# Eon - Configuration et administration

## Document de formation

**Anthony Leduc**

**État :** En Cours

**Date dernière modification :** 5 janv. 2011

**Objet du document :**

## -- Historique de modifications --

| Version | Date | Responsable | Modifications |
|---|---|---|---|
| 1.0 | 14 mai 2010 | Anthony Leduc | Création du document |
| 1.1 | 18 juin 2010 | Anthony Leduc | Première ébauche |
| 1.2 | 22 juin 2010 | Anthony Leduc | Modification de la carte heuristique EON |
| 1.3 | 5 juil. 2010 | Anthony Leduc | Homogéneisation de la mise en forme, Ajouter d'une section "Connexion annuaire LDAP", Amélioration du contenu de la documentation concernant "nagvis" |
| 1.4 | 5 janv. 2011 | Anthony Leduc | Corrections de bugs mineurs. Merci à Fe1lho pour ce report |

# Table des matières

# 1 - Préambule

## 1.1 - Pourquoi cette documentation ?

Il existe de nombreuses documentations sur la mise en place d'un logiciel de supervision.

Les ressources ne manquent pas et elles sont précieuses.

Cependant, au fil de mes lectures, il m'est arrivé d'être perdu par leur excédent d'informations.

Cette documentation n'a pas la prétention de faire de vous un expert de la supervision réseau. Il s'agit plus d'un guide pratique qui vous permettra, et je le souhaite, d'implémenter ce superbe logiciel de façon sereine.

## 1.2 - Remerciements

Avant de rentrer dans le vif du sujet, je souhaite remercier *François Pignet* pour ses cours portant sur la supervision et pour son enrichissant ouvrage « *Réseaux informatiques - supervision et administration* ». Je pense également aux membres actifs de la communauté de « *www.eyesofnetwork.com* » notamment à *Sébastien Fernandez* pour son précieux support.

Mes remerciements vont également à *Jean-Philippe Levy*, *Jérémie Bernard*, *Michael Aubertin* pour avoir crée ce superbe outil.

## 1.3 - Axes de progression

Cette documentation se veut le plus accessible possible et je vais essayer, volontairement, de m'astreindre au maximum des termes techniques.

Par ailleurs, la progression est faite en fonction des besoins et des difficultés que j'ai pu rencontrés. D'autres membres regretteront que certaines fonctionnalités ne soient pas abordées. Il ne tient qu'à vous de compléter cette documentation afin qu'elle devienne de plus en plus efficace et pertinente.

Les contributeurs n'hésiteront pas à compléter la partie « *historique* ».

## 1.4 - Nomenclature

Une ligne de commande à saisir dans la console est représentée sous cette forme :

```
/etc/init.d/xxx
```

Une information importante et qui réclame votre attention est représentée ainsi :

*Pensez à redémarrer le service*

Une information qui peut vous être utile est représentée de cette façon :

Faire « */ect/init.d/service restart* »

# 2 - Qu'est-ce que EON ?

**EON**

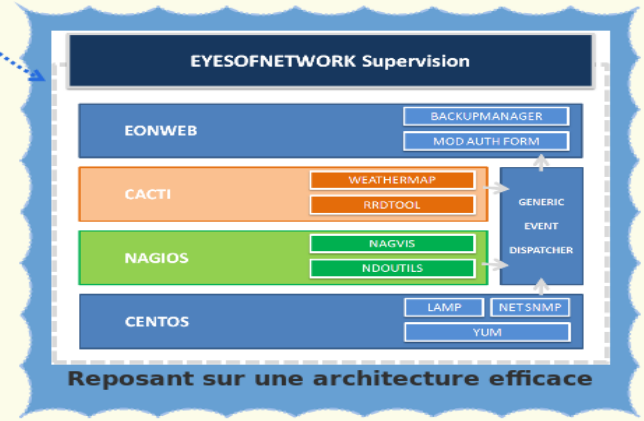
sponsor APX

- Un logiciel Open source
- rapports orientés processus ITIL
- Un ensemble des meilleurs logiciels de supervison
- Une installation et une mise à jour simplifiée
  - Une installation graphique
  - Mise à jour unifiée
- **Objectifs**
  - **réunir les différents acteurs du Système d'Information**
  - Chacun des ces acteurs dispose d'une vue correspondant à son métier.

qui sont :

| | |
|---|---|
| GED (Generic Event Dispatcher) | **gestion multi sites et sécurisée des évènements.** |
| NAGIOS | **gestion des incidents et des problèmes** |
| NAGIOSBP | **gestion de la criticité des applications** |
| NAGVIS | **cartogaphie personnalisée de la disponibilité** |
| CACTI | **gestion des performances** |
| WEATHERMAP | **cartographie de la bande passante** |
| BACKUP MANAGER | **Outil de sauvegarde de la solution** |
| EONWEB | **Interface Web unifiée de la solution** |
| EZGRAPH | **Librairie d'affichage des graphiques** |
| SNMPTT | **Traduction des traps snmp** |
| GLPI | **Gestion de parc** |
| Liliac | **Découverte de votre réseau de façon manuelle ou automatique** |

Le tout dans un DVD de 4 Go



# 3 - Scénario

Imaginons un scénario classique, qui servira de base pour la progression pédagogique de notre documentation.

Vous avez construit votre réseau au fil de l'eau en ajoutant des équipements pour répondre aux besoins naissants de l'entreprise sans avoir pris le temps d'en mesurer les impacts sur votre Système d'Informations. Aujourd'hui, vous faites face aux mécontentements de vos utilisateurs (clients selon l'orientation ITIL) car ils ne sont pas satisfaits de leur service informatique.

Afin de garantir une qualité de service auprès des utilisateurs et assurer une veille « *proactive* » du Système d'Information, vous souhaitez mettre en place un logiciel de supervision qui vous permettra de disposer d'outils permettant de mesurer et observer la qualité du réseau. Vous serez en mesure d'informer les utilisateurs d'une phase temporaire de service dégradé voire d'indisponibilité. L'impact pour l'utilisateur sera complètement différent, car il ne se positionnera plus en tant que « *victime* » puisqu'il sera prévenu par le service informatique en aval.

Vous venez d'installer EON.
Mais voilà, avouez-le, vous êtes perdu et vous ne savez pas par quoi commencer.

*Attribuer une adresse ip fixe à votre serveur de supervision*

*Se connecter à l'interface web « http://ip du serveur » du serveur de supervision login/password : admin/admin*

La toute première chose est de se rendre dans le logiciel « *Lilac* » .
Cliquez sur « *administration* » pour accéder à la partie « *administrative* » de l'interface web.


## 3.1 - Pourquoi superviser ?

Avant de démarrer la procédure d'autodécouverte des éléments actifs du réseau, il est recommandé de se poser les questions suivantes :

- *Quoi superviser et pourquoi ?*
- *Quels sont les évènements à remonter dans Nagios ?*
- *Déterminer les évènements critiques pour lesquels je dois être informé par mail ?*
- *Quels sont les personnes qui doivent être notifiées par mail ?*
- *Qui doit avoir accès à la console de supervision et quel est le niveau d'accès à leur attribuer ?*

Si nous reprenons notre scénario précédent, nous constatons des lenteurs sur notre réseau, sur nos serveurs, mais comment savoir ce qui ne va pas ? Nous ne disposons pas d'indicateurs qui pourraient nous alerter sur les mesures à prendre.

Des outils comme « *iperf* » ou un simple échange FTP permettent de mesurer la bande passante à un « *instant t* ».

Pour que le résultat de l'échange FTP soit probant, le fichier utilisé doit avoir une taille conséquente. Un fichier de 4go permet de voir si le réseau connaît des instabilités.

Mais avant tout, il est nécessaire de savoir ce que l'on souhaite mesurer.

L'idée est donc de construire un cahier des charges précis qui va permettre de définir quels sont les éléments à remonter et ce qui est important de superviser.

Suivant le scénario proposé, voici ce que nous pouvons superviser :

**Au niveau des imprimantes** :

- *Monitorer l' état des cartouches d'impressions et afficher une alerte si le niveau d'encre est inférieur à 20 %*
- *Comptabiliser le nombre de pages imprimées par imprimante en vue de créer des statistiques.*
- *Une personne responsable du stock d'impression doit être avertie par mail quand le toner d'une imprimante atteint un état critique.*

**Au niveau des serveurs** :

- *État du client AV (en service ou pas) sur l'ensemble des serveurs,*
- *taux d'occupation du CPU et de la mémoire. Une alerte sur l'écran Nagios sera émise si le seuil atteint 80 % et 90%,*
- *taux d'occupation des partitions physiques sur le disque dur*
- *Adresses dhcp restantes*
- *Nombre de mails envoyés par minute. Un seuil d'alerte est émis quand le nombre de mails émis est supérieur à 300 par minutes.*
- *Nombre d'utilisateurs connectés au serveur de messagerie*
- *etc..*

**Au niveau des graphiques (cacti)** :

*Pour tous les serveurs :*

- *CPU, Mémoire, partitions physiques, interface réseau, processus*

*Pour les éléments actifs (routeur, switch, firewall) :*

- *Débit des ports en entrée et sorties + erreur*
- *CPU, mémoire*

**Au niveau des cartes (nagvis, weathermap)** *:*

*Pour nagvis :*

- *Afficher une alerte sur le serveur si son état ou un service atteint un seuil d'avertissement ou critique*
- *Afficher sur une carte les différents routeurs et leurs états.*

*Pour weathermap :*

- *Afficher le débit en temps réel des liens entre les routeurs des associations et celui du siège.*

**Au niveau des rapports** :

- *La responsable du Système d'Information doit recevoir un rapport d'état de performance du réseau tous les lundis matin et si possible au format pdf.*

**Au niveau de la sauvegarde** :

- *Une sauvegarde des différents fichiers de configurations du serveurs et des BDD est réalisée tous les soirs par FTP. L'administrateur doit recevoir un mail si la sauvegarde a été réalisée correctement.*

**Divers :**

- *Si possible mettre une sonde ntop afin d'analyser le trafic du réseau*
- *Centraliser les logs des éléments actifs et des serveurs du SI sur le serveur de supervision*

Ce cahier des charges est loin d'être exhaustif. Il est là pour indiquer les grandes lignes à suivre et peut vous guider dans l'élaboration de votre propre cahier des charges

# Lilac

*Création et paramétrage des hôtes à superviser*

**Objectifs** :

- *Créer des hôtes dans lilac de façon manuel et automatique*
- *Ajouter et paramétrer des services en fonction des hôtes*
- *Personnaliser des templates existants*
- *Ajouter et personnaliser des commandes nagios*
- *Récupérer des mib et les exploiter avec snmpwalk*
- *Ajouter des plug-ins dans EON*
- *Ajouter des contacts et des groupes*
- *Exporter ses hôtes*
- *Comprendre et résoudre les erreurs liées à l'exportation.*

# 4 - Lilac

## 4.1 - Présentation de lilac

« La Plateforme Lilac est une collection d'outils conçus pour améliorer les applications open source de supervision, écrit par Lila Networks.

Les principales fonctionnalités sont les suivantes:

- *Support des périodes de temps de Nagios 3*
- *Supporte l'héritage multiple de gabarits*
- *Des gabarits d'hôtes capables de recevoir de services, des dépendances et des escalades*
- *Un outil d'import qui peut importer les configurations Nagios existantes ainsi que les imports d'installation Fruity*
- *Export avec contrôle de cohérence des fichiers générés ainsi que la sauvegarde des fichiers existants*
- *Outil d'autodécouverte pour ajouter rapidement l'infrastructure à superviser dans votre installation Nagios »*

source :

*http://wiki.monitoring-fr.org/addons/lilac-platform*

## 4.2 - Découvrir automatiquement un groupe d'hôtes

« *Lilac* » est un formidable outil qui permet de découvrir automatiquement les hôtes de votre réseau. Il s'appuie sur l'excellent logiciel « *nmap* » qui est un scanneur de port.

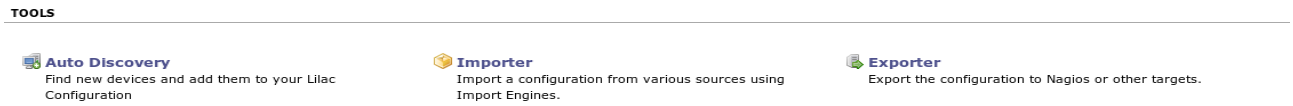
Nous allons voir comment ajouter automatiquement un hôte et lui affecter un template qui contient les services à monitorer.

Il est évidemment peu intéressant de faire un scan pour une seule machine, mais malgré tout c'est ce que nous allons faire, car cela va vous permettre de comprendre le fonctionnement de « *nmap* ».

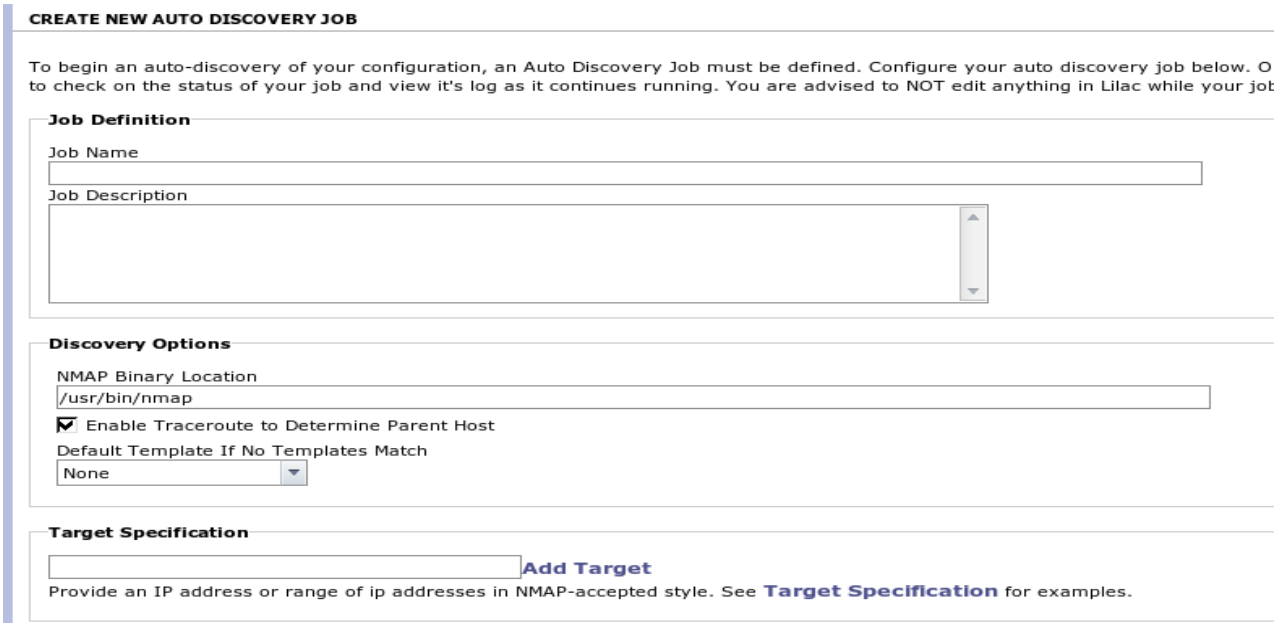
### 4.2.1 - Procédure

Dans « *Lilac* », sur la page principale, cliquez sur le lien « *Tools* »

Cliquez sur « *Auto discovery* »




Cette fenêtre apparaît




**Explications :**

- **Nmap Binary Location** :

*Emplacement de l'exécutable nmap .*

- **Enable Traceroute to determine parent host** :

*Cette option va essayer de déterminer quel est l'élément parent des hôtes découvert par nmap*

- **Default Template if no templates match** :

*Il est possible d'affecter un template à un hôte ou à groupe d'hôte.*

Pour le moment, choisir le template « **Ms_windows_2kx** » car nous souhaitons que le logiciel remonte les services génériques d'un serveur Windows 2003.

- **Target specification** :

*Il s'agit de l'adresse ip de l'hôte que l'on souhaite superviser.*

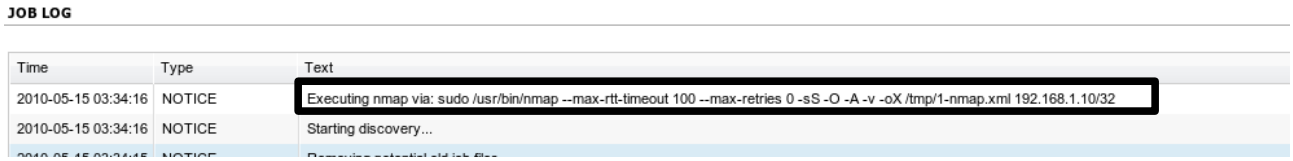
*Exemple pour un hôte: 192.168.1.x/32*

*Pour un groupe d'hôte : 192.168.1.x-x/32*

Pour notre 1er essai, nous allons remonter une seule machine.

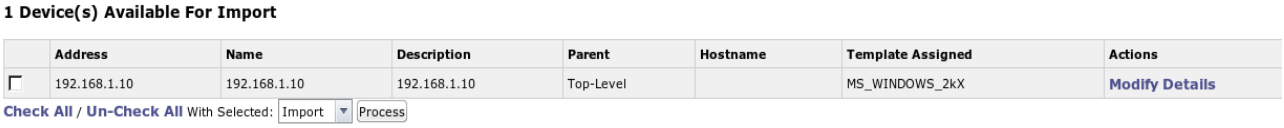
Cliquez sur « *Add Target* » puis sur « *begin auto discovery job* »

Le processus démarre, remarquez le paramètre qui est envoyé au logiciel « *nmap* »

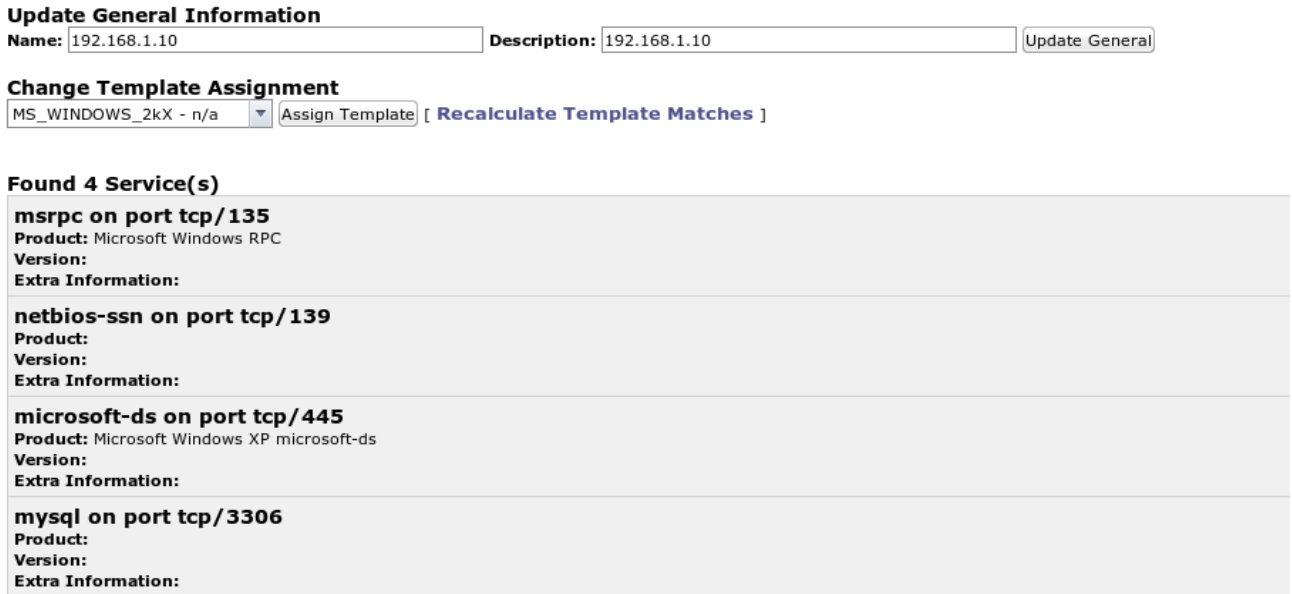



Après une certaine période, une barre verte vous informe que le processus de découverte est terminé et réussi. Cliquez dessus.

Un écran de ce type apparaît



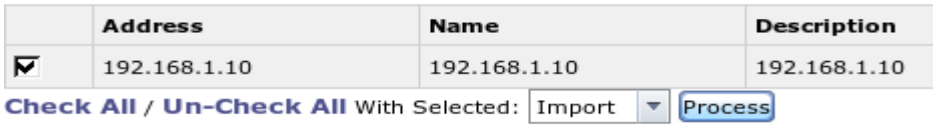

En cliquant sur « *Modify Details* » il est possible de voir les ports de l'hôte qui ont été découverts par « *nmap* ».




Notons qu'il est possible de modifier le template pour cet hôte. Il suffit de sélectionner le nouveau dans « *Change Template Assignement* »puis de cliquer sur « A*ssign Template* » et de cliquer sur « *return to device list* » (en haut à gauche).

Il vous est ainsi possible de récupérer un groupe d'hôtes et d'appliquer un template différent pour l'un d'entre eux.

Il reste plus qu'à importer, le périphérique dans la base de donnée en cochant la case et en cliquant sur « *Process* ».




## 4.3 - Personnaliser un hôte

### 4.3.1 - Procédure

L' hôte est importé. Il est consultable en cliquant sur le lien « *Network* »

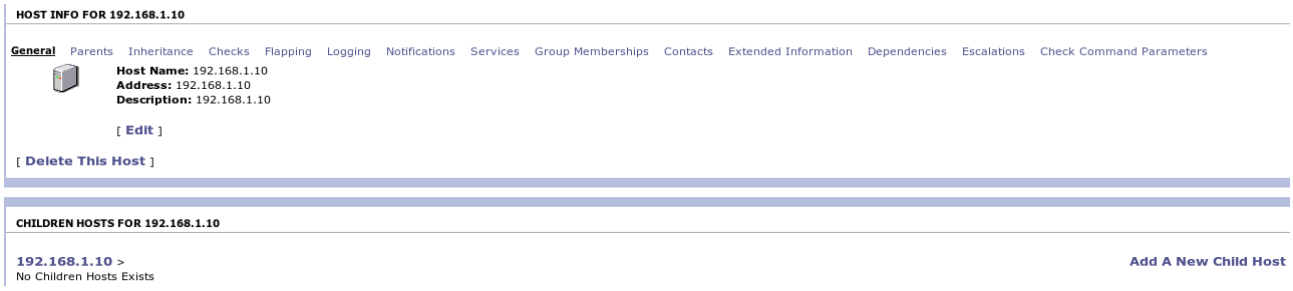

Une fenêtre apparaît et vous liste l'hôte que vous venez d'importer.


Le lien « *Add a new child host* » permet d'ajouter un hôte de façon manuelle. Cela est intéressant si le périphérique n'est pas découvert par « *nmap* ».

En général, si « *nmap* » ne retourne rien, c'est que le périphérique ou son adresse ip est déjà présent dans la BDD Sql de « *lilac* ».

Faites alors une recherche sur l'adresse ip dans le champ « *search* » pour le vérifier.

Nous allons maintenant personnaliser notre hôte en cliquant sur son adresse ip.

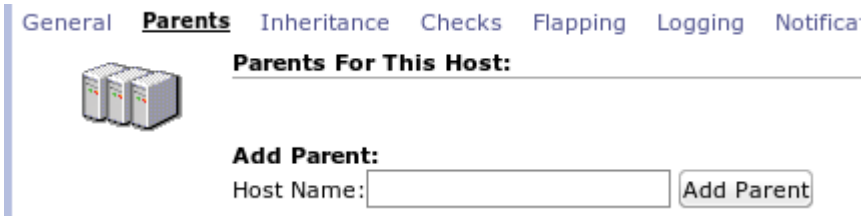



**Explication des menus :**

- **Add a new child host** :

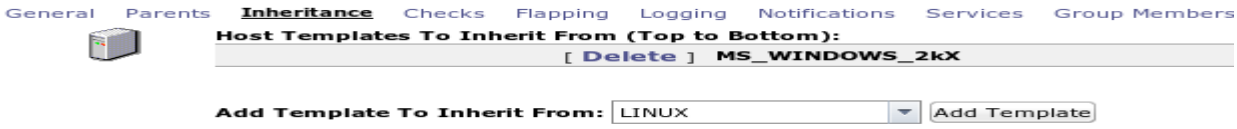
*Il est possible de définir des équipements enfants à ce serveur. Dans notre cas il n'y en a pas mais, on le verra plus tard, cette option est importante pour obtenir une cartographie la plus représentative de notre réseau.*

En cliquant sur le lien « *Parents* », il est possible de définir qui est le parent de cet hôte.




- Inheritance

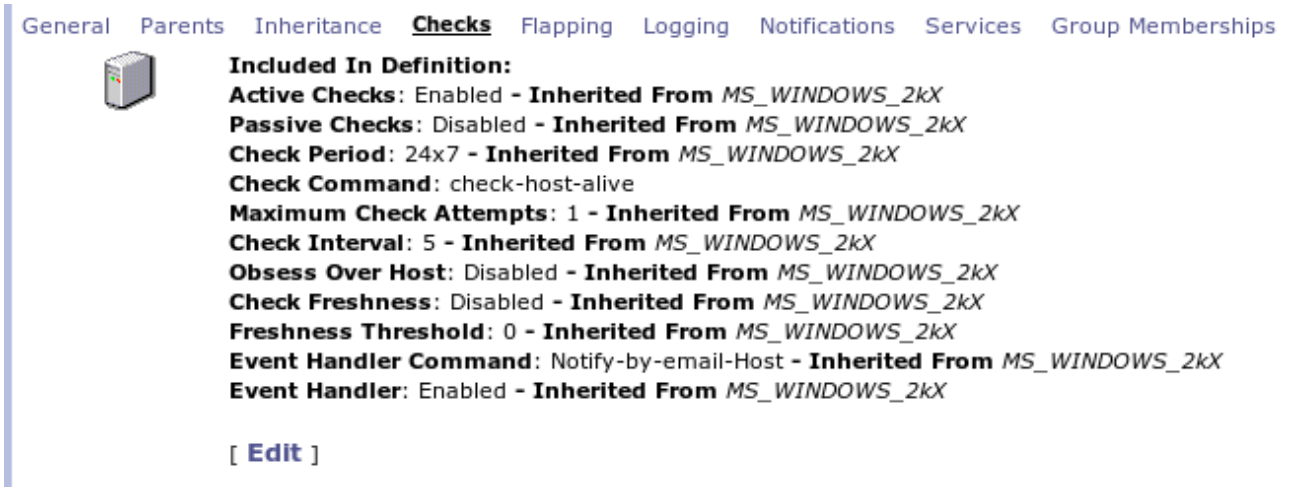
*Permet d'ajouter un ou plusieurs template à notre hôte*.




- **Le lien « Checks »**

*Le menu « check » vérifie la présence de l'équipement cible en utilisant la commande définie dans « Check Command »*

En cliquant sur « *Edit* », il vous est possible de personnaliser ce « *check* »




- **Active checks** :

*Cette directive définit si les contrôles actifs (les contrôles planifiés ou ceux à la demande) sont activés pour cet hôte.*

- **Passive checks** :

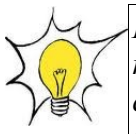
*Permet ou interdit à nagios de modifier l'état des équipements en fonction des traps snmp qu'il reçoit.*

- **Check period** :

*Période pendant laquelle nagios est autorisé à vérifier l'état de l'équipement*

- **Check command** :

*Commande utilisée pour faire cette vérification*



*La commande « check-host-alive » est utilisée pour déterminer si l'hôte est en service ou non. Typiquement, cette commande lance un ping vers l'hôte pour connaître son état. La commande doit retourner un état OK (0) sinon Nagios suppose que cet hôte est hors service.*

- **Maximum check attempts** :

*Nombre maximum de vérifications à effectuer avant de signaler un équipement comme éteint ou en erreur.*

- **Check interval** :

*Nombre de minutes entre deux vérifications.*

- **Event handler** :

*Commande à utiliser lors d'un changement d'état de l'équipement.*

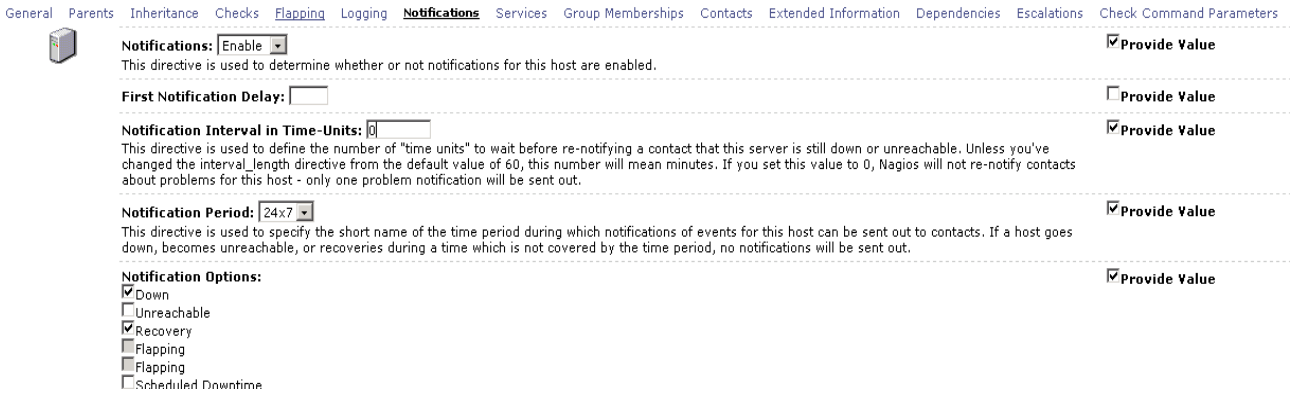
La commande « *Notify-by-email-host* » peut notifier le contact par mail, quand l'hôte est indisponible et quand son état redevient normal. (en fonction de ce qui à été paramétré dans « *Notifications* »). Afin d'éviter le spam de votre boite mail par « *nagios* », il est important de déterminer quels sont les éléments critiques pour lesquels vous devez recevoir un mail de notification.

- **Event handler enabled** :

*Autorise ou non l'utilisation de la commande « event handler » précédemment sélectionnée.*

- Lien « *notification* »

Ce menu vous permet de paramétrer les options de notification.




- **Notification Interval in Time-Units** :

*Une notification d'avertissement est envoyée une seule fois pour l'évènement en cours.*

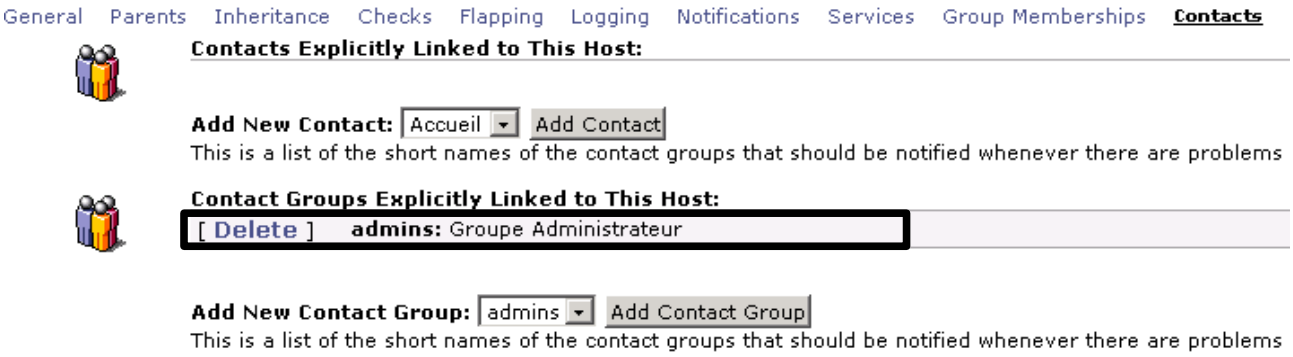
- **Notification Options** :

*Un mail est envoyé uniquement si l'état de l'hôte est « Down » ou « Recovery » (en se basant sur la capture)*

Validez en cliquant sur "*Update Notifications*".

Lien « contacts »

C'est dans ce menu que nous allons déclarer qui doit être prévenu pour cet équipement



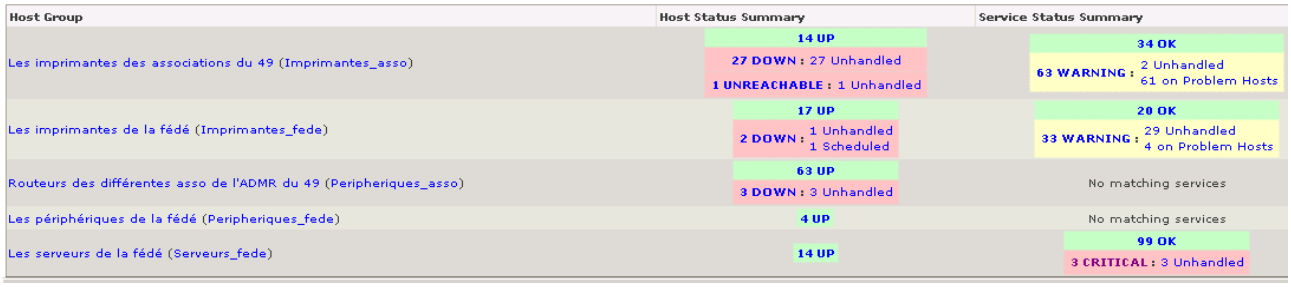

Ici, il s'agit du groupe « *administrateur* ».

Ceci n'est pas suffisant pour recevoir les mails puisque nous n'avons pas encore précisé notre adresse mail. Vous pouvez consulter le chapitre « *ajouter des contacts* »

## Lien « Group memberships »

Ce menu permet d'affecter l'hôte à un groupe.


Sur cette capture l'hôte fait partie du groupe « *serveurs_fede* ». Dans nagios, il sera maintenant possible de filtrer les hôtes en fonction de leurs groupes.

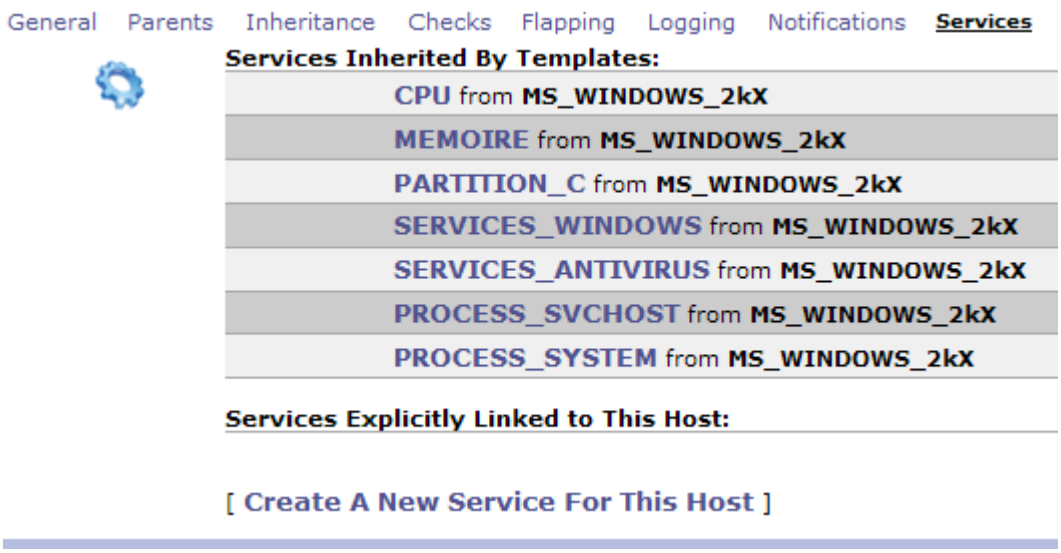



*Capture qui représente les différents groupes d'hôtes*

Pour créer un groupe d'hôtes, il suffit de cliquer sur le lien « *Host Group* » sur la fenêtre principale de « *lilac* » et de créer vos groupes.

## Lien services

Ce menu contient tous les services qui vont être utilisés pour superviser l'hôte.




Sur cette capture, le template « *MS_Windows_2kX* » propose un certain nombre de services par défaut.

Il est possible de cliquer sur chaque service et de modifier son comportement.

Chaque service fait appel à un script qui se trouve dans le répertoire « *plugins* » de « *nagios* » (/srv/eysofnetwork/nagios)

## 4.4 - Personnaliser un service

Nous allons personnaliser le service « *CPU* » en cliquant sur son lien. Nous arrivons à une fenêtre sensiblement identique que la précédente.

Cependant, faites attention, nous venons de cliquer sur un service appartenant au template « *Ms_windows_2kX* ». Cela signifie que nous allons modifier ce service pour tous les hôtes qui héritent de ce template.


Il est possible de créer un service spécifique à cet hôte qui n'héritera pas du template.

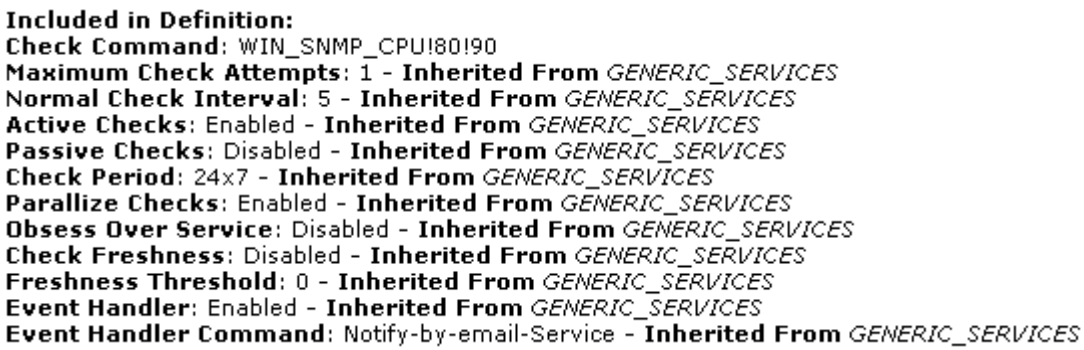
**Lien « Inheritance »**

Là aussi il s'agit d'un template mais pour les services

Ce template est consultable en cliquant sur le lien « *Templates* » en haut de la fenêtre « *lilac* »

**Lien « Checks »**

La même chose que pour l 'hôte sauf qu'il hérite du template « *generic services* » et que la commande de notification n'est plus « *notify-by-email-host* » mais « *notify-by-email-service* » puisque nous supervisons un service. Le contenu du mail sera différent.

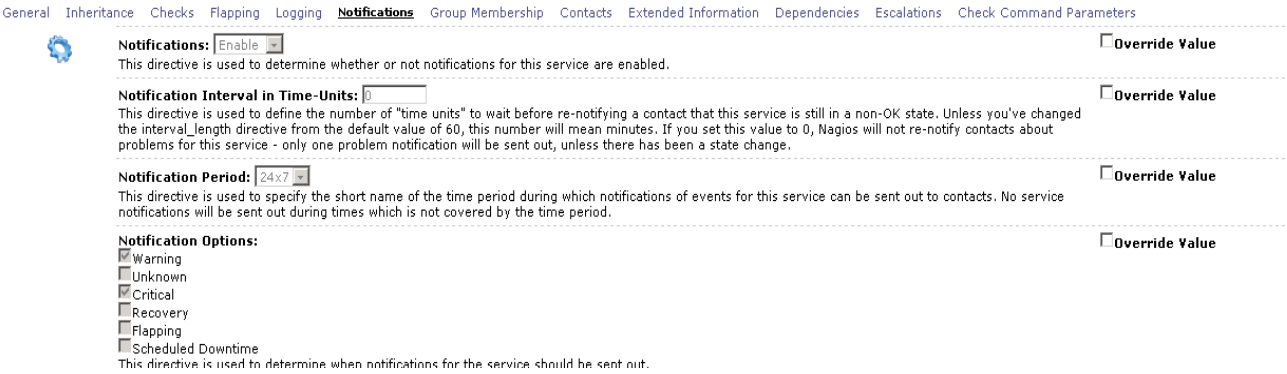



Enfin la commande de « *check* » fait appel à la commande « *win_snmp_cpu* » disponible dans « *Nagios commands* ».

Les valeurs « *!80!90 !* » sont des arguments que l'on passe à la commande, mais pour en comprendre le sens il faut d'abord en comprendre la structure.

## Lien « Notifications »

Il est possible d'être prévenu par mail en fonction de l'état du service.




## Lien « Group Memberships »

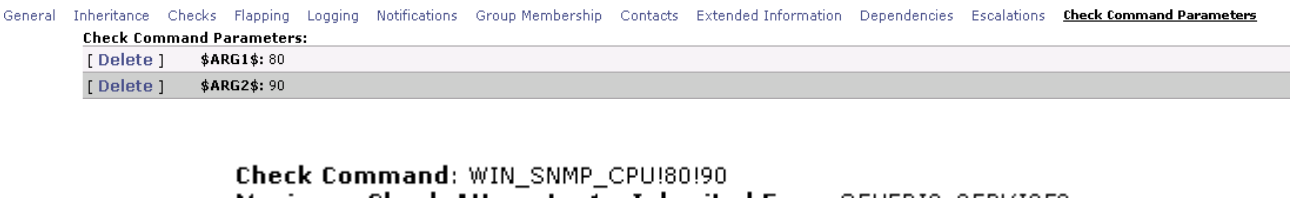
*Il est possible de spécifier si ce service fait partie d'un groupe de services.*

Lien « Contact »

*Qui doit être prévenu si ce service atteint le seuil d'avertissement ou de criticité ?*

## Lien « Check Command Parameters »

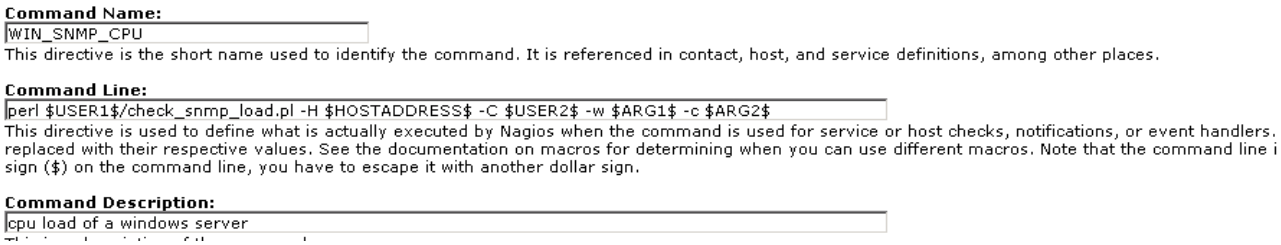
Ce menu permet de préciser les arguments que nous passons à notre commande



## 4.5 - Analyse d' une commande

Nous venons de voir que la commande « *win_snmp_cpu* » accepte des arguments. Mais nous ne savons toujours pas quel est le plug-in utilisé et surtout à quoi correspondent les arguments.

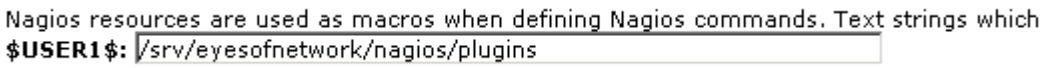
Dans « *lilac* », cliquez sur « *nagios commands* » puis sélectionner la commande « *win_snmp_cpu* ».




- **Command Line** :

**perl** : *La commande fait appel à un script perl.*

**$USER1$** : *correspond au contenu de la variable $USER1$ qui se trouve dans « Nagios Ressources »*




**Check_snmp_load.pl** : *C'est le plug-in qui est utilisé pour cette commande et qui se trouve dans le répertoire « /srv/eyesofnetwork/nagios/plug-ins ».*

**-H** : *adresse ip de l'hôte surpervisé*

**-C $USER2$** : *Idem que $USER1$ mais correspond à la valeur de $USER2$ qui est le nom de communauté*

**-w $ARGS1$** : *seuil à atteindre pour le niveau d'alerte*

**-c $ARGS2$** : *seuil à atteindre pour le niveau critique*

Donc la commande :

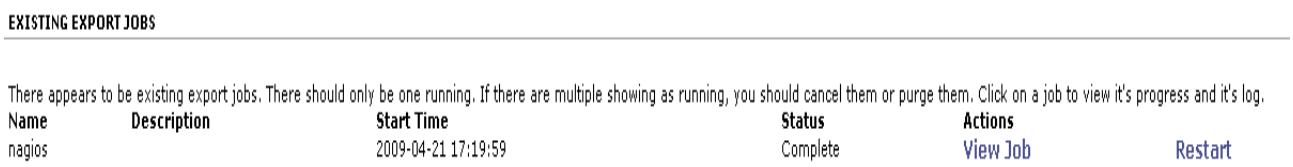

enverra une notification quand le **seuil d'avertissement** atteindra **80%** et une **alerte critique** à **90%**.

## 4.6 - Exportation de l'hôte vers nagios

L'exportation va permettre d'exporter les hôtes paramétrés dans « *lilac* » pour qu'ils puissent être supervisés par « *nagios* ».

Cliquez sur le lien « *Tools* » puis « *Exporter* ».

Un job a été créé par défaut pour l'exportation. Il suffit de cliquer sur « *Restart* » pour démarrer le processus d'exportation.




En cliquant sur « *View job* », on constate l'exécution de 2 directives, « *performing preflight check*» et « *performing nagios restart* »


- **Performing Preflight Check** :

*Cette commande permet de valider la cohérence des différents fichiers de configuration et si une erreur apparaît (élément manquant par exemple) alors le processus d'exportation s'interrompt.*

*L'option -v active le mobe « verbose » ou verbueux. (affiche le détail à l'écran)*

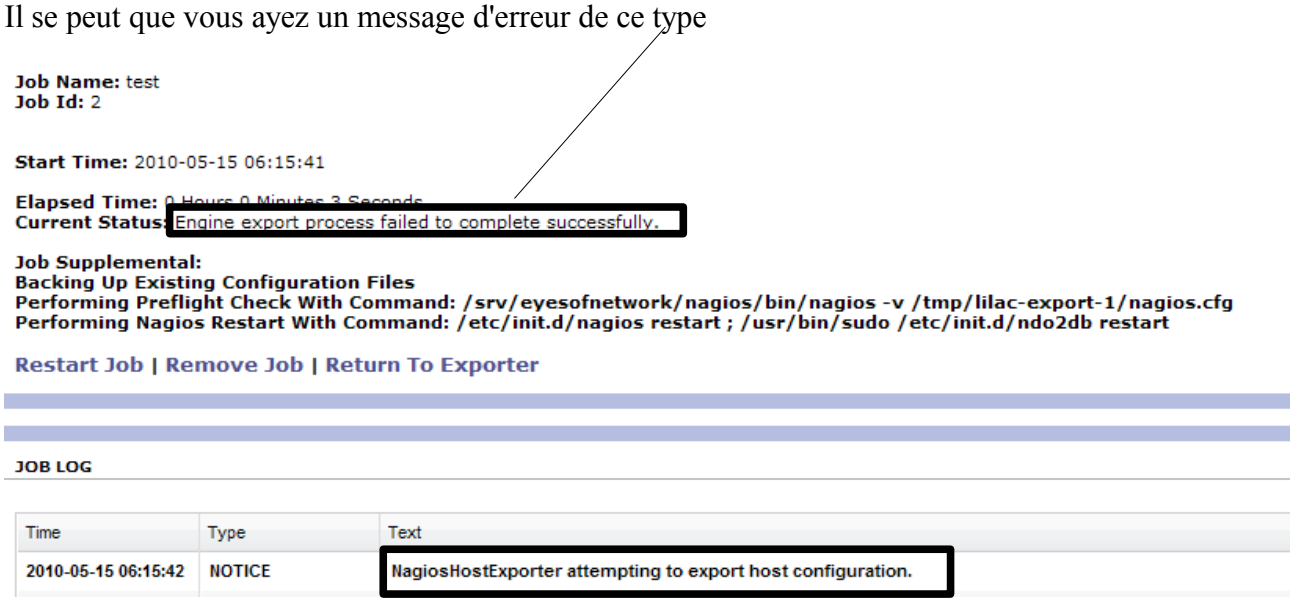
- **Performing Nagis Restart** :

*S'exécute après la commande précédente et redémarre le processus nagios. Si cette étape n'est pas réalisée alors Nagios ne relit pas ses différents fichiers de configurations.*

# 5 - Les erreurs

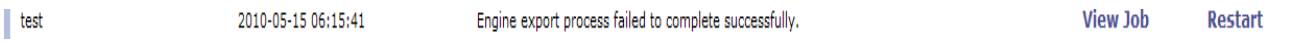
L'aspect désagréable de « *lilac* » sont les messages d'erreurs qui ne sont pas forcément explicites.

Il se peut que vous ayez un message d'erreur de ce type




Pour en apprendre un peu plus, il est nécessaire de lire le log détaillé qui est accessible en cliquant sur « *Return to exporter* »

Cliquez sur « *view job* »




Mais souvent le log détaillé s'avère illisible dû au nombre de pages générées.

Le plus simple est donc d'exécuter la commande « *performing preflight check* » en ligne de commande afin d' obtenir un log plus compréhensible.

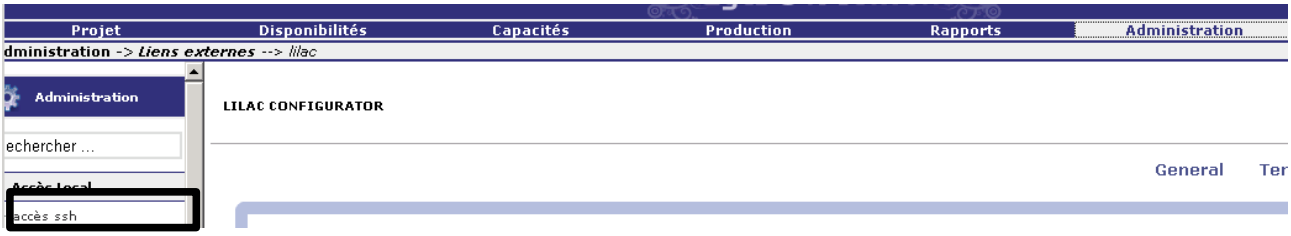
## 5.1 - Comprendre et corriger son erreur

Connectez-vous en ssh à partir de votre terminal sur le serveur (si vous êtes sur un client Linux)

```
ssh root@192.168.x.x
```

Sous « *Windows* » il existe le programme « *putty* » qui permet de se connecter en ssh.

Sinon dans « *EON* », en cliquant sur le lien « *Administration* » puis « *accès ssh* » dans la colonne de gauche.



Une fois authentifié sur le système, il suffit de rentrer cette commande

```
/srv/eyesofnetwork/nagios/bin/nagios -v /tmp/lilac-export-1/nagios.cfg
```

Il s'agit de l'emplacement de l'exécutable de nagios

Emplacement où se trouve le fichier en cours d'exportation.
Le dossier d'exportation porte le même numéro que celui de votre job.

Le process de vérification démarre et vous affiche les erreurs s'il y en a

```
Running pre-flight check on configuration data...

Checking services...
Warning: Service 'Bandwith' on host 'SRVDC1' has no default contacts or contactg
roups defined!
Warning: Service 'CPU' on host 'SRVDC1' has no default contacts or contactgroups
 defined!
```

L'erreur indique que pour ces services il n'y a pas de contact associé aux services.

Le message est clair, il suffit d'apporter une solution corrective à notre erreur et de relancer le processus d'exportation.

Si une erreur se produit, on recommence la manipulation en ligne de commande jusqu'à obtenir le message d'exportation réussi.

**JOB DETAILS**

**Job Name:** nagios
**Job Id:** 1

**Start Time:** 2010-06-06 22:52:32

**Elapsed Time:** 0 Hours 1 Minutes 13 Seconds
**Current Status:** Complete

**Job Supplemental:**
**Performing Preflight Check With Command: /srv/eyesofnetwork/nagios/bin/nagios -v /tmp/lilac-export-1/nagios.cfg**
**Performing Nagios Restart With Command: /usr/bin/sudo /etc/init.d/nagios restart ; /usr/bin/sudo /etc/init.d/ndo2db restart**

**Export Job Complete. Content Exported Successfully.**

Nous allons maintenant découvrir l'interface de « *Nagios* ».

# 6 - « *Nagios* » – superviser ses équipements réseaux

## 6.1 - Présentation de « *nagios* »

Revenez dans la fenêtre principale d' « *EON* » et cliquez sur « *nagios* » à gauche, au niveau de la rubrique « *lien externe* »

Une nouvelle fenêtre s'ouvre .

**Le menu de nagios est découpé en 4 rubriques** :

- *General,*
- *Current status,*
- *Reports,*
- *System*

**Catégorie «General »** :

Un écran sommaire qui contient le numéro de version de « *nagios* » et affiche si une mise à jour est disponible

Ne jamais faire la mise à jour d'un logiciel dans « *EON* » au risque de «**corrompre** » votre système. Il faut attendre la mise à jour du produit « *EON* ».


Nagios® Core™

**Version 3.2.0**

August 12, 2009

Check for updates

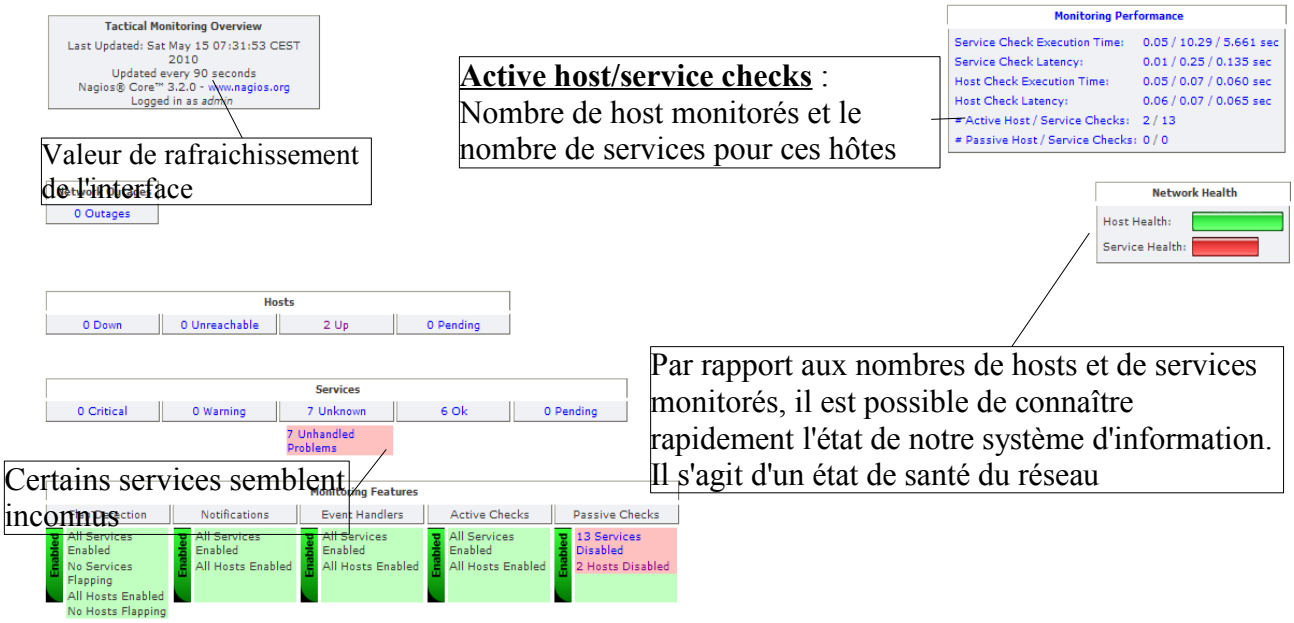
**Read what's new in Nagios Core 3**

**A new version of Nagios is available!**
Visit nagios.org to download Nagios 3.2.1.

Catégorie « Current Status » :

**Explications** :

- **tactical overview** : *vue globale tactique*




Cliquez sur « *7 unhandled problems* » si c'est votre cas afin de vérifier quels sont les services qui ne fonctionnent pas.

| Host | Service | Status | Last Check | Duration | Attempt | Status Information |
|---|---|---|---|---|---|---|
| 192.168.1.10 | CPU | UNKNOWN | 15-05-2010 07:35:49 | 0d 0h 28m 13s | 1/1 | ERROR: Description table : No response from remote host '192.168.1.10'. |
| | MEMOIRE | UNKNOWN | 15-05-2010 07:36:35 | 0d 0h 27m 27s | 1/1 | ERROR: Description/Type table : No response from remote host '192.168.1.10'. |
| | PARTITION_C | UNKNOWN | 15-05-2010 07:37:21 | 0d 0h 26m 41s | 1/1 | ERROR: Description/Type table : No response from remote host '192.168.1.10'. |
| | PROCESS_SVCHOST | UNKNOWN | 15-05-2010 07:38:07 | 0d 0h 25m 55s | 1/1 | ERROR: Process name table : No response from remote host '192.168.1.10'. |
| | PROCESS_SYSTEM | UNKNOWN | 15-05-2010 07:33:53 | 0d 0h 25m 9s | 1/1 | ERROR: Process name table : No response from remote host '192.168.1.10'. |
| | SERVICES_ANTIVIRUS | UNKNOWN | 15-05-2010 07:34:39 | 0d 0h 24m 23s | 1/1 | ERROR: Process name table : No response from remote host '192.168.1.10'. |
| | SERVICES_WINDOWS | UNKNOWN | 15-05-2010 07:35:26 | 0d 0h 23m 36s | 1/1 | ERROR: Process name table : No response from remote host '192.168.1.10'. |

Au niveau de la colonne « *status information* », « *nagios* » nous informe qu'il ne trouve pas les services qu'il doit superviser sur l'hôte.

Cela est normal puisque nous n'avons pas installé le service « *SNMP* » sur l'hôte.

Pour superviser les services d'un hôte il faut que celui-çi gère le protocole SNMP. Dans le cas contraire, à condition de posséder une adresse ip, vous ne pourrez superviser que son état (up ou down).

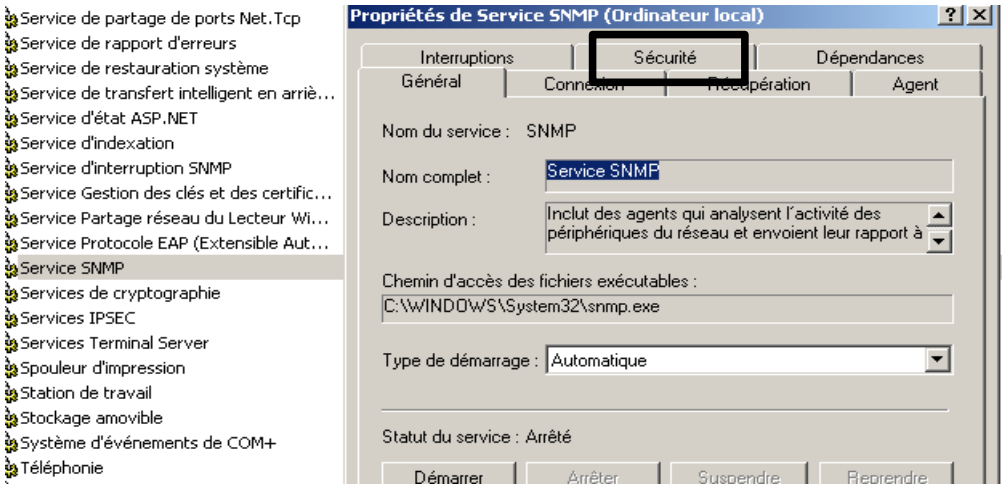
## 6.2 - Installation et configuration de l'agent

Pour installer l'agent snmp sur un OS Windows il faut suivre cette procédure :

1. *Dans ajout/suppression de programme, cliquez sur « ajout de composants windows/outils de gestion d'analyse/cocher snmp (pas le wmi) »*

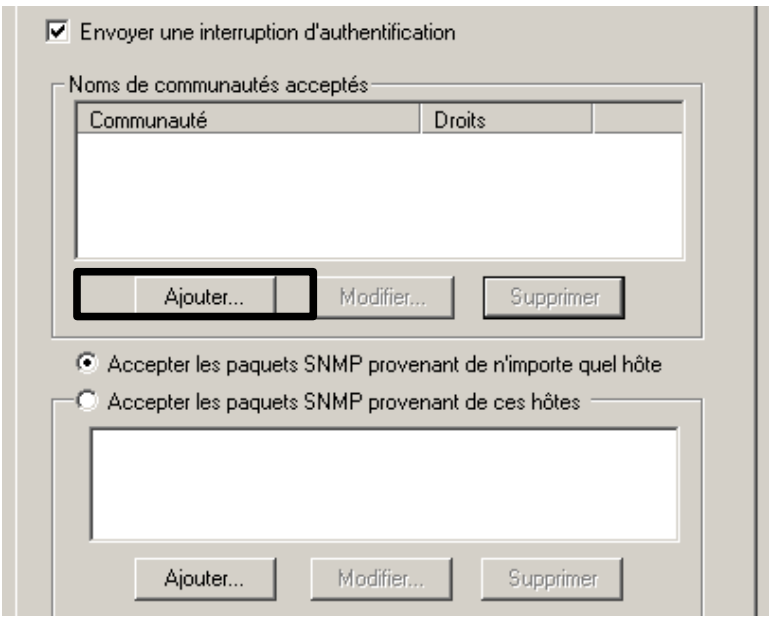
2. *Après installation, allez das « executer » et accéder aux services windows par « services.msc »*

3. *Cherchez le service « snmp » pour accéder à ses propriétés.*




4. *cliquez sur l'onglet «Sécurité »*

Cette fenêtre apparaît

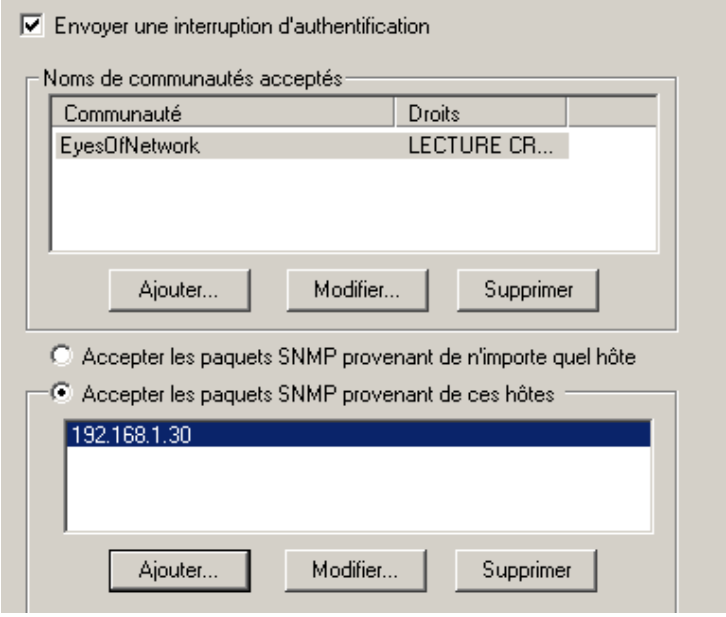



5. *Saisir le nom de la communauté : par défaut « EyesOfNetwork » en « Lecture - création »*

6. *puis sélectionner « accepter les paquets snmp provenant de ces hôtes » et saisir l'adresse*

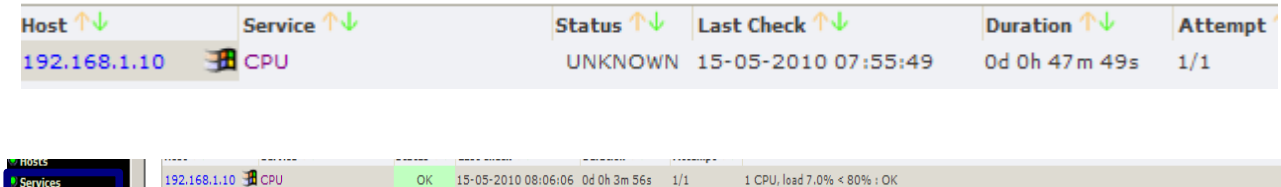
*ip de votre serveur de supervision.*

7. *Redémarrer le service SNMP.*




Il ne vous reste plus qu'à attendre le prochain « *check* » ou alors le forcer.

Après quelques minutes, le service est monitoré.





En revanche, un **avertissement critique** réside sur le « *service antivirus* » et sur le « *service windows* ». Cela est normal car nous ne disposons pas d'antivirus de chez symantec.

Nous allons donc modifier notre template afin de le configurer pour qu'il supervise les bons services

## 6.3 - Modification du template « *Ms_windows_2k* »

Pour rappel, ce template contient un service « *SERVICES_ANTIVIRUS* » qui vérifie que le service « *Symantec* » est présent et est démarré sur l'hôte.

Dans la configuration présentée, il s'agit de l'antivirus « *nod32* » qui est utilisé. Nous allons l'adapter pour qu'il monitore par défaut le service « *ESET Service*» pour tous les hôtes qui hériteront de ce template.

### 6.3.1 - Récupération du nom du service sur le serveur windows

La première chose à faire est de vérifier quel est le nom du service correspondant au client AV.

Dans les services (services.msc), notez le nom du service du client anti-virus

Pour « *NOD32* », il s'agit de « *ESET Service*. »

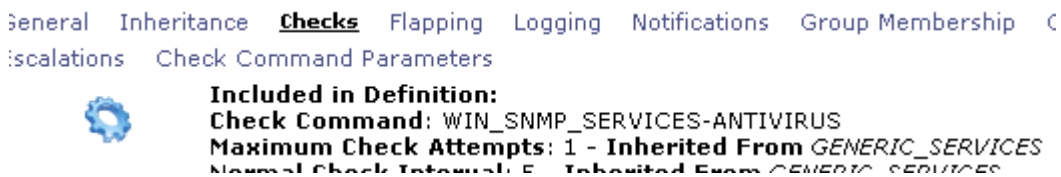

### 6.3.2 - Récupérer le nom de commande

« *Lilac* » contient un certain nombre de commande qui sont utilisées par les templates.

Pour connaître le nom de la commande utilisée par « *lilac* », il suffit de cliquer sur le lien « *Services-ANTIVIRUS* ».

Cette fenêtre apparaît.


Cliquez sur le lien « *checks* »




Nous savons maintenant que « *lilac* » utilise la commande « *WIN_SNMP_SERVICES-ANTIVIRUS* ».

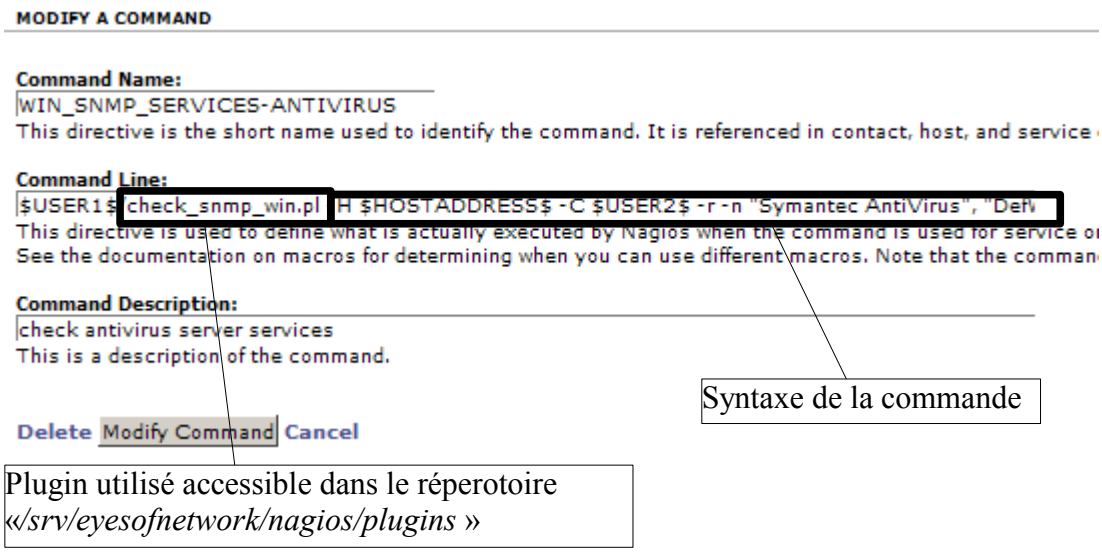
Cette commande est accessible dans « *Nagios Commands* » (page par défaut de lilac).

## 6.3.3 - Test de la commande

Nous allons vérifier quel est le plug-in utilisé par « *lilac* » pour exécuter la commande

« *WIN_SNMP_SERVICES-ANTIVIRUS* ».

En cliquant sur la commande, on obtient cette fenêtre :




Pour tester la commande dans la CLI, il faut se connecter en ssh au serveur de supervision.

```
ssh root@192.168.x.x
```

Puis accéder au répertoire « *plug-ins* » de « *nagios* »

```
cd /srv/eyesofnetwork/nagios/plug-ins
```

**Copier – coller** la syntaxe de la commande et l'adapter en fonction du contexte.

```
./check_snmp_win.pl -H ip de l'hôte -C nom de communauté -r -n « ESET Service »
```

Vous devriez obtenir un résultat équivalent

```
[root@EON plugins]# ./check_snmp_win.pl -H 192.168.1.10 -C EyesOfNetwork -r -n "ESET Ser
vice", "DefWatch"
1 services active (named "ESET Service,") : OK
```

La commande fonctionne. Il ne reste plus qu'à modifier la commande dans « *Nagios Commands* »

et remplacer « *Symantec AntiVirus* » par « *ESET Service* »

## 6.4 - Conclusion du chapitre

Ce chapitre a pour objectif de vous apporter les bases nécessaires à la compréhension de « *lilac* » et de « n*agios* ».

Vous trouverez suite à cette conclusion, un petit chapitre concernant les MIB (à quoi elle servent) et un ensemble de commandes qui peuvent vous servir.

## 6.5 - Un peu de théorie

### 6.5.1 - SNMP v1

La version 1 du protocole SNMP est défini dans la RFC 1157 et ne traite pas de la sécurité de l'accès à la MIB de l'agent.

Le nom de la communauté est transmis en clair dans les messages snmp et peut-être aisément découvert par des analyseurs de protocoles.

Une MIB est une base de donnée qui permet à l'agent de récupérer certaines informations sur le matériel ou le système.

Pour plus d'informations sur les mib, je vous invite à lire le passionnant ouvrage de Monsieur PIGNET « *réseaux informatiques – supervision et administration* » disponible aux éditions eni.

### 6.5.2 - SNMP v2

Amélioration du protocole en ajoutant la fonction « *Get_bulk* » qui permet au manager de demander en bloc plusieurs variables consécutives. Dans la version précédente, 1 requête = 1 réponse.

### 6.5.3 - SNMP v3

Dernière version du protocole qui vise à améliorer la sécurité des échanges entre le manager et l'agent en incluant une procédure d'identification (login/mot de passe) et en chiffrant les information des trames snmp.

Cependant ce protocole n'est pas implémenté sur tous les périphériques actifs. C'est le protocole v2 ou v1 qui est, encore, majoritairement utilisé.

Cela explique pourquoi, il n'est pas possible de saisir un mot de passe dans l'agent snmp de windows.

# 7 - CookBook

## 7.1 - Changer le nom de communauté dans « *EON* »

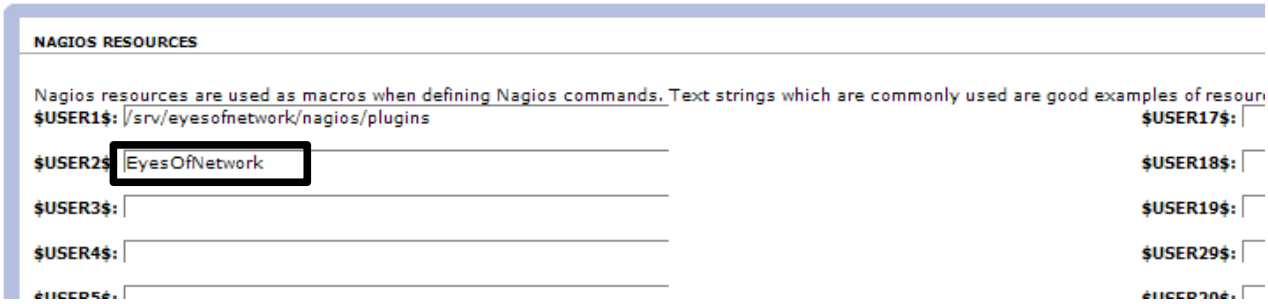
« *Eon* » supervise les hôtes dont le nom de communauté SNMP est « *EyesOfNetwork* ».

Cependant, il est tout à fait envisageable de le modifier.

Le changement de nom de communauté dans EON se fait à 2 endroits :

1. Dans la rubrique « *nagios* » , lien « *configuration* » puis « *nagios ressources* »

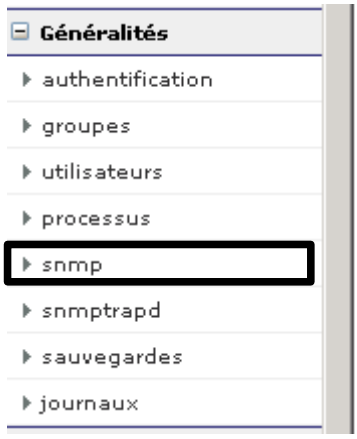
Vous obtenez cette fenêtre




2. Modifiez « *EyesOfNetwork* » par le nouveau nom de communauté

Ou ajoutez votre nouveau nom dans « *$USER3$* ». Il faudra penser à adapter vos commandes nagios qui utilisent la variable « *$USER2$* »

3. Puis revenir sur la page par défaut d' « *EON* » rubrique « *Généralités* » et « *snmp* »




4. Modifiez le nom de communauté par le nouveau

```
#         sec.name  source          community
com2sec notConfigUser  default       EyesOfNetwork
```

## 7.2 - Commande pour monitorer le taux d'occupation des disques dur

La commande permet de vérifier le taux d'occupation d'un disque ou plus en fonction de la valeur que vous allez renseignez à la variable.

Analysons la commande

**Command Name:**
PARTITION-FS_SNMP
This directive is the short name used to identify the command. It is referenced in contact, host, and service definitions, among

**Command Line:**
$USER1$/check_snmp_storage.pl -H $HOSTADDRESS$ -C $USER2$ -m $ARG1$ -w $ARG2$ -c $ARG3$
This directive is used to define what is actually executed by Nagios when the command is used for service or host checks, noti
replaced with their respective values. See the documentation on macros for determining when you can use different macros. N
($) on the command line, you have to escape it with another dollar sign.

- **-m $ARG1$** :

*Le commutateur -m permet de remonter des informations en fonction du nom utilisé dans la description de l'oid.*

- **-w $ARG2$** :

*Seuil pour le niveau warning*

- **-c $ARG3$** :

*Seuil pour le niveau critique*

Nous pouvons tester la commande dans la CLI en demandant de vérifier le taux d'occupation de l'espace disque du disque C.

```
[root@EON plugins]# ./check_snmp_storage -H 192.168.1.10 -C EyesOfNetwork -m [C] -w 80 -c 90 -v
V1 login : EyesOfNetwork
OID : .1.3.6.1.2.1.25.2.3.1.3.1 : A:\
OID : .1.3.6.1.2.1.25.2.3.1.3.2 : C:\ Label:  Serial Number d8c16dd5
OID : .1.3.6.1.2.1.25.2.3.1.3.3 : D:\
OID : .1.3.6.1.2.1.25.2.3.1.3.4 : E:\
OID : .1.3.6.1.2.1.25.2.3.1.3.5 : Virtual Memory
OID : .1.3.6.1.2.1.25.2.3.1.3.6 : Physical Memory
TrouvÃ© : 1 correspondances : 3 requÃªtes
Storage C:\ Label:  Serial Number d8c16dd5 : 6266202 used, 10482404 size, 4096 alloc unit
OK : C:\ Label:  Serial Number d8c16dd5: 60%used(24477MB/40947MB)  : < 80 %  | 'C:\ Label:  Serial Number d8c16dd5'=24477MB;32757;36852;0;40946
[root@EON plugins]#
```

Le commutateur « *-v* » correspond au mode verbose et affiche les OID utilisés par ce plug-in

Pour adapter la commande « *Partition-FS* » afin qu'il monitore toutes les partitions physiques du disque dur, il faut utiliser l'option « *-q* » avec pour valeur « *FixedDisk* »

```
$USER1$/check_snmp_storage.pl -H $HOSTADDRESS$ -C $USER2$ -m -q FixedDisk -w $ARG1$ -c $ARG2$
```

```
[root@localhost plugins]# ./check_snmp_storage.pl -H localhost -C EyesOfNetwork
-m -q FixedDisk -w 90 -c 95
/boot: 12%used(12MB/99MB) /: 16%used(1806MB/11097MB) (<90%) : OK
```

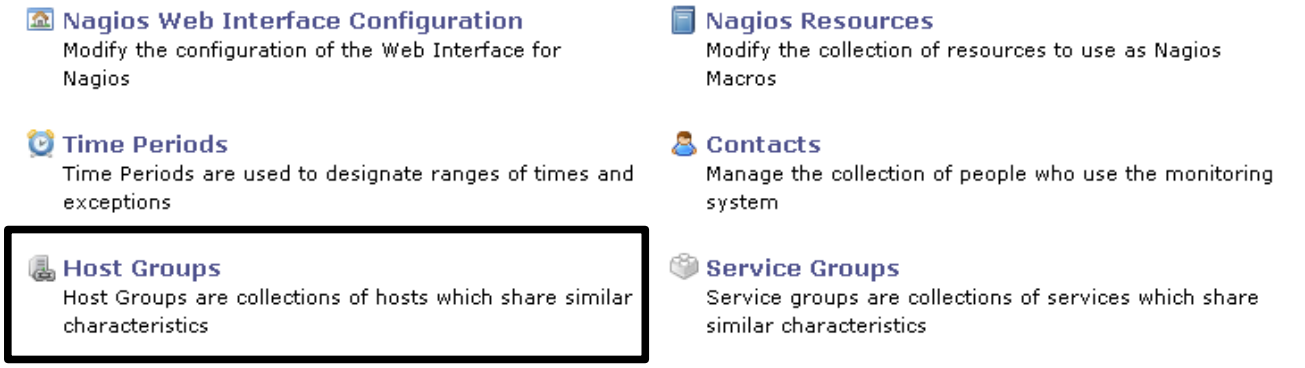
Ce qui donne comme résultat dans la CLI (check de l'espace disque du serveur de supervision) :

## 7.3 - Création de groupes d'hôtes

Il est possible de définir des groupes d'hôtes dans « *lilac* ».

Cela est très intéressant car dans « *nagios* », il sera possible de filtrer la liste des évènements par groupe d'hôtes.

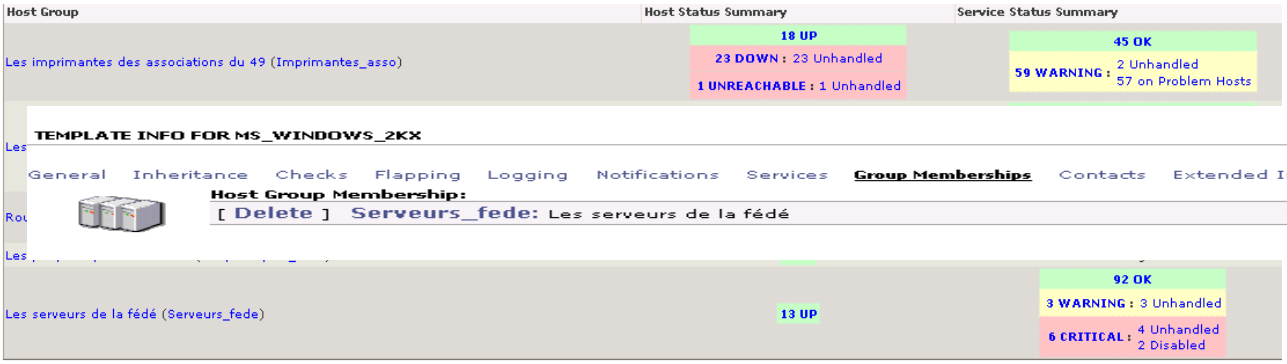
Sur la page générale de liliac, cliquez sur « *host groups* » et créer vos différents groupes.





Dans « *nagios* », en cliquant sur « *Host group - Summary* » nous obtenons cette fenêtre qui nous affiche un récapitulatif par « *HostGroup* »

Pour affecter un hôte à un groupe, soit vous le faites directement sur le template afin que la modification se fasse automatiquement à tous les hôtes qui héritent de celui-ci.




Soit vous le faite hôte par hôte. Dans tous les cas, il faut cliquer sur l'hôte ou le template et cliquer sur ce lien « *Group Memberships* » et sélectionner le groupe d'hôte.

## 7.4 - Relation « *Parents-Enfants* »

La relation « *parents-enfants* » va vous permettre d'obtenir une carte identique à votre topologie logique dans « *nagios* ». Le second intérêt est que si l'élément « *parent* » ne répond plus, « *nagios* » ne vous enverra pas de notifications pour ses enfants.

La 1ere étape est de définir qui est l'élément parent dans notre réseau. En général, c'est le routeur de périphérie. Celui qui permet de router vos paquets internes vers le réseau Internet.

Voici une partie des hôtes qui seront supervisés.

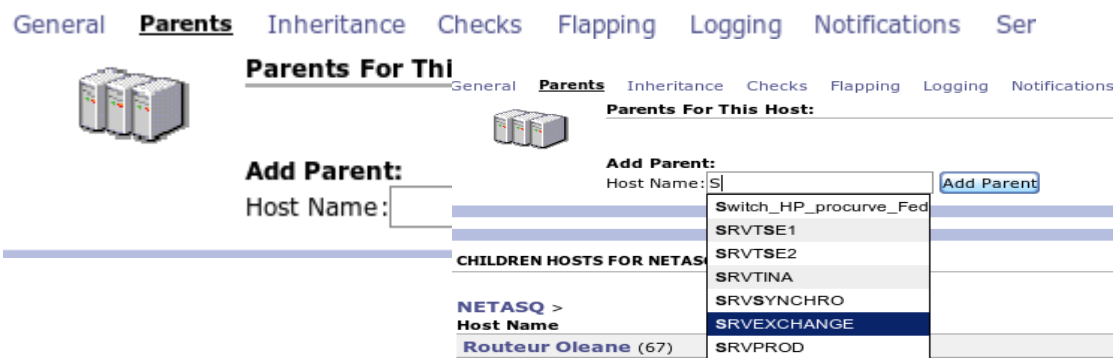

Nous avons un routeur, un switch manageable, et des serveurs qui sont connectés au switch.

La (1) à côté du routeur Oleane signifie qu'il possède 1 enfant.

L'ajout d'un enfant à un périphérique est très simple.

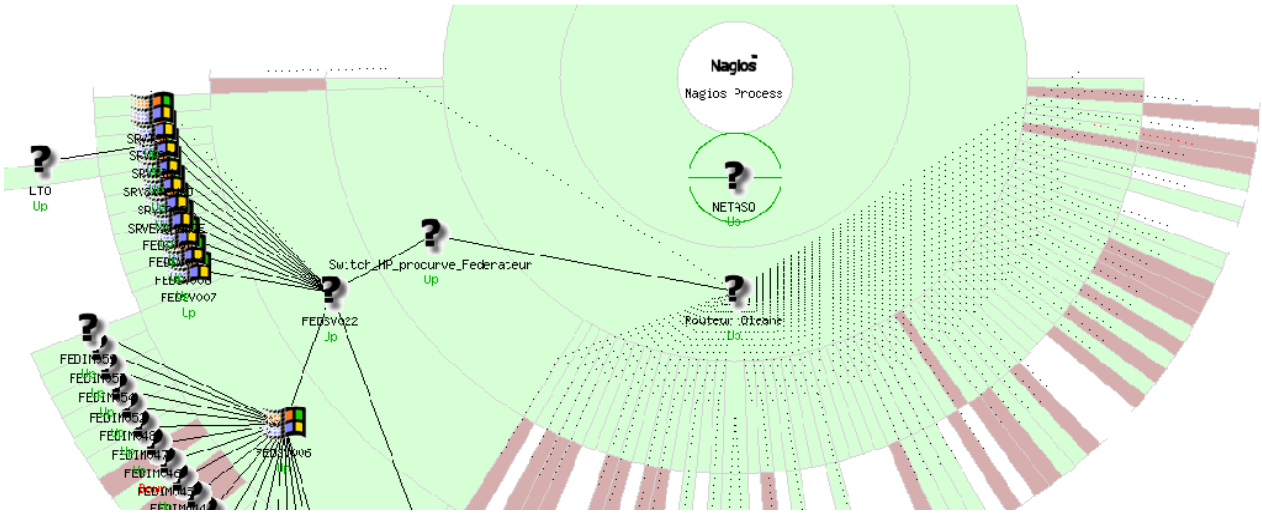
1. Cliquez sur l'hôte enfant puis sur le lien « *Parents* »

Vous arrivez sur cette fenêtre




2. Précisez l'hôte « *Parents* » et Validez.

Dans nagios, nous obtenons une carte de ce type :



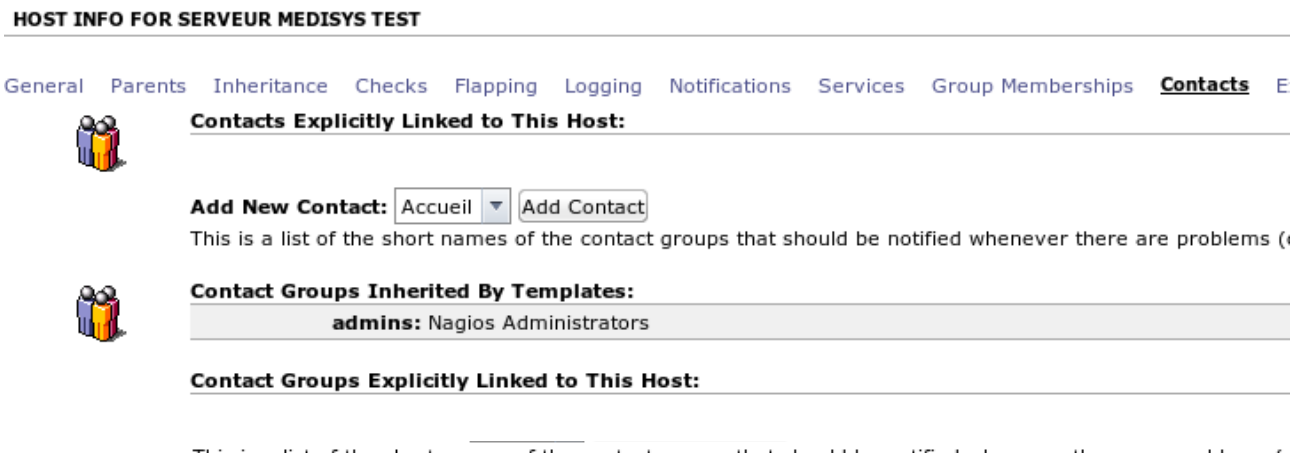

*Carte de nagios avec activation de filtres pour rendre la carte plus lisible*

La carte de « *nagios* » n'est pas forcement très lisible. Nous verrons plus tard, qu'il est possible de créer des cartes plus claires avec « *nagvis* ».

## 7.5 - Ajouter des contacts

1. Dans « *liliac* », sur la page de démarrage, cliquez sur « *contact* »
2. Editez le contact « *admin* » et lui donner une adresse mail

Si besoin, ajoutez vos contacts à des templates




## 7.6 - Ajout d'un plug-in pour monitorer les imprimantes

Nous allons utiliser ce plug-in « *SNMP Printer Check* » disponible sur Nagios Exchange.

Il est possible que le « *serveur postfix* » de « *nagios* » ne puissent pas relayer les mails provenant de « ***nagios@domaineltd.com*** » vers votre serveur de messagerie.
Pour corriger cette erreur, il suffit d'éditer le fichier « */etc/postfix/main.cf* » et d'ajouter ces 2 directives à la fin du fichier :

- ***relay_domains = votredomaine.fr***
- ***relayhost = ip du serveur de mail***

http://exchange.nagios.org/directory/plug-ins/Hardware/Printers/SNMP-Printer-Check/details

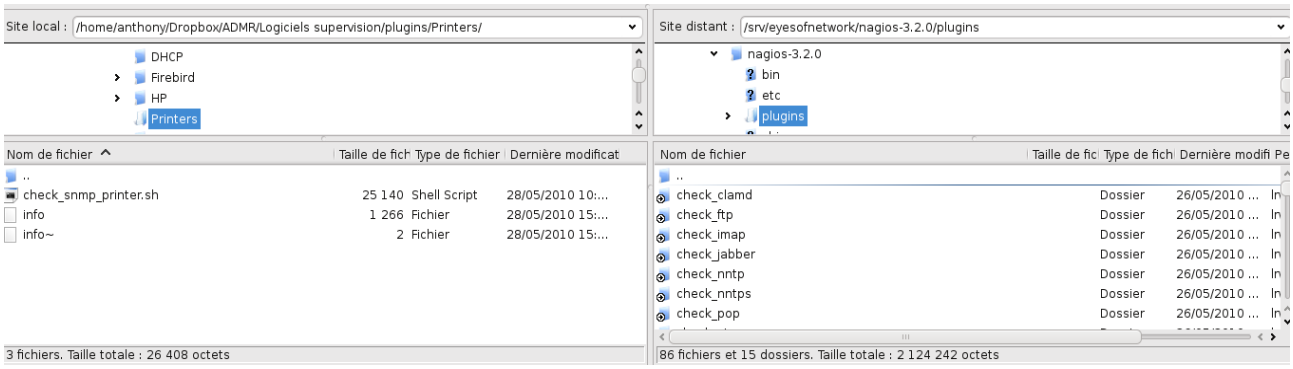
Après téléchargement du plug-in, nous allons l'envoyer dans le répertoire plug-ins du serveur de supervision.

1. Utilisez votre client FTP puis saisir l'adresse ip du serveur en précisant le port 22

Votre client doit gérer le protocole ssh ou utilisez « *winscp* »

2. Naviguez jusqu'au répertoire « */srv/eyesofnetwork/nagios/plug-ins* »
3. Sélectionnez votre plug-in et l'uploader.

*Connexion au serveur de supervision avec le client FTP Filezilla*




Le plug-in est uploadé mais n'est pas exécutable.

4. Accédez en ssh au serveur de supervision.
5. Naviguez dans le répertoire « *plug-ins* » et saisir cette commande pour le rendre exécutable.

```
Chmod 775 ./check_snmp_printer.sh
```

Si vous rencontrez une erreur de ce type « ***unknown ^M***» c'est que le fichier a été enregistré sous windows et qu'un problème de caractères existe.

Il faut saisir la commande « ***dos2unix nomfichier*** » pour régler ce problème

Testez ensuite votre plug-in avec une imprimante en saisissant la commande

```
./check_snmp_printers ip imprimante nom de communauté CONSUM TEST
```

soit

```
./check_snmp_printers 192.168.0.10 EyesOfNetwork CONSUM TEST
```

Pensez à activer le protocole SNMP sur l'imprimante ou photocopieur réseau

Cette commande a pour effet de vérifier ce qui peut-être supervisable sur l'hôte.

```
[root@fedpo098 plugins]# ./check_snmp_printer.sh 192.168.0.30 EyesOfNetwork CONSUM ALL
Black Cartridge is at 95% - OK!
```

Sur cette capture, la commande nous informe qu'il est possible de superviser le toner noir.

Pour superviser uniquement ce Toner  il faut saisir la commande suivante :

```
./check_snmp_printers 192.168.0.10 EyesOfNetwork CONSUMX "Black Cartridge"
```

Le plug-in « *check_snmp_printer* » contient beaucoup de commandes. Pour les lister, il suffit d'éditer le plug-in avec la commande « *vi* ».

En effet, le plug-in contient un bug qui empêche d'afficher l'aide de l'utilisateur.

Il nous reste plus qu'à créer un template en fonction du modèle d'imprimante.

## 7.7 - Création d'un template imprimante

Nous allons créer un template correspondant à notre modèle d'imprimante. Ainsi, quand une nouvelle imprimante correspondante à ce modèle sera ajoutée à notre parc, il suffira de le sélectionner le bon template et l'exporter dans nagios. Le gain de temps apporté par les templates est significatif.

1. Cliquez sur le lien « *Templates* » et cliquez sur « *Add a new host template* »
2. Donnez un nom à votre template, par exemple « *HP laserjet 1320* »
3. Cliquez sur le lien « *checks* » et complétez comme suit (c'est un exemple)

**Included In Template:**
**Initial State**: Up
**Active Checks**: Enabled
**Passive Checks**: Disabled
**Check Period**: 24x7
**Check Command**: check-host-alive
**Retry Interval**: 5
**Maximum Check Attempts**: 1
**Obsess Over Host**: Disabled
**Check Freshness**: Disabled
**Freshness Threshold**: 0

On vérifie que l'hôte est actif, mais on ne souhaite pas être averti par mail.
Nous estimons que le processus de démarrage et redémarrage d'une imprimante est à la charge de l'utilisateur et que cela fait partie du cycle de vie normal d'une imprimante.

4. Cliquez sur « *Group Memberships* », si votre template appartient à un groupe.
5. Cliquez sur le lien « *services* » pour y ajouter les services à superviser pour ce type d'imprimante
6. Donnez un nom à votre service. Ici « *Toner Noir* »
7. Puis cliquez sur le lien « *Inheritance* » et sélectionnez le template « *Generic service* »
8. Cliquez sur le lien « *check* » pour sélectionner la commande qui va être utilisée pour le check du service.
9. Activez l'option « *event handle*r » et la commande « *Notify-by-email-service* »
10. Puis cliquez sur le lien « *Notifications* » et sélectionnez les états « *critical* » dans « *Notifications options* »
11. Enfin, sélectionnez le contact qui doit être averti par mail quand le toner atteint le seuil critique ou d'avertissement.
12. Cliquez sur le lien « *check command parameters* » et renseignez le nom du toner qui est à superviser « T*oner Cartridge* » dans notre cas.

En cliquant sur le lien « *checks* » nous obtenons cet écran :

**Included in Definition:**
**Check Command**: check_toner!"Toner Cartridge "
**Maximum Check Attempts**: 1 - **Inherited From** *GENERIC_SERVICES*
**Normal Check Interval**: 5 - **Inherited From** *GENERIC_SERVICES*
**Active Checks**: Enabled - **Inherited From** *GENERIC_SERVICES*
**Passive Checks**: Disabled - **Inherited From** *GENERIC_SERVICES*
**Check Period**: 24x7 - **Inherited From** *GENERIC_SERVICES*
**Parallize Checks**: Enabled - **Inherited From** *GENERIC_SERVICES*
**Obsess Over Service**: Disabled - **Inherited From** *GENERIC_SERVICES*
**Check Freshness**: Disabled - **Inherited From** *GENERIC_SERVICES*
**Freshness Threshold**: 0 - **Inherited From** *GENERIC_SERVICES*
**Event Handler**: Enabled
**Event Handler Command**: Notify-by-email-Service

La commande « *check_toner* » n'existe pas dans « *Nagios Command*s ». C'est une commande que j'ai créée à partir du plug-in « *check_snmp_printers* ».

En voici la syntaxe :

```
$USER1$/check_snmp_printer.sh $HOSTADDRESS$ $USER2$ CONSUMX $ARG1$
```

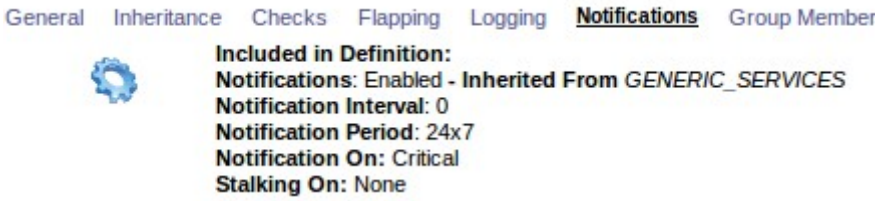
où « *$ARG1$* » correspond à l'élément qui doit être supervisé dans l'imprimante.

Pour résumer :

Nous demandons que le service « *Toner Noir* » qui utilise la commande « *Nagios* » « c*heck_toner* » vérifie le toner qui s'appelle « *Toner Cartridge* ».
Quand le toner atteint le seuil critique, défini par le plug-in, une notification par mail est envoyée grâce à la commande « *notify-by-email-service* ».

Sous réserve d'avoir paramétré le lien « *notification* » et « *contacts* »

Ce menu est important, car un mail sera envoyé seulement si le service atteint un niveau critique.

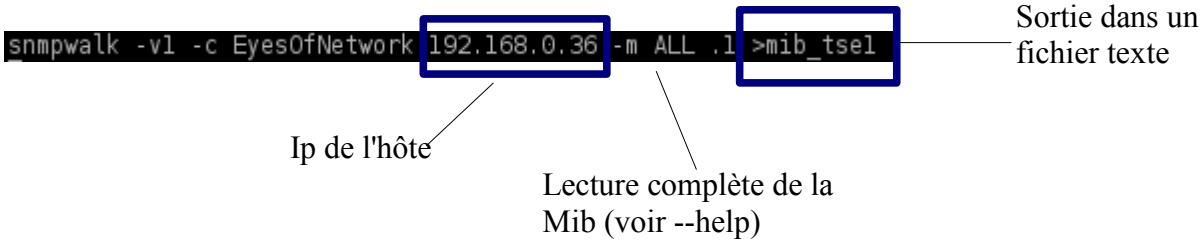



Vous pouvez maintenant créer d'autres templates ou ajouter des services à ce dernier.

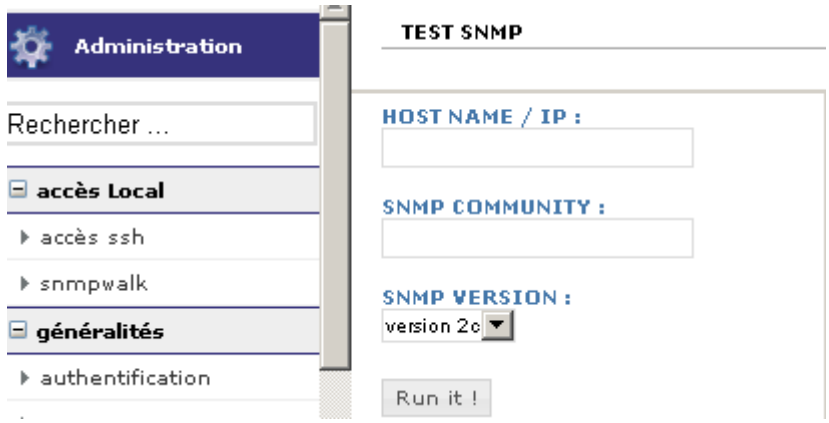
## 7.8 - Récupérer la MIB d'un hôte

Pour récupérer la MIB d'un hôte, vous avez 2 solutions :

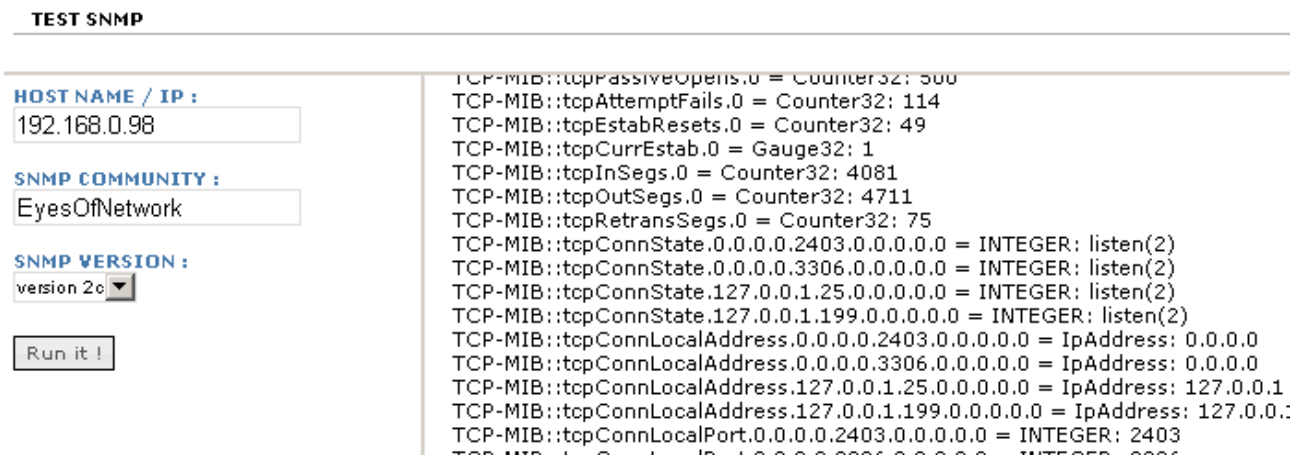
- La plus simple est de cliquer sur le lien « *snmpwalk* » disponible sur la page principale d' « *EON* »
- ou sen connectant en ssh et saisir la commande




Il ne reste plus qu'à récupéré le fichier généré avec « *filezilla* » (par exemple). Les puristes préfèreront la commande « *scp* ».




*Utilisation de la commande « snmpwalk » disponible sur l'interface d' « EON » (lien « administration »)*




Pour superviser ensuite un service spécifique avec « *check_snmp* » il vous suffit de déclarer l'oid que vous souhaitez checker.

Je vous invite à prendre connaissance de l'ouvrage de Monsieur PIGNET « S*upervision et réseaux* » qui vous permettra de comprendre la structure des OID.

## 7.9 - Superviser un serveur Exchange

« *Lilac* » propose de nombreuses commandes pour monitorer un serveur exchange US.

Nous allons apporter quelques modifications à ces commandes afin de les faire fonctionner sur un serveur Exchange FR.

Dans « *nagios commands* », cliquez sur la commande « *WIN_SERVICES_EXCHANGE* ».

Voici le nom des services à monitorer pour la version FR.

```
$USER1$/check_snmp_win.pl -H $HOSTADDRESS$ -C $USER2$ -n "Service d'administration IIS","Microsoft Exchange - Piles MTA","Gestion de Microsoft Exchange","Microsoft Exchange - Moteur de routage","Microsoft Exchange - Surveillance du syst.me","Microsoft Exchange - Banque d'informations","Simple Mail Transfer Protocol"
```

Les caractères joker (é, è etc...) sont à remplacer par des « . »

**Modification des commandes**

- « *WIN_EXCHANGE_MSG-SENT/MIN* » qui permet de connaître le nombre de mail envoyés par minute
- « *WIN_EXCHANGE_MSG_REFUSED_SIZE* » qui permet de connaître le nombre de messages refusés à cause de la taille du message
- « *WIN_EXCHANGE_CONNECTED_USERS* » qui permet de savoir le nombre d'utilisateurs connectés sur le serveur exchange
- « *WIN_EXCHANGE_TPS_REMISE* » qui permet de connaître le temps moyen de remise pour un message
- « *WIN_EXCHANGE_MSG_QUEUE_RECEPTION* » le nombre de messages en attente de réception placés dans la queue
- « *WIN_EXCHANGE_MSG_SEND_QUEUE* » le nombre de messages envoyés

Afin de pouvoir monitorer ces services pour la version FR d'exchange, il faut ajouter le service que l'on souhaite superviser dans le « *nsci.ini* » du client « *nsclient++* ».

Après installation de « *nsclient++* », éditez le « *nsc.ini* » et décommentez la ligne « *NRPEListener.dll* »

Puis ajouter une section [*NRPE Handlers*] qui contiendra nos différentes commandes NRPE

J'ai crée cette section après la section *[Wrapped Scripts]*

Examinons le service « *WIN_EXCHANGE_MSG-SENT/MIN* »

```
COUNTER -l "\MSExchangeIS Mailbox(_Total)\\Messages Sent/min","Messages Envoyés/min : %.f" -w 60 -c 90
```

**Explications** :

La commande utilise le compteur de performance de windows pour afficher son résultat.

Sur la version Fr d'exchange, le chemin d'accès pour afficher ce compteur est :

```
\MSExchangeIS Boîte aux lettres(_Total)\Messages envoyés/min
```

Nous allons donc inscrire une commande dans le « *nsci.ini* » qui va checké ce compteur.

On donnera un nom à cette commande et on demandera au serveur nagios de checker le nom de la commande.

Nous allons maintenant récupérer la liste des compteurs que ce serveur peut superviser.

Dans la cli de Windows, exécutez la commande :

```
nsclient++.exe CheckSystem listpdh >sortie.txt
```

Au vu de la liste impressionnante des counters il est préférable de sortir le résultat dans un fichier texte que vous pourrez consulter à loisir.

Dans le « *nsci.ini* » au niveau de la section [*NRPE handlers*] ajoutez la commande qui va checker ce compteur

```
check_messagesmin=inject checkCounter "Counter:Messages envoyes/min=\MSExchangeIS Boîte aux lettres(_Total)\Messages envoyés/min" ShowAll MaxWarn=120 MaxCrit=150
```

**Explications** :

- check_messagesmin : *il s'agit de l'identifiant qui va me permettre de checker ce compteur*

- counter:Messages envoyes : *Le résultat affichera « messages envoyes : xxx »*
- =\MSExchangeIS Boîte aux lettres(_Total)\Messages envoyés/min : *chemin du compteur pour ce service*
- Show all MaxWarn= *Seuil d'avertissement*

Redémarrez le service « *nsclient* » pour prendre en compte les changements.

Dans « *EON* », faire un check de cette commande

Et voilà le résultat.


Dans lilac, il ne reste plus qu'à créer ou modifier la commande

```
$USER1$/check_nt -H $HOSTADDRESS$ -p 12489 -v COUNTER -l "\\MSExchangeIS Mailbox(_Total)\\Messages Sent/min","Messages Envoyés/min : %.f" -w 60 -c 90
```

par

```
$USER1$/check_nrpe -H $HOSTADDRESS$ -c check_messages_en_min
```

**Pour le nombre de messages remis, nous obtenons cette commande** :

```
check_messages_rem_min=inject checkCounter "Counter:Messages remis/min=\MSExchangeIS Boîte aux lettres(_Total)\Messages remis/min" ShowAll MaxWarn=200 MaxCrit=300
```

Et dans lilac

```
$USER1$/check_nrpe -H $HOSTADDRESS$ -c check_messages_rem_min
```

**Pour le nombre de messages refuses en fonction de la taille** :

```
check_messages_refus_taille=inject checkCounter "Counter:Messages refuses (taille)=\Serveur SMTP(_Total)\Messages refusés : taille" ShowAll MaxWarn=60 MaxCrit=90
```

Et dans lilac

```
$USER1$/check_nrpe -H $HOSTADDRESS$ -c check_messages_refus_taille
```

**Nombre de sessions actives sur le serveur exchange** :

```
check_connect_actives=inject checkCounter "Counter:Ouverture de sessions clientes actives=\MSExchangeIS Boîte aux lettres(_Total)\Ouvertures de session client active" ShowAll MaxWarn=200 MaxCrit=250
```

Soit dans lilac

```
$USER1$/check_nrpe -H $HOSTADDRESS$ -c check_connect_actives
```

```
[root@fedpo098 plugins]# ./check_nrpe -H 192.168.0.12 -c check_connect_actives
OK: Ouverture de sessions clientes actives: 86|'Ouverture de sessions clientes actives'=86;200;250;
```

**Pour les messages dans la file d'attente d'envoi**

```
check_queue_sent=inject checkCounter "Counter:Messages en queue d'envoi=\MSExchangeIS Boîte aux lettres(_Total)\Taille de la file d'attente pour envoi" ShowAll MaxWarn=60 MaxCrit=90
```

soit dans lilac

```
$USER1$/check_nrpe -H $HOSTADDRESS$ -c check_queue_sent
```

```
[root@fedpo098 plugins]# ./check_nrpe -H 192.168.0.12 -c check_queue_sent
OK: Messages en queue d'envoi: 0|'Messages en queue d'envoi'=0;60;90;
```

## 7.10 - récupérer les adresses dhcp libre

Par défaut, Liliac propose un script « *check_dhcp_addfree* » qui retourne le nombre d'ip disponibles.

Le script n'existe malheureusement pas dans le répertoire « *plug-ins* ».

C'est à vous de le rajouter et de le rendre exécutable par un « *chmod 775* »

Vous pouvez le télécharger sur ce site :

http://lkco.gezen.fr/svn/supervision/trunk/plug-ins-nagios/Windows/

La syntaxe pour le tester est simple

```
./check_dhcp_addfree -H 192.168.0.5 -C EyesOfNetwork -w 8 -c 6 -s 192.168.0.0
```

**Explication** :

-s : *l'adresse ip réseau*

## 7.11 - Superviser un serveur ESXi 3.5

Par défaut, il n'est pas possible d'activer le protocole snmp dans ESXI à moins de posséder virtualcenter.

Cependant, il reste possible de l'activer en accédant à la CLI de « *vmware* ».

Sur le serveur ESXI, appuyer simutanément sur « *alt+F1* ».

Vous arrivez dans une fênêtre de log. Saisir dans le vide « *unsupported* » puis valider

Vous devez, ensuite, saisr votre mot de passe « *root* »

Un message apparaît et vous informe des dangers de la CLI.

**Editez le fichier « *snmp.xml* »**

```
vi /etc/vmware/snmp.xml
```

Puis appuyer sur « *I* » pour entrer en mode insertion.

**Modifier les valeurs contenues dans les balises par :**

```
<enable>False</enable><enable>true</enable><communities>mettre votre nom de communauté</communities> <targets> mettre ip du serveur de supervision.</targets>
```

Puis enregistrez les modifications, en appuyant sur « *echap* » puis « *:wq* » (write, quit)

Redémarrez le service en saisissant

```
/sbin/services.sh restart
```

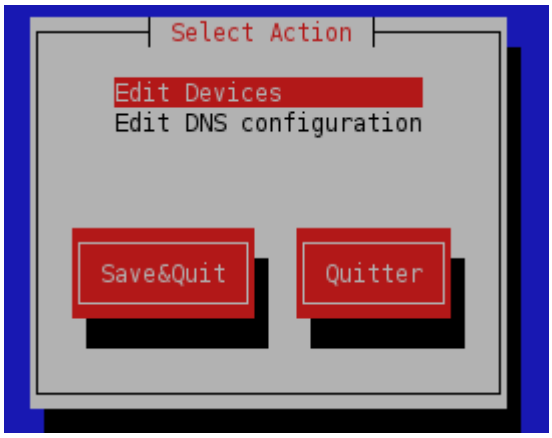
Pour vérifier si le snmp est activé, faites un « *snmpwalk* »

## 7.12 - Modification de l'adresse ip du serveur de supervision

1. Se connecter à la CLI
2. Saisir

```
system-config-network
```

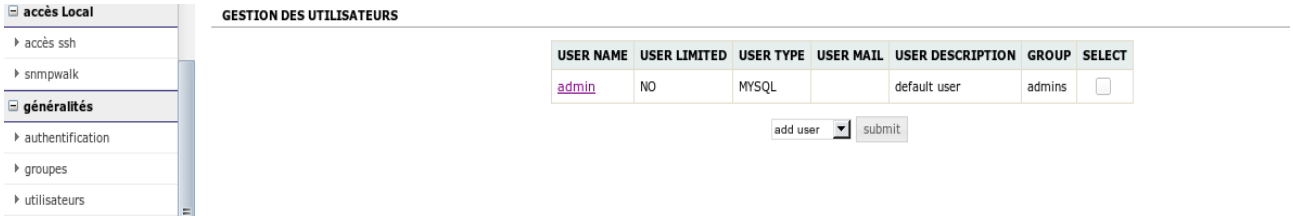
3. Cette fenêtre apparaît




Il ne vous reste plus qu'à procéder aux modifications et redémarrer le service réseau par

```
/etc/init.d/network restart
```

## 7.13 - Ajouter des users et donner des droits




Il est possible d'ajouter des utilisateurs et de modifier le mot de passe de connexion à l'interface web.

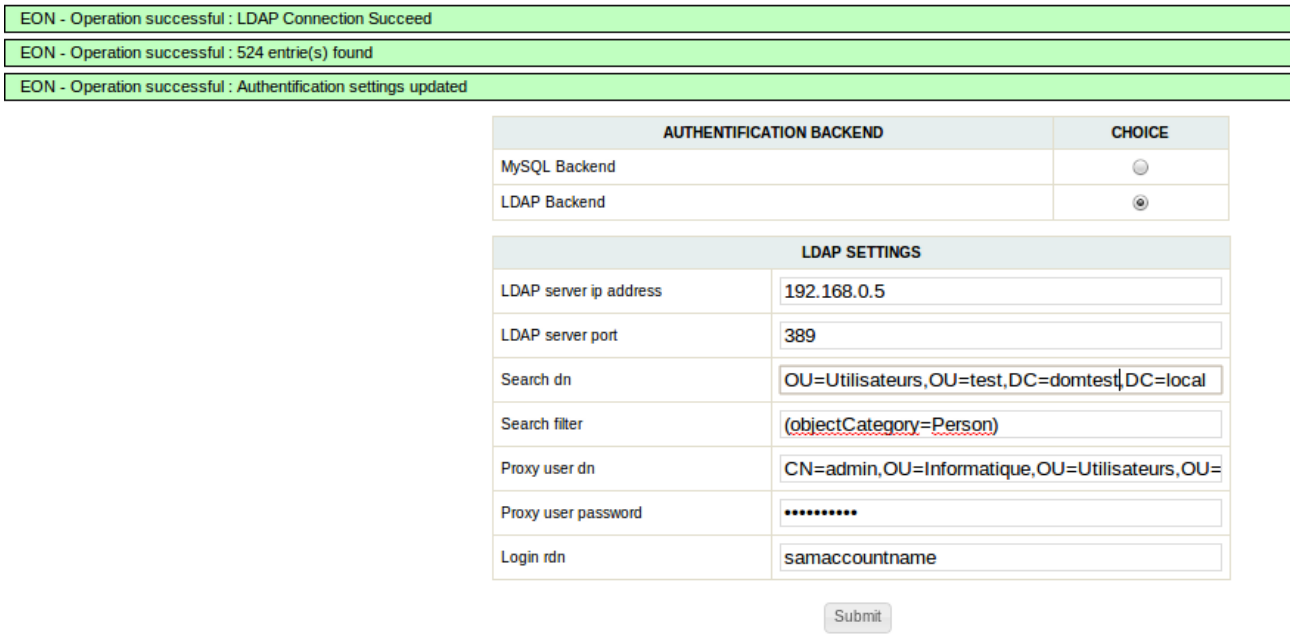
1. Sur la page principale d'EON, lien « *Administration* », cliquez sur « *utilisateurs* ».
2. Ajoutez votre utilisateur.
3. Donnez lui un mail.
4. Validez

## 7.14 - Connexion à un serveur LDAP Windows 2003 serveur FR

EON fournit un connecteur LDAP qui permet de vous connecteur à un annuaire Microsoft.

L'avantage est que vous pourrez ainsi récupérer vos identifiants de l'annuaire.

1. Cliquez sur « Administration » puis « Authentification » à gauche.
2. Sélectionner « LDAP Backend » puis remplissez les divers champs.



- LDAP server :

*Il s'agit de l'adresse ip de votre serveur LDAP.*

- Search dn :

*A remplir en fonction de votre environnement.*

*Par exemple :*

```
OU=Utilisateurs,OU=test,DC=domtest,DC=local
```

- Search filter :

```
(objectCategory=Person)
```

- Proxy user dn

```
CN=admin,OU=Informatique,OU=Utilisateurs,OU=test,DC=domtest,DC=local
```

- Proxy user password

*Mot de passe administrateur du domaine.*

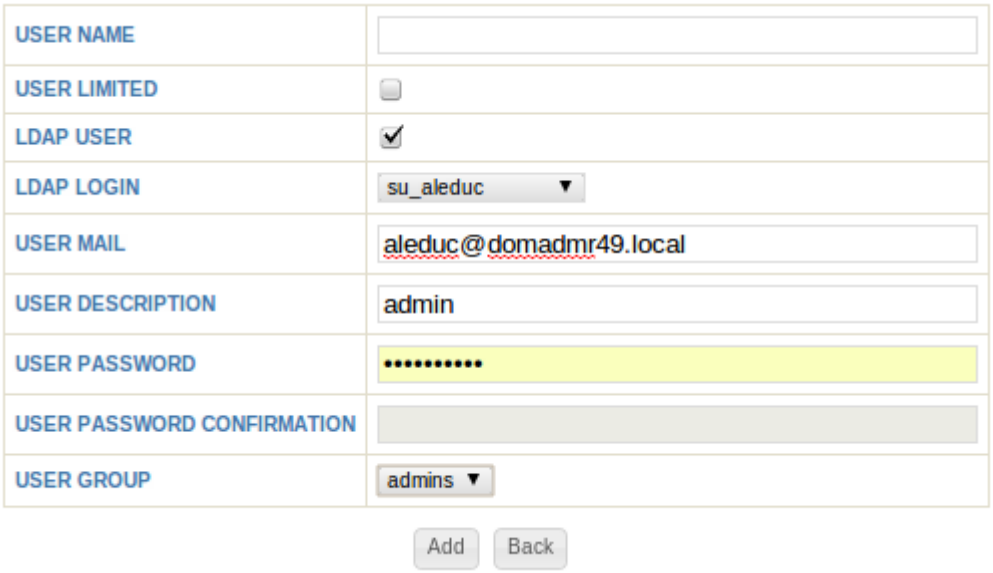
3. Cliquez sur « *submit* ».

Si tout es ok vous devriez obtenir une notification vous informant de la connexion réussie à l'annuaire.

Il reste à ajouter l'utilisateur.

4. Cliquez sur « *utilisateurs* » à gauche pour obtenir cet écran.

5. Cliquez sur « *Ldap User* » pour obtenir la liste des utilisateurs crée dans l'annuaire.




6. Renseignez le mail de l'utilisateur, sa description et validez.
7. Déconnectez-vous et loggez-vous avec vos identifiants LDAP

# CACTI

**Objectifs** :

- *Importer des périphériques provenant de « nagios » dans « cacti »*
- *Créer des graphiques*
- *Crée une arborescence avec « default tree »*
- *Supprimer des graphiques*

# 8 - Présentation de « *Cacti* »

Maintenant que vos équipements sont supervisés par « *nagios* » vous êtes alerté quant à leur état, mais vous n'avez que très peu de données sur leur utilisation réelle et encore moins quand il s'agit d'établir des tendances.

Car la fonctionnalité de « *nagios* » répondant à cette problématique est plutôt limitée et ne s'occupe que des états physiques, à savoir allumé ou éteint. C'est toujours utile, mais parfois il nous faut affiner un peu nos détections.

Pour cela nous allons de voir faire appel à un nouvel outil, j'ai nommé « *Cacti* ».

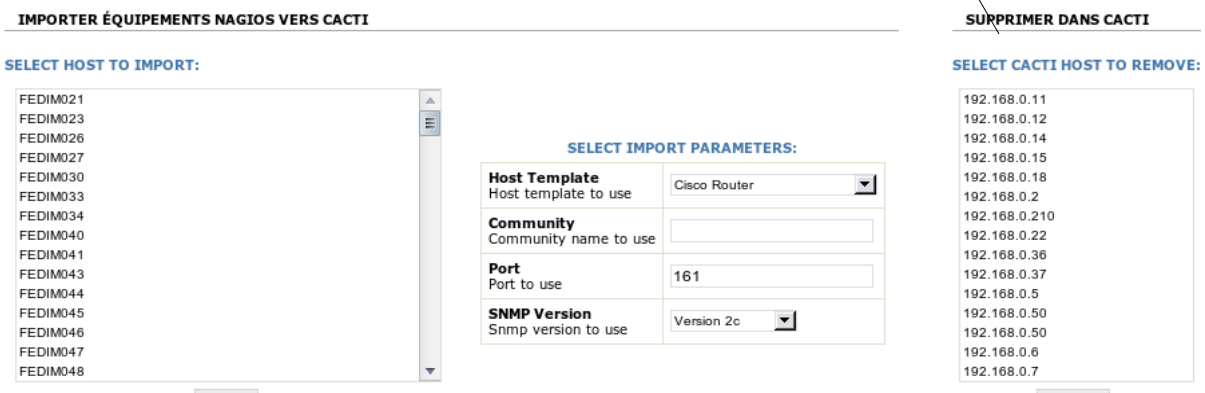
Si pour le moment la base de données de ce logiciel est encore vierge de toute information, et plutôt que de réécrire tout à la main, ce qui vous en conviendrez peut se révéler fastidieux, nous allons importer les données de « *nagios* » dans « *cacti* ».

## 1- Importer les hôtes vers Cacti

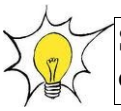
Dans « *EON* », cliquer sur le lien « *administration* » puis dans le menu de gauche sélectionnez « *importer vers cacti* »


Vous aurez une colonne vide.

Cette fenêtre apparaît

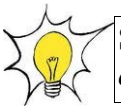


Sélectionnez l'hôte que vous souhaitez superviser et renseigner le template et son nom de communauté.



Si aucun template ne correspond à votre hôte, sélectionnez "*generic snmp-enabled host*" cela fera l'affaire et cliquez ensuite sur "*Import*".

Votre hôte apparaît maintenant dans la colonne de droite.



*Si l'importation ne s'effectue pas, vérifiez le nom du périphérique. S'il contient des caractères « é, è, _ », cela peut bloquer l'importation.*

Connectez-vous à « *Cacti* »


## 8.1 - Correction des erreurs liés à l'importation

Après importation, vos hôtes apparaissent dans le lien « *Devices* ».

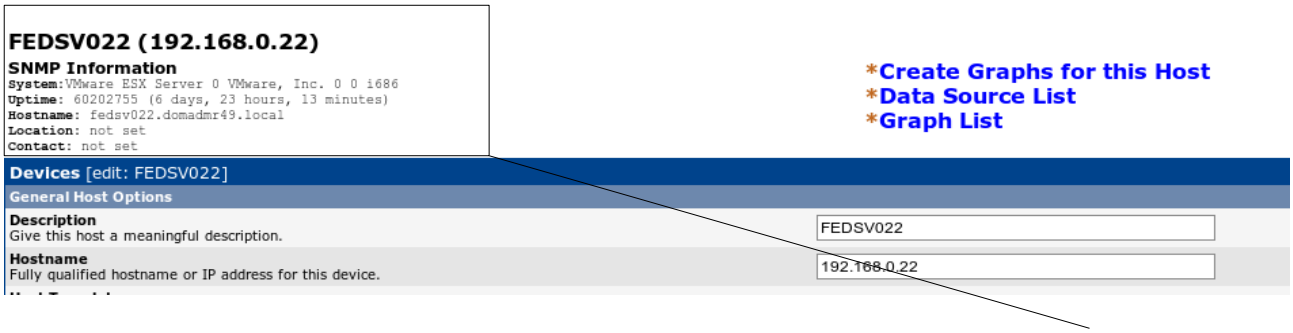

L'importation ne se déroule pas correctement. L'adresse ip de vos hôtes n'est pas importée.

Il va falloir la renseigner manuellement pour nos différents « *devices* ».

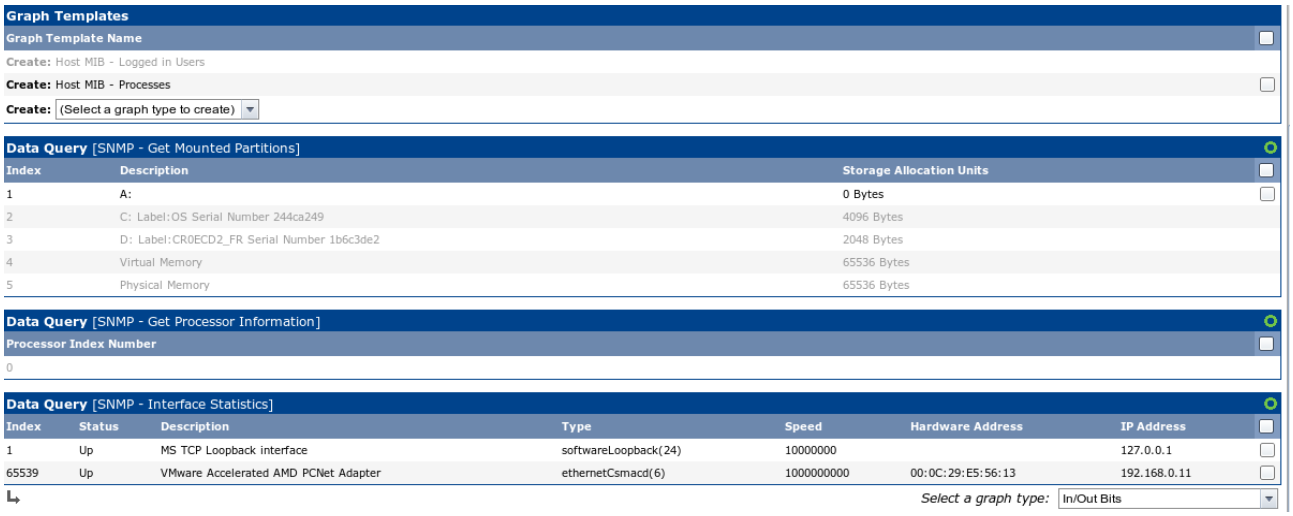
| Description** | ID | Graphs | Data Sources | Status | Event Count | Hostname |
|---|---|---|---|---|---|---|
| FEDSV022 | 57 | 0 | 0 | Up | 0 | 192.168.0.22 |
| NETASQ | 50 | 0 | 0 | Down | 286 | 192.168.0.2 |
| SRVAV | 56 | 7 | 7 | Up | 0 | 192.168.0.11 |

*Après correction du « hostname » par son « adresse ip », le statut de l'hôte est « up »*

Cliquez sur votre hôte pour accéder à la fenêtre suivante.




Renseignez son adresse ip puis valider. Revenez sur le périphérique et vérifiez la remontée d'informations.




Nous allons maintenant créer des graphiques en cliquant sur « *Create Graphs for this host* ».

Cliquez sur le « *rond vert* » pour dérouler les sections.

Sélectionner les éléments souhaités puis cliquez sur « *Create* ».

## 8.2 - Création de plusieurs vues (Graph tree)

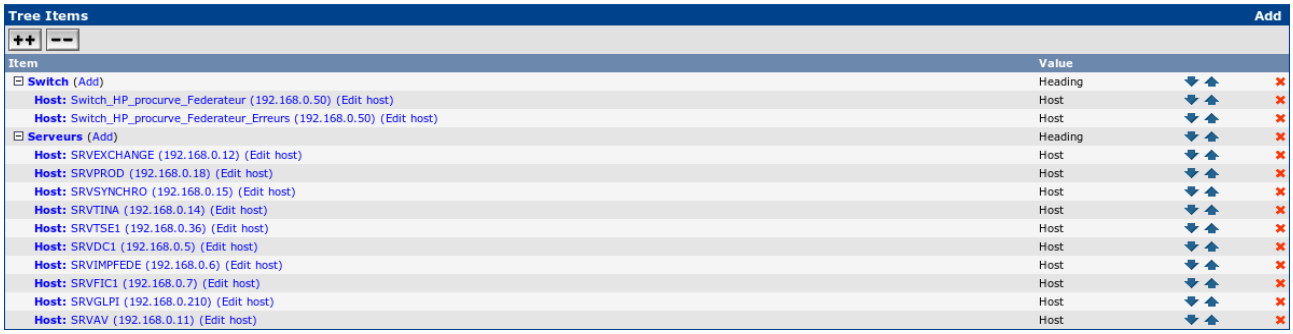
Nous allons créer plusieurs vues afin d'optimiser la lecture de nos graphiques.

1. Cliquez sur « *Graph Tree* »
2. Apparaît par défaut « *Default Tree* »


3. Cliquez sur « *Default Tree* » et le renommer en ce que vous voulez.

Notre société comporte ur es. J'ai renommé « *defaut tree* » par le nom du siège.

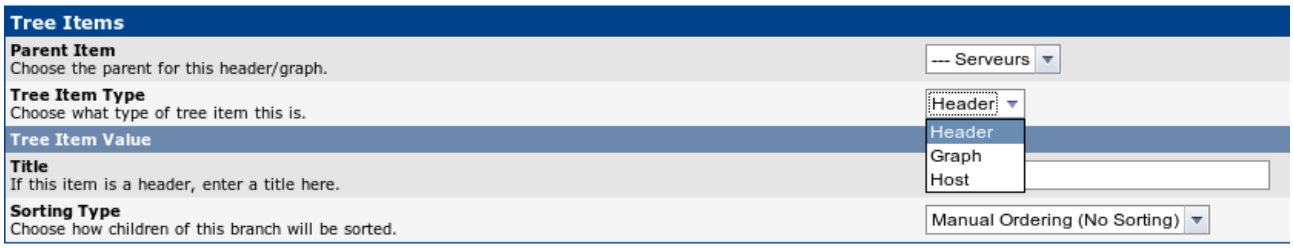

Voici ce que j'obtiens après avoir ajouté des équipements




Nous allons ajouter un « *host* » à notre catégorie « *serveurs* ».

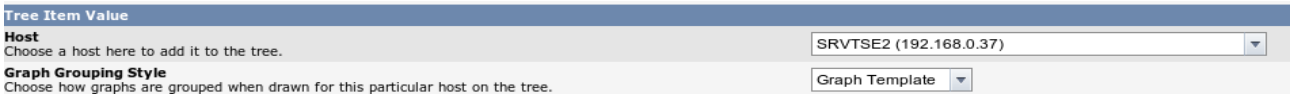
1. Cliquez sur « *Add* » à côté de « *Serveurs* »

Cette fenêtre apparaît




2. Le « *parent Item* » est correct
3. Sélectionner « *host* » dans le menu déroulant

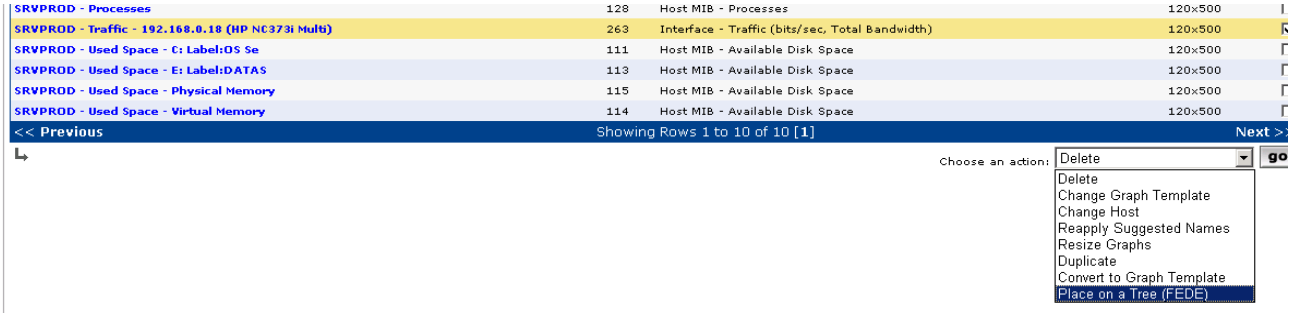
Une liste déroulante apparaît et nous demande de choisir notre hôte



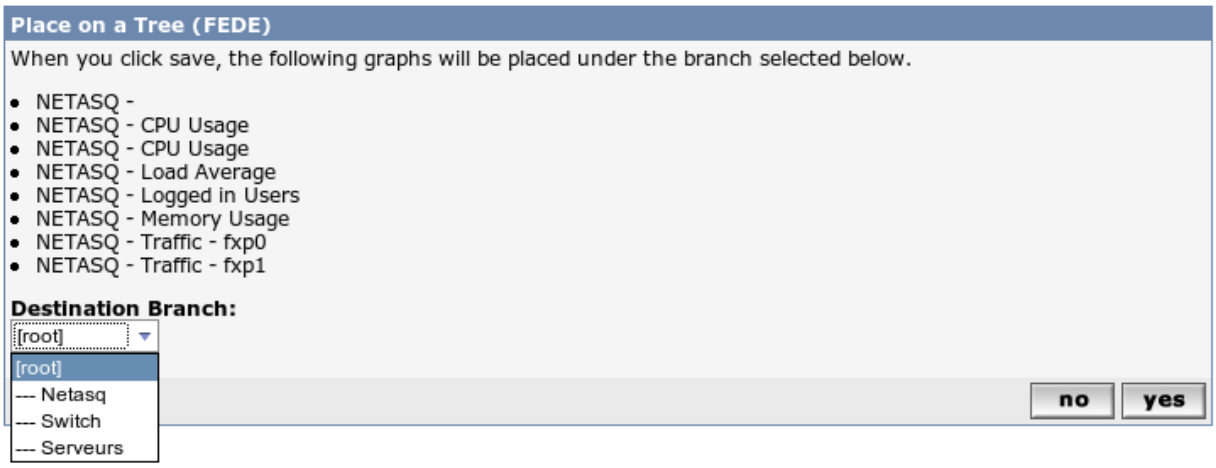

4. Sélectionnez-le et cliquez sur « *Create* »

Notre serveur est bien ajouté au « *Graph Tree* »

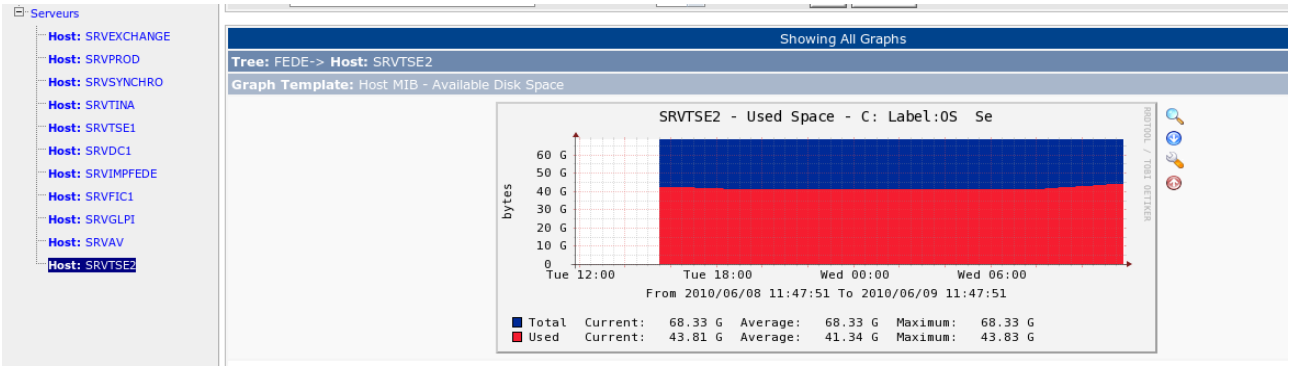

1. Cliquez ensuite sur « *Graph management* », sélectionnez les graphs que vous désirez voir apparaître. Puis sélectionnez « *Place on a tree* » dans la liste déroulante.




2. Sélectionnez la catégorie où doit apparaître le graph.




3. Cliquez ensuite sur le lien « *graph* »

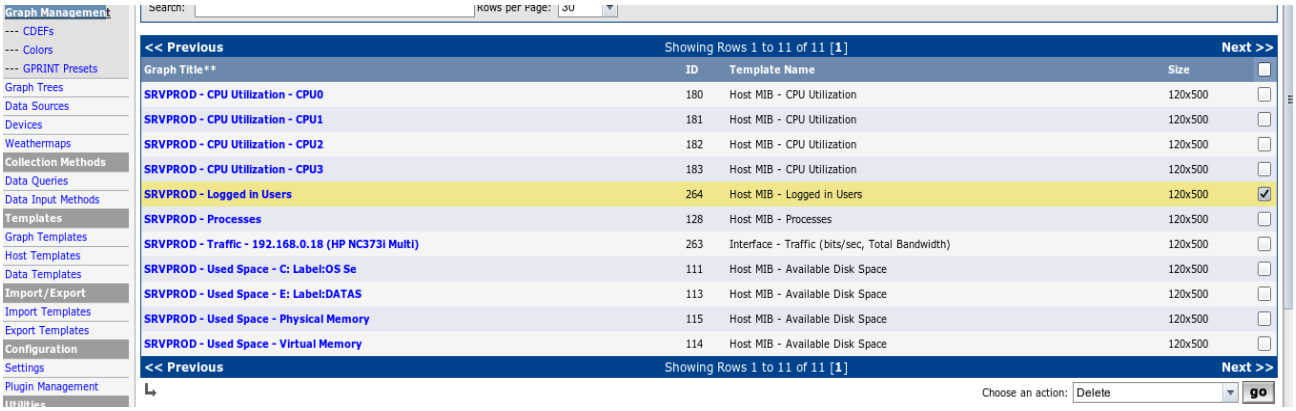

4. puis sélectionnez votre serveur pour visualiser les graphs

## 8.3 - Supprimer des graphiques pour certains hôtes

Il n'est pas nécessaire de tout grapher en fonction de vos hôtes.

Pour supprimer des graphs, il suffit de cliquer sur « *graph management* » et de sélectionner l'hôte souhaité.

Choisir « *delete* » dans la liste déroulante et cliquer sur « *go* »




## 8.4 - Conclusion

Cacti est un outil puissant et flexible. Nous avons fait le minimum de ce que nous propose l'outil.

Il est possible d'ajouter d'autres templates au logiciel si vous le désirez. La plupart sont disponibles sur le forum de cacti.

N'hésitez pas à lire la documentation qui est également très fournie

# Nagvis

Objectifs :

- *Administrer des cartes*
- *Ajouter des objets de type « machine »*
- *Paramétrer des objets*

# 9 - Presentation « *Nagvis* »

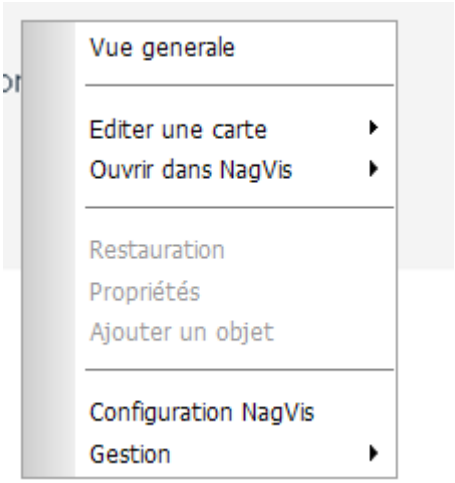
Comme vous l'avez peut-être vu, la cartographie de « *nagios* » est parfois assez limitée, surtout quand on commence à avoir beaucoup d'équipements supervisés. Pour pallier à cela, on a l'Automap de « *NagVis* » qui est nettement plus lisible et efficace, cependant il peut être utile de créer des vues d'équipements spécifiques, ou de pôles géographiques particuliers.

## 9.1 - Présentation de l'interface

1. Dans « *EON* », cliquez sur le lien « *Administration* » puis section « *cartographies* » et « *Nagvis* »


2. Faire un clic droit pour accéder au menu contextuel du logiciel

3. Le menu contextuel apparaît proposant différents sous-menus.



**En voici une explication :**

- Editer une carte:

*Lorsque vous avez déjà créé des cartes, ceci vous sert à les ouvrir en mode édition.*

- Ouvrir dans NagVis :

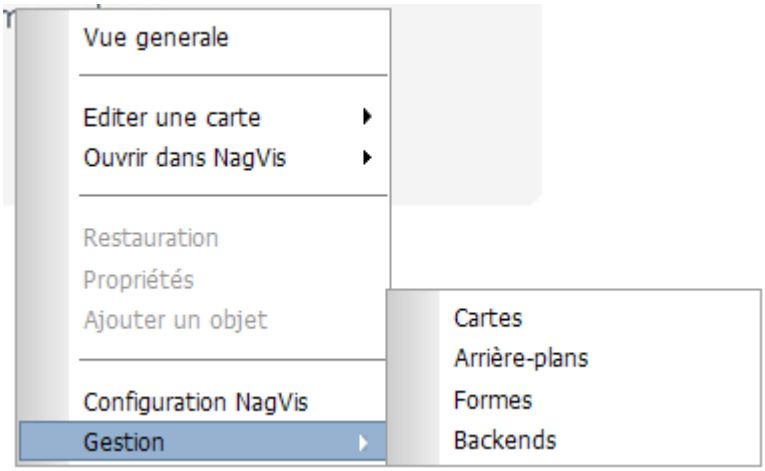
*Lorsque des cartographies sont disponibles, on peut par ce lien les ouvrir en mode consultation.*

- Configuration Nagvis :

*Accès au menu de configuration principal de NagVis.*

- Gestion :

*Propose un sous-menu selon le type d'objet à gérer*




- Gestion – Cartes :

*Permet de créer, modifier ou supprimer des cartographies, mais aussi de les exporter ou d'en importer*

- Gestion – Arrières plan :

*C'est ce lien qu'il vous faudra utiliser pour charger des images sur le serveur afin de les utiliser plus tard comme fonds pour vos cartes. Vous pouvez bien sûr supprimer celles qui existent déjà, ou encore les renommer.*

- Gestion – Formes :

*Ce menu vous permet de charger sur le serveur, ou d'en supprimer, des formes que vous pourrez utiliser ultérieurement et intégrer dans vos cartes.*

- *Gestion – Backends :*

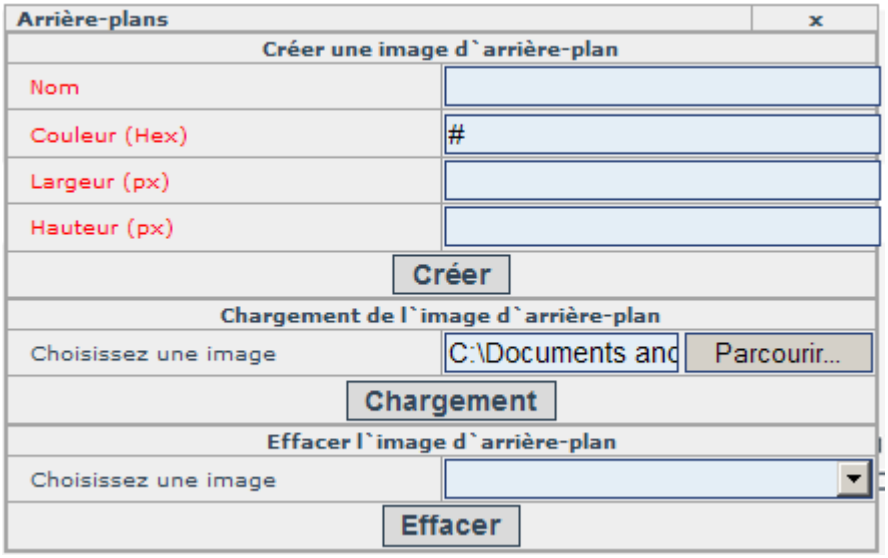
*Ce menu vous autorise à changer de backend pour les cartes NagVis, je vous déconseille d'y toucher avant d'être vraiment à l'aise avec cet outil.*

## 9.2 - Ajouter une carte

Nous allons maintenant ajouter notre carte dans « *Nagvis* ».

1. Sélectionnez le menu « *Gestion* » puis « *Arrières-plan* »

Cette fenêtre apparaît.




2. Sélectionner votre carte au format « *png* » uniquement.

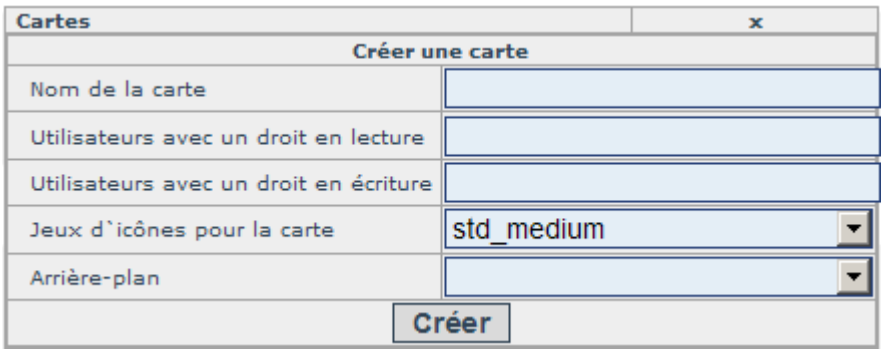
Sous visio, cliquez sur « *enregistrer au format web* » et sélectionnez « *png* » dans la liste déroulante.

3. Cliquez sur « *Créer* »

Vous revenez à l'écran d'accueil de « *Nagvis* ». La carte est maintenant importée dans la BDD. Nous allons la créer.

4. Cliquez sur « *Gestion - Cartes* »

Vous obtenez cet écran




5. Donnez un nom à votre carte

6. Renseignez le nom d'utilisateur pour les droits en « *Lecture et écriture* »

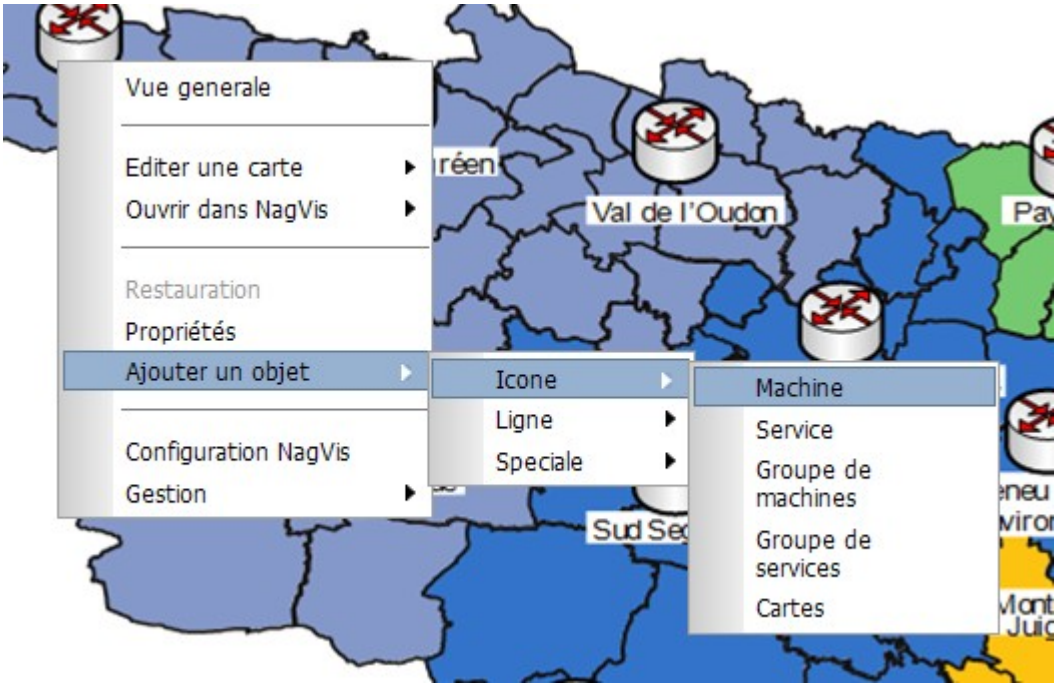
7. Sélectionnez en arrière plan la carte que vous venez d'importer

## 9.3 - Ajouter des objets

Nous allons ajouter un objet de type « *machine* » afin que « *Nagvis* » puisse superviser son état.

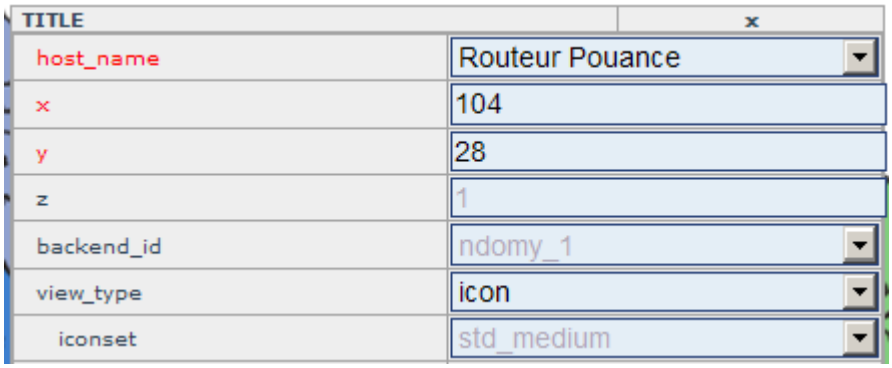
Pour ce faire, faites un clic droit sur la carte.

Ce menu apparaît :




1. Sélectionnez « *Ajouter un objet* » - « *Icône* » - « *Machine* »
2. Une croix apparaît, cliquez sur le périphérique que vous souhaitez superviser.

Ce menu apparaît :




3. Sélectionner l'hôte correspondant.

Choisissez si vous voulez monitorer les services ou seulement l'état de l'hôte

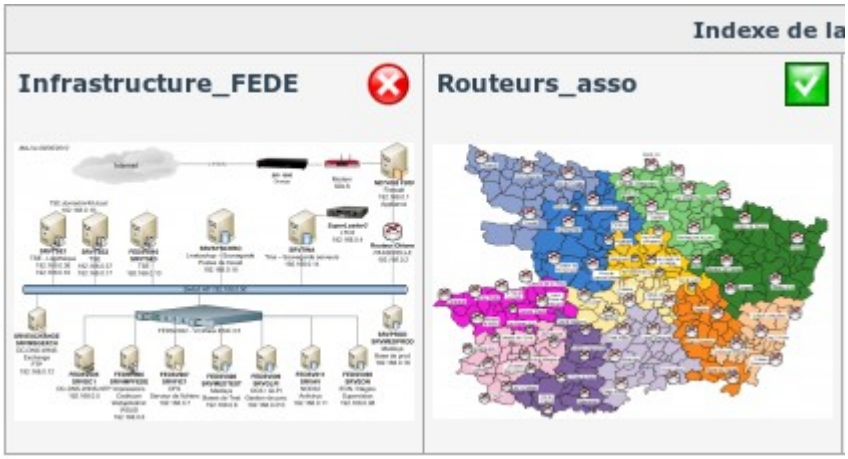
Dans mon cas, il s'agit d'un routeur non supervisable en SNMP. Seul son état m'intéresse.

| | |
|---|---|
| only_hard_states | Oui |
| recognize_services | Non |

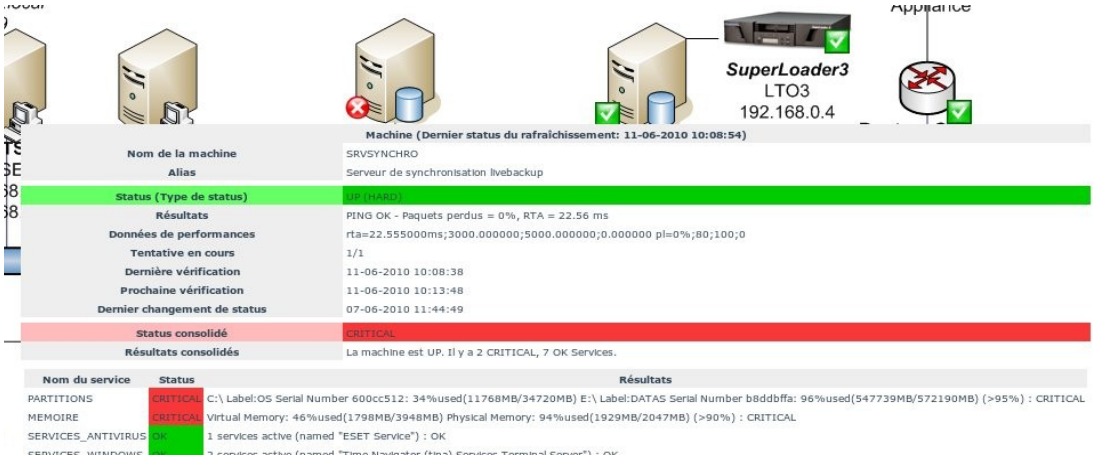
4. Après avoir ajouté un objet de type « *machine* », une case verte s'affiche et devient « *rouge* » si un service est **critique** ou si le périphérique est **down**, « *jaune* » si un service est en état **warning** et « *vert* » si tout est **ok.**

Pour visualiser votre carte, il suffit de cliquer dans « *EON* »,« *Disponibilités* » puis « *nagvis* ».

Voici ce qui apparaît :




*Vue globale des mes cartes.*



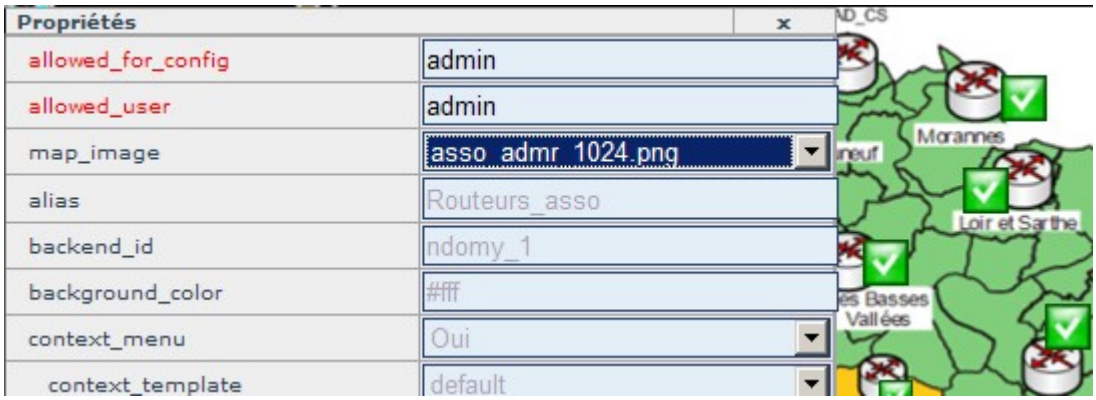

*Vue détaillée des serveurs. Un problème est remonté sur le serveur de sychro*

## 9.4 - Modifier une carte

En général, une carte représentant la topologie est soumis à modification. Elle évolue.

Pour modifier votre carte, il suffit de :

1. Ajouter votre nouvelle carte comme indiquée dans la procédure çi-dessus,
2. Editer la carte que vous souhaitez modifié.
3. Faire un clic-droit sur la carte et sélectionner « *Propriétés* ».
4. Puis sélectionner la nouvelle version de la carte.




## 9.5 - Supprimer une carte définitivement

Il arrive de temps en temps que votre carte ne se supprime pas définitivement car leur fichier de configuration existe toujours. De ce fait, elles apparaissent toujours sur « l'indexe de la carte ».


*Ici, nos cartes de tests sont toujours présentes malgré leur suppression dans l'outil.*

Pour les supprimer :

1. Se connecter en ssh ou par FTP au serveur de supervision.
2. Se rendre dans le répertoire

```
/srv/eyesofnetwork/nagvis/etc/maps
```

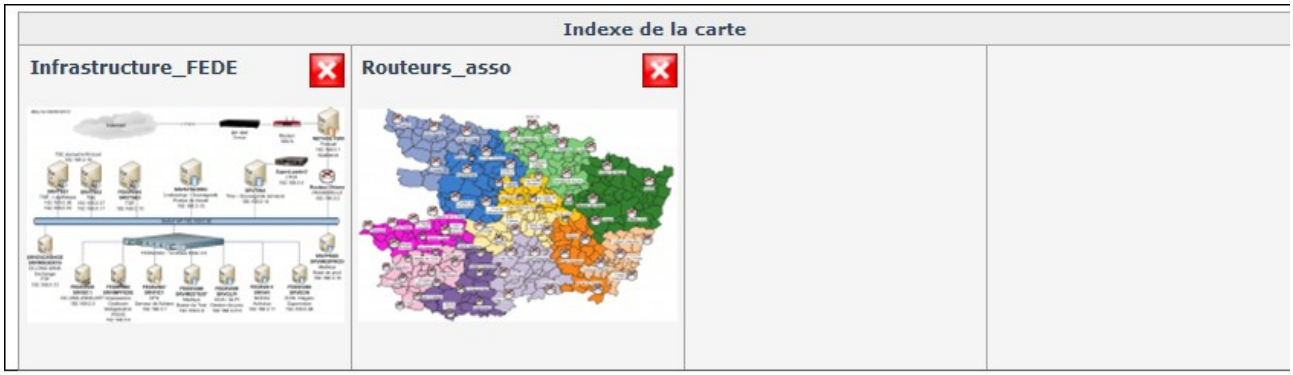
Les fichiers de configurations apparaissent

```
utobackup.status        Infrastructure_FEDE.cfg.bak  tototo.cfg
 automap.cfg            Routeurs_asso.cfg            tototototo.cfg
```

3. Supprimer les fichiers de configurations liés à vos carte

```
rm -f nom du fichier
```

Après suppression de ces 2 fichiers mes cartes disparaissent



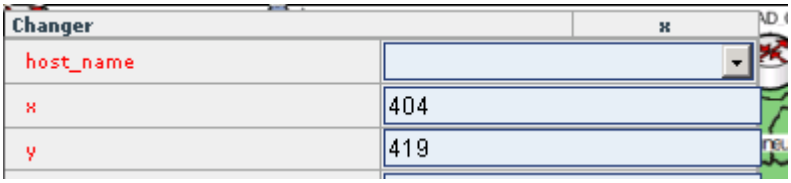

## 9.6 - Icône bleue

De temps en temps, suite à un arrêt à chaud du serveur de supervision ou à un renommage d'un hôte dans « *lilac* », l'icône d'un élément actif devient bleue dans « *nagvis* »


La plupart du temps, le nom d'hôte de l'élément actif présent dans la BDD de « *nagvis* » ne correspond plus avec le nom d'hôte présent dans les fichiers de configuration de « *nagios* ».

Pour recréer le lien, il suffit de laisser sa souris sur l'hôte dont le lien est rompu. (en mode edition) Un menu apparaît.

Cliquez sur « *Changer* ». Normalement, le champ « *hostname* » est vide.




Sélectionner le « *hostname* » correspondant à l'élément et cliquez sur « *Enregistrer* »

# Backup

**Objectifs** *:*

- *Paramétrer le fichier de configuration « backup-manager »*
- *Envoyer vos sauvegardes sur un serveur FTP*

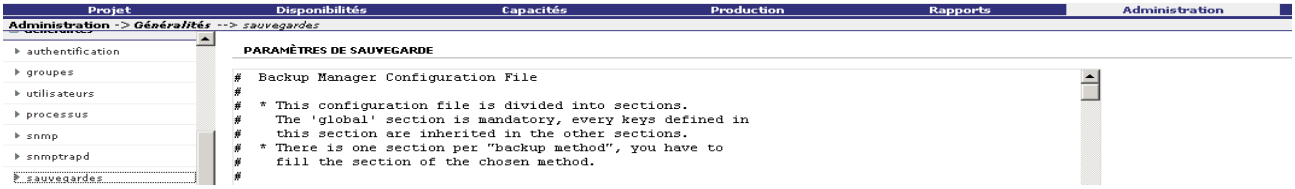
# 10 - Présentation de « *Backup-Manager* »

« *EON* » utilise un fichier de configuration pour réaliser les sauvegardes. Ce fichier n'est autre que l'excellent logiciel de sauvegarde « *backup-manager* »

http://www.backup-manager.org/

Tous les soirs, à 4h00 du matin une sauvegarde des bases de données des différents logiciels et de leurs fichiers de configuration est sauvegardée dans le répertoire « *var/archives* ».

Le script, qui est utilisé pour la sauvegarde est accessible en cliquant sur le lien « *Administration* » puis « *sauvegardes* ».




Une fois dénué de tous ses commentaires, le script ressemble à ça :

```
export BM_REPOSITORY_ROOT="/var/archives"
export BM_TEMP_DIR="/tmp"
export BM_REPOSITORY_SECURE="true"
export BM_REPOSITORY_USER="root"
export BM_REPOSITORY_GROUP="root"
export BM_REPOSITORY_CHMOD="770"
export BM_ARCHIVE_CHMOD="660"
export BM_ARCHIVE_TTL="5"
export BM_REPOSITORY_RECURSIVEPURGE="false"
export BM_ARCHIVE_PURGEDUPS="true"
export BM_ARCHIVE_PREFIX="$HOSTNAME"
export BM_ARCHIVE_STRICTPURGE="true"
export BM_ARCHIVE_NICE_LEVEL="10"
export BM_ARCHIVE_METHOD="tarball mysql"
export BM_TARBALL_NAMEFORMAT="long"
export BM_TARBALL_FILETYPE="tar.gz"
export BM_TARBALL_OVER_SSH="false"
export BM_TARBALL_DUMPSYMLINKS="false"
declare -a BM_TARBALL_TARGETS
BM_TARBALL_TARGETS[0]="/etc"
BM_TARBALL_TARGETS[1]="/home"
BM_TARBALL_TARGETS[2]="/srv"
```

```
export BM_TARBALL_TARGETS

export BM_TARBALL_BLACKLIST="/dev /sys /proc /tmp"

export BM_TARBALL_SLICESIZE="1000M"

export BM_TARBALL_EXTRA_OPTIONS=""

export BM_TARBALLINC_MASTERDATETYPE="weekly"

export BM_TARBALLINC_MASTERDATEVALUE="1"

export BM_MYSQL_DATABASES="cacti eonweb ged lilac mysql"

export BM_MYSQL_SAFEDUMPS="tBackup-Managerrue"

export BM_MYSQL_ADMINLOGIN="root"

export BM_MYSQL_ADMINPASS="root66"

export BM_MYSQL_HOST="localhost"

export BM_MYSQL_PORT="3306"

export BM_MYSQL_FILETYPE="bzip2"

export BM_MYSQL_EXTRA_OPTIONS=""

export BM_SVN_REPOSITORIES=""

export BM_SVN_COMPRESSWITH="bzip2"

declare -a BM_PIPE_COMMAND

declare -a BM_PIPE_NAME

eclare -a BM_PIPE_FILETYPE

declare -a BM_PIPE_COMPRESS

export BM_PIPE_COMMAND

export BM_PIPE_NAME

export BM_PIPE_FILETYPE

export BM_PIPE_COMPRESS

export BM_UPLOAD_METHOD=""

export BM_UPLOAD_HOSTS=""

export BM_UPLOAD_DESTINATION=""

export BM_UPLOAD_SSH_USER=""

export BM_UPLOAD_SSH_KEY=""

export BM_UPLOAD_SSH_HOSTS=""

export BM_UPLOAD_SSH_PORT=""
```

```
export BM_UPLOAD_SSH_PURGE="true"
export BM_UPLOAD_SSH_TTL=""
export BM_UPLOAD_SSHGPG_RECIPIENT=""
export BM_UPLOAD_FTP_SECURE="false"
export BM_UPLOAD_FTP_PASSIVE="true"
export BM_UPLOAD_FTP_USER=""
export BM_UPLOAD_FTP_PASSWORD=""
export BM_UPLOAD_FTP_HOSTS=""
export BM_UPLOAD_FTP_PURGE="true"
export BM_UPLOAD_FTP_TTL=""
export BM_UPLOAD_FTP_DESTINATION=""
export BM_UPLOAD_S3_DESTINATION=""
export BM_UPLOAD_S3_ACCESS_KEY=""
export BM_UPLOAD_S3_SECRET_KEY=""
export BM_UPLOAD_S3_PURGE="false"
export BM_UPLOAD_RSYNC_DIRECTORIES=""
export BM_UPLOAD_RSYNC_DESTINATION=""
export BM_UPLOAD_RSYNC_HOSTS=""
export BM_UPLOAD_RSYNC_DUMPSYMLINKS="false"
export BM_BURNING_METHOD="none"
export BM_BURNING_CHKMD5="false"
export BM_BURNING_DEVICE="/dev/cdrom"
export BM_BURNING_DEVFORCED=""
export BM_BURNING_ISO_FLAGS="-R -J"
export BM_BURNING_MAXSIZE="650"
export BM_LOGGER="true"
export BM_LOGGER_LEVEL="error"
export BM_LOGGER_FACILITY="user"
export BM_PRE_BACKUP_COMMAND=""
export BM_POST_BACKUP_COMMAND=""
```

Explications :

Nous allons expliquer quelques directives qui sont utilisées afin que vous puissiez adapter le script en fonction de vos besoins.

Sources :

http://doc.ubuntu-fr.org/backup-manager

http://wiki.backup-manager.org/index.php/Main_Page#Documentation

- BM_REPOSITORY_ROOT

*Répertoire où toutes vos archives seront stockés.*

- BM_TEMP_DIR

*Répertoire temporaire utilisé pendant la sauvegarde.*

- BM_REPOSITORY_SECURE

*Pour des raisons de sécurité le répertoire peut être accessible que par une paire utilisateur/groupe définis dans les directives « BM_REPOSITORY_USER », « BM_REPOSITORY_USER » et « BM_REPOSITORY_CHMOD »*

- BM_ARCHIVE_CHMOD

*Droits attribués aux fichiers de sauvegarde.*

*(660 = rw-rw---- soit « read, write pour le propiétaire, rw pour le groupe et rien pour les autres)*

- BM_ARCHIVE_TTL

*C'est la durée de vie (Time To Live) en jours d'une archive.*

- BM_REPOSITORY_RECURSIVEPURGE

*Purge récursive du répertoire de sauvegarde.*

- BM_ARCHIVE_PURGEDUPS

*Si deux archives (sauvegardes) successives sont identiques, backup-manager peut créer un lien au lieu de recréer une archive. (gain de place)*

- BM_ARCHIVE_PREFIX

*Donne un préfixe au nom de l'archive.*

- BM_ARCHIVE_STRICTPURGE

*Cette directive est utile si vous stocké toutes vos sauvegardes de différents backup-manager dans le même répertoire. En passant la valeur à « yes », BM ne supprimera pas les fichiers générés par d'autres BM et qui ont plus de 5 jours.*

- BM_ARCHIVE_NICE_LEVEL

*Quand BM génère une sauvegarde, cela sollicite le CPU. Afin d'éviter une charge CPU trop importante, cette directive affecte un niveau de priorité au processus.*

*Plus le « nive level » est élevé mieux c'est. Par défaut, BM utilise un « nice level » de 19 pour un environnement « Desktop ».*

- BM_ARCHIVE_METHOD

*La méthode permettant de créer les archives*

- BM_TARBALL_NAMEFORMAT

*Comment apparaissent les fichier dans la liste :*

- long : *liste tous les sous-répertoires puis le nom du fichier (ex : /home/toto/doc.odt)*
- short : *donne uniquement le nom du fichier (ex : doc.odt)*

- BM_TARBALL_FILETYPE

*C'est le type de compression désirée.*

- BM_TARBALL_DUMPSYMLINKS

*Est ce que backup-manager sauvegarde les répertoires pointés par des liens (raccourcis) ?*

- BM_TARBALL_TARGETS

*Répertoires à sauvegarder*

- BM_TARBALL_BLACKLIST

*Donner une liste noire qui comporte certains dossiers et fichiers à ne pas sauvegarder.*

- BM_TARBALL_SLICESIZE

*Détermine la taille maximale des archives*

- BM_TARBALL_EXTRA_OPTIONS

*Pour ajouter des options supplémentaires à « tar ».*

Par exemple, pour activer le mode verbueux :

```
BM_TARBALL_EXTRA_OPTIONS="-v"
```

- BM_TARBALLINC_MASTERDATETYPE

*Détermine la fréquence des sauvegardes complètes :*

- weekly : *toutes les semaines*

- monthly : *tous les mois*

- BM_TARBALLINC_MASTERDATEVALUE

*Le jour des sauvegardes complètes :*

- si weekly : *mettre un nombre de 0→6 (dimanche → samedi)*
- si monthly : *mettre un nombre de 1→31*

- BM_MYSQL_DATABASES

*Bases de données à sauvegarder*

- BM_MYSQL_SAFEDUMPS

Moyen utilisé pour sauvegarder les bdd. Actuellement la méthode la plus sûre puisqu'elle permet de réinjecter le fichier sql généré dans une autre bdd sans modification.

- BM_MYSQL_ADMINLOGIN

*Utilisateur mysql*

- BM_MYSQL_ADMINPASS

*Mot de passe de l'utilisateur mysql*

- BM_MYSQL_HOST

*Emplacement de la BDD*

- BM_MYSQL_PORT

*Port d 'écoute du serveur Mysql*

- BM_MYSQL_FILETYPE

*Format de compressions pour les BDD. Il faut utiliser « bunzip2 » pour les décompresser.*

- BM_UPLOAD_SSH/Rsync etc...

*Ces directives permettent de sauvegarder vos données sur un répertoire distant autre que celui en local.*

- BM_PRE_BACKUP_COMMAND

*Ici vous renseignez la commande à effectuer avant une sauvegarde*

- BM_POST_BACKUP_COMMAND

*Ici vous renseignez la commande à effectuer après une sauvegarde.*

## 10.1 - Modification du fichier de configuration pour sauvegarder par FTP

**Modifiez les directives suivantes** :

```
BM_UPLOAD_METHOD=""
```

par

```
BM_UPLOAD_METHOD="ftp"
```

```
BM_UPLOAD_FTP_USER=""
```

par

```
BM_UPLOAD_FTP_USER="votre login"
```

```
BM_UPLOAD_FTP_HOSTS=""
```

par

```
BM_UPLOAD_FTP_HOSTS="l'adresse ip de votre serveur ftp"
```

```
BM_UPLOAD_FTP_DESTINATION=""
```

par

```
BM_UPLOAD_FTP_DESTINATION="chemin du rép"
```

Connectez-vous ensuite en ssh puis démarrer le script qui se trouve dans « */usr/sbin* »

```
/usr/sbin/backup-manager -v
```

Le principe reste le même que ce soit pour « *rsync* », « *S3* », « *ssh* ».

# Syslog-ng

**Objectifs** :

- *Installer et configurer un client syslog pour windows*
- *Installer un service sur windows*
- *Créer des filtres dans syslog-ng*

# 11 - Présentation de « syslog-ng »

«*Syslog-ng* » est un serveur qui permet de centraliser les différents journaux d'évènements sur votre serveur de supervision. Cela permet donc de repérer plus rapidement et efficacement les défaillances de machines présentes sur un réseau.

## 11.1 - Installation du client Windows

L'agent snmp de windows permet d'envoyer des traps à un serveur de log mais malheureusement, ces journaux d'évènements ne répondent pas aux normes RFC 3164 du format syslog.

Nous allons utiliser un client « *syslog* » qui va nous permettre d'envoyer des traps compatibles.

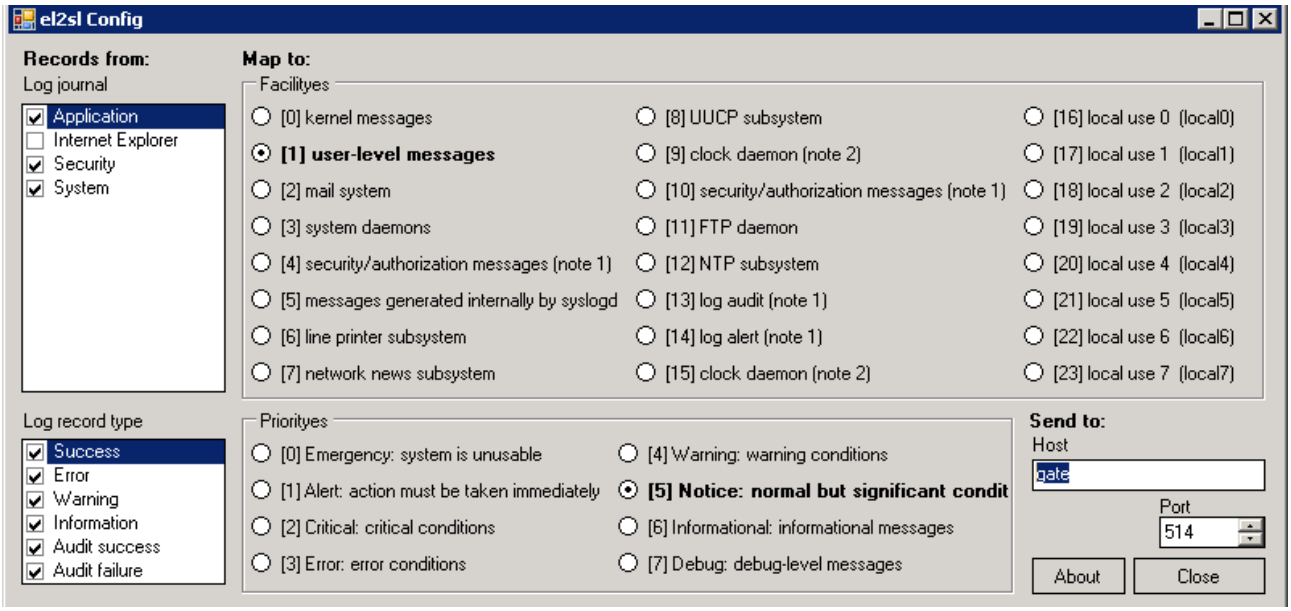
1. Téléchargez le client « *el2sl*» pour windows sur le site

http://sourceforge.net/projects/el2sl/

2. Installez-le

3. Se rendre dans le répertoire « *El2sl* » situé dans « *Program files* » et cliquez sur « *el2slconf* »

Cette fenêtre s 'ouvre :




4. Dans « *gate* », indiquez l'adresse ip de votre serveur de supervision. Laissez le port par défaut

5. Vous pouvez modifier pour chaque journaux, les types d'enregistrement qui seront envoyés au serveur en fonction de leur ordre d'importance (critical [2], Warning [4]...)

6. Cliquez sur « *close* ».

## 11.2 - Installation du service

La paramétrage est effectué, il ne reste plus qu'à installer le service avec l'utilitaire « *InstallUtil* » disponible dans « *Microsoft framework v2* »

1. Accéder au répertoire « *C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727* » en CLI.
2. Saisir cette commande

```
InstallUtil.exe -i "c:\Program Files\El2Sl\el2slservice.exe"
```

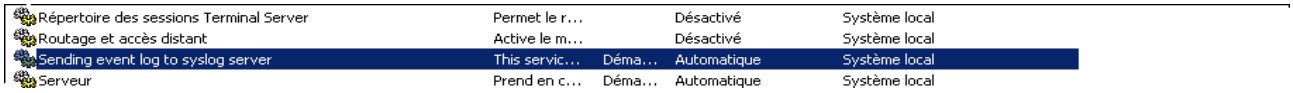
L'option « *-i* » précise qu'il faut installer le service.

La commande s'exécute mais un message d'erreur apparaît.

```
La phase de restauration est terminée.

L'installation traitée avec transaction est terminée.
L'installation a échoué et la restauration a eu lieu.
```

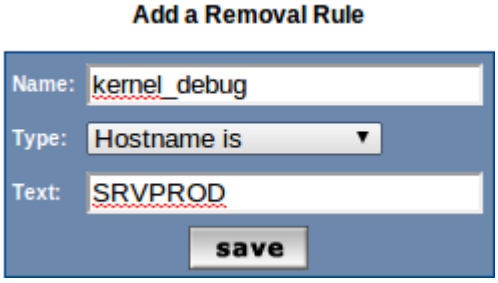
Malgré tout, le service est installé et vous pouvez le vérifier dans les services de Windows.




## 11.3 - Création d'une règle de suppression

Pour créer des règles de suppression, cliquez sur la croix rouge à droite du log puis donnez un nom à votre règle.


Par exemple pour supprimer tous les évènements provenant du serveur « *SRVPROD* » il suffit de cliquer sur la croix rouge et de compléter comme suit.




Ici nous supprimons tous les messages provenant du serveur « SRVPROD »

# Mise à jour du logiciel

**Objectifs** :

- *Copier vos sauvegardes de l'ancienne version vers la nouvelle*
- *Injecter les bases sql des différents logiciels de l'ancienne vers la nouvelle*

# 12 - Introduction pour la mise à jour d' « *EON* »

EON ne propose pas d'outil, à ce jour, de mise à jour automatique. Pour le moment la restauration de vos bases de données et des fichiers de configurations doivent se faire manuellement.

La procédure de mise à jour que vous allez suivre est largement inspirée de la documentation « *tutoriel migration eon v2* » de **Sébastien Fernandez.**

## 12.1 - Récuperer les backups

EON génère une sauvegarde tous les soirs à 4h00 du matin dans le répertoire « */var/archive* ».

La syntaxe du nom de fichier est la suivante « *année – mois - jours* ».

Récupérez la dernière sauvegarde avec « *Filezilla* » ou « *Winscp* ».

Vous devriez avoir comme répertoire :

- *srveon*
- *srveon -cacti*
- *srveonweb*
- *srveon-etc*
- *srveon -ged*
- *srveon -home*
- *srveon – lilac*
- *srveon – mysql*
- *srveon – srv*

Pour le moment, stockez-les sur votre disque dur.

## 12.2 - Installation de la nouvelle version

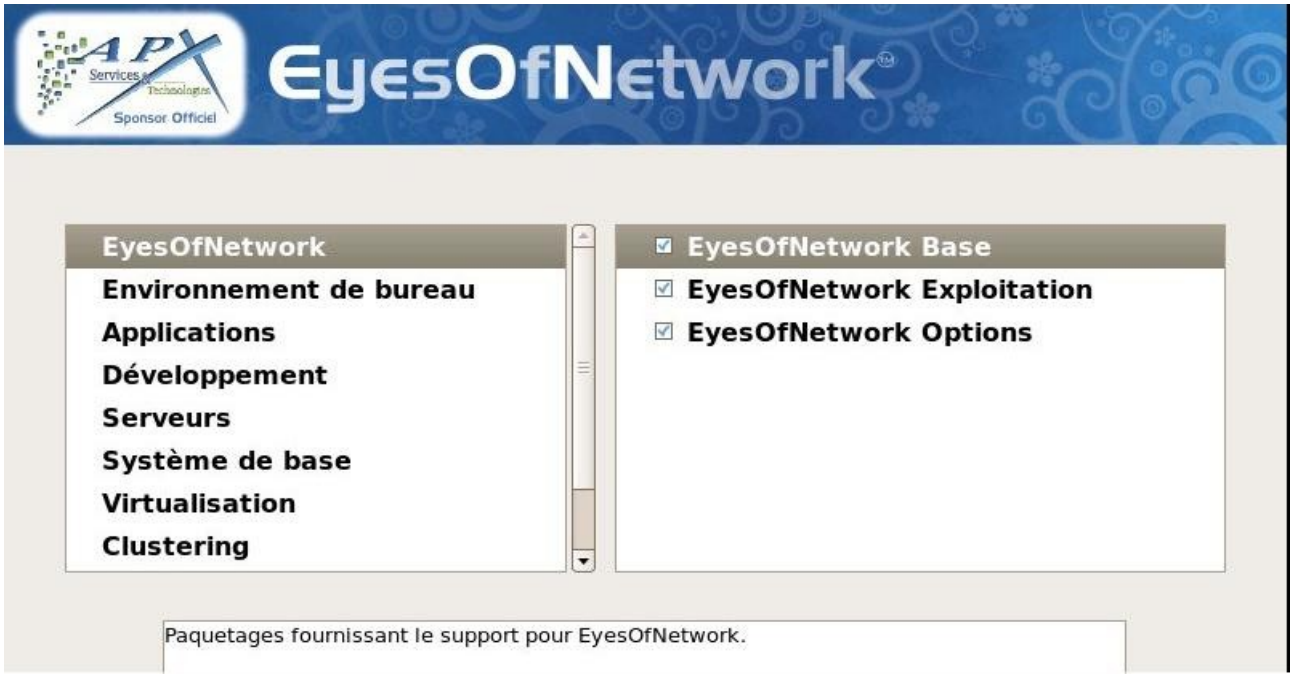
Faites une nouvelle installation d' « *EON* ».

Je ne devrais pas le préciser, car c'est du bon sens, mais faites une sauvegarde de votre serveur de supervision avant la nouvelle installation. On est jamais à l'abri d'une fausse manipulation ou d'une coupure de courant...

Lors de l'installation, cochez la case « *Paramètres personnalisées* » si vous souhaitez installer les composants comme « *syslog-ng* », « *ntop* » et « *fop* ».

« *Fop* » est utile si vous souhaitez utiliser le générateur de rapports.

Ces extensions ne sont disponibles que sur l'édition « dvd »




## 12.3 - Restauration

1. Connectez-vous sur la nouvelle version d' « *EON* » avec « *Filezilla* » ou « *winscp* ».
2. Créez un répertoire « *save* » dans le dossier « *srv* »
3. Uploader les fichiers de sauvegarde de l'ancienne version d' « *EON* ».
4. Connectez-vous avec putty pour décompresser des archives.

### 12.3.1 - Mise à jour de « *Postfix* »

1. Décompressez le fichier « *srveon-etc.xxxx.master.tar.gz* »

```
tar xvfz srveon-etc.xxxx.master.tar.gz
```

2. Un répertoire « *etc* » est crée. Remplacez le fichier « *main.cf* » extrait de la sauvegarde par le « *main.cf* » présent dans le répertoire « */etc/postfix/main.cf* ».

```
Mv etc/postfix/main.cf /etc/postfix/main.cf
```

3. Rechargez le service « *postfix* » pour la prise en compte de la nouvelle version du fichier de configuration.

```
/etc/init.d/postfix reload
```

Si vous avez d'autres fichiers de configurations, le procédé reste le même.

### 12.3.2 - Mise à jour de « *Nagios* »

1. Décompressez le répertoire « *srveon-srv.xxx.master.tar.gz* ».

Un répertoire « *srv* » est crée.

2. Coupez le service « *nagios* »

```
/etc/init.d/nagios stop
```

3. Si vous avez ajouté des plug-ins dans votre ancienne version, il faut les copier dans la nouvelle version.

```
cp –Rup /srv/save/srv/eyesofnetwork/nagios-xxx/plug-ins/* /srv/eyesofnetwork/nagios/plug-ins/
```

**Explications** :

- **-R** : *Mode récursif*. Il va traiter les sous-dossier présent dans le répertoire « plug-ins »
- **-u** : *Mode update* : Va jouter uniquement les nouveaux fichiers
- **-p** : *préserve les droits*

4. Si vous souhaitez copier vos images présentes dans votre ancienne version de « *nagios* »

```
cp -up  /srv/save/srv/eyesofnetwork/nagios-3.0.6/share/images/logos/* /srv/eyesofnetwork/nagios/share/images/logos/
```

5. Normalement les droits sont préservés mais au cas ou :

```
chmod 755 –R /srv/eyesofnetwork/nagios/*
```

et

```
chown –R nagios:eyesofnetwork /srv/eyesofnetwork/nagios/*
```

Nous allons maintenant importer la base de données sql de lilac de l'ancienne version de nagios dans cette version.

6. Décompressez le fichier sql « *srveon-lilac.xxxx.sql.bz2* »

```
bunzip2 srveon-lilac.xxxx.sql.bz2
```

7. Importez le fichier dans la BDD de « *lilac* »

```
mysql lilac -u root --password=root66 < /srv/save/lilac.sql
```

8. Connectez-vous à l'interface web d' « *EON* » (admin/admin) puis lancer une procédure d 'exportation dans lilac
9. Cliquez sur le lien « *Restart* » du job par défaut.
10. Connectez-vous à « *Nagios* » et vérifiez que vos équipements supervisés sont présent.

Ceci conclut notre upgrade de « Nagios »

### 12.3.3 - Mise à jour de « *Nagvis* »

1. Copiez les images ou les formes si vous en avez utilisé

```
cp –up /srv/save/srv/eyesofnetwork/nagvis/nagvis/images/maps/* /srv/eyesofnetwork/nagvis/nagvis/images/maps/
```

et

```
cp –up /srv/save/srv/eyesofnetwork/nagvis/nagvis/images/shapes/* /srv/eyesofnetwork/nagvis/nagvis/images/shapes/
```

2. Réaffectez le propriétaire et le groupe aux fichiers

```
chown -R nagios:eyesofnetwork /srv/eyesofnetwork/nagvis/nagvis/images/maps/*
```

3. Copier ensuite les fichiers de configuration des maps

```
cp –up /srv/save/srv/eyesofnetwork/nagvis/etc/maps/* /srv/eyesofnetwork/nagvis/etc/maps/
```

4. Réaffectez le propriétaire et le groupe aux maps

```
chown -R nagios:eyesofnetwork /srv/eyesofnetwork/nagvis/etc/maps/*
```

5. Se connecter à « *nagvis* » à partir de l'interface web et vérifiez que tout est ok.

En théorie, vous ne devriez pas rencontrer d'erreurs.

Ceci conclut notre mise à jour concernant l'outil « *Nagvis* »

### 12.3.4 - Mise à jour de « *Cacti* »

1. Copiez d'abord vos fichiers images map et ou icones de « *cacti/weathermap* » si vous en avez utilisé.

```
cp –up /srv/save/srv/eyesofnetwork/cacti/plug-ins/weathermap/images/* /srv/eyesofnetwork/cacti/plug-ins/weathermap/images/
```

Puis

```
cp –up /srv/save/srv/eyesofnetwork/cacti/plug-ins/weathermap/configs/nom_cartes /srv/eyesofnetwork/cacti/plug-ins/weathermap/configs/
```

2. Copiez les plugins snmp de votre répertoire (si vous en utilisez)

```
cp –up /srv/save/srv/eyesofnetwork/cacti/ressource/snmp-queries/* /srv/eyesofnetwork/cacti/ressource/snmp-queries/
```

3. Vérifiez que le propriétaire du plugin est « *cacti* » et le groupe est « *eyesofnetwork* ». Si non, faites :

```
chown cacti:eyesofnetwork plugin
```

4. Copiez les fichiers « *rra* » de « *cacti* ». Ce sont les fichiers de données générés par cacti en fonction de vos périphériques que vous « grapher »

```
cp –up /srv/save/srv/eyesofnetwork/cacti/rra/* /srv/eyesofnetwork/cacti/rra/
```

5. Décompressez l'archive « *srveon-cacti.bz2* »

```
bunzip2 srveon-cacti xxxx.sql.bz2
```

6. Importez le fichier sql dans la BDD de cacti

```
mysql cacti -u root --password=root66 < /srv/save/srveon-cacti.xxx..sql
```

7. Se connecter à l'interface web de « *cacti* » et vérifiez que tout soit ok.

### 12.3.5 - Mise à jour de l'interface Web d'EON

Cette étape est nécessaire si vous avez personnalisé l'interface web d' « *EON* » (ajout d'utilisateurs, groupes ou personnalisation du connecteur LDAP )

1. Décompressez le fichier sql « *srveon-eonweb* »

```
bunzip2 srveon-eonweb xxxx.sql.bz2
```

2. Importez le fichier sql dans la BDD

```
mysql eonweb -u root --password=root66 < /srv/save/srveon-eonweb.xxx..sql
```

# 13 - Axes de progressions

Afin d'enrichir cette documentation il serait intéressant d'inclure une explication d'utilisation sur ces outils :

- weathermap
- adaptation des rapports (modification logo etc...)