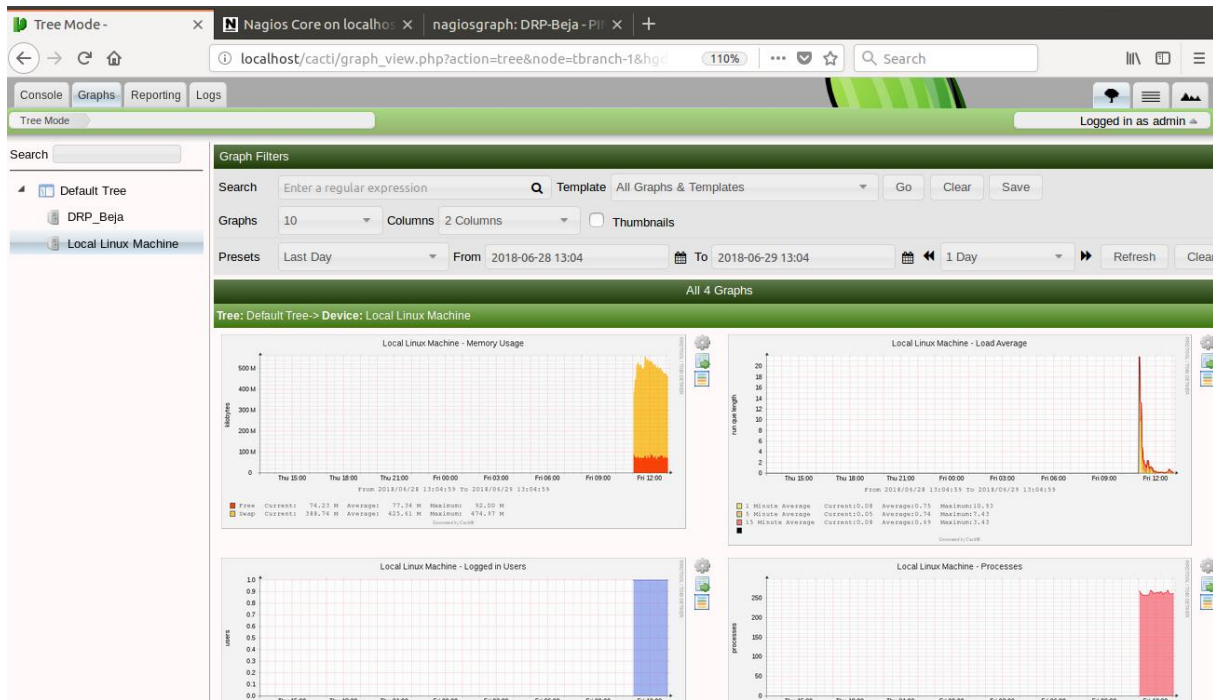


Figure 27: Graphes de différentes caractéristiques du Local host générés par Cacti

La solution qu'on a choisi offre la possibilité de Contrôler les paramètres de la hôte de façon graphique en donnant la possibilité de tracer des graphes d'évolution des caractéristiques systèmes en fonction de temps (figure26), ou bien à travers des fichiers LOG(figure28)

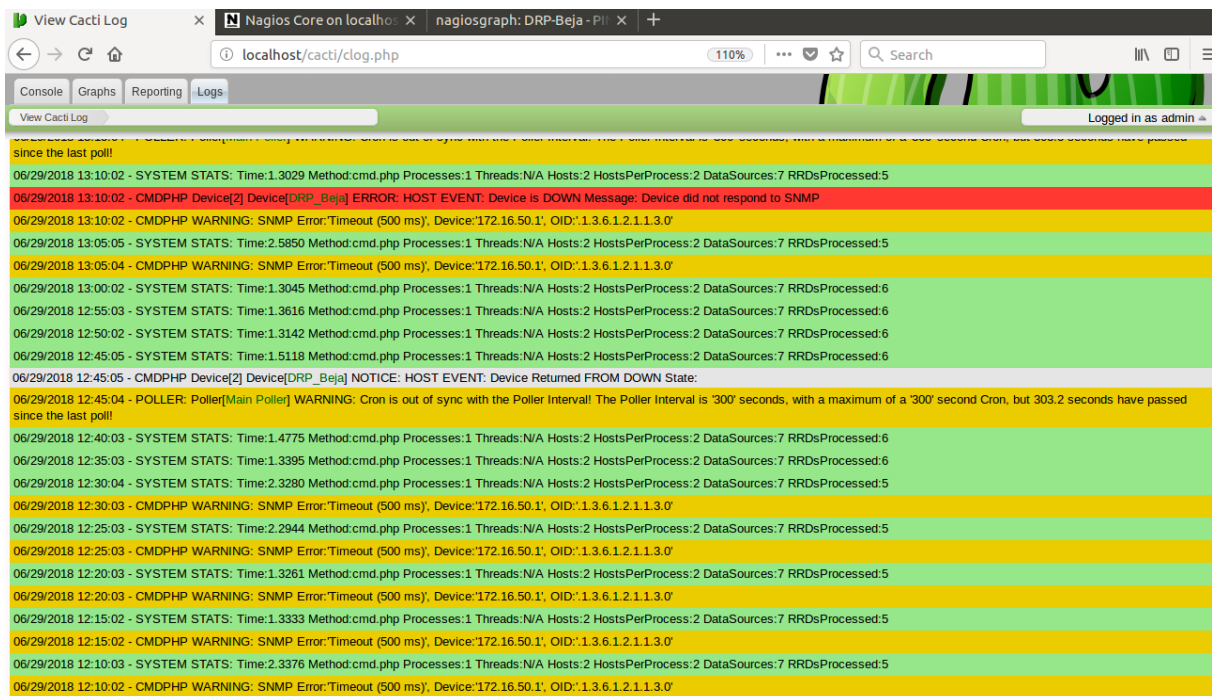


Figure 28: Fichiers Log générés par Cacti

6. Notification par mail

En plus les alertes visuelles dans les interfaces de Nagios et Cacti, on peut les paramétrer pour émettre des emails pour indiquer le dysfonctionnement d'un service ou d'un hôte,

Ce qui permet d'avoir un historique d'activité pour les temps où l'administrateur n'est pas présent

III. Conclusion

Dans ce chapitre on a étudié l'aspect pratique du projet en détaillant quelques étapes de la mise en place et l'utilisation de la solution. Et on a insisté sur la facilité de supervision et les alertes suite aux dysfonctionnements dans le réseau

Conclusion générale

Le domaine de la supervision est un domaine important dans l'administration des systèmes réseaux En constante évolution. Les solutions de supervision ouvertes ont montré qu'il a sa place dans le domaine professionnel.

Et comme on a déjà expliqué dans notre étude, la supervision est l'un des outils indispensable pour assurer la croissance de la performance d'une telle entreprise. Le but de ce projet consiste à choisir une solution de supervision qui répond aux besoins financiers et organisationnels de la poste tunisienne et il n'y avait pas de meilleure façon de satisfaire ce besoin que Nagios.

L'association de Nagios et Cacti a permis la constitution d'une solution de surveillance pour à la fois puissant et efficace.

Enregistre les configurations effectuées par l'administrateur dans une base de données, puis modifie les fichiers de configuration de Nagios en fonction du contenu de la base de données de Les données. Cela a grandement simplifié le travail de l'administrateur, contrairement à l'utilisation de Nagios seul.

Ce stage nous a permis de nous familiariser avec le système d'exploitation Linux dont Domaine est requis pour travailler dans les réseaux informatiques. L'établissement de Le service de surveillance Nagios permet actuellement à l'administrateur, l'ensemble du service IT, ainsi que les gestionnaires d'être informés de l'état du réseau en temps réel. Depuis l'introduction de Nagios, certains problèmes de réseau ont été résolus plus rapidement.

Références netographiques

- [1] <http://www.poste.tn/>
- [2] https://www.researchgate.net/publication/290447542_Supervision_centralisee_d%27infrastructures_distantes_en_reseaux_avec_gestion_des_alarms_et_notification_des_alertes
- [3] <http://www.nagios.org/> : le site officiel de Nagios
- [4] <http://www.nagios.sourceforge.net/> : documentation complète sur les fichiers de Nagios
- [5] <http://www.nagios.org/support/>
- [6] https://docs.cacti.net/manual:088:1_installation.1_install_unix
- [7] <https://www.youtube.com/watch?v=zQmE4IwNVvo>
- [8] <https://www.youtube.com/watch?v=XvyHmYRBRaA>
- [9] <https://support.nagios.com/kb/article.php?id=515>

Annexes

Installation et configuration de NAGIOS sous linux

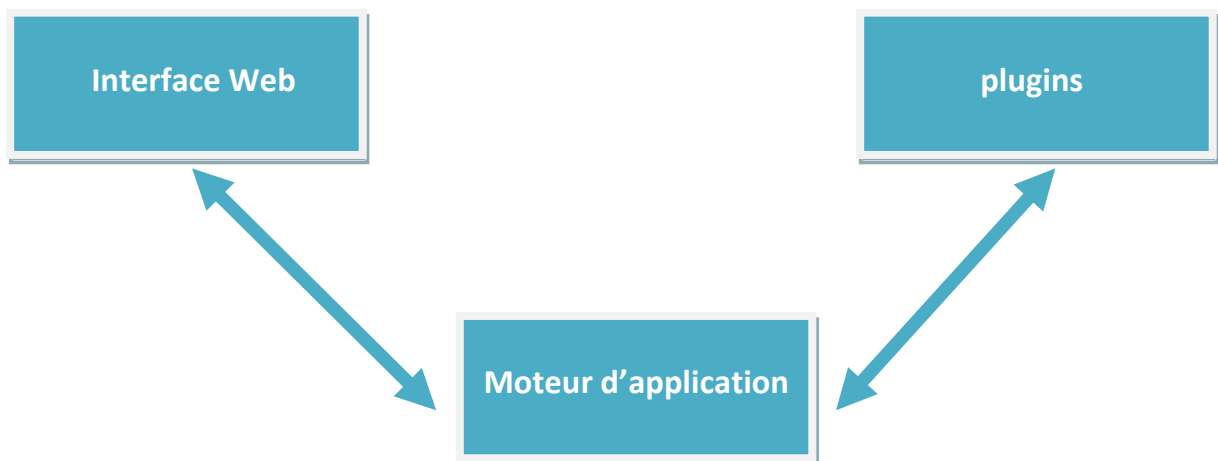
AIT EL MOUDEN ZAKARIYAA

Introduction

Nagios est une application permettant la surveillance système et réseau. Elle surveille les hôtes et services spécifiés, alertant lorsque les systèmes ont des dysfonctionnements et quand ils repassent en fonctionnement normal. C'est un logiciel libre sous licence GPL.

C'est un programme modulaire qui se décompose en trois parties :

- Le moteur de l'application qui vient ordonnancer les tâches de supervision.
- L'interface web, qui permet d'avoir une vue d'ensemble du système d'information et des possibles anomalies.
- Les sondes (appelées greffons ou plugins), une centaine de mini programmes que l'on peut compléter en fonction des besoins de chacun pour superviser chaque service ou ressource disponible sur l'ensemble des ordinateurs ou éléments réseaux du SI.



Installation de Nagios sous Linux

Pour le test j'ai utilisé un système Kali Linux.

Etape 1 : Création des utilisateurs et groupes qui lancent nagios

Les groupes nagios et nagioscmd :

```
sudo groupadd -g 5000 nagios
sudo groupadd -g 5001 nagioscmd
sudo mkdir -p /srv/nagios /etc/nagios /var/nagios
```

L'utilisateur nagios :

```
sudo useradd -u 5000 -g nagios -G nagioscmd -d /srv/nagios nagios
```

Création des répertoires systèmes pour nagios et changement de propriétaire :

```
sudo chown nagios:nagios /srv/nagios/ /etc/nagios/ /var/nagios/
```

Répertoire	Rôle
/srv/nagios	Contient les exécutables de nagios
/etc/nagios	Contient les fichiers de configuration de nagios
/var/nagios	Contient les fichiers d'état de nagios

Etape 2 : Installation des packages nécessaire pour la compilation de nagios

Descriptions de quelques packages:

Package	Description
build-essential	Contient une liste des packages nécessaires pour la construction des packages Debian.
libssl-dev	Ce paquet fournit les bibliothèques de développement pour libssl et libcrypto, Il fait partie de l'implémentation OpenSSL de SSL.
libpq-dev	Communication entre des programmes C et les bases de données PostgreSQL.
binutils	est un ensemble d'outils de développement logiciel maintenu par le projet GNU.

Pour les autres packages consulter le site web : <http://www.pkgs.org/>

La commande suivante rassemble tous les packages nécessaire :

```
sudo apt-get install build-essential libssl-dev binutils make libpq-dev  
libmysqlclient-dev libssl1.0.0 libgd-tools libpng12-dev libjpeg62-dev perl  
libperl-dev libperl5.14 libnet-snmp-perl libgd2-xpm-dev
```

Etape 3 : Téléchargement et installation du package nagios

Vous trouvez le package sur le lien : <http://sourceforge.net/projects/nagios/>

Dans notre cas, on a travaillé avec la version **nagios-4.1.0rc1**

Une fois le package est téléchargé ...

```
tar xvf nagios-4.1.0rc1.tar.gz  
cd nagios-4.1.0rc1
```

Configuration de la source avec les répertoires nagios déjà créés :

```
./configure --prefix=/srv/nagios --sysconfdir=/etc/nagios --  
localstatedir=/var/nagios --libexecdir=/srv/nagios/plugins --with-command-  
group=nagioscmd
```

Compiler les sources :

```
make all
```

Installation de nagios et nagios mode commande pour les commandes externes :

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

Installation de la configuration de base :

```
sudo make install-config
```

Etape 4 : Téléchargement et installation du package nagios plugins

Vous allez trouver le package à télécharger sur le même lien du package nagios.

Dans notre cas on a travaillé avec la version **nagios-plugins-2.0.3**.

Une fois le package est téléchargé ...

```
tar xvf nagios-plugins-2.0.3.tar.gz
cd nagios-plugins-2.0.3
```

Veillez vérifié la présence des package suivants sur votre machine :

```
sudo apt-get install m4 gettext autoconf libssl-dev libssl1.0.0 libpq-dev
libmysqlclient-dev fping qstat libldap2-dev libradius1-dev
```

Configuration des plugins avec les répertoires nagios :

```
./configure --prefix=/srv/nagios --sysconfdir=/etc/nagios --
localstatedir=/var/nagios --libexecdir=/srv/nagios/plugins --enable-perl-
modules
```

Compilation et installation :

```
sudo make all
sudo make install
```

Se déplacer vers le répertoire **nagios-4.1.0rc1/contrib** :

```
cd nagios-4.0rc1/contrib
```

Lancer le convertisseur des commandes de configuration :

```
make convertcfg
cp convertcfg /srv/nagios/bin
```



```
cd nagios-plugins-2.0.3
sudo sh -c "/srv/nagios/bin/convertcfg command.cfg commands >
/etc/nagios/objects/plugin-commands.cfg"
```

Se déplacer vers le répertoire `/etc/nagios` et ouvrir le fichier `nagios.cfg` :

```
cd /etc/nagios
vim nagios.cfg
```

Ajouter le fichier `plugin-commands.cfg` comme fichier de configuration en ajoutant la ligne suivante dans le fichier ouvert :

```
cfg_file=/etc/nagios/objects/plugin-commands.cfg
```

[Etape 5 : Configuration du nagios avec le serveur apache2](#)

On considère que les packages `apache2` et `php5` sont déjà installés.

Ajouter l'utilisateur d'apache2 au groupe `nagioscmd` :

```
sudo usermod -a -G nagioscmd www-data
```

! Le nom de l'utilisateur `apache2` par défaut c'est `'www-data'`, sinon vous pouvez vérifier avec la commande :

```
grep APACHE_RUN_USER /etc/apache2/*
```

Créer un fichier nommé `'nagios'` dans le répertoire `/etc/apache2/conf.d` est le remplir par le contenu suivant :

```
ScriptAlias /nagios/cgi-bin /srv/nagios/sbin
Alias /nagios /srv/nagios/share
<Directory "/srv/nagios/share">
    Options FollowSymLinks
    AllowOverride AuthConfig
    Order Allow,Deny
    Allow from All
    AuthName "Nagios Access"
    AuthType Basic
    AuthUserFile /etc/nagios/htpasswd.users
    require valid-user
</Directory>
```

```
<Directory "/srv/nagios/sbin">
  Options ExecCGI
  AllowOverride AuthConfig
  Order Allow,Deny
  Allow from All
  AuthName "Nagios Access"
  AuthType Basic
  AuthUserFile /etc/nagios/htpasswd.users
  require valid-user
</Directory>
```

Créer le fichier qui contient les utilisateurs qui peuvent s'authentifier à l'interface Web de nagios :

```
sudo htpasswd -bc /etc/nagios/htpasswd.users nagiosadmin <password>
```

Lancer les serveurs nagios et apache2 :

```
sudo service nagios start
sudo service apache2 reload
```

Si une erreur se produit lors du lancement du service nagios, essayer de se déplacer vers le répertoire **/etc/nagios/objects** et créer un autre fichier nommé **command.cfg** avec le même contenu de **commands.cfg** est changer son propriétaire à nagios du groupe nagios.

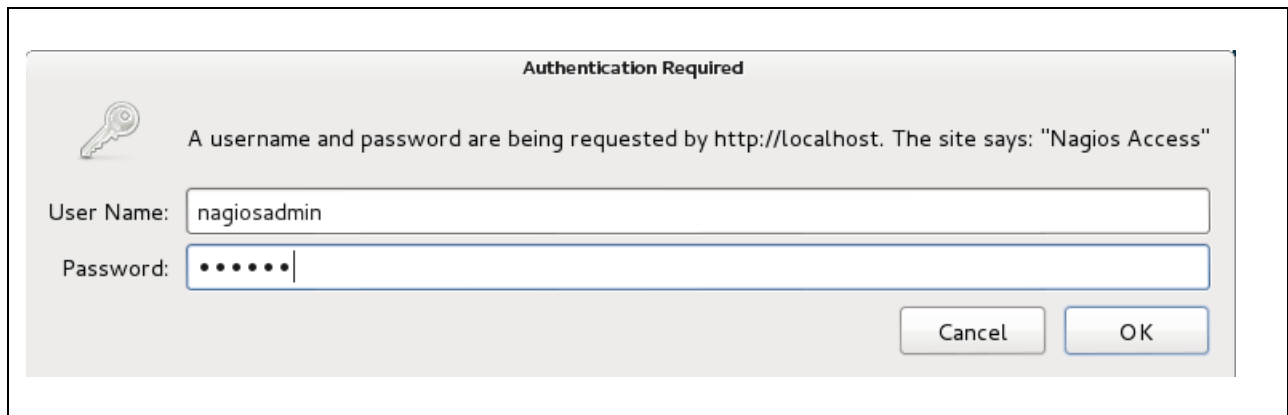
Si le service nagios est bien lancé, vous allez recevoir le message suivant :

```
root@zakariyaa:/etc/nagios/objects# service nagios start
Starting nagios: done.
```

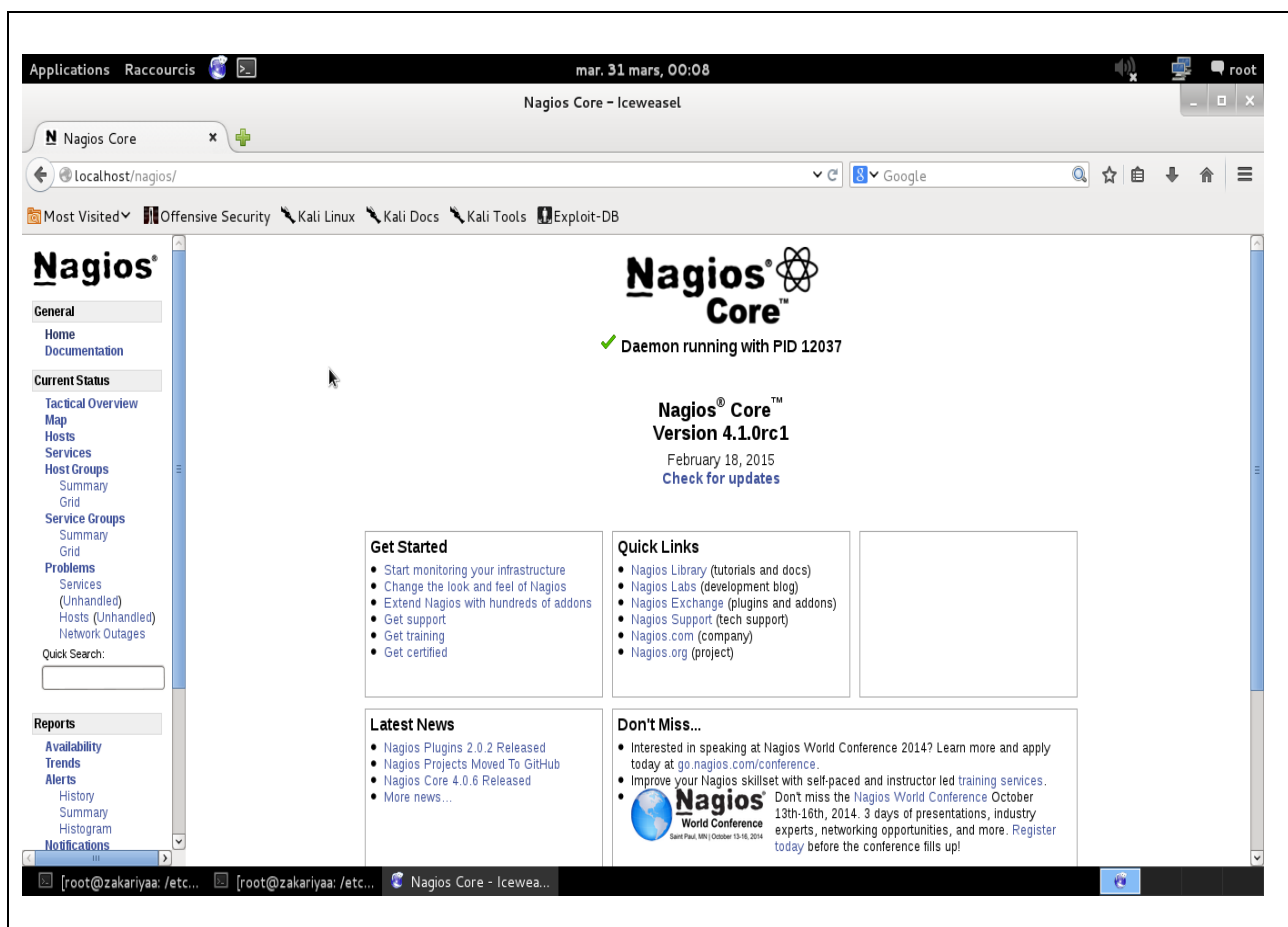
Etape 6 : l'IHM nagios

On essaye maintenant d'accéder à l'interface web sous l'url **localhost/nagios**

Une authentification est obligatoire, on tape les données que nous avons saisies dans l'étape précédente avec la commande **htpasswd**.



Après on obtient la page web suivant :



Documentation cacti

Présentation :

Cacti est un logiciel de supervision basé sur RRDtool permettant de surveiller l'activité de son architecture informatique à partir de graphiques quotidiens, hebdomadaires, mensuels et annuels.

Cacti est un logiciel écrit en PHP, s'appuyant sur une base de données MySQL pour stocker tous ses éléments de configuration et sur RRDtool pour créer les fichiers RRD, les peupler et obtenir les graphiques correspondants. Il a pour objectif de faciliter les manipulations parfois fastidieuses de RRDtool, néanmoins une bonne connaissance des fonctionnalités de cet outil est nécessaire pour apprécier l'utilisation de Cacti.

Il est librement téléchargeable sur le site <http://www.cacti.net>.

Pré-requis :

- Machine Ubuntu mis à jour et opérationnelle
- Apache : télécharger paquet apache2 :
apt-get install apache2
- MySQL : télécharger paquet mysql-server :
apt-get install mysql-server
- PHP : télécharger paquet php5
apt-get install php5
- phpmyadmin : télécharger les paquets phpmyadmin
apt-get install phpmyadmin

Installation de cacti (v0.8.8c)

1. Installer les paquets suivants :

- php5-mysql
- php5-cgi
- php5-cli
- php5-snmp
- php-pear
- snmp
- snmpd

2. Installer le paquet rrdtool :

apt-get install rrdtool

3. Télécharger cacti sur le site officiel, décompresser, renommer en "cacti" et envoyer par ftp sur le serveur et le mettre dans /var/www/html :

4. Créer la base de données cacti et l'utilisateur cacti974 pour cette base de données avec phpmyadmin qui aura tous les privilèges. Se placer dans le fichier /var/www/html/cacti et faire :

```
mysql -u root -p cacti<cacti.sql
```

5. Configurer dans le fichier de configuration /var/www/cacti/include/config.php les identifiants mysql le nom du serveur et le nom de la base de données

6. Ajouter sur la machine l'utilisateur de cacti

```
sudo useradd cacti974 -d /var/www/html/cacti -s /bin/false
```

et le mettre propriétaire des répertoires :

```
sudo chown -R cacti974 /var/www/html/cacti/rra /var/www/html/cacti/log
```

7.Éditez le fichier **/etc/crontab** pour y ajouter la ligne suivante :

```
*/5 * * * * cacti974 php5 /var/www/html/cacti/poller.php > /dev/null 2>&1
```

8. Editer le fichier **/etc/php5/apache2/php.ini** et décommenter la ligne suivante :

```
;extension=mysqli.so
```

Editer le fichier **/etc/php5/cli/php.ini** et décommenter la ligne suivante :

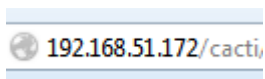
```
;extension=mysqli.so
```

Editer le fichier **/etc/php5/cgi/php.ini** et décommenter la ligne suivante :

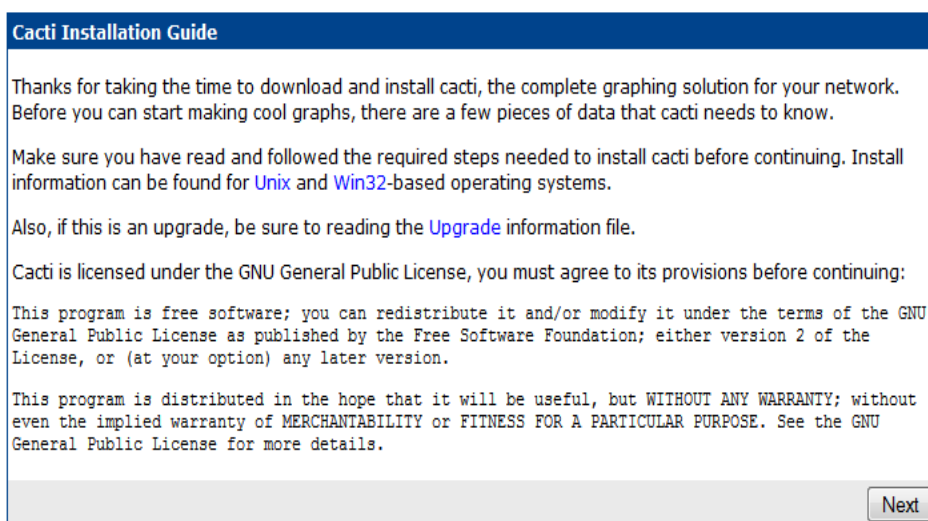
```
;extension=mysqli.so
```

9. Redémarrer Apache : `sudo /etc/init.d/apache2 restart`

10. Allez sur un navigateur et taper l'adresse suivante **@Ipserveur/cacti** comme ceci:



Cette page apparait cliquer sur Next :



Cliquer sur Next

Cacti Installation Guide

Please select the type of installation

The following information has been determined from Cacti's configuration file. If it is not correct, please edit 'include/config.php' before continuing.

Database User: cacti974
Database Hostname: localhost
Database: cacti
Server Operating System Type: unix

Cliquer sur Finish

Cacti Installation Guide

Make sure all of these values are correct before continuing.

[FOUND] RRDTool Binary Path: The path to the rrdtool binary.

[OK: FILE FOUND]

[FOUND] PHP Binary Path: The path to your PHP binary file (may require a php recompile to get this file).

[OK: FILE FOUND]

[FOUND] snmpwalk Binary Path: The path to your snmpwalk binary.

[OK: FILE FOUND]

[FOUND] snmpget Binary Path: The path to your snmpget binary.

[OK: FILE FOUND]

[FOUND] snmpbulkwalk Binary Path: The path to your snmpbulkwalk binary.

[OK: FILE FOUND]

[FOUND] snmpgetnext Binary Path: The path to your snmpgetnext binary.

[OK: FILE FOUND]

[FOUND] Cacti Log File Path: The path to your Cacti log file.

[OK: FILE FOUND]

SNMP Utility Version: The type of SNMP you have installed. Required if you are using SNMP v2c or don't have embedded SNMP support in PHP.

RRDTool Utility Version: The version of RRDTool that you have installed.

NOTE: Once you click "Finish", all of your settings will be saved and your database will be upgraded if this is an upgrade. You can change any of the settings on this screen at a later time by going to "Cacti Settings" from within Cacti.

Se logger, par default admin/admin



User Login

Please enter your Cacti user name and password below:

User Name:

Password:

Login

Changer ensuite le mot de passe et cliquer sur Save



User Login

***** Forced Password Change *****

Please enter a new password for cacti:

Password:

Confirm:

Save

On atterit sur l'interface d'administration, le serveur est fonctionnel

console graphs

Console Logged in as admin (Logout)

You are now logged into Cacti. You can follow these basic steps to get started.

- Create devices for network
- Create graphs for your new devices
- View your new graphs

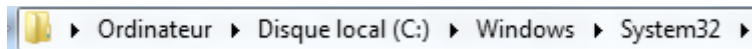
Version 0.8.8c

FR 09:18 27/01/2015

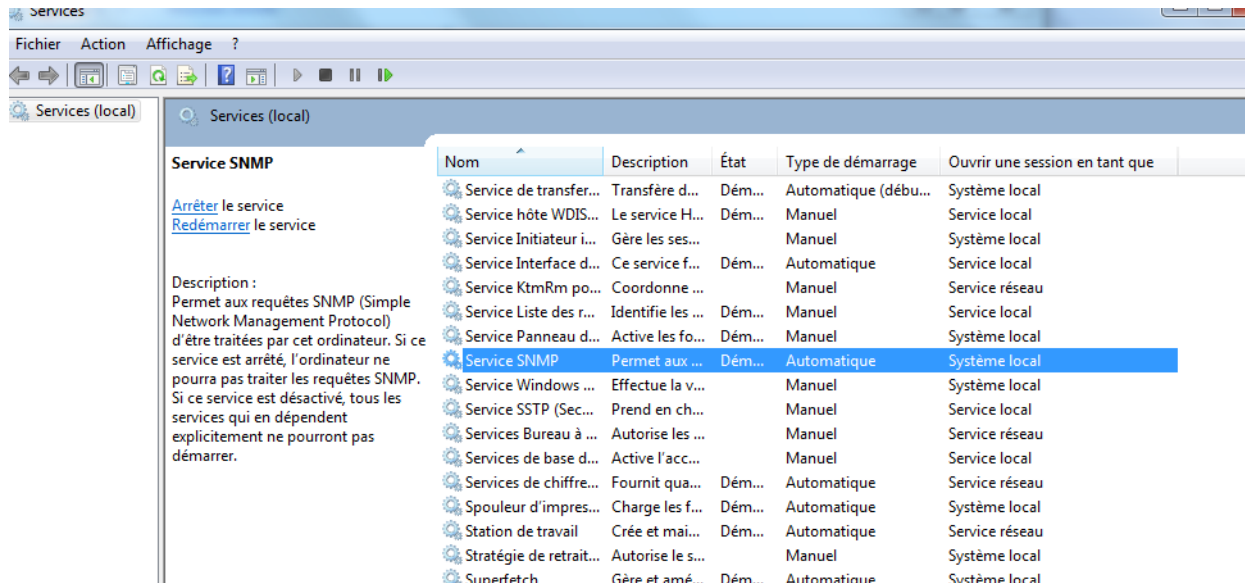
Test avec machine Windows 7 :

Configuration snmp sur la machine cliente :

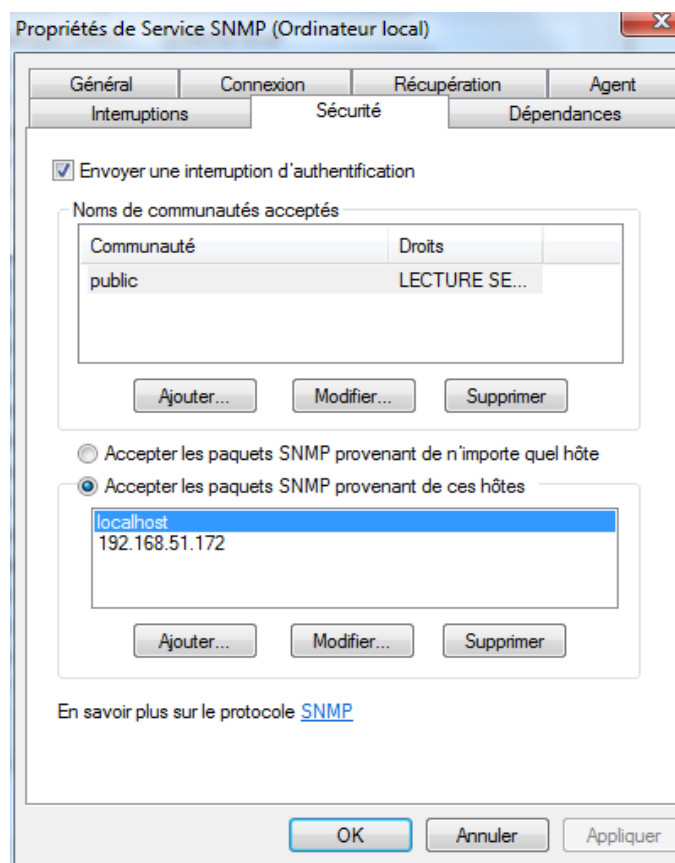
- Allez dans C:\Windows\System32



- Cliquer sur services.msc
- Dans la fenetre ouverte, cliquer sur Service SNMP



- Dans l'onglet Sécurité, renseigner l'adresse IP du serveur pour accepter les paquets snmp et dans Noms de communautés ajouter "public" et en droit Lecture seule



Installation Weathermap :


Prérequis :

- Installation si nécessaire du plugin Architecture, mais dans cette version de cacti , ce plugin est présente par défaut

Installation :

1. Aller sur le site de Network Weathermap et télécharger la dernière version de Weathermap :

<http://network-weathermap.com/download>

Post date	Version	Link	File	Size
Apr 10, 2013	0.97c	Release Information	 php-weathermap-0.97c.zip	2.86 MB

2. Dézipper le fichier, transférer le dossier obtenu (weathermap)sur le serveur dans le répertoire /var/www/html/cacti/plugins

3. Remplacer dans le fichier /var/www/html/cacti/include/plugins.php la ligne :

```
$plugins = array();
```

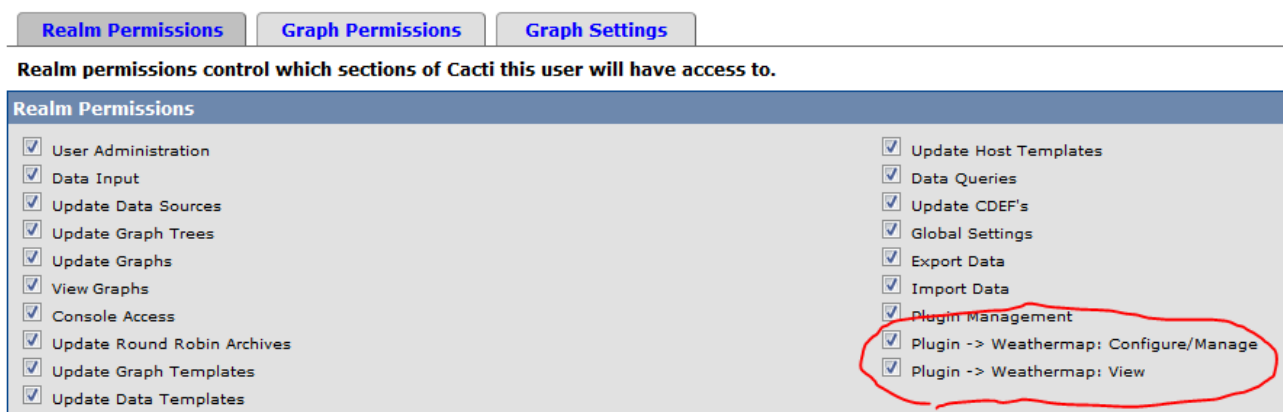
Par :

```
$plugins = array('weathermap');
```

Enregistrer le fichier

4. Aller dans l'interface WEB d'administration de cacti, puis vérifier les points suivant :

- dans User Management, cliquer sur admin puis vérifier que Weathermap est activé:



Realm Permissions Graph Permissions Graph Settings

Realm permissions control which sections of Cacti this user will have access to.

Realm Permissions

<input checked="" type="checkbox"/> User Administration	<input checked="" type="checkbox"/> Update Host Templates
<input checked="" type="checkbox"/> Data Input	<input checked="" type="checkbox"/> Data Queries
<input checked="" type="checkbox"/> Update Data Sources	<input checked="" type="checkbox"/> Update CDEF's
<input checked="" type="checkbox"/> Update Graph Trees	<input checked="" type="checkbox"/> Global Settings
<input checked="" type="checkbox"/> Update Graphs	<input checked="" type="checkbox"/> Export Data
<input checked="" type="checkbox"/> View Graphs	<input checked="" type="checkbox"/> Import Data
<input checked="" type="checkbox"/> Console Access	<input checked="" type="checkbox"/> Plugin Management
<input checked="" type="checkbox"/> Update Round Robin Archives	<input checked="" type="checkbox"/> Plugin -> Weathermap: Configure/Manage
<input checked="" type="checkbox"/> Update Graph Templates	<input checked="" type="checkbox"/> Plugin -> Weathermap: View
<input checked="" type="checkbox"/> Update Data Templates	

- vérifier que Weathermap apparait dans Plugins Management et en haut à gauche de l'interface WEB

The screenshot shows the Cacti web interface. At the top, there are three navigation tabs: 'console', 'graphs', and 'weathermap', with 'weathermap' circled in red. Below the tabs, the breadcrumb 'Console -> Plugin Management' is visible, and the user is logged in as 'admin'. The main content area is titled 'Plugin Management (Cacti Version: 0.8.8c, Plugin Architecture Version: 3.1)'. It features a search bar and a 'Rows: Default' dropdown. A table lists the installed plugins, with the 'weathermap' entry circled in red. The table has columns for 'Actions', 'name', 'Version', 'Load Order', 'Description**', 'Type', 'Status', and 'Author'. Below the table, there are two notes: 'NOTE: Please sort by 'Load Order' to change plugin load ordering.' and 'NOTE: SYSTEM plugins can not be ordered.'

Actions	name	Version	Load Order	Description**	Type	Status	Author
	weathermap	0.97b		PHP Network Weathermap	Old PIA	Active	Howard Jones

Annexe C

❖ Installation de NSClient

➤ Partie Serveur (Machine Windows Distante)

Il faudra installer et configurer NSClient++ sur le serveur Windows

- Télécharger la version NSClient-0.3.8.75.
- Dézipper le client sous le répertoire C:\NSClient++-Win32-0.3.8.
- Ouvrir une commande DOS (cmd.exe)
- Entrer les commandes suivantes :

```
C:\cd NSClient++-Win32-0.3.8
```

```
C:\cd NSClient++-Win32-0.3.8\NSClient++.exe/install
```

L'installation est donc achevée, vérifions donc que le service est autorisé à "Interagir avec le bureau"

(Marquer Local system account et Allow service to interact with desktop dans l'onglet « Log On » du gestionnaire de service) en ouvrant le gestionnaire des services.

- On passe maintenant à la modification du fichier de configuration sous c://nscclient/NSC.INI.
- Décommenter dans la première section [modules] tous les modules sauf **CheckWMI.dll** et **RemoteConfiguration.dll**

•Décommenter la ligne **allowed_hosts** dans la section [Settings] et ajoutant l'adresse du serveur Nagios aussi pour des mesure de sécurité on a la possibilité d'attribuer un password pour accéder à NSClient.

- **Démarrage NSClient:**

```
C:\cd NSClient++-Win32-0.3.8\NSClient++.exe/start
```

- **Arrêt NSClient**

```
C:\cd NSClient++-Win32-0.3.8\NSClient++.exe/stop
```

[Setting]

```
;/# OBFUSCATED PASSWORD
```

```
;/ This is the same as the password option but here you can store the password in an obfuscated manner.
```

```
;/ *NOTICE* obfuscation is *NOT* the same as encryption, someone with access to this file can still figure out the
```

```
;/ password. Its just a bit harder to do it at first glance.
```

```
;/obfuscated_password=Jw0KAUUdXIAAUwASDAAB
```

```
# PASSWORD
```

This is the password (-s) that is required to access NSClient remotely. If you leave this blank everyone will be able to access the daemon remotely.

```
password=admin
```

```
# ALLOWED HOST ADDRESSES
```

This is a comma-delimited list of IP address of hosts that are allowed to talk to the all daemons. If leave this blank anyone can access the daemon remotely (NSClient still requires a valid password).The syntax is host or ip/mask so 192.168.0.0/24 will allow anyone on that subnet access

```
allowed_hosts= 192.168.0.107
```

➤ Partie Cliente (serveur Nagios)

Juste on doit vérifier la présence de la commande check_nt sous /usr/local/nagios/libexec sinon le télécharger et l'ajouter parmi les autres commandes.

→ Depuis le terminal du serveur nagios testons si la machine Windows distante répond en tapant la commande suivante qui doit renvoyer la version de NSClient++ installée :

→ Maintenant que tout est prêt dans la machine Windows distante à superviser, on a plus qu'à ajouter la machine au serveur Nagios et essayer de récupérer les informations nécessaires grâce à la commande **check_nt** qui permet d'interroger à distance l'agent NSClient.

```
#cd /usr/local/nagios/libexec
```

```
#!/check_nt -H 62.245.223.181 -s admin -p 12489 -v CLIENTVERSION  
NSClient++ 0.3.8.75
```

Annexe D

❖ Installation de NRPE

➤ Partie Client (Serveur Linux)

Accéder au serveur Linux à superviser en tant que **root** et suivre les étapes suivantes :

- Création d'un utilisateur et groupe.
- Téléchargement, décompression et Installation des plugins Nagios Nagios-plugins-1.4.15

```
# cd /usr/sbin
# useradd nagios
# passwd nagios
# groupadd nagios
# usermod -G nagios nagios
#mkdir downloads
#cd downloads
#wget http://osdn.dl.sourceforge.net/sourceforge/nagiosaplugin/nagios-plugins-1.4.15.tar.gz
# tar xzf nagios-plugins-1.4.6.tar.gz
#cd nagios-plugins-1.4.6
#./configure
#make
#make install
#chown nagios.nagios /usr/local/nagios
#chown -R nagios.nagios /usr/local/nagios/libexec
```

- Téléchargement, décompression et Installation du plugin nrpe-2.12.

→L'installation est donc achevée, Passons à la configuration de /usr/local/nagios/etc/nagios/nrpe.cfg.

Et ajouter la ligne suivante dans /etc/services :

→Finalement lancer le daemon XINETD relatif à NRPE :

→On peut aussi utiliser les commandes suivante pour stopper, redémarrer ou déterminer l'état du

processus (démarré, stoppé) :

```
#wget http://osdn.dl.sourceforge.net/sourceforge/nagios/nrpe-2.12.tar.gz
```

```
#tar xzf nrpe-2.12.tar.gz
```

```
#cd nrpe-2.12
```

```
#!/configure
```

```
#make all
```

```
#make install-plugin
```

```
#make install-daemon
```

```
#make install-daemon-config
```

```
#make install-xinetd
```

```
Allowed_host = @ du serveur nagios
```

```
nrpe 5666/tcp # NRPE
```

```
# /etc/init.d/xinetd start
```

```
# /etc/init.d/xinetd stop
```

```
# /etc/init.d/xinetd status
```

```
# /etc/init.d/xinetd restart
```

➤ Au niveau du serveur Nagios

Au niveau du serveur serveur Nagios on refait les mêmes étapes pour l'installation de NRPE.

- Les plugins sont déjà installés.

- Téléchargement, décompression et Installation du plugin nrpe-2.12.
- ➔ Finalement lancer le daemon XINETD relatif à NRPE :
- ➔ Depuis le terminal du serveur nagios testons si la machine Windows distante répond en tapant la commande suivante qui doit renvoyer la version de NSClient++ installée :
- ➔ Vérifier que les requêtes (TCP sur port 12489) ne sont pas bloquées par un firewall sinon ajouter une règle pour autoriser le Firewall Iptable.