Supervision du réseau GSB avec EyesOfNework 3.1

Propriétés	Description
Type de publication	Côté labo
Intitulé court	**Supervision d'un réseau**
Intitulé long	Supervision des éléments importants du réseau du contexte GSB avec l'outil EyesOfNetwork.
Module	BTS SIO2 – SISR5
Transversalité	SISR3 SISR4 PPE
Présentation	Ce **côté labo** est à destination des enseignants, il sera suivi d'un TP pour les étudiants reprenant les mêmes besoins, avec des indications sur les scripts (plugins) à utiliser pour chaque élément à superviser.
Activités	**D3.3 - Administration et supervision d'une infrastructure**
Pré-requis	Avoir quelques notions sur la configuration et l'administration d'un serveur Linux. Avoir quelques notions sur la configuration et l'administration des éléments d'interconnexion Cisco. Avoir mis en place le contexte GSB modifié avec l'ajout d'une DMZ (réalisable avec le contexte de base).
Savoir-faire principaux	Justifier le choix d'une solution technique de supervision de réseau. Installer et configurer une solution de contrôle et de surveillance des communications. Installer et configurer une solution de supervision des éléments d'interconnexion. Contrôler et améliorer les performances du réseau. Valider et documenter une solution de supervision.
Outils	EyesOfNetwork : http://www.eyesofnetwork.com/?lang=fr MibBrowser de ManageEngine : http://www.manageengine.com/products/mibbrowser-free-tool/download.html Deux commutateurs, un commutateur-routeur et un routeur Cisco, un serveur DHCP/DNS sous Windows2008R2, une imprimante réseau, un point d'accès et un poste client sous Windows7. Quatre scripts PERL fournis : check_dhcp_addfree, check_snmp_cisco_memutil, check_snmp_cisco_loadavg check_snmp_printer
Mots-clés	Supervision, SNMP, TRAP, Interruption, Nagios, Nagvis, SNMPTT, ITIL
Auteur(es)	Daniel Régnier, avec les relectures attentives d'Apollonie Raffalli et de Roger Sanchez
Version	v 1.0

Présentation générale

Ce document présente une mise en place de la supervision du réseau du contexte GSB (ayant subi quelques modifications) avec l'outil EyesOfNetwork. L'objectif est de réaliser une cartographie (NAGVIS) simplifiée des éléments supervisés avec des niveaux d'alerte pour certains composants et des notifications via la messagerie locale du serveur de supervision.

Aucun agent de distribution de courrier aux clients n'est mis en place. Pour être opérationnel, nous devrions normalement configurer POSTFIX pour relayer les messages vers le serveur de messagerie de GSB.

Ce **côté labo** est à destination des enseignants, il sera suivi d'un TP pour les étudiants reprenant les mêmes besoins, avec des indications sur les scripts (plugins) à utiliser pour chaque élément à superviser.

La partie sur les interruptions (traps) SNMP, un peu plus complexe, n'est pas inclue dans le TP destiné aux élèves.

La distribution Linux de EyesOfNetwork est CENTOS, minimaliste et sans interface graphique. La configuration de la supervision est réalisée via une interface Web, unique. La présentation de EyesOfNetwork est accessible à l'adresse suivante : http://www.eyesofnetwork.com/?lang=fr

Parmi tous les composants de EyesOfNetwork, ce document n'aborde que les configurations de NAGIOS, NAGVIS et SNMPTT. Les éléments comme CACTI, WEATHERMAP ou l'intégration de GLPI/OCS/FUSION seront peut-être traités dans un autre Côté labo.

L'installation d'un serveur EyesOfNetwork est très simple, elle ne demande que très peu de compétence sous Linux. Elle est réalisée à partir d'un fichier ISO d'environ 1 Go, téléchargeable à l'adresse suivante : http://www.eyesofnetwork.com/?page_id=48&lang=fr

Pour la mise en place de cette réalisation, il semble plus judicieux de virtualiser ce serveur.

Les équipements supervisés sont trois commutateurs et un routeur Cisco, un serveur DHCP/DNS sous Windows2008R2, une imprimante réseau, un point d'accès et un poste client sous Windows7.

Ce document comprend six parties :

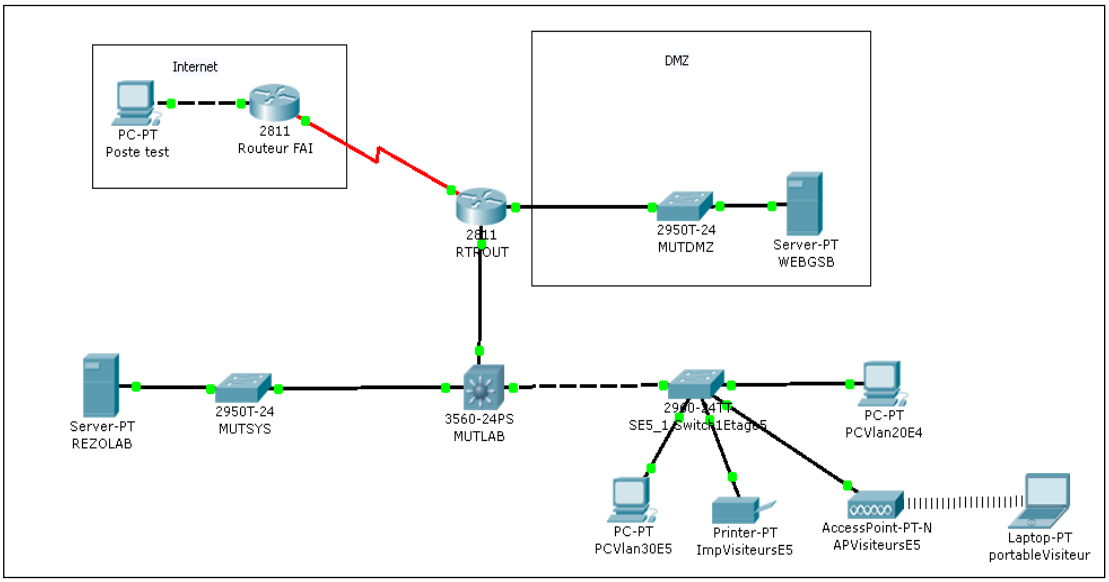
- progression de la réalisation ;
- présentation du contexte GSB modifié et des besoins de supervision ;
- principes de configuration de la supervision ;
- ajouts d'éléments à superviser ;
- création de la carte NAGVIS des équipements supervisés ;
- mise en place d'une supervision à l'aide des interruptions (traps) SNMP.

Une table des matières détaillée est présentée à la fin du document, page 65.

Progression de la réalisation

Présentation du contexte GSB modifié

1. Schéma du réseau modifié



2. Modifications par rapport au contexte GSB

- Simplification du schéma réseau :
  - un seul commutateur pour les serveurs,
  - un seul commutateur pour les services.

- Point d'accès Visiteurs étage 5 :
  - Nom : APVisiteursE5
  - IP : 192.168.150.220/24

- Ajout d'une imprimante Visiteurs pour les tests :
  - Nom : ImpVisiteursE5
  - IP : 192.168.150.200/24

- Ajout d'une DMZ à l'aide du routeur RTROUT :
  - IP réseau de la DMZ : 10.0.0.0/24
  - Interfaces du routeur RTROUT :
    - Réseau local : 172.18.0.2/30 (Vlan sortie)
    - DMZ : 10.0.0.254/24,
    - Internet : 86.86.1.1/24
  - Configuration NAT-PAT et ACL

- Tous les commutateurs sont administrables à partir d'une adresse IP compatible avec le VLAN 10 (Réseau et Système), MUTSYS : 192.168.10.2, SE5_1 (Swich1Etage5) : 192.168.10.11 et MUTLAB : 192.168.10.1 (voir annexe 1).

Remarque :
Le contexte GSB de base est utilisable : le routeur RTROUT est remplacé par un proxy, mais il est alors nécessaire de définir les adresses IP sur les matériels d'interconnexion (voir annexe 1).

3. Les besoins de supervision

L'administrateur du réseau GSB souhaite mettre en place une supervision des éléments importants du réseau.
Il a décidé de superviser les éléments suivants :

- Au niveau du serveur REZOLAB :
  - taux d'occupation du CPU et de la mémoire,
  (Seuils : avertissement 80 %, alerte critique 90%).

- Taux d'occupation des partitions physiques sur les disques durs,
  (Seuils : avertissement 70 %, alerte critique 85%) ;

  - nombre d'adresses DHCP restantes sur le réseau des visiteurs (192.168.150.0/24),
  (Seuils : avertissement 5 adresses, alerte critique 2 adresses) ;

  - service DNS actif.

- Au niveau du routeur-commutateur MUTLAB :
  - état (actif ou pas) ;

  - taux d'occupation du CPU et de la mémoire ;

  - activité des liens avec les autres matériels d'interconnexion (commutateurs MUTSYS (Fa0/2) et Switch1Etage5 (Fa0/5), routeur RTROUT (Fa0/7), trafic en entrée et en sortie,
  (Seuils : avertissement 90%,90%, alerte critique 95%,95%).

- Au niveau des commutateurs MUTSYS et SE5_1 (Switch1Etage5) :
  - état (actif ou pas) ;

  - taux d'occupation du CPU et de la mémoire.

- Au niveau du routeur RTROUT de la DMZ :
  - état (actif ou pas) ;

  - taux d'occupation du CPU et de la mémoire ;

  - activité des liens avec le fournisseur d'accès (S0/0/0) et le commutateur de la DMZ (G0/1), trafic en entrée et en sortie (E, S), (Seuils : avertissement 90%,90%, alerte critique 95%,95%).

- Au niveau de l'imprimante réseau ImpVisiteursE5 :
  - niveau du cartouche d'impression (Seuils : avertissement 20%, alerte critique 10%) ;

  - niveau du bac d'alimentation des feuilles (Seuils : avertissement 10%, alerte critique 5%) ;

  - nombre de pages imprimées (supervision sans alerte).

- Au niveau du point d'accès visiteurs APVisiteursE5 :
  - état (actif ou pas) ;

  - surveillance du nombre de clients WiFi connectés (voir remarque).

Remarque : le point d'accès utilisé ne permet pas de surveiller le nombre de clients connectés via SNMP, pour les tests, c'est la surveillance d'une variable de la MIB de l'équipement qui sera utilisée (*stTrErrorCount*), qui comptabilise le nombre de transmissions en erreur.

- Supervision d'équipement à l'aide des interruptions SNMP (TRAP SNMP) :
  - surveillance du poste PCVlan30E5, nommé v30e5p001 (vlan-étage-prise) :
    - alerte si conflit d'adresse IP (surtout pour les tests) ;
    - alerte si un disque est sur le point d'être saturé.

Principes de configuration de la supervision

Le principe de cette supervision est présenté en prenant comme exemple la surveillance du CPU, de la mémoire et des disques durs du serveur REZOLAB. Cette configuration est réalisée avec des commandes qui interrogent régulièrement les éléments de ce serveur via des requêtes SNMP. En fonction des résultats et de niveaux d'alertes définis, un administrateur désigné dans les contacts reçoit une notification par messagerie (locale).

1. Installation de EyesOfNetwork (EoN)

Différents documents sur la configuration de EyesOfNetwork sont téléchargeables à l'adresse suivante : http://www.eyesofnetwork.com/?page_id=495&lang=fr
Pour une description détaillée de l'installation, voir le document :
http://www.eyesofnetwork.com/eonrepo/Eon%203.1%20Installation.pdf

Pour une mise en œuvre sous HyperV (Windows2008R2), lors de la création de la machine virtuelle, il est nécessaire de spécifier une carte réseau héritée.

Pendant l'installation, saisir les paramètres réseaux suivants :

Nom du serveur	:	srveon.gsbeu.intra	
Adresse IP du serveur	:	172.16.0.11	(Compatible avec le vlan 300, serveurs)
Masque	:	255.255.128.0 (/17)	
Passerelle par défaut	:	172.16.0.1	(Passerelle du vlan 300)
Serveur DNS	:	172.16.0.10	(Serveur DNS REZOLAB)

2. Configuration de SNMP sur les hôtes

Rappel sur SNMP : voir annexe 2.
Il est nécessaire de définir le même nom de communauté sur tous les hôtes à superviser (postes, serveurs, imprimantes, commutateurs et routeurs Cisco) : nous utiliserons ici le nom **gsbintra**.

2.1 Service SNMP sur Windows 7

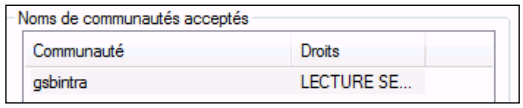
Installation et configuration de l'agent SNMP sur les systèmes Windows.

Installation du service SNMP sur Windows 7 :

- *Panneau de configuration*, *Afficher* par : Catégorie, clic sur le lien *Programmes*,
- sous *Programmes et fonctionnalités*, clic sur le lien Activer ou désactiver des fonctionnalités Windows,
- cochez la case *Protocole SNMP* avec le sous-dossier (Fournisseur SNMP WMI), bouton *OK*.

Configuration du service SNMP sur Windows :

- *Panneau de configuration*, *Afficher* par : Petites icônes,
- *outils d'administration, Services*,
- clic droit sur Service SNMP, *Propriétés*,
- onglet *Sécurité* :
  - ajouter une communauté avec le bouton *Ajouter…*, sélectionner LECTURE SEULE dans la liste déroulante,
  - dans la zone "*Nom de la communauté"*, saisir **gsbintra**, bouton *Ajouter*,
- cocher "*Accepter les paquets SNMP provenant de n'importe quel hôte"* (*peu sécurisé*),
- boutons *Appliquer* et bouton *OK*.
- redémarrer le service SNMP.



2.2 Service SNMP sur Cisco

Sur chacun des éléments d'interconnexion, utiliser les instructions suivantes :

```
>enable
#configuration terminal
#(config)snmp-server community gsbintra
```

3. Configuration du serveur

Par défaut, le serveur EoN n'a pas d'interface graphique. La connexion au serveur SSH (installé par défaut) en ligne de commande à partir d'un utilitaire (comme « putty » dans un environnement client sous Windows) s'effectue via :

Login : *root*
Password : *mot de passe défini à l'installation*

3.1 Configuration réseau

Si la configuration saisie à l'installation ne convient plus, vérifier l'adresse actuelle avec *ifconfig*.

Pour modifier l'adresse IP de l'interface eth0 : fichier /etc/sysconfig/network-scripts/ifcfg-eth0
Saisir une adresse IP compatible avec le réseau 172.16.0.0 /17, exemple : 172.16.0.11/17 :

```
DEVICE=eth0
BOOTPROTO=static
IPADDR=172.16.0.11
NETMASK=255.255.128.0
NETWORK=172.16.0.0
BROADCAST=172.16.127.255
ONBOOT=yes
HWADDR=00:15:5d:0a:04:14
```

Nom du serveur et passerelle par défaut : fichier /etc/sysconfig/network
Pour HOSTNAME, saisir un nom de la forme : srveon.gsbeu.intra
Saisir la passerelle par défaut : 172.16.0.1 (adresse IP du VLAN 300) :

```
NETWORKING=yes
NETWORKING_IPV6=no
HOSTNAME=srveon.gsbeu.intra
GATEWAY=172.16.0.1
```

Résolution de noms (DNS) : fichier /etc/resolv.conf
Saisir le nom du domaine et l'adresse IP du serveur DNS :

```
search gsbeu.intra
nameserver 172.16.0.10
```

Pour relancer le daemon réseau : *service network restart*

Pour valider immédiatement le nouveau nom : taper *hostname srveon.gsbeu.intra*

Pour tester la connexion vers les autres éléments du réseau, vous pouvez déployer les utilitaires habituels comme le « ping ».

3.2 Service de messagerie

La notification des alertes peut se faire via des messages mail.
Par défaut, EoN installe un serveur de messagerie SMTP, POSTFIX, mais aucun agent de distribution de courrier aux clients n'est en place. Pour être opérationnel, nous devrions normalement configurer POSTFIX pour relayer les messages vers le serveur de messagerie de GSB.

Dans cette première étude, la configuration de POSTFIX ne sera pas modifiée et les messages tests seront consultés localement.

Tests de lecture des messages (MAIL) :

a) Envoyer un message
Taper la commande : *mail root@srveon.gsbeu.intra*
Saisir l'objet : essai de messagerie
Saisir le texte du message : test de message
Pour terminer : touche *Entrée*, saisir le point et touche *Entrée*
Ne pas saisir d'adresse pour la transmission d'une copie du message (Cc :) : touche *Entrée*
b) Lire le message
Taper la commande : *mail*
Sélectionner le numéro du message à lire.
Pour terminer, taper q.

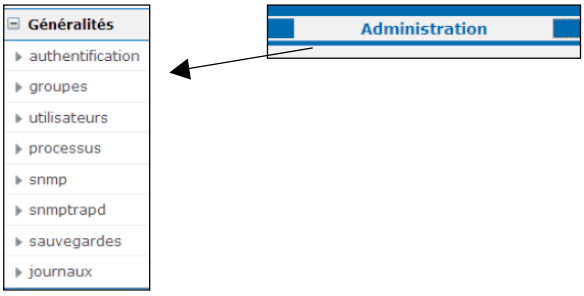
4. Configuration initiale de EoN

4.1 Connexion au site Web d'administration d'EoN

Taper l'adresse IP du serveur EoN (ici 172.16.0.11) dans un navigateur et saisir les informations suivantes :

- identifiant : admin
- mot de passe : admin

Pour commencer, le menu Administration va nous permettre d'accéder aux Généralités :



4.2. Configuration de SNMP sur le serveur EoN

Pour également surveiller notre serveur EoN, nous allons définir le même nom de communauté (en l'espèce **gsbintra**) sur l'agent SNMP mis en place par le service SNMPD.

4.2.1 Le service SNMPD

Menu Administration, Généralités/snmp
Dans le fichier de configuration du service SNMPD, remplacer le nom par défaut de la communauté *"community EyesOfNetwork"* par **gsbintra** :

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

Bouton *Update*.

4.2.2 Relance du service SNMPD

Menu *Administration, Généralités/processus*
Utiliser le lien *restart* du processus SNMP agent pour relancer ce service :

SNMP agent	UP	1704	stop restart reload
SNMP trap agent	UP	1718	stop restart reload

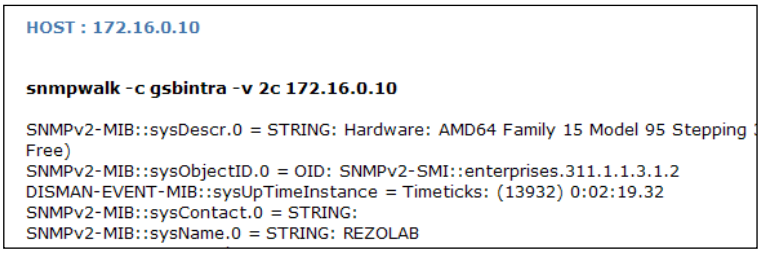
4.3 Test SNMP à partir du serveur EoN

Menu *Administration Généralités/snmpwalk*

Saisir l'IP de l'élément à tester et le nom de la communauté SNMP, ici nous testons l'accès au serveur REZOLAB, d'adresse 172.16.0.10 :

Bouton *"Run It !"* :

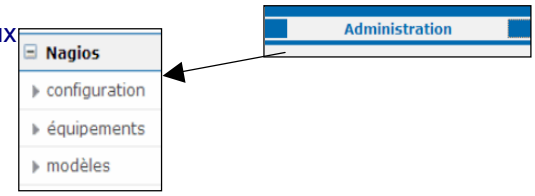
Résultat :



Tester les différents éléments à superviser.

4.4 Les variables de NAGIOS

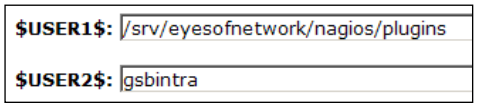
Le menu Administration nous permet d'accéder aux éléments de configuration de Nagios :



Il reste à configurer le nom de la communauté utilisée par le serveur Nagios pour interroger les éléments supervisés.

Menu *Administration, Nagios/configuration*
Utiliser le lien *Nagios Ressources* :

Modifier la valeur de la variable **$USER2$** contenant EyesOfNetwork par le nouveau nom de communauté **gsbintra** :



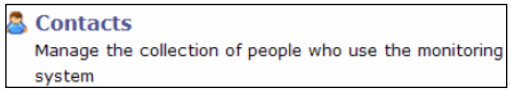
En bas, bouton *"Update Ressource Configuration"*
Noter le contenu de la variable **$USER1$** qui indique le chemin où sont placés les plugins.

5. Configuration des contacts dans EoN

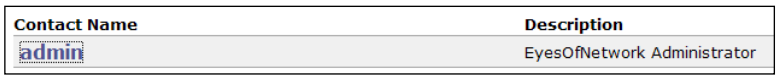
5.1 Renseignement de l'adresse mail du contact

Le contact prédéfini dans EoN se nomme admin.

Menu *Administration, Nagios/configuration*
Utiliser le lien *Contacts* :



Le lien admin permet de configurer ce contact :

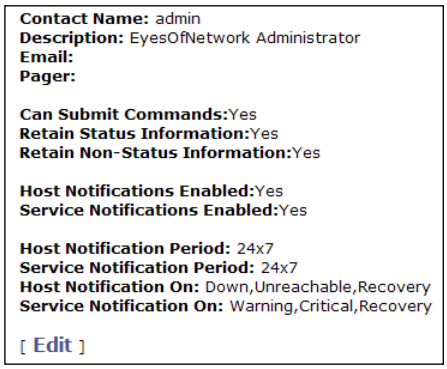


Nous retrouvons les paramètres de notification, notamment :

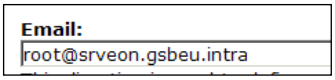
- *"Host Notification On"* : Notification liées à l'équipement

- *"Service Notification On"* : Notification liées à un service

Pour saisir l'adresse du contact, utiliser le lien *Edit* :

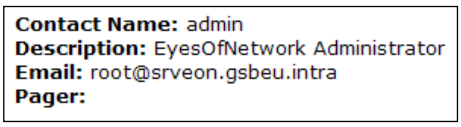


Saisir l'adresse root@srveon.gsbeu.intra dans la zone Email :



Bouton *"Modify Contact"*.

Nous obtenons :



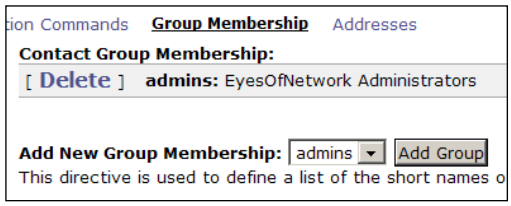
5.2 Les groupes de contacts

Pour faciliter la notification des évènements, c'est le groupe Admins qui est prédéfini dans EoN. Mais il est possible de spécifier un autre groupe ou un contact spécifique pour un équipement.

5.2.1 Affectation d'un contact à un groupe

Vérifier que le contact admin est bien dans le groupe Admins.

Utiliser le lien *"Group Membership"* :



Nous pouvons affecter le contact à plusieurs groupes à l'aide du bouton *"Add Group"* :

5.2.2 Ajout d'un nouveau groupe de contacts

Menu *Administration, Nagios/configuration*
Utiliser le lien *"Contact Groups"* :

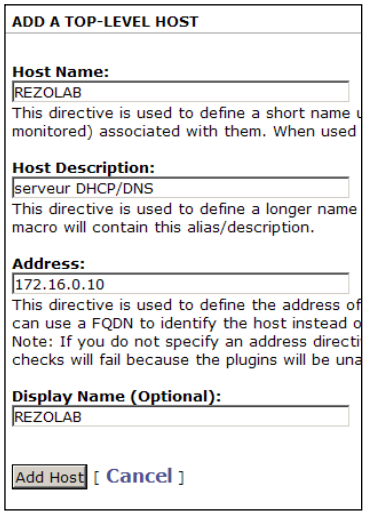
6. Ajout du serveur REZOLAB

Menu *Administration, Nagios/équipements* (ou Menu *Administration, Nagios/configuration*, lien *Network*).

6.1 Ajout d'un équipement

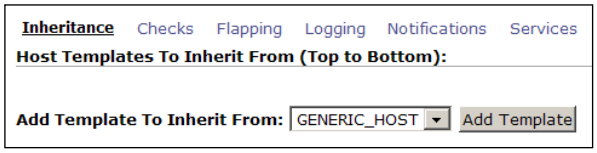
- Utiliser le lien *"Add A New Child Host"* et renseigner les informations :

Host Name	: REZOLAB
Host Description	: Serveur DHCP/DNS
Address	: 172.16.0.10
Display Name	: REZOLAB



Valider avec le bouton *"Add Host"*.

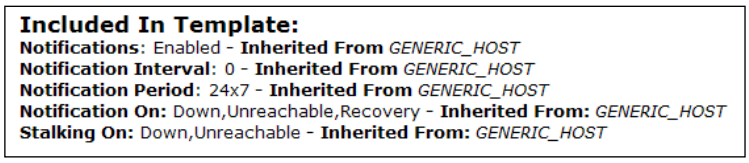
- Utiliser le lien *Inheritance*, et sélectionner dans la liste déroulante "GENERIC_HOST" :



Valider avec le bouton *"Add Template"*.

- Utiliser le lien *Contacts* et vérifier que le groupe Admins est déjà défini grâce au Template "GENERIC_HOST" :

- Utiliser le lien *Notifications* et vérifier que les paramètres de notifications sont définis grâce au template "GENERIC_HOST" :

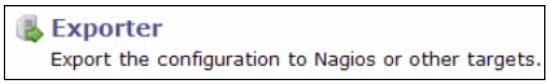


Remarque : l'explication des différents paramètres est présentée en 8

6.2 Transfert d'un équipement dans Nagios

Utiliser le lien *Tools* en haut à droite.

Utiliser le lien *Exporter* :



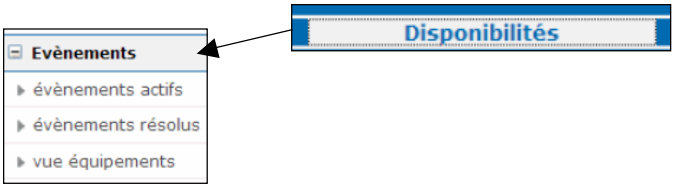
Utiliser le lien *Restart (Job)* :

Attendre le message *Export Job ... Successfully* :

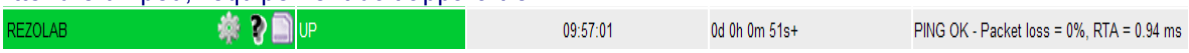
Remarque : cette procédure de transfert est obligatoire après chaque modification de la configuration d'un équipement. Elle met à jour les fichiers de configuration de Nagios (voir annexe 4).

6.3 Vue de l'équipement dans Nagios

Le menu *Disponibilités* nous permet d'accéder à la supervision des équipements :

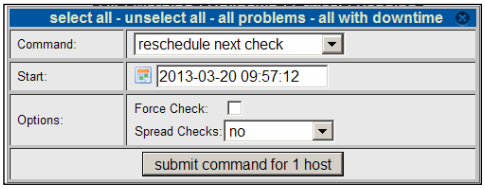


Pour voir notre serveur REZOLAB :
Menu *Disponibilités, Évènements/vue équipements*,
Attendre un peu, l'équipement doit apparaître :



Si l'état est *"Status : PENDING"*, utiliser ce lien *PENDING* :

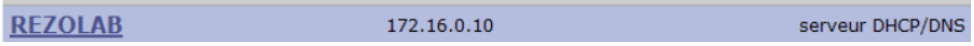
Une fenêtre s'ouvre, elle permet de relancer la commande de supervision de l'équipement à l'aide du bouton *"submit command for 1 host"* :



7. Analyse des éléments de configuration d'un hôte

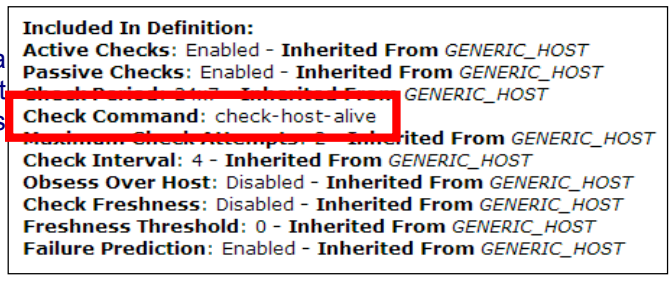
Menu *Administration, Nagios/équipements*

Ouvrir les paramètres de configuration avec le lien REZOLAB :



- Lien *Checks*

Ces options permettent de vérifier la présence de l'équipement cible en utilisant notamment la commande définie dans *"Check Command"* :



Présentation des principales options :

*** 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 (voir **21**. et annexe 2).

*** Check Period** : période pendant laquelle Nagios est autorisé à vérifier l'état de l'équipement.

*** Check Command** : commande utilisée pour faire cette vérification.
Ici, la commande *"check-host-alive"* est utilisée pour déterminer si l'hôte est actif ou non sur le réseau. Typiquement, cette commande lance un ping vers l'hôte pour connaître son état. La commande retourne un état OK (0) si l'hôte répond.

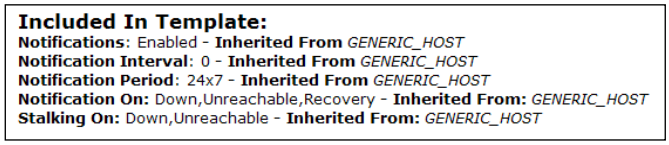
*** Maximum Check Attempts** : nombre maximum de vérifications à effectuer avant de signaler un équipement comme éteint ou en erreur.

*** Check Interval** : nombre de minutes entre deux vérifications. Ici, l'équipement est interrogé toutes les 4 mn.

*** Event Handler Command** : 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 a été paramétré dans *Notifications*). Afin d'éviter le spam de la 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** : autorise ou non l'utilisation de la commande *"Event Handler Command"* précédemment sélectionnée.

- Lien *Notification*
Ce lien permet de paramétrer les options de notification.



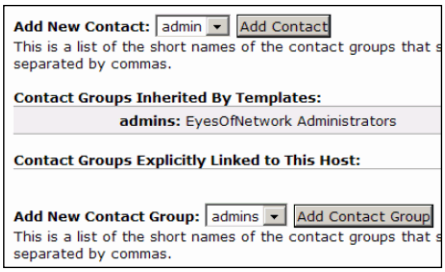
Présentation des principales options :

*** Notification Interval** : nombre de minutes entre les notifications concernant un équipement. Ici, avec 0, une seule notification d'avertissement est envoyée pour l'évènement en cours.

*** Notification On** : un mail est envoyé suivant l'état de l'hôte. Ici, nous avons Down, Unreachable ou Recovery.

- Lien *Contacts*
Il est possible d'ajouter un contact spécifique *"Add New Contact"* et bouton *"Add Contact"*.

De même, il est possible d'ajouter un groupe supplémentaire *"Add New Contact Group"* et bouton *"Add Contact Group"*.



- Lien *"Group Memberships"*
Ce lien permet d'affecter l'hôte à un groupe afin d'avoir des vues par type d'équipements.

- Lien *Services*
Ce lien permet de définir les services supervisés pour cet équipement.
Pour l'instant, aucun service n'est supervisé pour l'hôte créé. Seule la commande check-host-alive (PING) est utilisée pour connaître l'état général de l'équipement.

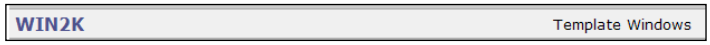
Remarque : chaque service fait appel à un script qui se trouve dans le répertoire plugins de Nagios : (/srv/eyesofnetwork/nagios/plugins)

8. Modèles (Template) de services

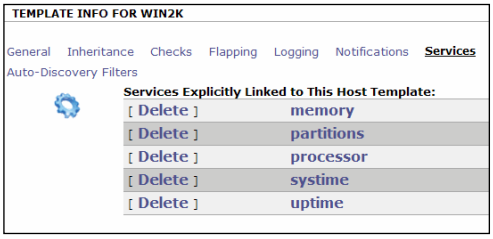
EoN contient des modèles (templates) de définition de services en fonction des équipements à superviser.

Menu *Administration, Nagios/modèles*

Pour voir les services associés au modèle WIN2K, utiliser le lien *WIN2K* :



Utiliser le lien *Services*, cinq services sont supervisés dans ce modèle :

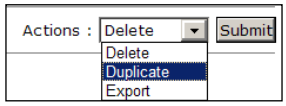


8.1 Ajout d'un modèle de services à partir d'une copie de modèle

Pour simplifier notre supervision, nous allons créer un nouveau modèle qui ne supervise, pour les équipements Windows, que les trois premiers services.

Cocher la case à droite du modèle WIN2K :

En haut, dans la liste Actions, sélectionner *Duplicate* et bouton *Submit* :

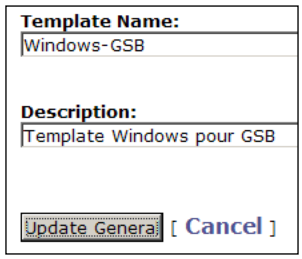


A l'avertissement, répondre OK.

Une copie du modèle est créée avec un nom de la forme WIN2K-nnnn (les numéros sont aléatoires).
Utiliser le lien *WIN2K-nnnn* :

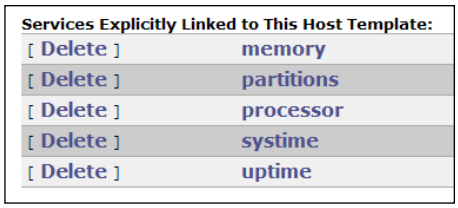
Modifier le nom : utiliser le lien *General* et lien *Edit* :
Saisir un nouveau nom pour ce modèle : **Windows-GSB**
Et une description : **Template windows pour GSB**

Bouton *"Update General"* :



Modifier/Supprimer des services : lien *Services*

Utiliser le lien *Delete* pour supprimer les deux derniers services : **systime** et **uptime** :



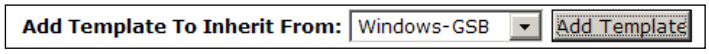
8.2 Affectation du nouveau modèle de services

Nous allons affecter ce nouveau modèle à notre hôte REZOLAB.

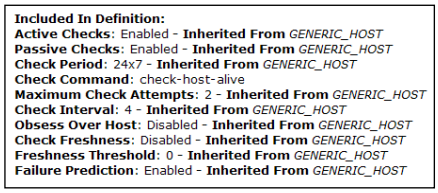
Menu *Administration, Nagios/équipements*, dans le tableau, utiliser le lien *REZOLAB*.
Utiliser le lien *Inheritance*, et pour supprimer le modèle "GENERIC_HOST", utiliser le lien *Delete*.

Sélectionner le modèle Windows-GSB dans la liste *"Add Template To inherit From"*.

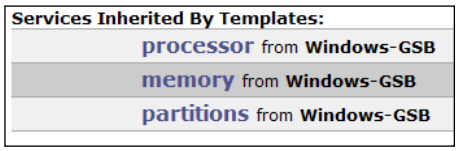
Valider avec le bouton *"Add Template"* :



Utiliser le lien *Checks*
Vérifier que l'état général de l'hôte est toujours testé avec la commande ***check-host-alive***, notre modèle **Windows-GSB** étant dérivé du modèle GENERIC_HOST :



Utiliser le lien *Services*
Vérifier la présence des trois services définis dans le modèle Windows-GSB :



Utiliser le lien *"Group Memberships"*
Le groupe d'équipements du modèle Windows-GSB est un groupe nommé WINDOWS.

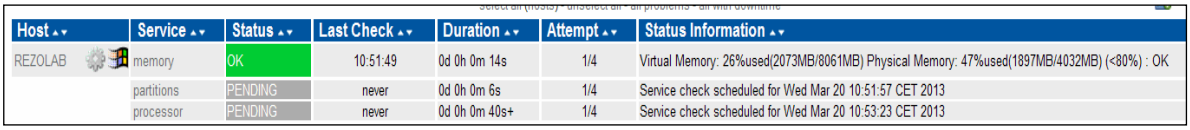
Remarque : Windows-GSB a été créé à partir d'une copie du modèle WINDOWS (Template) auquel est affecté le groupe d'équipements nommé WINDOWS.

8.3 Test dans Nagios

- Transférer vers Nagios
Menu *Tools / Exporter / Restart*, attendre le message *Export Job ... Successfully*

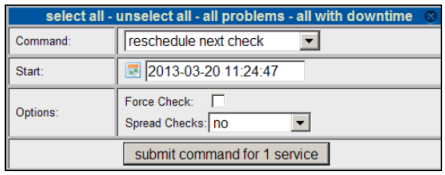
- Vue des services de l'équipement dans Nagios
Menu *Disponibilités, Évènements/vue services*, attendre un peu…

Pour chaque service, nous retrouvons son état (Status: OK, WARNING, CRITICAL) et une information sur cet état :

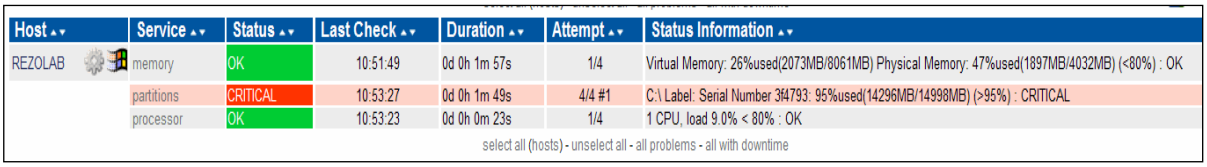


Host	Service	Status	Last Check	Duration	Attempt	Status Information
REZOLAB	memory	OK	10:51:49	0d 0h 0m 14s	1/4	Virtual Memory: 26%used(2073MB/8061MB) Physical Memory: 47%used(1897MB/4032MB) (<80%) : OK
	partitions	PENDING	never	0d 0h 0m 6s	1/4	Service check scheduled for Wed Mar 20 10:51:57 CET 2013
	processor	PENDING	never	0d 0h 0m 40s+	1/4	Service check scheduled for Wed Mar 20 10:53:23 CET 2013

Si l'état d'un service est ***"Status : PENDING"***, utiliser ce lien *PENDING* :
Une fenêtre s'ouvre, elle permet de relancer la commande de supervision de ce service à l'aide du bouton ***"submit command for 1 service"*** :



Résultat :



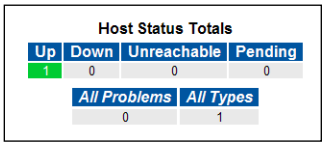
Host	Service	Status	Last Check	Duration	Attempt	Status Information
REZOLAB	memory	OK	10:51:49	0d 0h 1m 57s	1/4	Virtual Memory: 26%used(2073MB/8061MB) Physical Memory: 47%used(1897MB/4032MB) (<80%) : OK
	partitions	CRITICAL	10:53:27	0d 0h 1m 49s	4/4 #1	C:\ Label: Serial Number 3f4793: 95%used(14296MB/14998MB) (>95%) : CRITICAL
	processor	OK	10:53:23	0d 0h 0m 23s	1/4	1 CPU, load 9.0% < 80% : OK

select all (hosts) - unselect all - all problems - all with downtime

Remarque : J'ai un petit problème avec mon lecteur C: !

En haut de la page, nous retrouvons différents liens pour superviser et analyser l'état des équipements :

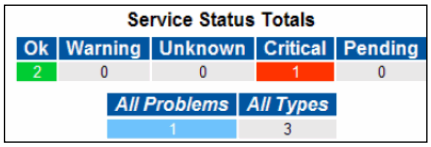
Liens sur la connexion des hôtes :



Host Status Totals			
Up	Down	Unreachable	Pending
1	0	0	0

All Problems	All Types
0	1

Liens sur les services :



Service Status Totals				
Ok	Warning	Unknown	Critical	Pending
2	0	0	1	0

All Problems	All Types
1	3

Menu *Disponibilités, Évènements/vue équipements*

Les liens en haut à gauche permettent d'afficher une vue des équipements suivants différents critères :

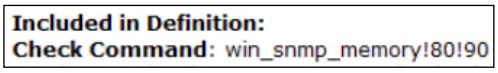
Utiliser le lien *REZOLAB*, les liens en haut à gauche permettent d'obtenir des renseignements sur cet hôte.

Avec le lien *"View Status Detail For This Host"*, nous retrouvons les services de l'hôte :

9. Personnalisation d'un service

Nous allons personnaliser le service ***memory*** afin d'avoir un avertissement à partir d'un niveau assez faible d'utilisation (30%, juste pour les tests).

Menu *Administration Nagios/équipements*,
Utiliser le lien *REZOLAB*, le lien *Services* et le lien ***memory***,
Pour voir la commande utilisée, lien *Checks* :



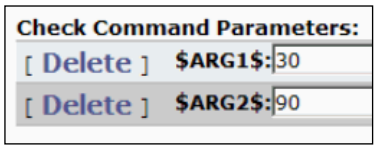
La commande utilisée "*win_snmp_memory*" est disponible dans "*Nagios commands*" (voir le **11.**).

Les valeurs « !80!90 ! » sont des arguments que nous passons à la commande. Ici, le 80 (en pourcentage) spécifie le seuil d'utilisation pour déclencher un avertissement (WARNING) et 90 spécifie le seuil d'utilisation pour déclencher une alerte critique (CRITICAL).

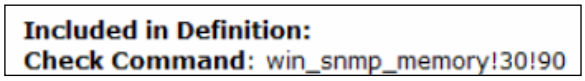
9.1 Changement des valeurs des seuils

Pour modifier les arguments (seuils) de la commande, utiliser le lien "*Check Command Parameters*" :

Pour le premier argument ($ARG1$), saisir 30 et bouton *Update* :
ATTENTION : ne pas oublier le bouton *Update* après chaque modification d'argument.



Vérifier avec le lien *Checks* que les arguments sont maintenant : « !30!90 ! »



9.2 Test dans Nagios

- Transférer vers Nagios
Menus *Tools / Exporter / Restart*, attendre le message *"Export Job ... Successfully"*

- Vue de l'équipement et de ses services dans Nagios
Menu *Disponibilités, Évènements/vue services*

Si l'état du service "*memory*" n'a pas changé, click dans la colonne *Status* du service concerné.
La fenêtre pour rafraichir l'état du service s'ouvre, utiliser le bouton ***"submit command for 1 service"***.

Pour le service "*memory*", on doit obtenir l'état ***"Status : WARNING"*** (en jaune) :

Host	Service	Status	Last Check	Duration	Attempt	Status Information
REZOLAB	memory	WARNING	11:28:53	0d 0h 4m 37s	4/4 #1	Virtual Memory: 26%used(2076MB/8061MB) Physical Memory: 47%used(1900MB/4032MB) (>30%) : WARNING

La colonne *Status* information nous indique bien que l'utilisation de la mémoire est >30%.

9.3 La notification

Utiliser le lien *"View Notifications For This Host"* :

Une notification pour le service *memory* à destination du contact admin a été déclenchée :

Host	Service	Type	Time	Contact	Notification Command
REZOLAB	memory	WARNING	2013-03-20 11:27:47	admin	notify-by-email-service

Sur le serveur EoN, en ligne de commandes, taper la commande : *mail*
Un message concernant une alerte sur la mémoire doit apparaître.
Taper le numéro de ce message pour lire son contenu et retrouver les données de cette notification.
Pour quitter : taper q

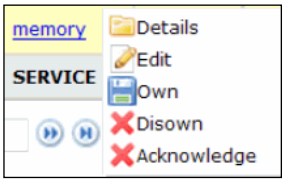
9.4 Le suivi des évènements

- Résultat dans Nagios :
Menu *Disponibilités, Évènements/évènements actifs*

☐	REZOLAB	memory	!		Virtual Memory: 30%used(2395MB/8061MB) Physical Memory: 56%used (2273MB/4032MB) (30%) : WARNING

Nous obtenons un évènement WARNING, concernant le service *memory* de REZOLAB avec une description du problème.

- Pour supprimer cet élément des évènements actifs (considéré comme résolu) :
Click droit dans la ligne de l'évènement, menu *Acknowledge*

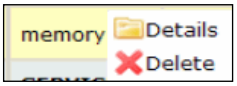


Remarque :
Le menu ***Details*** permet d'avoir plus d'informations, dont l'adresse IP de l'équipement.
Le menu ***Own*** permet de définir le compte qui prend en charge cet évènement.

- Pour visualiser les évènements résolus :
Menu *Disponibilités, Évènements/évènements résolus*

☐	REZOLAB	memory	!	admin@172.16.0.11	Virtual Memory: 29%used(2377MB/8061MB) Physical Memory: 56% used(2255MB/4032MB) (30%) : WARNING

- Pour supprimer cet évènement résolu :
Click droit dans la ligne de l'évènement, menu *Delete*



- Remettre un seuil d'avertissement à 80% pour le service "*memory*" (Menu *Administration*) et rafraîchir l'état de ce service avec le bouton ***"submit command for 1 service"*** (Menu *Disponibilités, Évènements/vue services*)
Pour le service *"memory"*, nous devons retrouver l'état ***"Status : OK"*** (en vert).

- Pour visualiser les évènements résolus :
Menu *Disponibilités, Évènements/évènements résolus*

☐	REZOLAB	memory	OK		Virtual Memory: 29%used(2328MB/8061MB) Physical Memory: 55%used (2209MB/4032MB) (80%) : OK
☐	REZOLAB	memory	!		Virtual Memory: 29%used(2328MB/8061MB) Physical Memory: 55%used (2209MB/4032MB) (30%) : WARNING

Si l'évènement WARNING du service memory de REZOLAB n'a pas été traité manuellement (Menu *Acknowledge*), cet évènement (WARNING) est placé automatiquement dans les évènements résolus avec l'évènement (OK), correspondant au rafraîchissement de l'état.

Une nouvelle notification pour le service "*memory*" a été déclenchée (lien *"View Notifications For This Host"*):

Host	Service	Type	Time	Contact	Notification Command	Information
REZOLAB	memory	OK	2013-04-10 11:25:41	admin	notify-by-email-service	Virtual Memory:

Cette notification correspond aussi au rafraîchissement de l'état (OK).

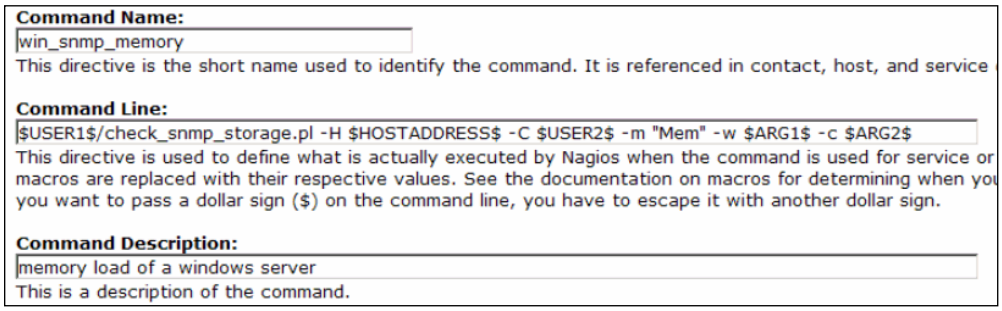
10. Analyse d'une commande Nagios

10.1 La commande dans Nagios

La commande *"win_snmp_memory"* accepte des arguments. Mais nous ne savons toujours pas quel est le plugin utilisé et surtout à quoi correspondent ces arguments. Ces informations sont spécifiées dans Nagios.

Menu *Administration, Nagios/configuration*
Utiliser le lien *"Nagios Commands"* :

Sélectionner la commande *"win_snmp_memory"* :



Command Line :
$USER1$: correspond au contenu de la variable $USER1$ vue dans "*Nagios Ressources*", c'est le chemin des plugins : /srv/eyesofnetwork/nagios/plugins (voir **4.4**).

Check_snmp_storage.pl : c'est le plugin qui est utilisé pour cette commande (.pl : c'est un script perl).

-H $HOSTADDRESS$: adresse IP de l'hôte supervisé contenu dans la variable $HOSTADDRESS$

-C $USER2$: la valeur de $USER2$ est le nom de la communauté, ici gsbintra (voir **4.4**).

-m "Mem" : Indique le type de stockage supervisé, ici, c'est la mémoire.

-w $ARG1$: premier argument, seuil à atteindre pour le niveau d'alerte (w=warning).

-c $ARG2$: deuxième argument, seuil à atteindre pour le niveau critique (c=critical)

Donc, pour l'hôte REZOLAB, la commande utilisée pour le service memory, "win_snmp_memory!80 !90", correspond à :

check_snmp_storage.pl –H 172.16.0.10 –C gsbintra –m "Mem" –w 80 –c 90

Ce qui donne avec le chemin :
/srv/eyesofnetwork/nagios/plugins/check_snmp_storage.pl –H 172.16.0.10 –C gsbintra –m "Mem" –w 80 –c 90

10.2 Test du script en ligne de commandes

Il est possible de tester ce script directement sur le serveur Eon. Se placer dans le dossier /srv/eyesofnetwork/nagios/plugins : *cd /srv/eyesofnetwork/nagios/plugins/*

Lancer le script avec les arguments spécifiés (faire précéder la commande de ./) :

./check_snmp_storage.pl –H 172.16.0.10 –C gsbintra –m "Mem" –w 80 –c 90

Vous devez obtenir les mêmes informations que dans la zone "*Information status*".
Pour avoir un résultat plus détaillé, nous pouvons ajouter l'argument –v à la fin de la commande :

./check_snmp_storage.pl –H 172.16.0.10 –C gsbintra –m "Mem" –w 80 –c 90 –v

Remarque : -v signifie le mode "verbose".
L'aide sur le script peut être obtenu avec l'argument –h, soit : *./check_snmp_storage.pl –h | more*
Nous retrouvons une présentation des différents arguments qu'il est possible d'utiliser avec ce script.

Ajouts d'éléments à superviser

11. Ajout d'un service de supervision DHCP

Nous allons commencer par ajouter un service de supervision des adresses IP libres du serveur DHCP.
Par défaut, EoN propose une commande pour superviser le nombre d'adresses IP disponibles. Mais cette commande utilise un script "check_dhcp_addfree" qui n'est pas dans le répertoire plugins.

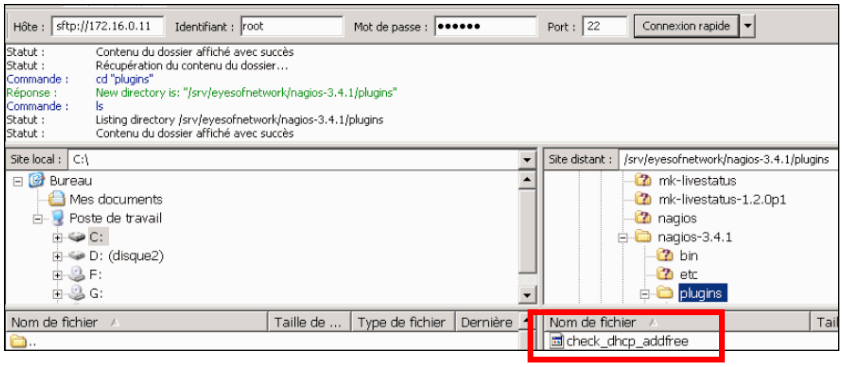
Nous pouvons télécharger ce script à l'adresse suivante :
http://lkco.gezen.fr/svn/supervision/trunk/plugins-nagios/Windows/

11.1 Ajout d'un script dans le répertoire plugins

Éventuellement, supprimer l'extension .txt du script téléchargé.
Pour transférer ce script sur le serveur EoN, nous allons utiliser un client FTP compatible avec SSH.

Exemple avec FileZilla Client

Pour la connexion :
- Hôte : 172.16.0.11
- Identifiant : root
- Mot de passe : (*Voir installation*)
- Port : 22



Transférer le script dans le répertoire /srv/eyesofnetwork/nagios/plugins

Il reste à rendre ce script exécutable par Nagios (qui utilise le compte nagios)
Sur le serveur EoN, taper les commandes suivantes (en étant positionné dans le répertoire plugins) :
- Changer de propriétaire : *chown nagios check_dhcp_addfree*
- Définir les droits : *chmod 775 check_dhcp_addfree*

Ce script (celui que j'ai testé) a un petit bug, il faut ajouter une directive pour son exécution.
Ouvrir le script avec vi et ajouter "–w" à la fin de la première ligne : #! /usr/bin/perl -w

- Tester le script :
Obtenir de l'aide : *./check_dhcp_addfree –h | more*

Nous retrouvons les arguments déjà utilisés au **10.2**, soit – H, -C, -w et -c
L'argument nouveau pour ce script est –s, il représente le réseau de l'étendue DHCP à tester.

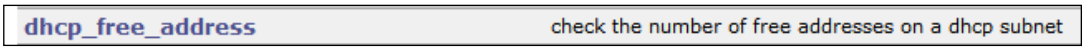
Nous voulons tester l'étendue DHCP du réseau Visiteurs de GSB, soit l'adresse réseau 192.168.150.0 avec les seuils : avertissement 5 adresses, alerte critique 2 adresses.

Lancer le script avec les arguments suivants :
./check_dhcp_addfree –H 172.16.0.10 –C gsbintra –s 192.168.150.0 –w 5 –c 2

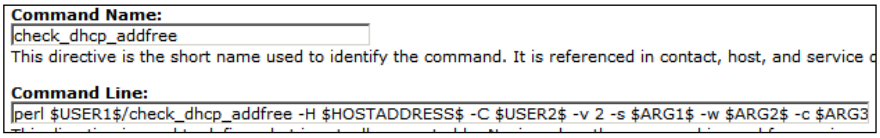
11.2 Modification de la commande Nagios

Nous allons commencer par modifier le nom de la commande Nagios qui permet de superviser le nombre d'adresses IP disponibles. Il semble plus pratique de donner le même nom à la commande que celui du script.

De même, nous allons vérifier le nombre d'arguments de cette commande.
Menu *Administration, Nagios/configuration*
Utiliser le lien "*Nagios Commands*" et sélectionner la commande "*dhcp_free_address*" :



Dans la zone "*Command Name*", changer le nom de la commande pour mettre check_dhcp_addfree :



Bouton "*Modify Command*".

Nous retrouvons les trois arguments :

-s $ARG1$: premier argument, adresse IP réseau de l'étendue à tester.

-w $ARG2$: deuxième argument, seuil à atteindre pour le niveau d'alerte (w=warning).

-c $ARG3$: troisième argument, seuil à atteindre pour le niveau critique (c=critical).

Remarque : le paramètre –v 2 indique la version SNMP à utiliser.

11.3 Ajout du service DHCP-GSB à notre équipement

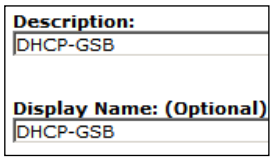
Nous allons maintenant ajouter un service pour superviser les adresses IP disponibles du serveur DHCP REZOLAB, pour l'étendue des visiteurs.

Menu *Administration Nagios/équipements*, utiliser le lien *REZOLAB* et le lien *Services*.

Utiliser le lien "*Create A New Service For This Host*"

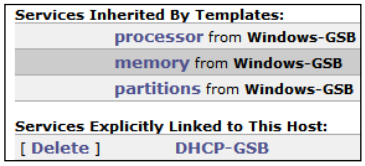
Saisir le nom du nouveau service : DHCP-GSB

Bouton "*Add Service*".



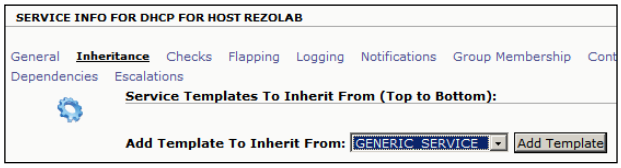
Configurer ce nouveau service pour l'équipement :

Utiliser le lien *DHCP-GSB* :



- Utiliser le lien *Inheritance*, et sélectionner dans la liste déroulante "GENERIC_SERVICE" :

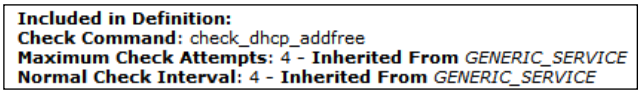
Valider avec le bouton "*Add Template*".



- Utiliser le lien *"Checks et le lien Edit"*

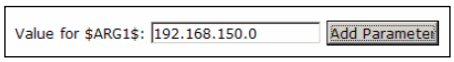
Pour la zone "*Check Command*", cocher la case "*Provide Value*" et sélectionner dans la liste déroulante notre commande Nagios *"check_dhcp_addfree*" :

Bouton "*Update Checks*" :

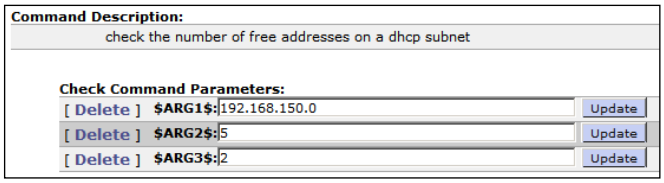


Pour définir les arguments de notre commande, utiliser le lien "*Check Command Parameters*" :

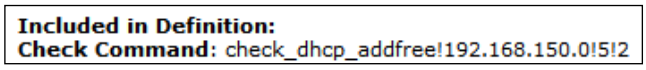
Pour **$ARG1$,** saisir l'adresse IP du réseau de l'étendue supervisée (ici le réseau des visiteurs : 192.168.150.0) et bouton "*Add Parameter*" :



De même, ajouter les arguments $ARG2$ et $ARG3$, pour saisir les seuils d'avertissement (5) et d'alerte (2) :



Vérifier avec le lien *Checks* que les arguments sont maintenant : 192.168.150.0!5!2



11.4 Test dans Nagios

- Transférer vers Nagios

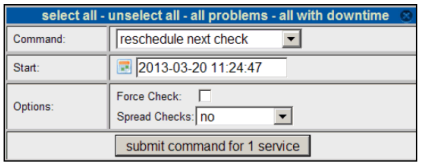
Menus *Tools / Exporter / Restart*, attendre le message *"Export Job ... Successfully"*

- Vue de l'équipement et de ses services dans Nagios

Menu *Disponibilités, Évènements/vue services*

Si l'état du service est *"Status : PENDING"*, utiliser ce lien *PENDING* :

Relancer la commande de supervision de ce service à l'aide du bouton "*submit command for 1 service*" :



Host	Service	Status	Last Check	Duration	Attempt	Status Information
REZOLAB	DHCP-GSB	OK	17:19:56	0d 0h 0m 6s	1/4	OK: Free addresses: 101 : Used addresses: 0

La colonne "*Status information*" nous indique le nombre d'adresses IP libres et le nombre d'adresses utilisées.

12. Ajout d'un service de supervision DNS

Nous allons ajouter un service de supervision du serveur DNS. Par défaut, EoN propose une commande pour superviser si un service Windows est actif. Cette commande se nomme "*win_services*" et utilise le script "*Check_snmp_win.pl*" disponible dans le répertoire plugins.

- Tester le script :

Obtenir de l'aide : *./check_snmp_win.pl –h | more*

Nous retrouvons les arguments déjà utilisés – H et –C. L'argument pour tester un service à partir de son nom est –n.

Nous allons essayer de tester un service nommé : DNS

Lancer le script avec les arguments suivants :

./check_snmp_win.pl –H 172.16.0.10 –C gsbintra –s DNS

Résultat :

```
[root@srveon plugins]# ./check_snmp_win.pl -H 172.16.0.10 -C gsbintra -n DNS
2 services active (matching "DNS") : WARNING
```

Deux services contiennent la chaîne de caractère DNS.

Nous allons donc lancer le script avec un argument supplémentaire qui liste tous les services :

./check_snmp_win.pl –H 172.16.0.10 –C gsbintra –s DNS –v | more

Résultat :
Le nom complet du service est donc "Serveur DNS".

```
Filter : DNS
Desc : Alimentation
Desc : Connaissance des emplacements r.seau
Desc : Emplacement prot.g.
Desc : Plug-and-Play
Desc : Serveur DNS
Name : Serveur DNS, Index : 11.83.101.114.118.101.117.114.32.68.78.83
```

Nous réalisons donc un dernier test avec les arguments suivants :
./check_snmp_win.pl –H 172.16.0.10 –C gsbintra –s "serveur DNS"

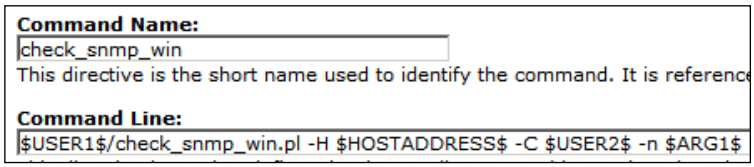
12.1 Modification d'une commande Nagios

Nous allons commencer par modifier le nom de la commande Nagios qui permet de superviser un service Windows. Il semble plus pratique de donner le même nom à la commande que celui du script. De même, nous allons vérifier le nombre d'arguments de cette commande.

Menu *Administration, Nagios/configuration*
Utiliser le lien "*Nagios Commands*" et sélectionner la commande "*win_services*" :

Dans la zone "*Command Name*", changer le nom de la commande pour mettre check_snmp_win :

Bouton "*Modify Command*".



Nous retrouvons un seul argument : -n $ARG1$ (nom du service à tester).

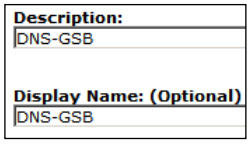
12.2 Ajout du service DNS-GSB à notre équipement

Nous allons maintenant ajouter un service pour superviser le serveur DNS de REZOLAB.

Menu *Administration Nagios/équipements*, utiliser le lien *REZOLAB* et le lien *Services*.
Utiliser le lien "*Create A New Service For This Host*"

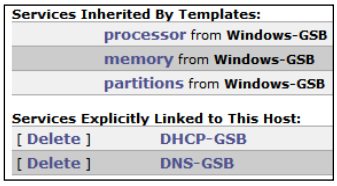
Saisir le nom du nouveau service : DNS-GSB

Bouton "*Add Service*".



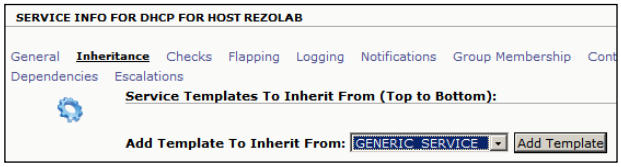
Configurer ce nouveau service pour l'équipement

Utiliser le lien *DNS-GSB* :



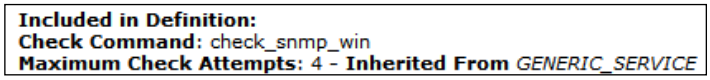
Utiliser le lien *Inheritance*, et sélectionner dans la liste déroulante "GENERIC_SERVICE" :

Valider avec le bouton "*Add Template*".



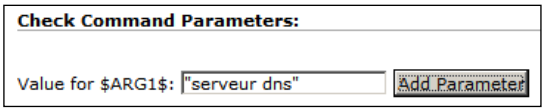
Utiliser le lien *Checks* et le lien *Edit*
Pour la zone "*Check Command*", cocher la case "*Provide Value*" et sélectionner dans la liste déroulante notre commande "*check_snmp_win*" :

Bouton "*Update Checks*" :

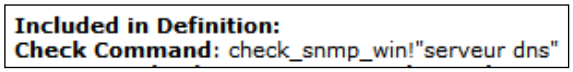


Pour définir l'argument de notre commande, utiliser le lien "*Check Command Parameters*" :

Pour $ARG1$, saisir le nom du service Windows "serveur DNS" et bouton "*Add Parameter*" :



Vérifier l'argument avec le lien *Checks* :



12.3 Test dans Nagios

- Transférer vers Nagios
Menus *Tools / Exporter / Restart*, attendre le message *"Export Job ... Successfully"*

- Vue de l'équipement et de ses services dans Nagios
Menu *Disponibilités, Évènements/vue services*

Si l'état du service est "*Status : PENDING*", utiliser ce lien *PENDING*.

Relancer la commande de supervision de ce service à l'aide du bouton "*submit command for 1 service*" :

Host	Service	Status	Last Check	Duration	Attempt	Status Information
REZOLAB	DHCP-GSB	OK	17:19:56	0d 0h 0m 6s	1/4	OK: Free addresses: 101 : Used addresses: 0
	DNS-GSB	OK	17:19:48	0d 0h 0m 14s	1/4	1 services active (matching "serveur dns") : OK
	memory	OK	17:18:33	0d 0h 41m 45s	1/4	Virtual Memory: 25%used(2029MB/8061MB) Phys used(1897MB/4032MB) (<80%) : OK
	partitions	CRITICAL	17:16:38	2d 6h 28m 5s	4/4 #1	C:\ Label: Serial Number 3f4793: 95%used(14296M (>95%) : CRITICAL
	processor	OK	17:17:29	2d 6h 26m 39s	1/4	1 CPU, load 8.0% < 80% : OK

La colonne "*Status information*" de DNS-GSB nous indique que le service est actif.

12.4 Tests d'alerte des services DHCP et DNS
Sur le serveur REZOLAB, définir une étendue de trois adresses et arrêter le service DNS.

Relancer la commande de supervision de ces services à l'aide du bouton "*submit command for 1 service*" :

Host	Service	Status	Last Check	Duration	Attempt	Status Information
REZOLAB	DHCP-GSB	WARNING	17:23:05	0d 0h 0m 17s	1/4	WARNING: Not enough addresses free: 3 (< 5)
	DNS-GSB	CRITICAL	17:23:18	0d 0h 0m 4s	1/4	No services matching "serveur dns" found : CRITICAL

Le service DHCP-GSB est WARNING et le service DNS-GSB est CRITICAL. La colonne "*Status information*" de DHCP-GSB nous indique qu'il n'y a que trois adresses de libres (3<5).

Remarque : pour vérifier en ligne de commandes la présence des notifications correspondantes sur le serveur EoN, taper la commande : *mail* (pour quitter : taper q)

13. Ajout du commutateur-routeur MUTLAB
Ne pas oublier de configurer la communauté sur ce commutateur (voir **2.2**).

Par défaut, EoN propose deux commandes pour superviser le CPU et la mémoire des matériels Cisco mais ces commandes utilisent des scripts "*check_snmp_cisco_loadavg*" et "*check_snmp_cisco_memutil*" qui ne sont pas dans le répertoire plugins.

Nous pouvons télécharger ces scripts dans une archive (nagios-plugin-cisco-snmp.tar.gz) à l'adresse suivante :
https://www.monitoringexchange.org/inventory/Check-Plugins/Network/Cisco/Cisco-SNMP-device-monitoring

13.1 Ajout des scripts dans le répertoire plugins
Avec FileZilla (voir **11.1**), transférer les scripts "*check_snmp_cisco_memutil*" et "*check_snmp_cisco_loadavg*" de l'archive dans le répertoire : /srv/eyesofnetwork/nagios/plugins

Il reste à rendre ces scripts exécutables par Nagios (qui utilise le compte nagios) :
Changer de propriétaire : *chown nagios Nomduscript*
Définir les droits : *chmod 775 NomDuScript*

- Tester les scripts :
Pour obtenir de l'aide : *./check_snmp_cisco_loadavg –h | more*
./check_snmp_cisco_memutil –h | more

Nous retrouvons les arguments déjà vus : -H, -C, -w et –c

13.2 Modification des commandes Nagios pour le matériel Cisco

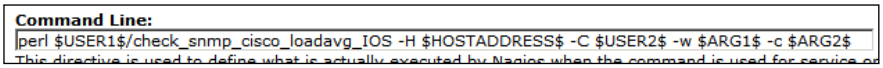
Nous allons commencer par adapter les commandes Cisco correspondantes de Nagios.
De même, nous allons vérifier le nombre d'arguments de ces commandes.

- Commande pour le CPU
Menu *Administration, Nagios/configuration*

Utiliser le lien "*Nagios Commands*" et sélectionner la commande "*cisco_cpu_ios*" :

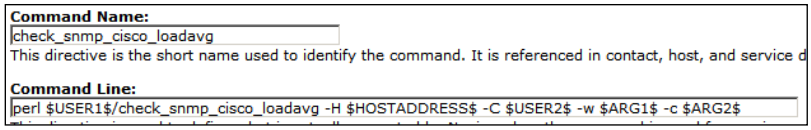
Dans la zone "*Command Name*", changer le nom de la commande pour mettre : check_snmp_cisco_loadavg

Dans la zone "*Command Line*", modifier le nom du script en enlevant à la fin les caractères "_IOS":



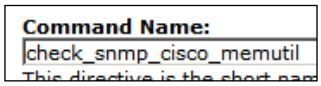
Nous obtenons :

Bouton "*Modify Command*".



- Commande pour la mémoire
Menu *Administration, Nagios/configuration*
Utiliser le lien "*Nagios Commands*" et sélectionner la commande "*cisco_memory*" :

Dans la zone "*Command Name*", changer le nom de la commande pour mettre check_snmp_cisco_memutil :



Bouton "*Modify Command*".

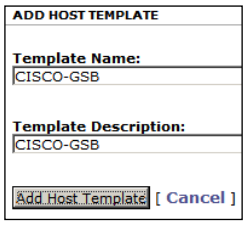
Pour les deux commandes, nous retrouvons bien les deux arguments :
-w $ARG2$: deuxième argument, seuil à atteindre pour le niveau d'alerte (w=warning).
-c $ARG3$: troisième argument, seuil à atteindre pour le niveau critique (c=critical).

13.3 Ajout d'un modèle d'hôte pour Cisco

Nous allons créer un nouveau modèle pour superviser les matériels Cisco de GSB.

Menu *Administration, Nagios/modèles*, lien "*Add A New Host Template*" :

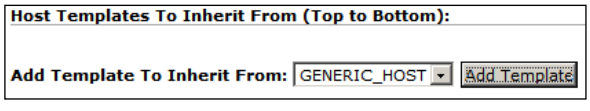
Définir le nom du nouveau modèle : CISCO-GSB
Et une description : CISCO-GSB



Bouton "*Add Host Template*".

Utiliser le lien *Inheritance* et sélectionner dans la liste déroulante : GENERIC_HOST

Valider avec le bouton "*Add Template*".



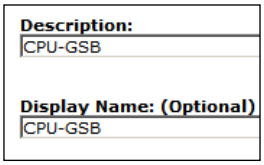
13.3.1 Ajout du groupe du type d'équipements à ce modèle

Utiliser le lien "*Group Memberships*".
Dans la liste déroulante "*Add New Host Group Membership'*, sélectionner CISCO et bouton "*Add Group*" :

13.3.2 Ajout du service CPU à ce modèle

Utiliser le lien *Services* et le lien "*Create A New Service For This Template*".

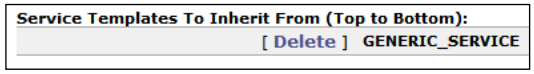
Saisir le nom du nouveau service : CPU-GSB
Bouton "*Add Service*".



Configurer ce nouveau service pour ce modèle :
Utiliser le lien *CPU-GSB* et le lien *Inheritance* .

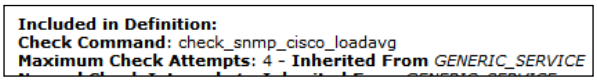
Sélectionner dans la liste déroulante "GENERIC_SERVICE" :

Valider avec le bouton "*Add Template*".



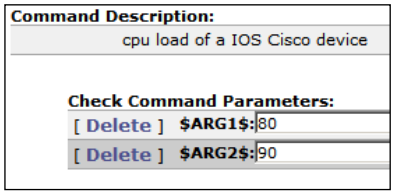
- Utiliser le lien *Checks* et le lien *Edit*
Pour la zone "*Check Command*", cocher la case "*Provide Value*" et sélectionner dans la liste déroulante notre commande check_snmp_cisco_loadavg :

Bouton "*Update Checks*" :

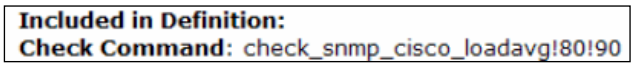


Pour définir les arguments de ce service, utiliser le lien "*Check Command Parameters*" :

Ajouter les arguments $ARG1$ et $ARG2$, pour saisir les seuils d'avertissement (80) et d'alerte (90) :



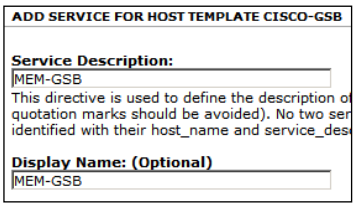
Vérifier les arguments avec le lien *Checks* :

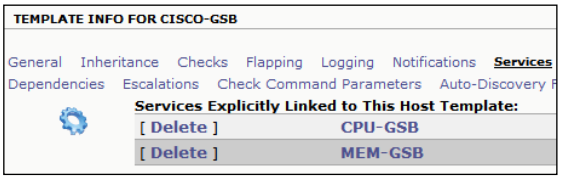


13.3.3 Ajout du service MEM à ce modèle

Utiliser le lien *Services* et le lien "*Create A New Service For This Template*".

Saisir le nom du nouveau service : MEM-GSB
Bouton "*Add Service*".

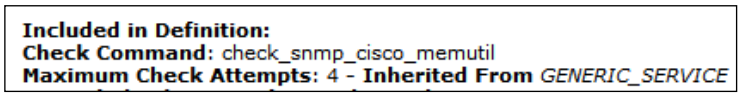




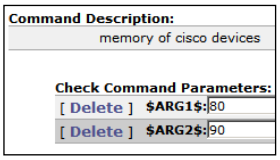
Configurer ce nouveau service pour ce modèle :
Utiliser le lien *MEM-GSB* et le lien *Inheritance* , sélectionner dans la liste "GENERIC_SERVICE".
Valider avec le bouton "*Add Template*".

Utiliser le lien *Checks* et le lien *Edit*
Pour la zone "*Check Command*", cocher la case "*Provide Value*" et sélectionner dans la liste déroulante notre commande check_snmp_cisco_memutil" :

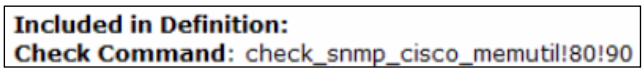
Bouton "*Update Checks*" :



Pour définir les arguments de ce service, utiliser le lien "*Check Command Parameters*" :
Ajouter les arguments $ARG1$ et $ARG2$, pour saisir les seuils d'avertissement (80) et d'alerte (90) :



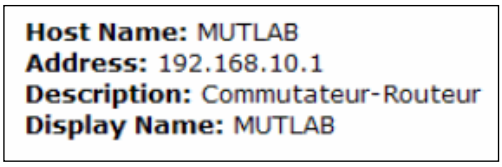
Vérifier les arguments avec le lien *Checks* :



13.4 Ajout de l'équipement MUTLAB (Commutateur-routeur)

Menu *Administration, Nagios/équipements*
- Utiliser le lien "*Add A New Child Host*" et renseigner les informations :

Host Name	: MUTLAB
Host Description	: Commutateur-Routeur
Address	: 192.168.10.1
Display Name	: MUTLAB

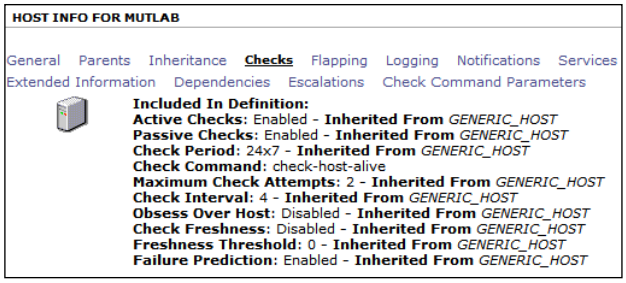


Valider avec le bouton "*Add Host*".

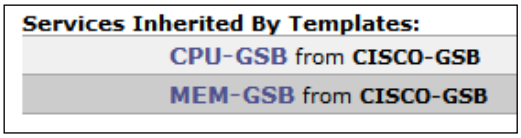
- Utiliser le lien *Inheritance* , et sélectionner dans la liste déroulante "CISCO-GSB" :

Valider avec le bouton "*Add Template*".

- Utiliser le lien *Checks* pour vérifier que la zone "*Check Command*" contient bien la commande "check-host-alive" (PING) :



- Utiliser le lien *Services* pour vérifier que les services hérités du modèle CISCO-GSB sont présents :



13.5 Test dans Nagios

- Transférer vers Nagios
Menus *Tools / Exporter / Restart*, attendre le message *"Export Job ... Successfully"*

- Vue de l'équipement et de ses services dans Nagios
Menu *Disponibilités, Évènements/vue services*

Si l'état est "*Status : PENDING*", utiliser ce lien *PENDING* et le bouton "*submit command for 1 service*" :

Host	Service	Status	Last Check	Duration	Attempt	Status Information
MUTLAB	CPU-GSB	OK	20:55:06	0d 0h 0m 23s	1/4	Status is OK - CPU load average (5 min): 7 %
	MEM-GSB	OK	20:55:01	0d 0h 0m 10s	1/4	Status is OK - MEMORY: total: 79.04 MB, used: 19.94 MB (25%), free: 59.10 MB

14. Ajout de services de supervision de ports pour MUTLAB

Par défaut, EoN propose une commande pour superviser une interface ou un port. Cette commande se nomme "*check_snmp_interface*" et utilise un script nommé "*check_snmp_int.pl*".

Tester le script :
Pour obtenir de l'aide : *./check_snmp_int.pl –h | more*

Nous retrouvons les arguments déjà utilisés – H et –C, mais aussi beaucoup d'autres comme :

-n : nom de l'interface testée
-r : obligation de spécifier exactement le nom de l'interface recherchée
-k : supervise le débit entrée et sortie
-w : seuils d'avertissements en entrée et en sortie, de la forme nn,nn
-c : seuils d'alertes critiques en entrée et en sortie, de la forme nn,nn
-u : Spécifie des niveaux de seuils en pourcentage

Pour connaître le nom et l'état de tous les ports FastEthernet, lancer le script avec les arguments suivants :

./check_snmp_int.pl –H 192.168.10.1 –C gsbintra –n Fast

Le nom complet FastEthernet0/2 est affiché dans le résultat.

Pour connaître les seuils du port FastEthernet0/2, lancer le script avec les arguments suivants :

./check_snmp_int.pl –H 192.168.10.1 –C gsbintra –r –n FastEthernet0/2 –w 90,90 –c 95,95 -u

Ici, le port n'est pas actif :

```
[root@srveon plugins]# ./check_snmp_int.pl -H 192.168.10.1 -C gsbintra -r -n Fas
tEthernet0/2 -k -w 90,90 -c 95,95 -u
FastEthernet0/2:DOWN: 1 int NOK : CRITICAL
```

Pour connaître les seuils du port FastEthernet0/5, lancer le script avec les arguments suivants :

./check_snmp_int.pl –H 192.168.10.1 –C gsbintra –r –n FastEthernet0/5 –w 90,90 –c 95,95 -u

```
[root@srveon plugins]# ./check_snmp_int.pl -H 192.168.10.1 -C gsbintra -r -n Fas
tEthernet0/5 -k -w 90,90 -c 95,95 -u
FastEthernet0/5:UP No usable data on file (1 rows) :(1 UP): UNKNOWN
```

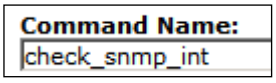
Le port est UP, mais les données sur les débits ne sont pas accessibles.
(À voir : en attendant un peu, ça fini par marcher, pas de trafic ou autre ?)

14.1 Modification de la commande Nagios de supervision d'une interface (port)

Nous allons commencer par adapter la commande correspondante de Nagios.
De même, nous allons vérifier le nombre d'arguments de cette commande.

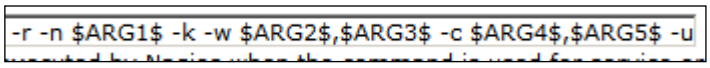
Menu *Administration, Nagios/configuration*
Utiliser le lien "*Nagios Commands*" et sélectionner la commande "*check_snmp_interface*" :

Dans la zone "*Command Name*", changer le nom de la commande pour mettre check_snmp_int :



Dans la zone "Command Line", à la fin de la commande, ajouter le paramètre –u :

Bouton "*Modify Command*".



Nous retrouvons les cinq arguments :

-s $ARG1$: nom de l'interface supervisée.
-w $ARG2$,$ARG3$: seuils (entrée/sortie) à atteindre pour le niveau d'avertissement.
-c $ARG4$,$ARG5$: seuils (entrée/sortie) à atteindre pour le niveau d'alerte.

14.2 Ajout de services de supervision des ports de MUTLAB

Menu *Administration Nagios/équipements*, utiliser le lien MUTLAB et le lien *Services*,

Utiliser le lien "*Create A New Service For This Host*"
Saisir le nom et la description du service : MUTLAB-F02
Bouton "*Add Service*" :

Description: MUTLAB-F02
Display Name: MUTLAB-F02

- Configurer ce nouveau service pour l'équipement :
Utiliser le lien *MUTLAB-F02* et le lien *Inheritance*.
Sélectionner dans la liste déroulante "GENERIC_SERVICE" et valider avec le bouton "*Add Template*".
Utiliser le lien *Checks* et le lien *Edit*.
Pour la zone "*Check Command*", cocher la case "*Provide Value*" et sélectionner dans la liste déroulante notre commande Nagios "*check_snmp_int*" :

Check Command: check_snmp_int **Provide Value**

Bouton "*Update Checks*" :

Included in Definition:
Check Command: check_snmp_int
Maximum Check Attempts: 4 - **Inherited From** *GENERIC_SERVICE*

Pour définir les arguments de notre commande, utiliser le lien "*Check Command Parameters*" :

Ajouter les différents arguments, bouton "*Add Parameter*" avec les valeurs suivantes :

Check Command Parameters:

[Delete]	**$ARG1$:**	FastEthernet0/2
[Delete]	**$ARG2$:**	90
[Delete]	**$ARG3$:**	90
[Delete]	**$ARG4$:**	95
[Delete]	**$ARG5$:**	95

Vérifier avec le lien *Checks* :

Included in Definition:
Check Command: check_snmp_int!FastEthernet0/2!90,90!95,95

Recommencer la procédure pour les services des ports FastEthernet0/5 et FastEthernet07 :

Services Inherited By Templates:
CPU-GSB from **CISCO-GSB**
MEM-GSB from **CISCO-GSB**

Services Explicitly Linked to This Host:
[Delete] MUTLAB-F02
[Delete] MUTLAB-F05
[Delete] MUTLAB-F07

Lien *Checks* pour MUTLAB-F05 :

Included in Definition:
Check Command: check_snmp_int!FastEthernet0/5!90,90!95,95

Lien *Checks* pour MUTLAB-F07 :

Included in Definition:
Check Command: check_snmp_int!FastEthernet0/7!90,90!95,95

14.3 Test dans Nagios

- Transférer vers Nagios
Menus *Tools / Exporter / Restart*, attendre le message *"Export Job ... Successfully"*

- Vue de l'équipement et de ses services dans Nagios
Menu *Disponibilités, Évènements/vue services*

Si l'état est "*Status : PENDING*", utiliser ce lien *PENDING* et le bouton "*submit command for 1 service*" (pour le test, les ports FastEthernet0/2 et FastEthernet0/7 ne sont pas connectés) :

Host	Service	Status	Last Check	Duration	Attempt	Status Information
MUTLAB	CPU-GSB	OK	23:41:19	0d 0h 54m 58s	1/4	Status is OK - CPU load average (5 min): 7 %
	MEM-GSB	OK	23:38:12	0d 0h 54m 3s	1/4	Status is OK - MEMORY: total: 79.04 MB, used: 19.87 MB (25%), free: 59.17 MB
	MUTLAB-F02	CRITICAL	23:40:48	0d 0h 9m 10s	4/4 #1	FastEthernet0/2:DOWN: 1 int NOK : CRITICAL
	MUTLAB-F05	OK	23:41:51	0d 0h 1m 17s	1/4	FastEthernet0/5:UP (0.0%/0.0%):1 UP: OK
	MUTLAB-F07	CRITICAL	23:40:52	0d 0h 8m 39s	4/4 #1	FastEthernet0/7:DOWN: 1 int NOK : CRITICAL

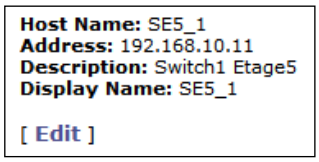
15. Ajout des commutateurs SE5_1 et MUTSYS

15.1 Ajout de l'équipement SE5_1

Menu *Administration, Nagios/équipements*

- Utiliser le lien "*Add A New Child Host*" et renseigner les informations :

Host Name	: SE5_1
Host Description	: Switch1 Etage5
Address	: 192.168.10.11
Display Name	: SE5_1



Valider avec le bouton "*Add Host*" :

- Utiliser le lien *Inheritance*, et sélectionner dans la liste déroulante "CISCO-GSB" :

Valider avec le bouton "*Add Template*" :

15.2 Test dans Nagios

- Transférer vers Nagios

Menus *Tools / Exporter / Restart*, attendre le message *"Export Job ... Successfully"*

- Vue de l'équipement et de ses services dans Nagios

Menu *Disponibilités, Évènements/vue services*

Si l'état est "*Status : PENDING*", utiliser ce lien *PENDING* et le bouton "*submit command for 1 service*" :

Host	Service	Status	Last Check	Duration	Attempt	Status Information
SE5_1	CPU-GSB	OK	23:00:31	0d 0h 0m 10s	1/4	Status is OK - CPU load average (5 min): 5 %
	MEM-GSB	OK	22:59:59	0d 0h 0m 42s	1/4	Status is OK - MEMORY: total: 30.09 MB, used: 9.68 MB (32%), free: 20.41 MB

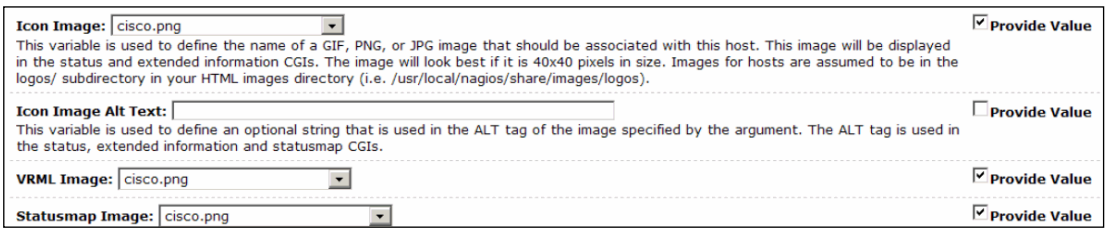
Remarque : Le point d'interrogation à coté du nom SE5_1 indique que l'icône associé à ce type d'équipement n'est pas défini dans le modèle CISCO-GSB.

15.3 Modification du modèle d'hôte CISCO-GSB

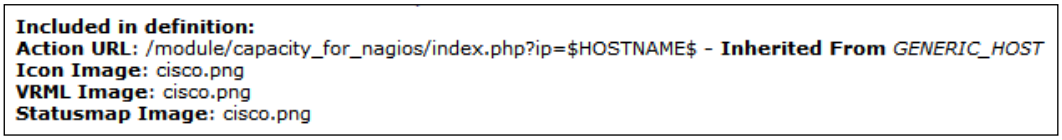
Nous allons ajouter l'icône correspondant à ce type de matériel.

Menu *Administration, Nagios/modèles* et sélectionner le modèle CISCO-GSB,
Utiliser le lien "*Extended Information*" :
Utiliser le lien *Edit*.

Pour les zones concernées par une image, cocher la case "*Provide Value*" et sélectionner dans la liste déroulante l'icône de l'équipement cisco.png :



Bouton "*Update Extended Information*" :

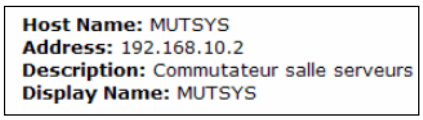


15.4 Ajout de l'équipement MUTSYS

Menu *Administration, Nagios/équipements*

- Utiliser le lien "*Add A New Child Host*" et renseigner les informations :

Host Name	: MUTSYS
Host Description	: Commutateur salle serveurs
Address	: 192.168.10.2
Display Name	: MUTSYS



Valider avec le bouton "*Add Host*" :

- Utiliser le lien *Inheritance*, sélectionner dans la liste déroulante "CISCO-GSB" et valider avec le bouton "*Add Template*".

15.5 Test dans Nagios

- Transférer vers Nagios

Menus *Tools / Exporter / Restart*, attendre le message *"Export Job ... Successfully"*

- Vue de l'équipement dans Nagios

Menu *Disponibilités, Évènements/vue équipements* :

Tous les équipements de modèle CISCO-GSB ont le même icône et les mêmes services CPU-GSB et MEM-GSB :

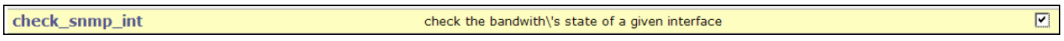
16. Ajout du routeur RTROUT

Cet ajout est identique à celui du commutateur SE5_1. Nous allons juste personnaliser la commande *check_snmp_int* pour ne pas avoir à saisir les seuils de chaque interface. Par contre, ces seuils seront toujours les mêmes pour tous les services qui utilisent cette commande.

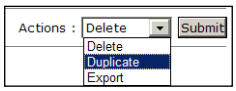
16.1 Ajout d'une commande Nagios à partir d'une copie de commande

Menu *Administration, Nagios/configuration* et utiliser le lien "*Nagios Commands*"

Cocher la case à droite de la commande *check_snmp_int* :



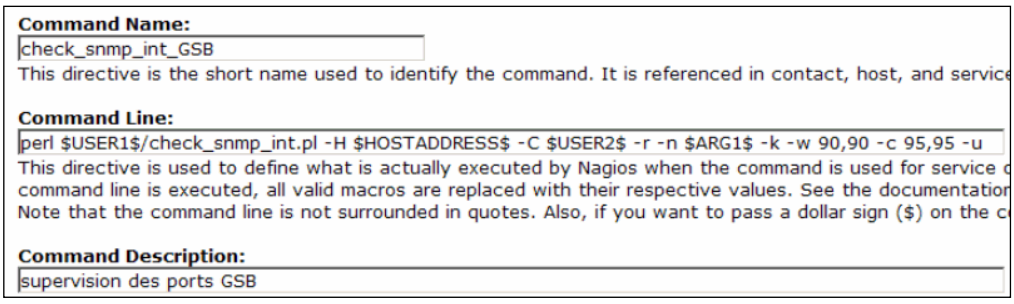
En haut, dans la liste *Actions*, sélectionner *Duplicate* et bouton *Submit* :
A l'avertissement, répondre OK.



Une copie de la commande est créée avec un nom de la forme check_snmp_int-nnnn :
Utiliser le lien *check_snmp_int-nnnn* :

Modifier les informations de la commande :

"Command Name"	: remplacer par check_snmp_int_GSB.
"Command Line"	: remplacer les arguments 2 et 3 par les valeurs 90,90 et les arguments 4 et 5 par 95,95.
"Command Description"	: supervision des ports GSB.



Bouton "*Modify Command*".

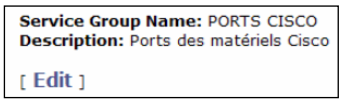
16.2 Ajout d'un groupe de service

Comme de nombreux services concernent des ports de matériel Cisco, il est intéressant de rassembler tous ces services dans un groupe.

Menu *Administration, Nagios/configuration*
Utiliser le lien "*Service Groups*" :

Utiliser le lien "*Add A New Service Group*" et renseigner les informations :

Service Group Name : PORTS CISCO
Description : Ports des matériels Cisco



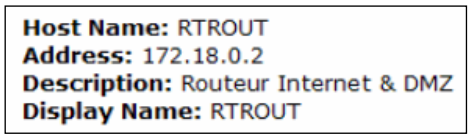
Bouton "Add Service Group" :

16.3 Ajout de l'équipement RTROUT

Menu *Administration, Nagios/équipements*

- Utiliser le lien "*Add A New Child Host*" et renseigner les informations :

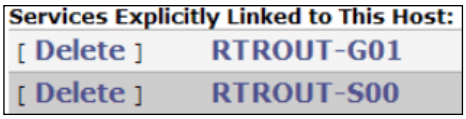
Host Name : RTROUT
Host Description : Routeur Internet & DMZ
Address : 172.18.0.2
Display Name : RTROUT



Valider avec le bouton "*Add Host*" :

- Utiliser le lien *Inheritance*, et sélectionner dans la liste déroulante "CISCO-GSB" et bouton "*Add Template*".

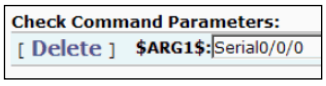
- Utiliser le lien *Services* et ajouter deux services (voir **14.2**) pour superviser les ports GigabitEthernet0/1 et Serial0/0/0, nommés RTROUT-G01 et RTROUT-S00 :



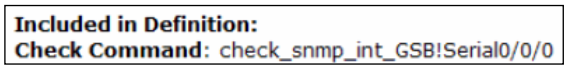
Pour ces deux services, spécifier la nouvelle commande à utiliser *check_snmp_int_GSB*.
Lien *Checks* :

Pour ces deux services, spécifier le seul argument de cette commande, qui correspond au nom de l'interface.

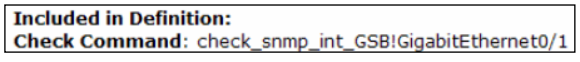
Utiliser le lien "*Check Command Parameters*" :



Nous devons obtenir pour RTROUT-S00 :



Et pour RTROUT-G01 :



Pour ces deux services, spécifier le groupe d'affectation du service.
Utiliser le lien du service et le lien "*Group MemberShip*"

Dans la liste déroulante, sélectionner PORTS CISCO :
Bouton "*Add Service* Group".

De la même manière, nous allons affecter les trois services MUTLAB-F02, MUTLAB-F05, MUTLAB-F07 de l'équipement MUTLAB au groupe de services PORTS CISCO.

16.4 Test dans Nagios

- Transférer vers Nagios
Menus *Tools / Exporter / Restart*, attendre le message *"Export Job ... Successfully"*

- Vue de l'équipement et de ses services dans Nagios
Menu *Disponibilités, Évènements/vue services*

- Vue des services du groupe PORTS CISCO dans Nagios
Menu *Disponibilités, Évènements/groupes de services*

Service Group	Host Status Summary	Service Status Summary
Ports des matériels Cisco (PORTS CISCO)	2 UP	4 OK 1 CRITICAL : 1 Unhandled

17. Ajout de l'imprimante ImpVisiteursE5

Dans les exemples présentés, le nom de la communauté défini sur l'imprimante est : **gsbintra**.
Si ce nom de communauté ne peut pas être modifié, utiliser le nom de la communauté par défaut défini sur l'imprimante : **public**.
Pour les éléments de l'imprimante, il nous faut une commande de supervision. Nous pouvons télécharger un script nommé *check_snmp_printer* à l'adresse suivante :
http://exchange.nagios.org/directory/plug-ins/Hardware/Printers/SNMP-Printer-Check/details

17.1 Ajout de l'équipement ImpVisiteursE5

Menu *Administration, Nagios/équipements*
- Utiliser le lien "*Add A New Child Host*" et renseigner les informations :

Host Name : ImpVisiteursE5
Host Description : Imprimante des visiteurs de l'étage 5
Address : 192.168.150.200
Display Name : ImpVisiteursE5

Host Name: ImpVisiteursE5
Address: 192.168.150.200
Description: Imprimante des visiteurs de l'étage 5
Display Name: ImpVisiteursE5

Valider avec le bouton "*Add Host*" :

- Utiliser le lien *Inheritance*, sélectionner dans la liste déroulante "PRINTER" et bouton "*Add Template*".

17.2 Test dans Nagios

- Transférer vers Nagios
Menus *Tools / Exporter / Restart*, attendre le message *"Export Job ... Successfully"*

- Vue de l'équipement et de ses services dans Nagios
Menu *Disponibilités, Évènements/vue services*

Si l'état est "*Status : PENDING*", utiliser ce lien *PENDING* et le bouton "*submit command for 1 host*" :

Host	Status	Last Check	Duration	Status Information
ImpVisiteursE5	UP	15:57:12	0d 0h 0m 18s+	PING OK - Packet loss = 0%, RTA = 0.68 ms

17.3 Ajout du script dans le répertoire plugins

Avec FileZilla (voir **11.1**), transférer le script *check_snmp_printer* dans : /srv/eyesofnetwork/nagios/plugins

Rendre ce script exécutable par Nagios (qui utilise le compte nagios) :
Changer de propriétaire : *chown nagios check_snmp_printer*
Définir les droits : *chmod 775 check_snmp_printer*

- Tester le script
Obtenir de l'aide : *./check_snmp_printer –h | more*

L'argument nouveau pour ce script est –x, il permet de spécifier l'élément de l'imprimante interrogé en utilisant différentes options.

Exemples : -x "CONSUM" : niveau de la cartouche d'encre (ou toner)
-x "PAGECOUNT" : compteur des pages imprimées (cumulé)
-x "TRAY" : niveau des bacs d'alimentation papier

Remarque : dans les commandes suivantes, remplacer "gsbintra" par "public" si la communauté n'a pas été changée sur l'imprimante.

Lancer le script avec les arguments suivants :
./check_snmp_printer –H 192.168.150.200 –C gsbintra –x "MODEL"

Nous obtenons le nom du modèle, pour l'exemple, c'est une EPSON EPL-N2050.

Lancer le script avec les arguments suivants :
./check_snmp_printer –H 192.168.150.200 –C gsbintra –x "CONSUM TEST"

Nous obtenons le nom des consommables de l'imprimante :

```
Consumables you may monitor:
"Toner Cartridge S051070"
```

Lancer le script avec les arguments suivants :
./check_snmp_printer –H 192.168.150.200 –C gsbintra –x "CONSUM Toner" –w 20 -c 5

Nous obtenons :

```
Toner Cartridge S051070 is at CRITICAL level! | Toner Cartridge S051070=0;20;5;
```

Remarque : nous ne sommes pas obligé de spécifier le nom complet du consommable, sauf si l'imprimante possède plusieurs consommables commençant par "Toner".

Lancer le script avec les arguments suivants :
./check_snmp_printer –H 192.168.150.200 –C gsbintra –x "PAGECOUNT"

Nous obtenons le nombre de pages :

```
Pagecount is 104,601|Pages=104,601;
```

Lancer le script avec les arguments suivants :
./check_snmp_printer –H 192.168.150.200 –C gsbintra –x "TRAY ALL"

```
Tray 1 status is UNKNOWN! Tray 2 is at CRITICAL level - please refill with more
8.2 x 11.6 paper. Tray 3 is at 7% - OK! | Tray 3=7;20;5;
```

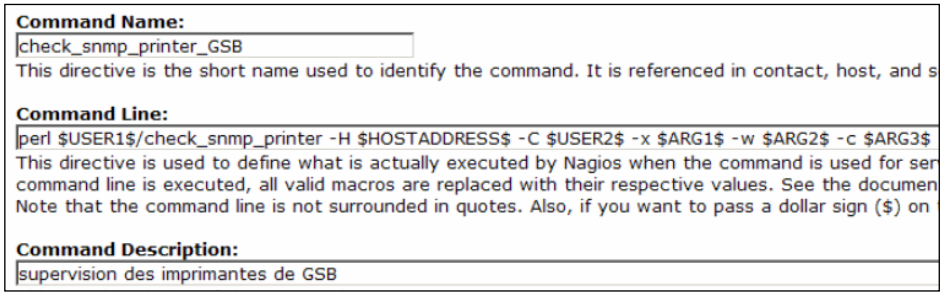
Seul le bac 3 (Tray 3) est utilisé.

Relancer le script avec les arguments suivants pour ne superviser que le bac 3 :
./check_snmp_printer –H 192.168.150.200 –C gsbintra –x "TRAY 3" –w 20 –c 5

17.4 Ajout de la commande Nagios de supervision d'une imprimante

Menu *Administration, Nagios/configuration* et utiliser le lien "*Nagios Commands*"
Utiliser le lien : "*Add A New Command*"

Saisir les informations de la commande :
"Command Name" : check_snmp_printer_GSB
"Command Description" : supervision des imprimantes de GSB
"Command Line" : perl $USER1$/check_snmp_printer –H $HOSTADDRESS$ –C $USER2$ –x $ARG1$ –w $ARG2$ –c $ARG3$



Bouton "*Create Command*".

Remarque: la communauté **gsbintra** est utilisée avec $USER2$, si le nom de la communauté de l'imprimante est public, il est possible de remplacer cette variable par le mot public ou ajouter une variable $USER3$ qui contient la valeur « public ».

17.5 Ajout des services de supervision de l'imprimante

Nous allons créer trois services de supervision pour cette imprimante :

- toner-GSB : pour la supervision de la cartouche d'encre,
- pages-GSB : pour afficher le nombre de pages imprimées (supervision sans alerte),
- bacs-GSB : pour la supervision du bac d'alimentation des feuilles.

17.5.1 Service toner-GSB

Menu *Administration Nagios/équipements*, utiliser le lien *ImpVisiteursE5*, et le lien *Services*.

- Utiliser le lien "*Create A New Service For This Template*"
Saisir le nom du nouveau service : toner-GSB et bouton "*Add Service*".

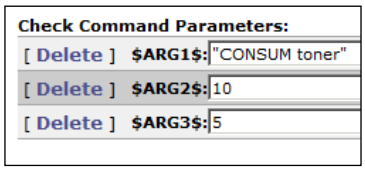
- Utiliser le lien *toner-GSB* et le lien *Inheritance*, sélectionner dans la liste "GENERIC_SERVICE".
Valider avec le bouton "*Add Template*".

- Utiliser le lien *Checks* et le lien *Edit*
Pour la zone "*Check Command*", cocher la case "*Provide Value*" et sélectionner dans la liste déroulante notre commande *check_snmp_printer_GSB* :

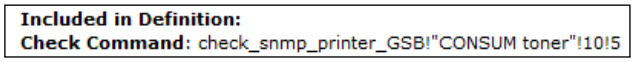
Bouton "*Update Checks*".

- Pour définir les arguments de ce service, utiliser le lien "*Check Command Parameters*" :

Ajouter les différents arguments, bouton "*Add Parameter*" avec les valeurs suivantes :

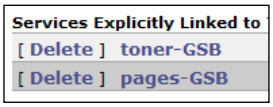


Vérifier les arguments avec le lien *Checks* :



17.5.2 Service pages-GSB

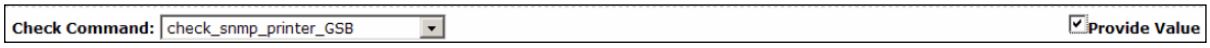
- Utiliser le lien "*Create A New Service For This Template*"
Saisir le nom du nouveau service : pages-GSB et bouton "*Add Service*".



- Utiliser le lien *pages-GSB* et le lien *Inheritance*, sélectionner dans la liste "GENERIC_SERVICE".
Valider avec le bouton "*Add Template*".

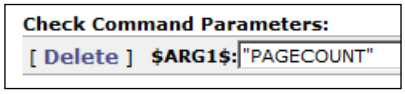
- Utiliser le lien *Checks* et le lien *Edit*

Pour la zone "*Check Command*", cocher la case "*Provide Value*" et sélectionner dans la liste déroulante notre commande *check_snmp_printer_GSB* :

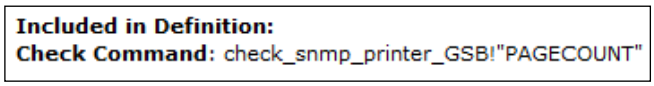


Bouton "*Update Checks*".

- Pour définir les arguments de ce service, utiliser le lien "*Check Command Parameters*" :
Ajouter un argument, bouton "*Add Parameter*" avec la valeur suivante (un seul argument suffit avec PAGECOUNT) :

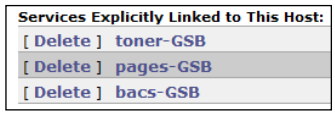


Vérifier les arguments avec le lien *Checks* :



17.5.3 Service bacs-GSB

- Utiliser le lien "*Create A New Service For This Template*"
Saisir le nom du nouveau service : bacs-GSB et bouton "*Add Service*".



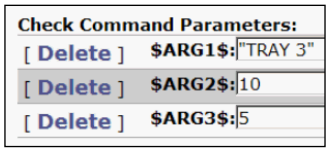
- Utiliser le lien *bacs-GSB* et le lien *Inheritance*, sélectionner dans la liste "GENERIC_SERVICE".
Valider avec le bouton "*Add Template*".

- Utiliser le lien *Checks* et le lien *Edit*
Pour la zone "*Check Command*", cocher la case "*Provide Value*" et sélectionner dans la liste déroulante notre commande check_snmp_printer_GSB" :

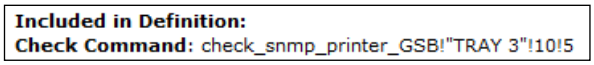
Bouton "*Update Checks*".

- Pour définir les arguments de ce service, utiliser le lien "*Check Command Parameters*" :

Ajouter les différents arguments, bouton "*Add Parameter*" avec les valeurs suivantes :



Vérifier les arguments avec le lien *Checks* :



17.6 Test dans Nagios

- Transférer vers Nagios
Menus *Tools / Exporter / Restart*, attendre le message *"Export Job ... Successfully"*

- Vue de l'équipement et de ses services dans Nagios
Menu *Disponibilités, Évènements/vue services*

Si l'état est "*Status : PENDING*", utiliser ce lien *PENDING* et le bouton "*submit command for 1 service*" :

Host	Service	Status	Last Check	Duration	Attempt	Status Information
ImpVisiteursE5	bacs-GSB	OK	17:01:23	0d 0h 0m 3s	1/4	Tray 3 is at 7% - OK!
	pages-GSB	OK	16:58:41	0d 0h 14m 19s	1/4	Pagecount is 104,601
	toner-GSB	CRITICAL	16:59:29	0d 0h 11m 31s	4/4 #3	Toner Cartridge S051070 is at CRITICAL level!

Remarque : pour le service bacs-GSB, le niveau d'avertissement est à 10, mais l'état n'est pas WARNING. Il y a un problème avec le plugin, mais si nous passons le niveau d'alerte critique à 10, nous avons bien un état CRITICAL.

18. Ajout du point d'accès sans fil APVisiteurE5

Comme pour tous les autres équipements, définir le nom de la communauté **gsbintra** sur le point d'accès.

Malheureusement, pour la réalisation de ce document, le point d'accès utilisé, un DLINK DWL-2100AP, ne permet pas de récupérer le nombre de clients sans fil connectés. Mais une solution de supervision d'une variable de la MIB du point d'accès est proposée avec l'utilisation du script "*check_snmp*" et la création du service correspondant. Cette variable est "*stTrErrorCount*", elle comptabilise le nombre de transmissions en erreur.

L'annexe 3 présente une méthode pour trouver cette variable et l'identifiant (OID) correspondant.

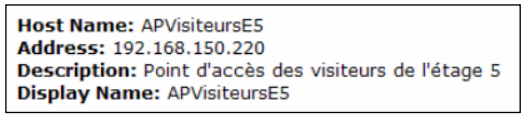
18.1 Ajout de l'équipement APVisiteursE5

Menu *Administration, Nagios/équipements*

- Utiliser le lien "*Add A New Child Host*" et renseigner les informations :

Host Name	: APVisiteursE5
Host Description	: Point d'accès des visiteurs de l'étage 5
Address	: 192.168.150.220
Display Name	: APVisiteursE5

Valider avec le bouton "*Add Host*" :



- Utiliser le lien *Inheritance*, sélectionner dans la liste déroulante "WIFI" et bouton "*Add Template*" :

18.2 Test dans Nagios

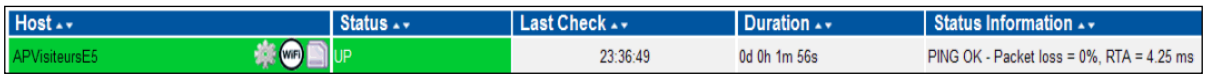
- Transférer vers Nagios

Menus *Tools / Exporter / Restart*, attendre le message *"Export Job ... Successfully"*

- Vue de l'équipement et de ses services dans Nagios

Menu *Disponibilités, Évènements/vue services*

Si l'état est "*Status : PENDING*", utiliser ce lien *PENDING* et le bouton "*submit command for 1 host*" :



Host	Status	Last Check	Duration	Status Information
APVisiteursE5	UP	23:36:49	0d 0h 1m 56s	PING OK - Packet loss = 0%, RTA = 4.25 ms

18.3 Ajout d'un service de supervision du nombre de clients WiFi

Par défaut, EoN propose un script "*check_snmp*" qui permet de tester une variable de la MIB.

18.3.1 Test du script

Obtenir de l'aide : *./check_snmp –h | more*

L'argument nouveau pour ce script est -o, il permet de spécifier l'OID de la variable qui contient la valeur recherchée.
Pour le premier test, nous allons rechercher le SSID, l'identifiant est .1.3.6.1.4.1.171.11.37.4.1.1.1.1 (voir annexe 3).

Remarque : Le début de l'OID : .1.3.6.1.4.1 peut-être remplacé par le mot *enterprises*.

Lancer le script avec les arguments suivants pour obtenir le nom du premier SSID :

./check_snmp –H 192.168.150.220 –C gsbintra –o enterprises.171.11.37.4.1.1.1.1.0

Ou :

./check_snmp –H 192.168.150.220 –C gsbintra –o enterprises.171.11.37.4.1.1.1.1 -n

Remarque :
Pour obtenir la valeur de la variable, nous ajoutons 0 à la fin de l'OID.
L'argument –n correspond à l'appel *SNMP GETNEXT* (obtenir la prochaine valeur à partir de l'OID spécifié).

Nous obtenons le nom du SSID : `SNMP OK - "VisiteursGSB" |`

Avec ce type de valeur, il est inutile d'utiliser les arguments des niveaux de critères –w (warning) et –c (critical).

Pour tester ces niveaux, nous allons interroger l'OID enterprises.171.11.37.4..4.3.1.1.9.0 qui correspond à la variable *stTrErrorCount* (voir annexe 3).

Lancer le script avec les arguments suivants :
./check_snmp –H 192.168.150.220 –C gsbintra –o enterprises.171.11.37.4..4.3.1.1.9.0 –w 100 –c 200

Avec cet exemple, nous obtenons :

```
SNMP WARNING - *162* | SNMPv2-SMI::enterprises.171.11.37.4.4.3.1.1.9.0=162
```

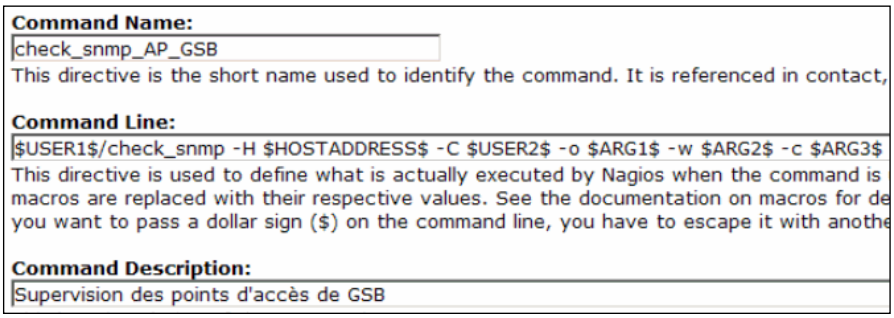
Pour la supervision du point d'accès WiFi de GSB, nous utiliserons cette variable à la place du nombre de clients Wifi connectés.

18.3.2 Ajout de la commande de supervision du point d'accès dans Nagios

Menu *Administration, Nagios/configuration* et utiliser le lien "*Nagios Commands*"
Utiliser le lien "*Add A New Command*" :

Saisir les informations de la commande :

"Command Name" : check_snmp_AP_GSB
"Command Description" : Supervision des points d'accès de GSB
"Command Line" : $USER1$/check_snmp –H $HOSTADDRESS$ –C $USER2$ –o $ARG1$ –w $ARG2$ –c $ARG3$



Bouton "*Create Command*"

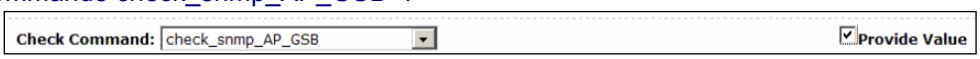
18.3.3 Ajout du service de supervision des points d'accès

Menu *Administration Nagios/équipements*, utiliser le lien *APVisiteursE5*, et le lien *Services*.

- Utiliser le lien "*Create A New Service For This Template*"
Saisir le nom du nouveau service : clientsWiFi-GSB et bouton "*Add Service*".

- Utiliser le lien *Inheritance*, sélectionner dans la liste déroulante "GENERIC_SERVICE".
Valider avec le bouton "*Add Template*".

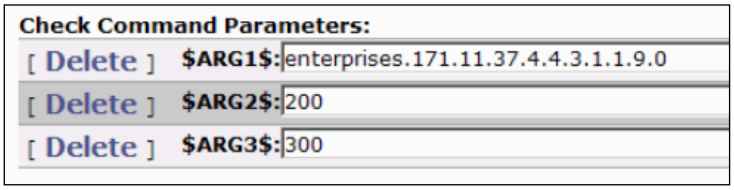
- Utiliser le lien *Checks* et le lien *Edit*
Pour la zone "*Check Command*", cocher la case "*Provide Value*" et sélectionner dans la liste déroulante notre commande check_snmp_AP_GSB" :



Bouton "*Update Checks*".

- Pour définir les arguments de ce service, utiliser le lien "*Check Command Parameters*" :

Ajouter les différents arguments, bouton "*Add Parameter*", avec les valeurs suivantes :



Vérifier les arguments avec le lien *Checks* :

18.4 Test dans Nagios

- Transférer vers Nagios

Menus *Tools / Exporter / Restart*, attendre le message *"Export Job ... Successfully"*

- Vue de l'équipement et de ses services dans Nagios

Menu *Disponibilités, Évènements/vue services*

Si l'état est "*Status : PENDING*", utiliser ce lien *PENDING* et le bouton "*submit command for 1 service*" :

Host	Service	Status	Last Check	Duration	Attempt	Status Information
APVisiteursE5	clientsWiFI-GSB	OK	23:46:40	0d 0h 1m 2s	1/4	SNMP OK - 12

19. Définition d'un parent

La relation "parents-enfants" va permettre de hiérarchiser la supervision des équipements. Si un élément parent ne répond plus, Nagios n'enverra pas de notifications pour ses enfants. Nous allons donc limiter les notifications inutiles.

Il faut définir les éléments parents du réseau. Dans notre cas, nous allons commencer par le commutateur SE5_1, qui est parent de l'imprimante ImpVisiteursE5 et du point d'accès APVisiteurE5. Pour l'instant, l'ensemble des équipements se présente sous cette forme :

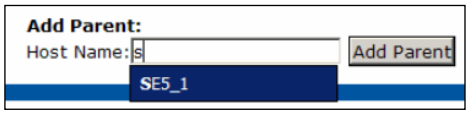
Host Name	Address	Description
APVisiteursE5	192.168.150.220	Point d'accès des visiteurs de l'étage 5
ImpVisiteursE5	192.168.150.200	Imprimante des visiteurs de l'étage 5
localhost	127.0.0.1	EyesOfNetwork Network Server
MUTLAB	192.168.10.1	Commutateur-Routeur
MUTSYS	192.168.10.2	Commutateur salle serveurs
REZOLAB	172.16.0.10	serveur DHCP/DNS
RTROUT	172.18.0.2	Routeur Internet & DMZ
SE5_1	192.168.10.11	Switch1 Etage5

19.1 Ajout des enfants à SE5_1

Menu *Administration, Nagios/équipements* et utiliser le lien ImpVisiteursE5

Utiliser le lien *Parents*.

Dans la zone "*Host Name*", saisir SE5_1 :



Bouton "*Add Parent*" :

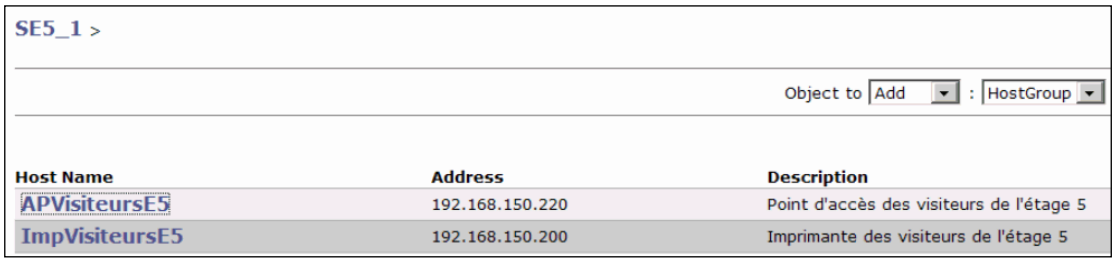
Faire de même avec le point d'accès APVisiteursE5.

Menu *Administration, Nagios/équipements* :

Host Name	Address	Description
localhost	127.0.0.1	EyesOfNetwork Network Server
MUTLAB	192.168.10.1	Commutateur-Routeur
MUTSYS	192.168.10.2	Commutateur salle serveurs
REZOLAB	172.16.0.10	serveur DHCP/DNS
RTROUT	172.18.0.2	Routeur Internet & DMZ
SE5_1 (2)	192.168.10.11	Switch1 Etage5

SE5_1 (2) a maintenant deux équipements enfants.

L'imprimante et le point d'accès sont accessibles en utilisant le lien SE5_1 :

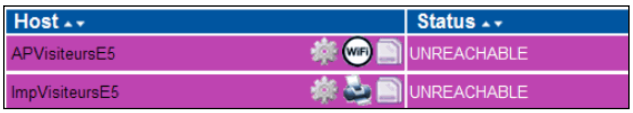


19.2 Test dans Nagios

Pour le test, arrêter le commutateur SE5_1.

- Transférer vers Nagios
Menus *Tools / Exporter / Restart*, attendre le message *"Export Job ... Successfully"*

- Vue des équipements dans Nagios
Menu *Disponibilités, Évènements/vue équipements* :



APVisiteursE5 et ImpVisiteursE5 se trouvent dans l'état "*Status UNREACHABLE*" et non "*Status DOWN*".

20. Vues de l'ensemble des équipements

20.1 Vue des équipements

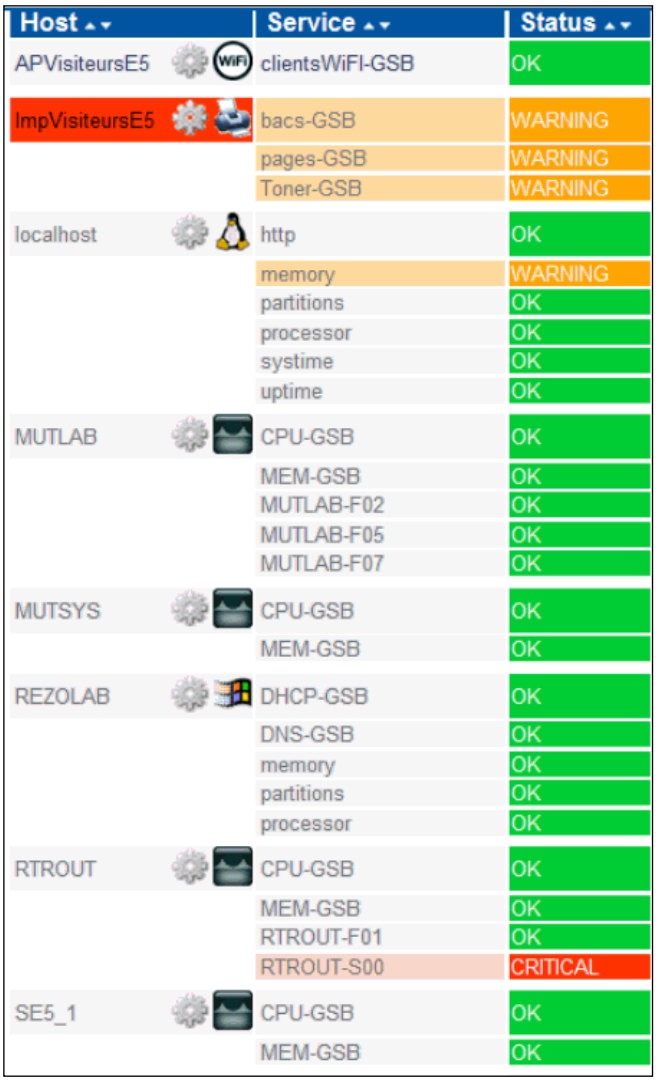
Menu *Disponibilités, Évènements/vue équipements* :

Remarque : l'imprimante est arrêtée.

20.2 Vue de tous les services des équipements

Menu *Disponibilités, Évènements/vue services* :

Remarque : l'imprimante est arrêtée, la mémoire du serveur de supervision est dans l'état WARNING et le port S0/0/0 du routeur RTROUT n'est pas connecté.



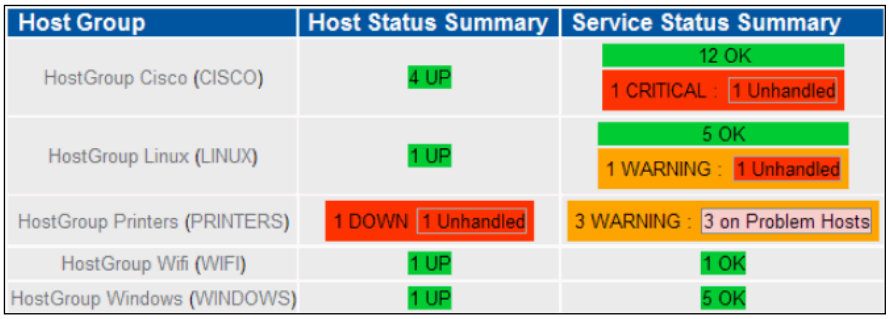
Host	Service	Status
APVisiteursE5	clientsWiFI-GSB	OK
ImpVisiteursE5	bacs-GSB	WARNING
	pages-GSB	WARNING
	Toner-GSB	WARNING
localhost	http	OK
	memory	WARNING
	partitions	OK
	processor	OK
	systime	OK
	uptime	OK
MUTLAB	CPU-GSB	OK
	MEM-GSB	OK
	MUTLAB-F02	OK
	MUTLAB-F05	OK
	MUTLAB-F07	OK
MUTSYS	CPU-GSB	OK
	MEM-GSB	OK
REZOLAB	DHCP-GSB	OK
	DNS-GSB	OK
	memory	OK
	partitions	OK
	processor	OK
RTROUT	CPU-GSB	OK
	MEM-GSB	OK
	RTROUT-F01	OK
	RTROUT-S00	CRITICAL
SE5_1	CPU-GSB	OK
	MEM-GSB	OK

20.3 Vue par type d'équipement (par groupe)

Avec plusieurs équipements et types d'équipements différents, il est intéressant d'avoir une vue des hôtes par groupe.

- Vue par groupe d'équipement dans Nagios

Menu *Disponibilités, Évènements/groupes d'équipements*



Host Group	Host Status Summary	Service Status Summary
HostGroup Cisco (CISCO)	4 UP	12 OK 1 CRITICAL : 1 Unhandled
HostGroup Linux (LINUX)	1 UP	5 OK 1 WARNING : 1 Unhandled
HostGroup Printers (PRINTERS)	1 DOWN 1 Unhandled	3 WARNING : 3 on Problem Hosts
HostGroup Wifi (WIFI)	1 UP	1 OK
HostGroup Windows (WINDOWS)	1 UP	5 OK

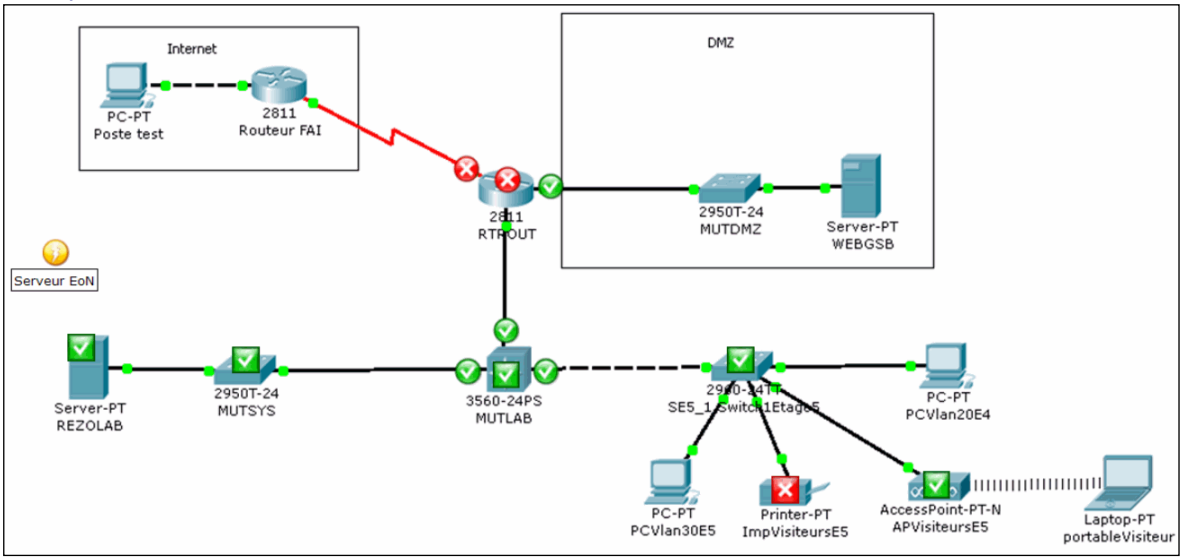
Remarque : l'imprimante est arrêtée, la mémoire du serveur de supervision est dans l'état WARNING et le port S0/0/0 du routeur RTROUT n'est pas connecté.

Cartographie des éléments supervisés

21. La carte Nagvis

Nagvis remplace avantageusement la cartographie Nagios. Nagvis va permettre d'afficher l'état des différents éléments de notre réseau en s'appuyant sur le schéma de celui-ci.

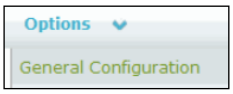
Exemple de résultat avec notre réseau GSB :



21.1 Modification du langage

Menu *Administration, Cartographies/nagvis*

Menu *Options/General Configuration* :

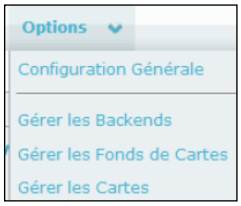


Utiliser la liste déroulante de la zone *language* pour sélectionner fr_FR et tout en bas, bouton *Save*.

21.2 Insertion du fond de carte dans Nagvis

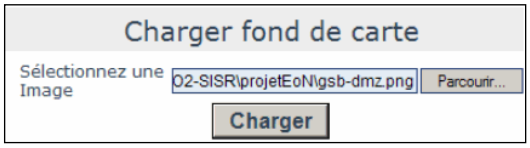
Création du fichier gsb-dmz.png avec Cisco Packet Tracer : *File/Print …/Print to file…*

Menu *Options/Gérer les Fonds de Cartes* :



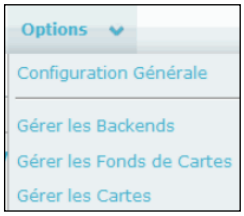
Dans la zone "*Charger fond de carte*", à l'aide du bouton *Parcourir*, rechercher le fichier gsb-dmz.png :

Bouton *Charger* :



21.3 Création de la carte

Menu *Options/Gérer les cartes*

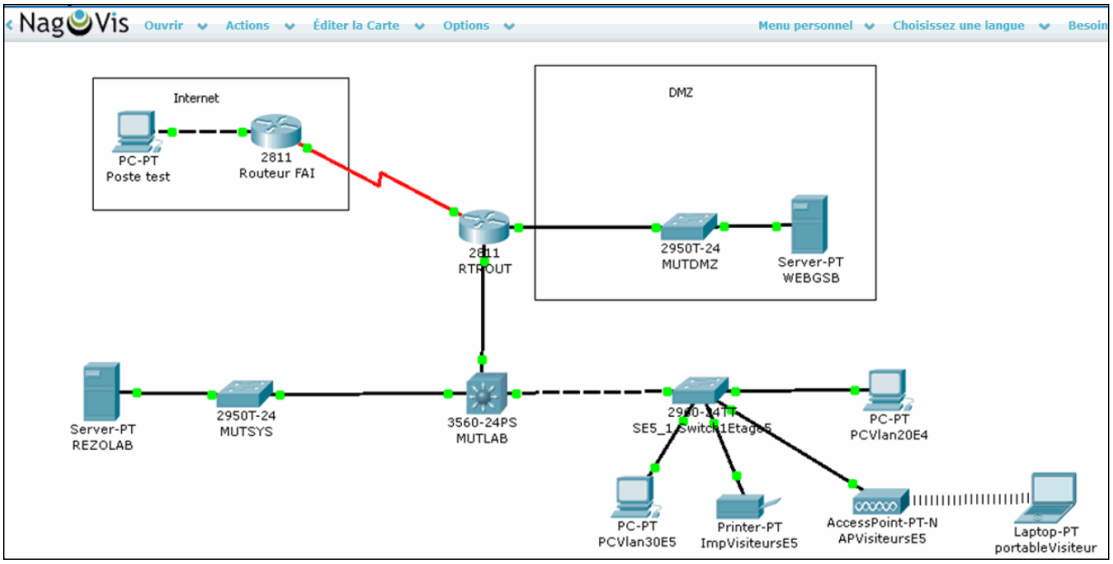


Dans la zone "*Créer une carte*" ;

Saisir le nom de la carte : GSB.
Saisir la taille des icônes de la carte.
Utiliser la liste déroulante pour sélectionner le fond de carte : gsb-dmz.png.

Bouton *Créer* :

Résultat :

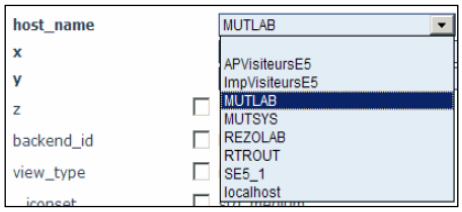


21.4 Insertion des hosts

Menu *Éditer la carte/Ajouter une icône/Host* :

Positionner la croix sur l'équipement concerné (ici MUTLAB) et *click*.

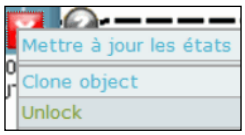
Dans la liste déroulante *host_name*, sélectionner MUTLAB :



(On retrouve dans la liste les hôtes définis dans Nagios)

Bouton *Sauvegarder*.

Pour déplacer l'icône (ou modifier l'équipement), il faut débloquer l'élément.
Click droit sur l'icône, *Unlock* :



Il est aussi possible de Bloquer/Débloquer l'ensemble des équipements de la carte pour les modifier.

Menu *Éditer la Carte/Tout Bloquer/Débloquer* :

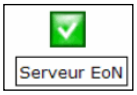
Une fois "débloquer", il est possible de modifier la configuration des icônes.

Clic droit sur l'icône :

Insérer l'ensemble des équipements sur la carte.

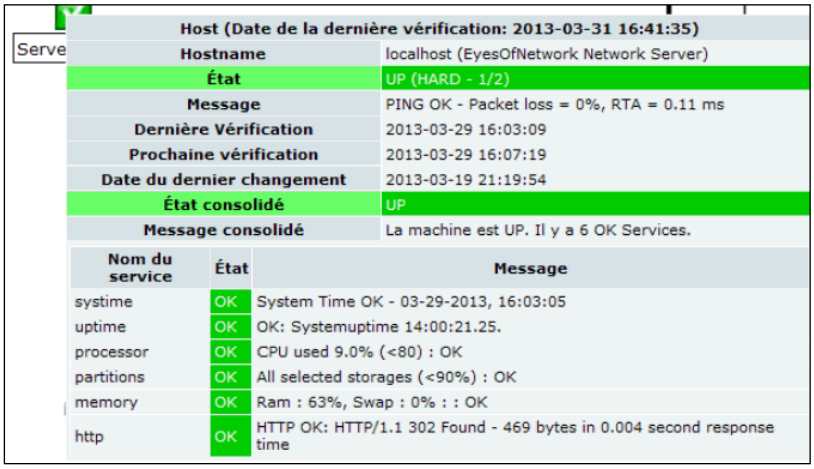
Pour le serveur EoN (localhost), l'insertion peut se faire avec un label :

Bouton *Sauvegarder*.



Lorsque l'équipement est "bloquer", il est possible de voir son état en passant la souris dessus :

Ici, tout est OK, donc l'icône est carré et vert

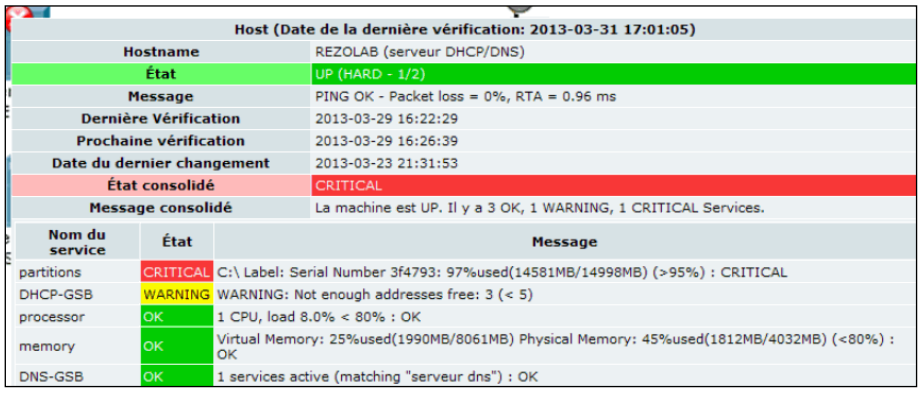


Host (Date de la dernière vérification: 2013-03-31 16:41:35)	
Hostname	localhost (EyesOfNetwork Network Server)
État	UP (HARD - 1/2)
Message	PING OK - Packet loss = 0%, RTA = 0.11 ms
Dernière Vérification	2013-03-29 16:03:09
Prochaine vérification	2013-03-29 16:07:19
Date du dernier changement	2013-03-19 21:19:54
État consolidé	UP
Message consolidé	La machine est UP. Il y a 6 OK Services.

Nom du service	État	Message
systime	OK	System Time OK - 03-29-2013, 16:03:05
uptime	OK	OK: Systemuptime 14:00:21.25.
processor	OK	CPU used 9.0% (<80) : OK
partitions	OK	All selected storages (<90%) : OK
memory	OK	Ram : 63%, Swap : 0% : : OK
http	OK	HTTP OK: HTTP/1.1 302 Found - 469 bytes in 0.004 second response time

Si un service de l'équipement est en alerte (WARNING ou CRITICAL), l'icône de l'équipement est rond et de la couleur de l'alerte.

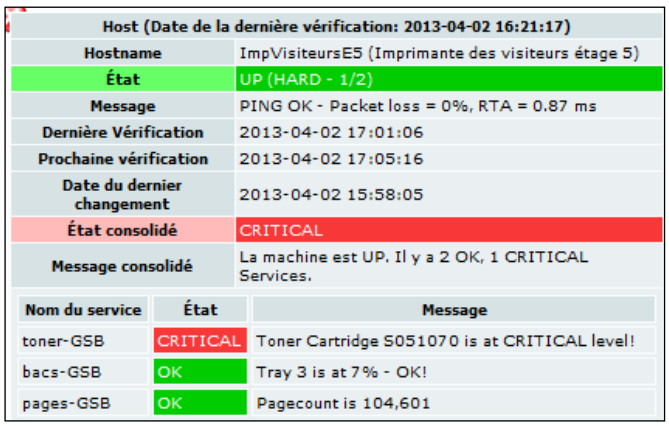
REZOLAB :



Host (Date de la dernière vérification: 2013-03-31 17:01:05)	
Hostname	REZOLAB (serveur DHCP/DNS)
État	UP (HARD - 1/2)
Message	PING OK - Packet loss = 0%, RTA = 0.96 ms
Dernière Vérification	2013-03-29 16:22:29
Prochaine vérification	2013-03-29 16:26:39
Date du dernier changement	2013-03-23 21:31:53
État consolidé	CRITICAL
Message consolidé	La machine est UP. Il y a 3 OK, 1 WARNING, 1 CRITICAL Services.

Nom du service	État	Message
partitions	CRITICAL	C:\ Label: Serial Number 3f4793: 97%used(14581MB/14998MB) (>95%) : CRITICAL
DHCP-GSB	WARNING	WARNING: Not enough addresses free: 3 (< 5)
processor	OK	1 CPU, load 8.0% < 80% : OK
memory	OK	Virtual Memory: 25%used(1990MB/8061MB) Physical Memory: 45%used(1812MB/4032MB) (<80%) : OK
DNS-GSB	OK	1 services active (matching "serveur dns") : OK

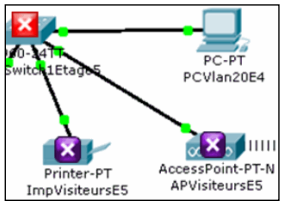
Imprimante ImpVisiteursE5 :



Host (Date de la dernière vérification: 2013-04-02 16:21:17)	
Hostname	ImpVisiteursE5 (Imprimante des visiteurs étage 5)
État	UP (HARD - 1/2)
Message	PING OK - Packet loss = 0%, RTA = 0.87 ms
Dernière Vérification	2013-04-02 17:01:06
Prochaine vérification	2013-04-02 17:05:16
Date du dernier changement	2013-04-02 15:58:05
État consolidé	CRITICAL
Message consolidé	La machine est UP. Il y a 2 OK, 1 CRITICAL Services.

Nom du service	État	Message
toner-GSB	CRITICAL	Toner Cartridge S051070 is at CRITICAL level!
bacs-GSB	OK	Tray 3 is at 7% - OK!
pages-GSB	OK	Pagecount is 104,601

Si un équipement est arrêté (*Down* : carré rouge), les équipements enfants ont un carré violet ("*Status UNREACHABLE*") :



21.5 Insertion des services

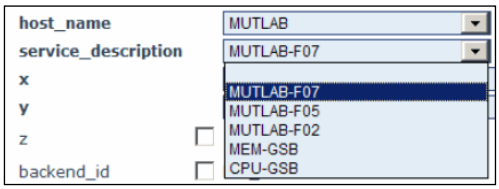
Il est possible également d'insérer un service spécifique d'un équipement. Pour le réseau GSB, nous allons insérer les services associés aux ports supervisés des matériels d'interconnexion (MUTLAB et RTROUT).

Menu *Éditer la carte/Ajouter une icône/Service* :

Positionner la croix sur le lien de MUTLAB vers RTROUT et *click* :

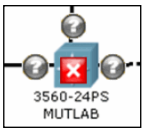
Dans la liste déroulante *host_name*, sélectionner MUTLAB et dans la liste déroulante *service_description*, sélectionner MUTLAB-F07 :

Bouton *Sauvegarder*.



Insérer tous les services de supervisions concernant les ports de MUTLAB et RTROUT sur la carte.

Si un équipement est arrêté (*Down* : carré rouge), ses services sont gris (*UNKNOWN*) :



21.6 Tests

Menu *Disponibilités, Cartographies/nagvis*
En positionnant le pointeur de la souris sur le nom de la carte :

Nous obtenons un résumé de l'état des équipements :

Carte (Date de la dernière vérification: 2013-05-13 18:51:21)		
Nom de la carte	GSB (GSB)	
État consolidé	DOWN	
Message consolidé	Il y a 2 CRITICAL, 1 DOWN, 1 WARNING, 5 UP, 4 OK Objets.	
Nom de l'objet	**État**	**Message**
ImpVisiteursE5	DOWN	La machine est DOWN. Il y a 3 WARNING Services.
RTROUT	CRITICAL	La machine est UP. Il y a 3 OK, 1 CRITICAL Services.
RTROUT-S00	CRITICAL	Serial0/0/0:DOWN: 1 int NOK : CRITICAL
localhost	WARNING	La machine est UP. Il y a 5 OK, 1 WARNING Services.
APVisiteursE5	UP	La machine est UP. Il y a 1 OK Services.
MUTSYS	UP	La machine est UP. Il y a 2 OK Services.
MUTLAB	UP	La machine est UP. Il y a 5 OK Services.
SE5_1	UP	La machine est UP. Il y a 2 OK Services.
REZOLAB	UP	La machine est UP. Il y a 5 OK Services.
RTROUT-F01	OK	GigabitEthernet0/1:UP (0.0%/0.0%):1 UP: OK
		3 more items...

Remarque : l'imprimante est arrêtée, le port S0/0/0 du routeur RTROUT n'est pas connecté et la mémoire du serveur de supervision est dans l'état WARNING.

En cliquant sur la carte, nous obtenons le graphique présenté en exemple au **21.**

En positionnant le pointeur de la souris sur le routeur RTROUT, nous obtenons un résumé de l'état de l'équipement :

Host (Date de la dernière vérification: 2013-05-13 19:07:11)	
Hostname	RTROUT (Routeur Internet & DMZ)
État	UP (HARD - 1/2)
Message	PING OK - Packet loss = 0%, RTA = 1.00 ms
Dernière Vérification	2013-04-16 21:36:58
Prochaine vérification	2013-04-16 21:41:00
Date du dernier changement	2013-04-16 20:06:53
État consolidé	CRITICAL
Message consolidé	La machine est UP. Il y a 3 OK, 1 CRITICAL Services.

Nom du service	État	Message
RTROUT-S00	CRITICAL	Serial0/0/0:DOWN: 1 int NOK : CRITICAL
RTROUT-G01	OK	GigabitEthernet0/1:UP (0.0%/0.0%):1 UP: OK
MEM-GSB	OK	Status is OK - MEMORY: total: 320.44 MB, used: 38.79 MB (12%), free: 281.65 MB
CPU-GSB	OK	Status is OK - CPU load average (5 min): 0 %, temperature normal

Remarque : Le port S0/0/0 du routeur RTROUT n'est pas connecté, donc l'état consolidé de l'équipement est *CRITICAL*.

En positionnant le pointeur de la souris sur le service RTROUT-G01 (routeur RTROUT), nous obtenons un résumé de l'état de ce service :

Service (Date de la dernière vérification: 2013-05-13 19:07:11)	
Hostname	RTROUT (Routeur Internet & DMZ)
Nom du service	RTROUT-G01
État consolidé	OK
Message consolidé	GigabitEthernet0/1:UP (0.0%/0.0%):1 UP: OK
Dernière Vérification	2013-04-16 21:36:42
Prochaine vérification	2013-04-16 21:40:42
Date du dernier changement	2013-04-16 21:32:42

En positionnant le pointeur de la souris sur le serveur EoN, nous retrouvons l'état consolidé *WARNING* à cause de la mémoire :

Host (Date de la dernière vérification: 2013-05-13 18:54:45)	
Hostname	localhost (EyesOfNetwork Network Server)
État	UP (HARD - 1/2)
Message	PING OK - Packet loss = 0%, RTA = 0.10 ms
Dernière Vérification	2013-04-16 21:22:10
Prochaine vérification	2013-04-16 21:26:20
Date du dernier changement	2013-04-16 02:53:58
État consolidé	WARNING
Message consolidé	La machine est UP. Il y a 5 OK, 1 WARNING Services.

Nom du service	État	Message
memory	WARNING	Ram : 84%, Swap : 17% : > 80, 20 : WARNING
uptime	OK	OK: Systemuptime 1 day, 1:33:59.92.
systime	OK	System Time OK - 04-16-2013, 21:22:11
partitions	OK	All selected storages (<90%) : OK
http	OK	HTTP OK: HTTP/1.1 302 Found - 469 bytes in 0.007 second response time
processor	OK	CPU used 13.0% (<80) : OK

Un équipement qui change d'état est pendant plusieurs secondes entouré d'un carré de la couleur de l'avertissement :

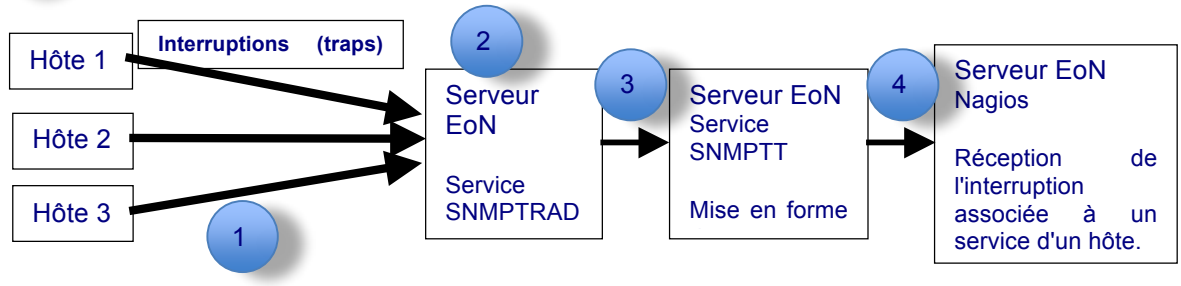
Supervision à l'aide des interruptions (TRAPs) SNMP

22. Configuration de la récupération des interruptions (traps) SNMP

Pour éviter de trop charger le réseau et le serveur EoN, il est intéressant de récupérer des alertes sur les équipements à partir des interruptions (traps) SNMP (voir annexe 2).

Le principe sur NAGIOS :

1. Une application ou le système d'un équipement envoie une interruption SNMP au serveur EoN (NAGIOS) ;
2. Le service SNMPTRAPD récupère cette interruption (trap) en écoutant sur le port UDP 162 ;
3. Ce service passe ensuite cette information au service SNMPTT (SNMP Trap Translator) qui permet de rendre cette interruption plus lisible en utilisant les MIB et des règles de format de présentation ;
4. SMMPTT transmet ensuite cette interruption mise en forme, à NAGIOS, en utilisant la commande *submit_check_result*.



22.1 Le service SNMPTRAPD

Menu *Administration, Généralités/snmptrapd*

Dans le fichier de configuration du service SNMPTRAPD, remplacer le nom de la communauté EyesOfNetwork, par **gsbintra** :

```
ignoreauthfailure yes
authCommunity log,execute,net gsbintra
traphandle default /srv/eyesofnetwork/snmptt/bin/snmptthandler
```

Bouton *Update*.

Ce fichier de configuration est : /etc/snmp/snmptrapd.conf.

Commentaires sur les lignes :

- La première ligne permet d'accepter toutes les interruptions
- La seconde définit entre autre, le nom de la communauté
- La dernière transmet toutes les interruptions à snmptt

Pour relancer le service SNMPTRAPD :

Menu *Administration, Généralités/processus*

Utiliser le lien *restart* du processus "*SNMP trap agent*" pour relancer ce service :

SNMP agent	UP	1704	stop restart reload
SNMP trap agent	UP	1718	stop restart reload

22.2 Configuration de snmptt.ini

Le fichier de configuration de snmptt est : /srv/eyesofnetwork/snmptt/etc/snmptt.ini

Modifier ce fichier (avec vi ou en utilisant FileZilla Client pour récupérer/modifier/replacer ce fichier)

Vérifier la configuration des éléments suivants :

- La résolution de noms doit être activée :

```
37  # Set to 1 to enable DNS resolution
38  dns_enable = 1
```

- Le nom relatif (et non FQDN) doit être utilisé :

```
46  # based on the list of domains in strip_domain_list
47  strip_domain = 1
```

Remarque :
Si strip_domain = 0 :
Les noms des équipements concernés par une interruption seront de la forme nomposte.gsbeu.intra

Si strip_domain = 2 :
Il est nécessaire de spécifier le domaine utilisé dans strip_domain_liste

```
53  strip_domain_list = <<END
54  gsbeu.intra
55  END
```

Modifier la configuration de l'élément suivant :
Ce module Perl permet l'interprétation étendue des OID.

```
71  net_snmp_perl_enable = 1
```

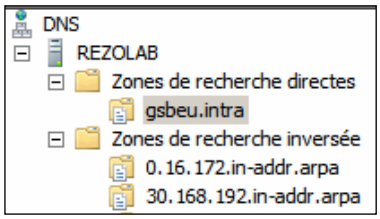
Relancer le service sur le serveur srveon avec l'instruction suivante : *service snmptt restart*.

22.3 Configuration du serveur DNS

Les interruptions (traps) sont émises par une adresse IP (celle de l'équipement) qui est convertie en nom d'hôte par SNMPTT, à l'aide d'une résolution de noms de domaine inverse (enregistrement DNS de type PTR).

Il est donc nécessaire de mettre en place cette résolution inverse sur notre serveur DNS REZOLAB.
Pour ce document, la résolution inverse n'est mise en place que pour le réseau d'adresse 192.168.30.0/24 correspondant au VLAN 30.

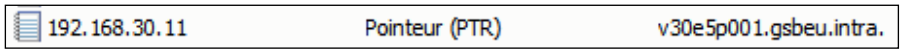
Pour un serveur DNS sous Windows2008R2 :
- clic droit sur *Zones de recherche inversée*, *Nouvelle zone…,* bouton *Suivant*,
- sélectionner *Zone principale*, bouton *Suivant* deux fois,
- saisir l'ID réseau, soit 192.168.30, bouton *Suivant* deux fois,
- autoriser les mises à jour dynamiques (nécessaire pour les clients DHCP), bouton *Suivant* et bouton *Terminer* :



Remarque :
Pour les clients DHCP, il est nécessaire de mettre en place le DNS dynamique.

Si la mise à jour dynamique du DNS n'est pas en place, il est toujours possible de faire des tests avec un client configuré en statique. Dans ce cas, il est nécessaire d'ajouter manuellement le client dans la zone de recherche inversée : (click droit sur la zone *30.168.192.in-addr.arpa*, *Nouveau pointeur (PTR)*…).

Avec le poste client sous Windows7, nommé v30e5p001 (PCVlan30E5), nous obtenons par exemple :

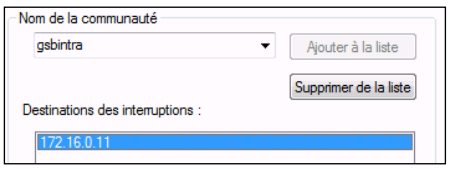


22.4 Configuration de l'agent SNMP de l'équipement

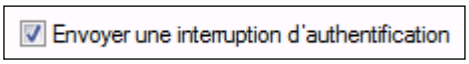
L'équipement qui va transmettre les interruptions SNMP doit être configuré, notamment en précisant l'adresse IP du serveur qui reçoit ces informations, ici notre serveur EoN.

Pour GSB, nous allons configurer l'agent SNMP du poste client sous Windows7.

Configuration du service SNMP sur Windows :
- *panneau de configuration*, *Afficher* par : Petites icônes,
- *outils d'administration, Services*,
- clic droit sur *Service SNMP*, *Propriétés*,
- *onglet Interruptions*, dans la liste, saisir la communauté : **gsbintra**
- bouton *Ajouter à la liste*,
- bouton *Ajouter…*,
- saisir l'adresse IP du serveur : 172.16.0.11, bouton *Ajouter*,
- bouton *Appliquer*.



Pour les tests, nous allons configurer les interruptions d'authentification :
- *onglet Sécurité*,
- cocher "*Envoyer une interruption d'authentification*" :
- bouton *Appliquer* et bouton *OK*.
- redémarrer le service SNMP.



23. Mise en place des interruptions (traps) SNMP sur NAGIOS

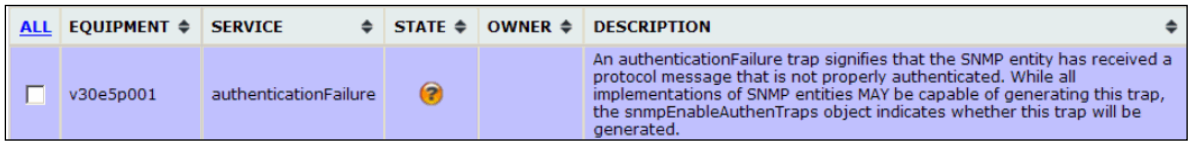
23.1 Test de réception des interruptions par le serveur EoN

Se placer dans le dossier /srv/eyesofnetwork/nagios/plugins : *cd /srv/eyesofnetwork/nagios/plugins/*

Pour déclencher une interruption SNMP à partir du poste v30e5p001, nous allons lancer un script à destination de l'hôte v30e5p001, mais avec un mauvais nom de communauté :

./check_snmp_storage.pl –H v30e5p001 –C gsb –m "Mem" –w 80 –c 90

- Résultat dans Nagios :
Menu *Disponibilités, Évènements/évènements actifs*

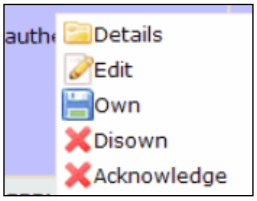


ALL	EQUIPMENT	SERVICE	STATE	OWNER	DESCRIPTION
☐	v30e5p001	authenticationFailure	?		An authenticationFailure trap signifies that the SNMP entity has received a protocol message that is not properly authenticated. While all implementations of SNMP entities MAY be capable of generating this trap, the snmpEnableAuthenTraps object indicates whether this trap will be generated.

Nous obtenons un évènement qui correspond bien au poste v30e5p001 (la résolution inverse fonctionne) avec un nom de service (*authenticationFailure*) et une description qui correspond bien à un problème d'identification SNMP.

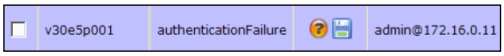
Nous pouvons affirmer que la résolution inverse de SNMPTT fonctionne, car lorsque l'interruption est récupérée par SNMPTT, la trame ne contient que l'adresse IP de l'agent SNMP qui l'a transmis. A partir de cette IP, SNMPTT a trouvé le nom de l'hôte v30e5p001 avec la résolution DNS inverse.

- Pour supprimer cet élément des évènements actifs (considéré résolu) :
Click droit dans la ligne de l'évènement, menu *Acknowledge*

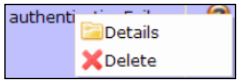


Remarque : le menu *Details* permet d'avoir plus d'informations, dont l'adresse IP de l'équipement.

- Pour visualiser les évènements résolus :
Menu *Disponibilités, Évènements/évènements résolus*



- Pour supprimer cet élément résolu :
Click droit dans la ligne de l'évènement, menu *Delete*.

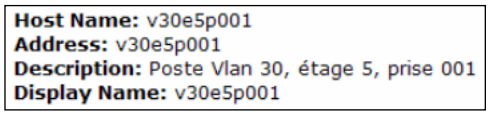


23.2 Ajout d'un équipement en mode passif

Le mode passif correspond à un équipement qui n'est pas interrogé périodiquement par Nagios. Les alertes éventuelles seront transmises directement par l'équipement via les interruptions (traps) SNMP.

Menu *Administration, Nagios/équipements*
- Utiliser le lien "*Add A New Child Host*" et renseigner les informations :

Host Name : v30e5p001
Host Description : Poste Vlan 30, étage 5,
Address : v30e5p001
Display Name : v30e5p001

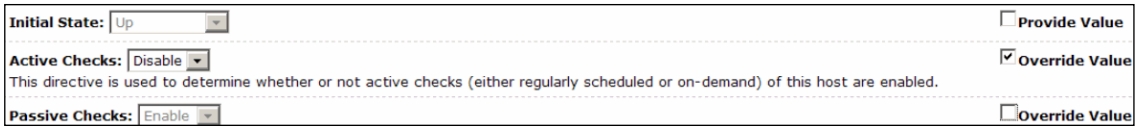


Valider avec le bouton "*Add Host*".

Remarque : le poste étant client DHCP, il est possible grâce à la résolution DNS de renseigner son nom plutôt que son adresse IP (qui peut varier).

- Utiliser le lien *Inheritance*, sélectionner dans la liste déroulante "GENERIC_HOST", bouton "*Add Template*".

- Utiliser le lien *Checks* et le lien *Edit*
Pour la zone "Active *Checks*", cocher la case "Override Value" et sélectionner *Disable* dans la liste déroulante :



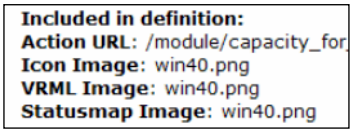
Bouton "*Update Checks*".

Explications :
- "Initial State" Up : par défaut, l'état de l'équipement est Up.

- "Active *Checks*" Disable : cette directive définit que les contrôles planifiés sont désactivés pour cet hôte. La commande "*check-host-alive*" n'est pas utilisée périodiquement par Nagios pour déterminer si l'hôte est actif sur le réseau.

- Avec ces directives, lorsque le poste client est arrêté, aucune alerte et notification ne sont transmises par NAGIOS.

- Utiliser le lien "*Extended Information*" et le lien *Edit*, définir les images associées aux clients Windows :



23.3 Test dans Nagios
- Transférer vers Nagios
Menus *Tools / Exporter / Restart*, attendre le message *"Export Job ... Successfully"*

- Vue de l'équipement et de ses services dans Nagios
Menu *Disponibilités, Évènements/vue équipements*

Par défaut, l'état est "*Status : UP*" :

La croix rouge indique que c'est un équipement passif : "*checks of this host have been disabled*".

Il est possible de forcer le test de l'équipement avec le lien UP et le bouton "*submit command for 1 host*" :

Résultat si le poste est arrêté :

Attention, l'état "*Status : DOWN*" ne changera pas, même si l'équipement est démarré. Il est nécessaire d'utiliser une nouvelle fois le bouton "*submit command for 1 host*" pour forcer la mise à jour de cet état.

Avant d'utiliser "*Submit* ….", utiliser l'option "*Force Check*" pour forcer le test :

23.4 Ajout d'un service en mode passif
Pour récupérer les interruptions SNMP de cet équipement, il est nécessaire de définir un service en mode passif. Attention, le nom de ce service sera utilisé dans les fichiers de configuration des interruptions de snmptt.

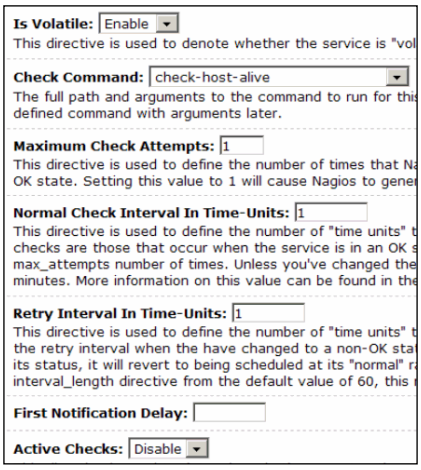
- Menu *Administration Nagios/équipements*, utiliser le lien *v30e5p001*, et le lien *Services*,

- Utiliser le lien "*Create A New Service For This Template*"
Saisir le nom du nouveau service : TRAP-GSB et bouton "*Add Service*".

- Utiliser le lien *Inheritance*, sélectionner dans la liste "GENERIC_SERVICE", et bouton "*Add Template*".

- Utiliser le lien *Checks* et le lien *Edit*, cocher les cases "Override Value" pour définir les éléments suivants :

- Is Volatile : Enable
- Check Command : check-host-alive
- Maximun Check Attempts : 1
- Normal Check Interval In Time-Units : 1
- Retry Interval In Time-Units : 1
- Active Cheks : Disable



Bouton "*Update Checks*".

Explications :

- Le service est défini comme volatile, si une deuxième interruption arrive avant que la première soit remise à OK, une nouvelle notification est transmise.

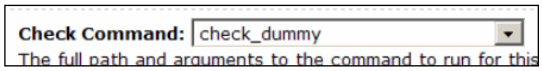
- La commande "*check-host-alive"* (simple PING) permet de remettre le service à OK après un problème, en forçant le test sur l'équipement. Il est possible ici d'utiliser une autre commande "*check_dummy*", qui remet l'état du service à OK, sans contacter réellement l'équipement (voir ci-dessous).

- Le service est passif (*Active Checks : Disable*), la commande n'est pas utilisée périodiquement par Nagios pour déterminer l'état de ce service.

- Une alerte est déclenchée dès que l'état du service n'est plus OK ("*Maximun Check Attempts: 1*").

Remise de l'état à OK avec la commande *check_dummy* (autre solution) :

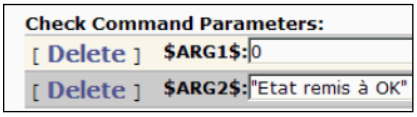
- Utiliser le lien *Checks* et le lien *Edit*
Pour la zone "*Check Command*", cocher la case "*Provide Value*" et sélectionner dans la liste déroulante la commande check_dummy" :



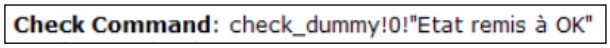
Bouton "*Update Checks*".

- Pour définir les arguments de cette commande, utiliser le lien "*Check Command Parameters*".

Ajouter les différents arguments, bouton "*Add Parameter*" avec les valeurs suivantes (0 indique un état OK) :



Vérifier les arguments avec le lien *Checks* :



Cette deuxième solution ne nécessite pas d'avoir l'équipement actif pour remettre l'état du service à OK.

23.5 Test dans Nagios

- Transférer vers Nagios
Menus *Tools / Exporter / Restart*, attendre le message *"Export Job ... Successfully"*

- Vue de l'équipement et de ses services dans Nagios
Menu *Disponibilités, Évènements/vue services*

Pour mettre à jour l'état du service, utiliser le lien de la colonne "*Status*", cocher l'option "*Force Check*" et bouton "*submit command for 1 service*" :

Résultat avec la commande *check-host-alive* (dans la description, nous retrouvons notre PING) :

Résultat avec la commande *check_dummy* (dans la description, nous retrouvons le texte associé) :

La croix rouge indique que c'est un service passif : "*checks of this service have been disabled*"

24. Configuration de SNMPTT pour l'interruption authenticationFailure

SMMPTT transmet les interruptions mises en forme, à NAGIOS, avec la commande *submit_check_result*.
Pour plus d'informations sur SNMPTT, voir le site à l'adresse suivante : http://www.snmptt.org/

24.1 Test de la commande submit_check_result

Cette commande est située dans le dossier /srv/eyesofnetwork/nagios/plugins/eventhandlers/.
Pour se placer dans ce dossier : *cd /srv/eyesofnetwork/nagios/plugins/eventhandlers/*

Pour voir les arguments utilisés par cette commande, taper l'instruction : *cat submit_check_result*
Le résultat affiche quatre arguments :

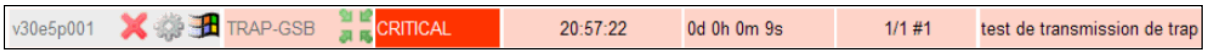
- $1 : Nom de l'hôte qui est concerné par le service faisant l'objet de l'interruption SNMP.
- $2 : Description du service (en fait le nom du service dans Nagios).
- $3 : Code de l'alerte (OK=0, WARNING=1, CRITICAL=2, UNKNOWN=3).
- $4 : Le texte qui peut être associé à l'alerte.

Lancer la commande avec les arguments suivants :

./submit_check_result v30e5p001 TRAP-GSB 2 "test de transmission de trap"

- Vue de l'équipement et de ses services dans Nagios
Menu *Disponibilités, Évènements/vue services*

Résultat pour le service TRAP-GSB du poste v30e5p001 :



Nous retrouvons bien l'alerte *CRITICAL* =2 et le texte associé.

IMPORTANT : le nom du service (TRAP-GSB) utilisé dans la commande doit-être le même que celui défini dans Nagios.

Remettre l'état du service à OK : utiliser le lien de la colonne "*Status*", cocher l'option "*Force Check*" et bouton "*submit command for 1 service*".

24.2 Utiliser la commande submit_check_result dans un fichier de configuration de SNMPTT

Nous voulons maintenant que l'interruption *authenticationFailure* vue au **23.1** soit affectée au service TRAP-GSB du poste v30e5p001.

Les interruptions traitées sont définies dans un fichier snmptt.conf. Des fichiers snmptt.conf sont déjà définis et placés dans le dossier : /srv/eyesofnetwork/snmptt/etc/mibs/

Le fichier qui traite l'interruption *authenticationFailure* (vue au **23.1**) est : snmptt.conf.SNMPv2-MIB.txt

Modifier ce fichier (avec vi ou en utilisant FileZilla Client pour récupérer/modifier/replacer ce fichier)

Rechercher l'interruption dont le nom est *authenticationFailure*, déclarée avec l'instruction EVENT.

Commenter la ligne 35 et ajouter les lignes 36 et 38 :

```
33  EVENT authenticationFailure .1.3.6.1.6.3.1.1.5.5 "Status Events" Normal
34  FORMAT $*
35  #EXEC /srv/eyesofnetwork/ged/scripts/ged-snmptt "$r" "$N" "$s" "$D" "$aA" "$r" "" "$c" "$*"
36  EXEC /srv/eyesofnetwork/nagios/plugins/eventhandlers/submit_check_result $r TRAP-GSB 2 "$r $aA $C $E $D $*"
37  SDESC
38  Test d'erreur sur le nom de la communauté :
39  An authenticationFailure trap signifies that the SNMP
40  entity has received a protocol message that is not
41  properly authenticated.  While all implementations
42  of SNMP entities MAY be capable of generating this
43  trap, the snmpEnableAuthenTraps object indicates
44  whether this trap will be generated.
45  EDESC
```

La ligne 36 utilise la commande *submit_check_result* et la ligne 38 ajoute un commentaire en français.

Explications :
C'est la ligne 35 qui permettait de renseigner les évènements actifs (GED) de l'interruption *authenticationFailure* du test réalisé en **23.1** avec la commande *ged-snmptt* et une suite de variables.

La nouvelle ligne 36 utilise la commande submit_check_result qui permet d'affecter cette interruption au service d'un équipement, avec ses quatre arguments (hôte, service, alerte, texte) :

- hôte : Le nom de l'hôte est contenu dans la variable $r
- service : TRAP-GSB, comme défini dans Nagios
- alerte : 2, correspond à CRITICAL
- texte : composé de variables décrites ci-dessous

Les variables :

$r	: Nom de l'hôte (agent SNMP)
$aA	: Adresse IP de l'agent SNMP
$C	: Nom de la communauté
$E	: OID de l'entreprise
$D	: Description de l'interruption, contenue entre SDESC et EDESC
$*	: Affiche les éventuelles autres informations (variables) contenues dans la trame trap

Pour plus d'informations, consulter le site à l'adresse suivante :
http://www.snmptt.org/docs/snmptt.shtml#SNMPTT.CONF-Configuration-file-format

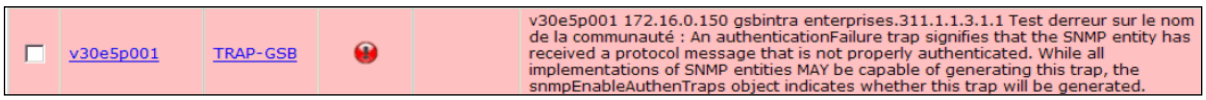
Relancer le service sur le serveur srveon avec l'instruction suivante : *service snmptt restart*

24.3 Test de l'interruption authenticationFailure

Se placer dans le dossier /srv/eyesofnetwork/nagios/plugins : *cd /srv/eyesofnetwork/nagios/plugins/*

Déclencher une nouvelle interruption SNMP à partir du poste v30e5p001, avec le script du **23.1** :
./check_snmp_storage.pl –H v30e5p001–C gsb –m "Mem" –w 80 –c 90

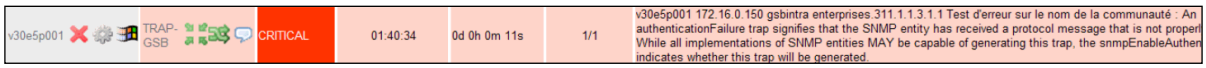
Résultat dans Nagios :
Menu *Disponibilités, Évènements/évènements actifs*



Nous obtenons toujours l'évènement qui correspond au poste v30e5p001, mais avec le nom du service **TRAP-GSB** et une description qui reprend le format défini dans le fichier snmptt.conf.SNMPv2-MIB.txt, avec l'adresse IP, la communauté, l'OID et la phrase en français "Test d'erreur sur le nom de la communauté :".

Remarque : Pour les tests, l'adresse IP de v30e5p001 est 172.16.0.150 et non l'adresse 192.168.30.11.

Menu *Disponibilités, Évènements/vue services*



L'état du service TRAP-GSB est bien passé à *CRITICAL* et ce changement a déclenché une notification :

Remettre l'état du service à OK : utiliser le lien de la colonne "*Status*", cocher l'option "*Force Check*" et bouton "*submit command for 1 service*".

25. Configuration des interruptions sur le poste v30e5p001

Le poste v30e5p001 est sous Windows7. Ce système propose un outil pour convertir en interruptions SNMP les messages d'erreur du système et des applications qui sont normalement transmis dans les journaux des évènements. Cet outil se nomme **evntwin.exe**.

Rappel des éléments à superviser :
- conflit d'adresse IP (surtout pour les tests) ;
- disque sur le point d'être saturé.

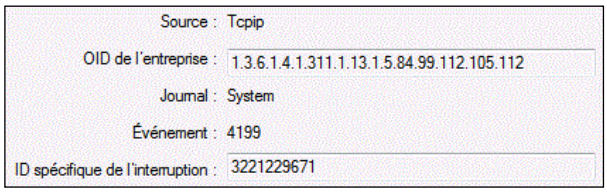
Sur le poste client v30e5p001, dans la zone *Démarrer/"Rechercher les programmes et fichiers",* taper le nom de l'outil evntwin.exe et touche *Entrée*.

Sélectionner *personnalisée* dans Type de configuration et bouton *Modifier*.

Pour récupérer le conflit d'adresse IP :
- Dans la fenêtre sources de l'évènement, développer System et sélectionner Tcpip,
- Dans la fenêtre de droite, Évènements, faire un double clic sur l'évènement N° 4199 :

- Noter l'OID correspondant à cet évènement : (.1.3.6.1.4.1.311.1.13.1.5.84.99.112.105.112)

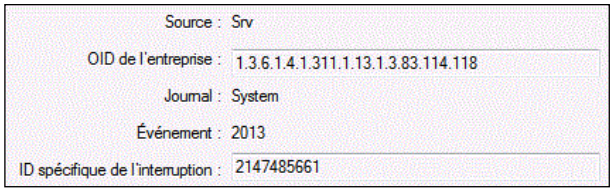
- Bouton *Ok* pour valider.



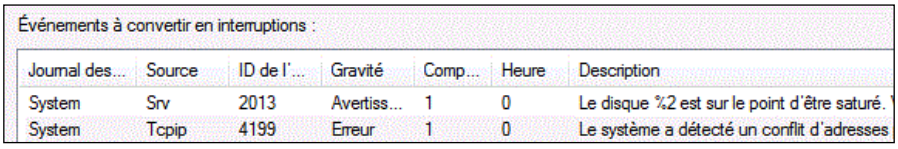
Pour récupérer l'alerte sur le disque :
- Dans la fenêtre sources de l'évènement, développer System et sélectionner Srv,
- Dans la fenêtre de droite, Évènements, faire un double clic sur l'évènement N° 2013 :

- Noter l'OID correspondant à cet évènement : (.1.3.6.1.4.1.311.1.13.1.3.83.114.118)

- Bouton *Ok* pour valider.



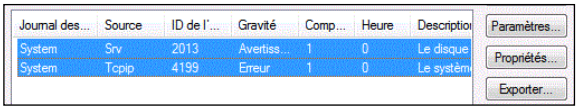
Bouton *Appliquer* :



Bouton *OK* pour fermer le convertisseur d'évènements.

Remarque :
Pour configurer rapidement d'autres postes (avec le même système et les mêmes interruptions), il est possible de sauvegarder cette configuration :

- Sélectionner tous les évènements à convertir en interruptions et bouton *Exporter*…



- Enregistrer le fichier events.cnf.

Le contenu du fichier events.cnf :

```
1  #pragma add "System" "Srv" 2147485661 1 0
2  #pragma add "System" "Tcpip" 3221229671 1 0
```

Pour appliquer ces interruptions SNMP sur d'autres postes à partir de ce fichier events.cnf :
En ligne de commandes, utiliser l'instruction suivante : *evntcmd.exe events.cnf*

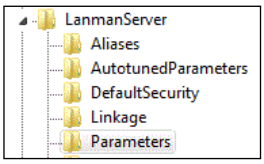
```
C:\>evntcmd.exe events.cnf
Outil de configuration Convertisseur d'événement en interruption Microsoft (R)
Copyright (c) Microsoft Corporation. Tous droits réservés.

[Wrn05] Ligne de commande analysée correctement.
[Wrn05] Fichier de configuration 'events.cnf' analysé correctement.
[Wrn05] Registre connecté à 'localhost'.
[Wrn05] Commandes traitées correctement.
```

Vérifier avec evntwin.exe que les évènements sont bien convertis en interruptions SNMP.

Modification de la base de registre
L'évènement sur le disque de la source Srv nécessite sous Windows7 de modifier la base de registre.
Sur le poste client v30e5p001, dans la zone *Démarrer/"Rechercher les programmes et fichiers*", taper regedit.exe et touche *Entrée*.

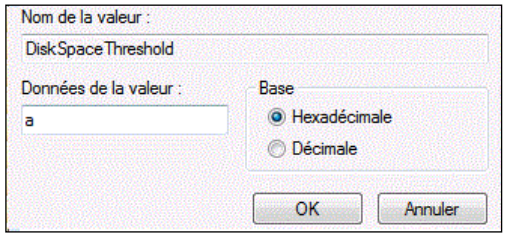
Sélectionner le chemin suivant :
HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters



Il faut ajouter deux nouvelles valeurs DiskSpaceThreshold et LowDiskSpaceMinimum :
- Clic droit, *Nouveau/Valeur DWORD 32 bits*
- Avec le menu *Renommer*, saisir le nom de la valeur : DiskSpaceThreshold
- Clic droit sur ce nom, menu *Modifier*…

- Saisir 'a' dans la zone Données de la valeur :
(Correspond à 10, soit 10%)

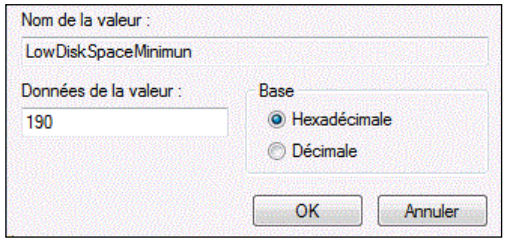
- Bouton *OK*.



- Clic droit, *Nouveau/Valeur DWORD 32 bits*
- Avec le menu *Renommer*, saisir le nom de la valeur : LowDiskSpaceMinimum
- Clic droit sur ce nom, menu *Modifier*…

- Saisir 190 dans la zone Données de la valeur :
(Correspond à 400, soit 400 Mo)

- Bouton *OK*.



Remarque :
Une autre source, nommée eventlog, permet aussi de générer le même évènement N°2013. Mais cette source n'a pas fonctionné pendant les tests.

26. Configuration de SNMPTT pour les interruptions du poste v30e5p001

Cette configuration est valable pour tous les postes fixes de GSB sous Windows7.

26.1 Création d'un fichier de configuration MIB pour SNMPTT

Pour prendre en compte les interruptions des postes sous Windows7, nous allons créer un nouveau fichier nommé : /srv/eyesofnetwork/snmptt/etc/mibs/snmptt.conf.microsoft.txt.

Créer ce fichier (avec vi ou en utilisant FileZilla Client pour créer/copier ce fichier).
Pour la prise en compte des conflits d'adresse IP, ajouter les lignes suivantes :

```
#Trap GSB pour les postes sous Windows7
EVENT ConflitIP .1.3.6.1.4.1.311.1.13.1.5.84.99.112.105.112.* "Status Events" Normal
FORMAT $*
EXEC /srv/eyesofnetwork/nagios/plugins/eventhandlers/submit_check_result $r TRAP-GSB 2 "$r $aA $e $D ip:$7 mac:$8"
SDESC
Conflit adresse IP pour cet hôte
EDESC
#
```

Explications :
Pour prendre en compte toutes les interruptions SNMP issues de l'identifiant (OID) relevé au **25.** (.1.3.6.1.4.1.311.1.13.1.5.84.99.112.105.112), ce dernier est complété par (.*).

Les variables $7 et $8 permettent de récupérer les informations des variable-bindings de la trame TRAP SNMP, comme on peut le voir sur la capture de trame suivante :

```
⊟ trap
    enterprise: 1.3.6.1.4.1.311.1.13.1.5.84.99.112.105.112 (iso.3.6.1.4.1.311.1.13.1.5.84.99.112.105.112)
    agent-addr: 172.16.0.150 (172.16.0.150)
    generic-trap: enterpriseSpecific (6)
    specific-trap: -1073737625
    time-stamp: 1593647
  ⊟ variable-bindings: 8 items
    ⊞ 1.3.6.1.4.1.311.1.13.1.9999.1.0: 4c652073797374e86d6520612064e974656374e920756e20...
    ⊞ 1.3.6.1.4.1.311.1.13.1.9999.2.0: 556e6b6e6f776e
    ⊞ 1.3.6.1.4.1.311.1.13.1.9999.3.0: 77696e37
    ⊞ 1.3.6.1.4.1.311.1.13.1.9999.4.0: 31
    ⊞ 1.3.6.1.4.1.311.1.13.1.9999.5.0: 30
    ⊞ 1.3.6.1.4.1.311.1.13.1.9999.6.0: <MISSING>
    ⊞ 1.3.6.1.4.1.311.1.13.1.9999.7.0: 3137322e31362e302e3130
    ⊞ 1.3.6.1.4.1.311.1.13.1.9999.8.0: 30302d31392d44422d45372d33392d3337
```

$7 et $8 contiennent respectivement l'adresse IP et l'adresse Mac de l'élément en conflit avec notre poste.

Pour la prise en compte de la saturation d'un disque, ajouter les lignes suivantes :

```
EVENT PbDisque .1.3.6.1.4.1.311.1.13.1.3.83.114.118.* "Status Events" Normal
FORMAT $*
EXEC /srv/eyesofnetwork/nagios/plugins/eventhandlers/submit_check_result $r TRAP-GSB 1 "$r $aA $e $D lecteur: $6 lecteur: $7"
SDESC
Disque sur le point d'être saturé, source srv
EDESC
#
```

Explications :
L'identifiant (OID : .1.3.6.1.4.1.311.1.13.1.3.83.114.118) est aussi complété par (.*).
Pour cette interruption, nous avons choisi de définir un niveau d'alerte à 1 (WARNING).

Pour prendre en compte ce nouveau fichier, il faut modifier le fichier de configuration de snmptt : /srv/eyesofnetwork/snmptt/etc/snmptt.ini

Modifier ce fichier (avec vi ou en utilisant FileZilla Client pour récupérer/modifier/replacer ce fichier)

A la fin du document, dans la zone [**TrapFiles**], créer la ligne 617 qui ajoute une référence à notre fichier snmptt.conf.microsoft.txt dans la liste des fichiers de configuration snmptt :

```
613  [TrapFiles]
614  # A list of snmptt.conf files (this is NOT the snmptrapd.conf file).
615  # and filename.  Ex: '/srv/eyesofnetwork/snmpttt/etc/mibs.conf'
616  snmptt_conf_files = <<END
617  /srv/eyesofnetwork/snmptt/etc/mibs/snmptt.conf.microsoft.txt
```

Relancer le service sur le serveur srveon avec l'instruction suivante : *service snmptt restart*

26.2 Tests des interruptions du poste v30e5p001

26.2.1 Test de conflit IP

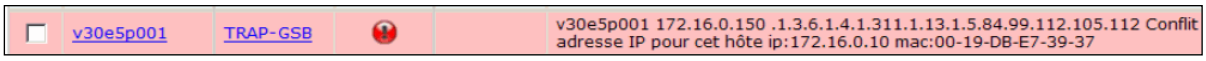
Pour commencer, nous allons tester l'interruption de conflit d'adresse IP à partir du poste v30e5p001.

Sur v30e5p001, ajouter une deuxième adresse IP qui rentre en conflit avec un autre équipement.

- Propriétés de la carte réseau
- protocole Internet version 4 (TCP/IPv4), bouton *Propriétés*
- Bouton *Avancé*…, bouton *Ajouter*…
- Saisir l'adresse IP et le masque, bouton *Ajouter*
- Bouton *OK* trois fois, bouton *Fermer*.

Remarque : Normalement, on obtient une fenêtre d'avertissement de conflit d'adresse IP. Mais si on réalise plusieurs tests identiques, cette fenêtre (et l'interruption SNMP) n'apparait qu'une fois sur deux.

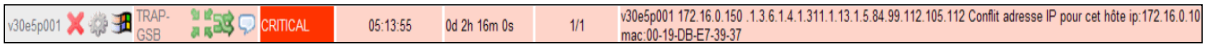
- Résultat dans Nagios :
Menu *Disponibilités, Évènements/évènements actifs*



La description reprend le format défini dans le fichier snmptt.conf.microsoft.txt, avec le nom et l'adresse IP de l'agent SNMP, l'OID, la phrase "Conflit adresse IP pour cet hôte", l'IP et l'adresse MAC de l'équipement en conflit.

Remarque : Pour les tests, l'adresse IP est toujours 172.16.0.150 et non l'adresse 192.168.30.11.

Menu *Disponibilités, Évènements/vue services*



L'état du service TRAP-GSB est bien passé à *CRITICAL*.

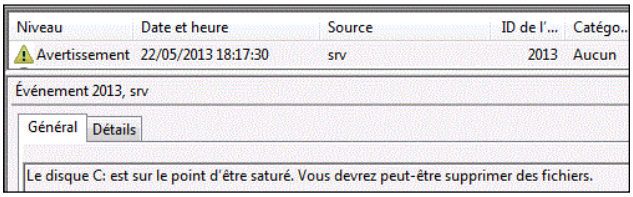
Remettre l'état du service à OK : utiliser le lien de la colonne "*Status*", cocher l'option "*Force Check*" et bouton "*submit command for 1 service*".

26.2.2 Test de saturation de disque

Copier suffisamment de données sur une partition pour que l'espace libre soit inférieur à 10% de sa taille. Redémarrer le poste v30e5p001, l'évènement sur la saturation du disque met un certain temps avant d'être affiché dans l'observateur d'évènements.

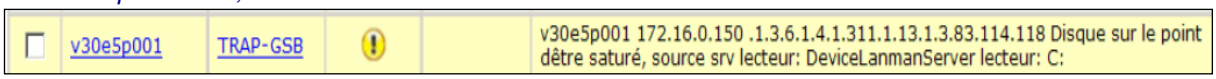
Vérifier l'alerte dans Observateur d'évènements :
- *Panneau de configuration/Outils d'administration/Observateur d'évènements*
- *Journaux Windows/Système*
- Éventuellement, utiliser un filtre sur le journal pour n'afficher que le niveau de type Avertissement :

- Attendre pour voir l'évènement 2013 :



Une fois l'évènement affiché dans l'observateur, on peut vérifier le résultat dans EoN.

- Résultat dans Nagios :
Menu *Disponibilités, Évènements/évènements actifs*



La description reprend le format défini dans le fichier snmptt.conf.microsoft.txt, avec le nom et l'adresse IP de l'agent SNMP, l'OID, la phrase "Disque sur le point d'être saturé …" et le lecteur C.

Menu *Disponibilités, Évènements/vue services*
L'état du service TRAP-GSB est bien passé à *WARNING*.

ANNEXES

ANNEXE 1 : Configurations des commutateurs

Ces configurations sont les modifications à apporter par rapport aux configurations de base du contexte GSB.

Tous les commutateurs sont administrables à partir d'une adresse IP compatible avec le VLAN 10 (Réseau et Système), MUTSYS : 192.168.10.2, SE5_1 (Swich1Etage5) : 192.168.10.11 et MUTLAB : 192.168.10.1.

1.1 Configuration de MUTSYS

Dans la configuration de base, tous les ports sont dans le vlan par défaut et le commutateur ne possède aucune configuration IP.

Création des vlans 10 (Réseau et Système) et 300 (Serveurs) :

```
>enable
#configuration terminal
#(config)vlan 300
#(config-vlan)exit
#(config)vlan 10
#(config-vlan)exit
```

Définition de l'adresse IP sur le vlan 10 :

```
#(config)interface vlan 10
#(config-if)ip address 192.168.10.2 255.255.255.0
#(config-if)no shutdown
#(config-if)exit
```

Définition de la passerelle par défaut :

```
#(config)ip default-gateway 192.168.10.1
```

Affectation des ports 1 à 4 (serveur REZOLAB, serveur de supervision, …) au vlan 300 (Serveurs) :

```
#(config)interface range f0/1 – f0/4
#(config-if-range)switchport access vlan 300
#(config-if-range)exit
```

Étiquetage (mode trunk) du port 5 (port d'interconnexion avec MUTLAB) :

```
#(config)interface f0/5
#(config-if)switchport mode trunk
#(config-if)exit
```

1.2 Configuration de SE5_1 (Swich1Etage5)

Dans la configuration de base, le commutateur ne possède aucune configuration IP.

Création du vlan 10 (Réseau et Système) :

```
>enable
#configuration terminal
#(config)vlan 10
#(config-vlan)exit
```

Définition de l'adresse IP sur le vlan 10 :

```
#(config)interface vlan 10
#(config-if)ip address 192.168.10.11 255.255.255.0
#(config-if)no shutdown
#(config-if)exit
```

Définition de la passerelle par défaut :

```
#(config)ip default-gateway 192.168.10.1
```

Pour le port 1 (port d'interconnexion avec MUTLAB) déjà étiqueté pour les vlans 20, 30, 99, 150 (mode trunk), ajout du vlan 10 :

```
#(config)interface f0/1
#(config-if)switchport trunk allowed vlan 10,20,30,99,150
#(config-if)exit
```

1.3 Configuration de MUTLAB

Dans la configuration de base, le commutateur-routeur possède déjà une adresse IP compatible avec le vlan 10 (192.168.10.1/24) et une table de routage qui permet de communiquer avec tous les vlans.
Le vlan 150 (Visiteurs) peut uniquement interroger les serveurs DNS et DHCP locaux.

Il reste donc à modifier la configuration des ports d'interconnexion et les règles de filtrage pour autoriser les trafics SNMP et ICMP entre le vlan 150 (Visiteurs) et notre serveur de supervision (172.16.0.11).

Pour le port 2 (port d'interconnexion avec MUTSYS), suppression de l'affectation au vlan 300 et étiquetage du port (mode trunk) :

```
>enable
#configuration terminal
#(config)interface f0/2
#(config-if)no switchport access vlan 300
#(config-if)switchport trunk encapsulation dot1q
#(config-if)switchport mode trunk
#(config-if)exit
```

Pour le port 5 (port d'interconnexion avec SE5_1), déjà étiqueté pour les vlans 20, 30, 99, 150 (mode trunk), ajout du vlan 10 :

```
#(config)interface f0/5
#(config-if)switchport trunk allowed vlan 10,20,30,99,150
#(config-if)exit
```

Ajout de nouvelles règles de filtrage dans la liste 101 pour autoriser le trafic ICMP avec le serveur :

```
#(config)access-list 101 permit icmp host 172.16.0.11 192.168.150.0 0.0.0.255
#(config)access-list 101 permit icmp 192.168.150.0 0.0.0.255 host 172.16.0.11
```

Ajout de nouvelles règles de filtrage dans la liste 101 pour autoriser les requêtes SNMP du serveur :

```
#(config)access-list 101 permit udp host 172.16.0.11 192.168.150.0 0.0.0.255 eq snmp
#(config)access-list 101 permit udp 192.168.150.0 0.0.0.255 eq snmp host 172.16.0.11
```

ANNEXE 2 : Le protocole SNMP, les interruptions (traps), les concepts de OID et de MIB
(Adapté de Wikipedia)

Le protocole **SNMP (Simple Network Management Protocol)** permet de contrôler à distance l'état des principaux constituants du réseau.

Sur chaque composant du réseau qui peut être administré – **MN** (*Managed Node*) ou nœud *manageable* (station, serveur, imprimante réseau, concentrateur, commutateur, routeur, onduleur…), nous installons un **agent SNMP**. Cet agent est un programme qui enregistre en permanence certaines informations relatives au composant et les stocke dans une base de données : la **MIB (Management Information Base)**.

La structure de la MIB est hiérarchique : les informations sont regroupées dans une structure arborescente. Chaque information a un **OID (object identifier)**, suite de chiffres séparés par des points, qui l'identifie de façon unique.

Depuis une **station d'administration**, nous pouvons alors interroger chaque nœud *manageable* du réseau, prendre connaissance de son état, consulter les informations (nombre d'octets reçus ou émis...), configurer certaines caractéristiques (interdire l'emploi de tel ou tel port…), etc.

SNMP utilise le modèle client-serveur où le client est représenté par la station d'administration – **NMS (Network Management Station**) ou Manager - qui interroge des serveurs représentés par les agents SNMP implantés sur les nœuds administrables.

Une requête SNMP est un datagramme UDP habituellement à destination du port 161. Dans les versions 1 et 2 du protocole, une requête SNMP contient un nom appelé communauté, utilisé comme mot de passe.

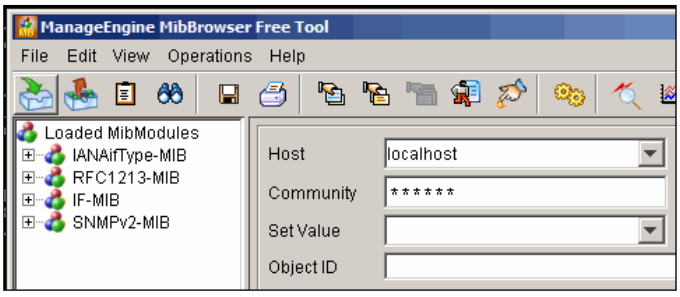
Le protocole SNMP définit aussi un concept **d'interruption** (ou **trap**). Une fois défini, si un certain évènement se produit, comme par exemple le dépassement d'un seuil, l'agent envoie un paquet UDP à un serveur. Ce processus d'alerte est utilisé dans les cas où il est possible de définir simplement un seuil d'alerte. Les interruptions (traps) SNMP sont envoyées en UDP sur le port 162.

ANNEXE 3 : Trouver une variable de la MIB du point d'accès avec l'outil MibBrowser

L'outil utilisé pour parcourir la MIB du point d'accès est MibBrowser de ManageEngine, téléchargeable à l'adresse suivante : http://www.manageengine.com/products/mibbrowser-free-tool/download.html

Cette annexe ne décrit pas toutes les fonctionnalités de cet outil.

Une fois installé, nous obtenons :



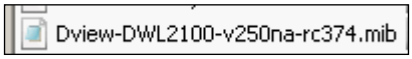
Il faut ajouter la MIB du point d'accès qu'il est possible de télécharger à l'adresse suivante :
http://www.dlink.com.au/tech/download/download.aspx?product=DWL-2100AP

Zone SNMP, fichier nommé : Dview-DWL2100-v250na-rc374.mib

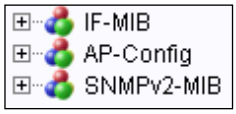
Copier ce fichier dans : C:\Program Files (x86)\ManageEngine\MibBrowser Free Tool\mibs

Arrêter et relancer MibBrowser.
Pour charger la nouvelle MIB, utiliser le bouton "*Load MIB Module*" :

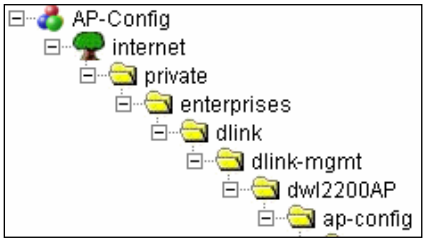
Sélectionner le fichier téléchargé et bouton Ouvrir.



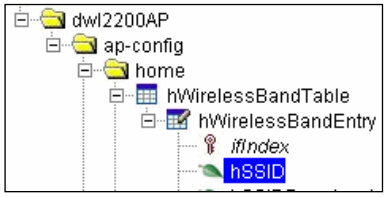
Nous obtenons maintenant un nouveau dossier nommé AP-Config dans la zone "*Loaded MibModules*" :



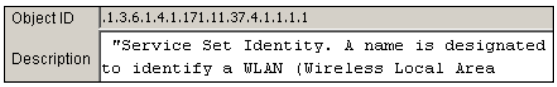
En parcourant AP-Config, nous découvrons que le module téléchargé chez DLINK est spécifique au point d'accès DWL-2200AP :



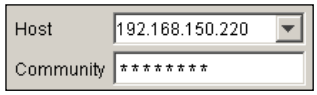
En allant plus loin, nous découvrons la variable qui contient la valeur du SSID :



Dans la zone en bas à droite, nous trouvons l'identifiant (OID) correspondant (.1.3.6.1.4..171.11.37.4.1.1.1.1) :

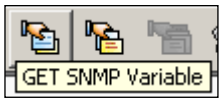


Il est possible de lire le contenu de cette variable avec MibBrowser.
Renseigner les zones Host (192.168.150.220) et Community (**gsbintra**) :

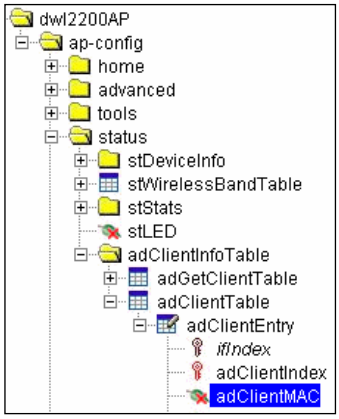


Utiliser les boutons "*Get SNMP Variable*" ou "*GETNEXT SNMP Variable*" :

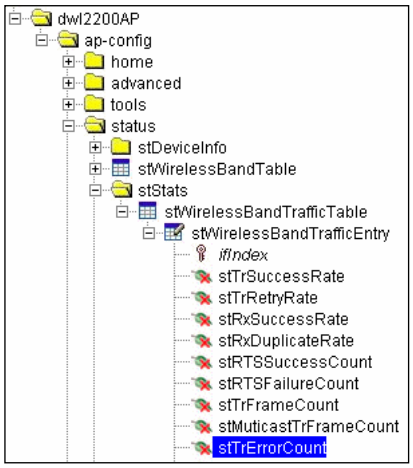
Le résultat s'affiche dans la fenêtre de droite.



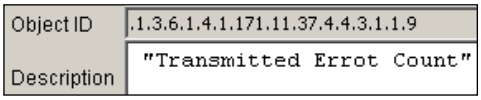
Pour la supervision des visiteurs de GSB, il est possible de trouver la liste des adresses Mac des clients WiFi avec la variable *adClientMac*, mais *adClientIndex* n'est pas accessible pour récupérer le nombre de clients connectés.



Pour les tests de supervision d'un service du point d'accès de GSB, nous allons donc prendre la variable *stTrErrorCount*, qui comptabilise le nombre de transmissions en erreur :



Dans la zone en bas à droite, nous trouvons l'identifiant (OID) correspondant (.1.3.6.1.4.1.171.11.37.4..4.3.1.1.9) :



Remarque : La partie de l'OID 171.11.37 correspond à dlink.dlink-mgmt.dwl2200AP

ANNEXE 4 : Extraits de certains fichiers Nagios de configuration de cette supervision

Les fichiers Nagios de configuration des équipements sont dans le dossier : /srv/eyesofnetwork/nagios/etc/objects/

Il est possible de modifier directement ces fichiers avec un éditeur de texte et de relancer Nagios avec l'instruction suivante : service nagios restart

Pour retrouver ces modifications dans EyesOfNework, il est nécessaire d'utiliser une procédure d'importation, **mais attention**, EyesOfNetwork ne récupère pas les configurations des modèles (templates) (voir annexe 5).

4.1 Le fichier contacts.cfg

Ce fichier contient la configuration des contacts de Nagios. Ici, nous retrouvons l'adresse mail du contact **admin** définie au **5.1**.

```
define contact {
    contact_name    admin
    alias   EyesOfNetwork Administrator
    email   root@srveon.gsbeu.intra
    pager
    host_notifications_enabled  1
    service_notifications_enabled   1
    host_notification_period    24x7
    service_notification_period 24x7
    can_submit_commands 1
    retain_status_information   1
    retain_nonstatus_information    1
    host_notification_options   d,u,r
    service_notification_options    w,c,r
    host_notification_commands  notify-by-email-host
    service_notification_commands   notify-by-email-service
}
```

4.2 Le fichier hosts.cfg

Ce fichier contient tous les équipements créés. Nous retrouvons la configuration de l'équipement **REZOLAB**, définie au **6.1**.

```
114  define host {
115      host_name    REZOLAB
116      check_command    check-host-alive
117      max_check_attempts  2
118      check_interval  4
119      passive_checks_enabled  1
120      check_period    24x7
121      obsess_over_host    0
122      check_freshness 0
123      freshness_threshold 0
124      active_checks_enabled   1
125      notification_interval   0
126      notification_period 24x7
127      notifications_enabled   1
128      failure_prediction_enabled  1
129      action_url  /module/capacity_for_nagios/index.php?ip=$HOSTNAME$
130      icon_image  win40.png
131      vrml_image  win40.png
132      statusmap_image win40.png
133      alias   serveur DHCP/DNS
134      display_name    REZOLAB
135      address 172.16.0.10
136      notification_options    d,u,r
137      stalking_options    d,u
138      contact_groups  admins
139      hostgroups  WINDOWS
140  }
```

4.3 Le fichier services.cfg

Ce fichier contient la définition de tous les services associés aux équipements, comme par exemple le service DHCP-GSB de REZOLAB créé au **11.3**.

```
415  define service {
416      host_name    REZOLAB
417      service_description DHCP-GSB
418      max_check_attempts  4
419      normal_check_interval   4
420      active_checks_enabled   1
421      passive_checks_enabled  1
422      check_period    24x7
423      parallelize_check   1
424      obsess_over_service 0
425      check_freshness 0
426      freshness_threshold 0
427      notification_interval   0
428      notification_period 24x7
429      notifications_enabled   1
430      display_name    DHCP-GSB
431      check_command   check_dhcp_addfree!192.168.150.0!5!2
432      notification_options    w,c,r
433      stalking_options    w,c
434      contact_groups  admins
435  }
```

4.4 Le fichier commands.cfg

Ce fichier contient toutes les commandes Nagios utilisées par les équipements.

Exemples :

- Commande *check_dhcp_addfree* définie au **11.2** :

```
268 define command {
269     command_name    check_dhcp_addfree
270     command_line    perl $USER1$/check_dhcp_addfree -H $HOSTADDRESS$ -C $USER2$ -v 2 -s $ARG1$ -w $ARG2$ -c $ARG3$
271 }
```

- Commande *check_snmp_int_GSB* définie au **16.1** :

```
408 define command {
409     command_name    check_snmp_int_GSB
410     command_line    perl $USER1$/check_snmp_int.pl -H $HOSTADDRESS$ -C $USER2$ -r -n $ARG1$ -k -w 90,90 -c 95,95 -u
411 }
```

- Commande *check_snmp_printer_GSB* définie au **17.4** :

```
413 define command {
414     command_name    check_snmp_printer_GSB
415     command_line    perl $USER1$/check_snmp_printer -H $HOSTADDRESS$ -C $USER2$ -x $ARG1$ -w $ARG2$ -c $ARG3$
416 }
```

4.5 Le fichier hostgroups.cfg

Ce fichier contient la définition des groupes d'hôtes, comme celui nommé CISCO utilisé au **13.3.1**.

```
43  define hostgroup {
44      hostgroup_name  CISCO
45      alias   HostGroup Cisco
46  }
```

4.6 Le fichier servicegroups.cfg

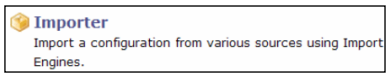
Ce fichier contient la définition des groupes de services, comme le groupe PORTS CISCO défini au **16.2**.

```
28  define servicegroup {
29      servicegroup_name   PORTS CISCO
30      alias   Ports des matériels Cisco
31  }
```

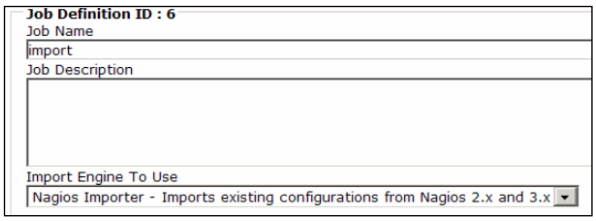
ANNEXE 5 : Procédure d'importation des fichiers Nagios

Menu *Administration, Nagios/configuration* et utiliser le lien *Tools* en haut à droite.

Utiliser le lien *Importer* :

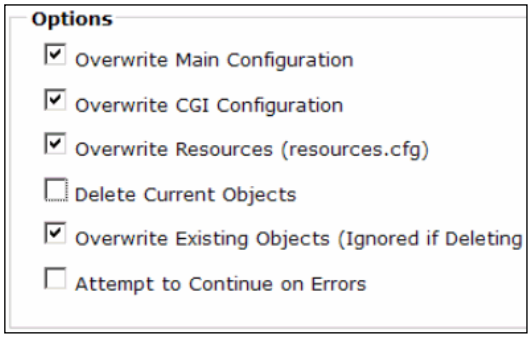


Donner un nom à la procédure et dans la liste déroulante "*Import Engine To Use*", sélectionner une importation à partir de fichiers Nagios :



Dans les options, si nous voulons conserver les modèles définis dans EyesOfNetwork, il est nécessaire de décocher "*Delete Current Objects*" :

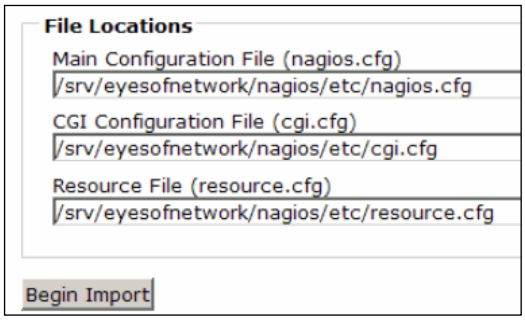
Par contre, même si "*Overwrite Existing Objects*" est coché, les équipements déjà présents dans EyesOfNetwork se retrouvent en double.



IMPORTANT : Il est donc nécessaire de supprimer tous les équipements déjà créés avant de lancer cette procédure.

Définir les chemins des fichiers de configuration :

Bouton "*Begin Import*".



Attendre le message "*Import Job Complet …. Successfully*" :

Table des matières