GAULTIER Baptiste

Rapport de Stage:

Introduction à la supervision réseau sous GNU/Linux

Promotion 2005-2007
I.U.T de Rouen - Département GTR

Remerciements

Je tiens ici à remercier le service « Réseau et Télécommunications » de la Vill
Havre qui m'a accueilli pendant ces deux mois et demi de stage. Cette équip
permis de découvrir le monde de l'entreprise, le travail au sein d'une équipe
contraintes de développement et d'organisation. Toutes ces informations qu
fait de ce stage un enrichissement personnel et professionnel. Tout d'abord,
porte toute ma gratitude à M. Alain Fremont (Ingénieur réseau) sans qui mon
stage n'aurait pu avoir lieu. Je tiens à lui montrer toute ma reconnaissance p
s'être rendu disponible dans une période très difficile. Je tiens également à
remercier M. Jean-Luc Thorel (Responsable de l'équipe Système et Réseau) qui
m'a permis de continuer mon stage dans les meilleures conditions. Un grand
merci à M. Matthieu Clavier (Responsable Sécurité Informatique) pour ses co
et toutes les réponses qu'il m'a apportées. Merci également à M. Sébastien
Henderson, David Tassel, Phillipe Arbe, pour m'avoir accueilli dans leurs locaux et
pour m'avoir apporter support et écoute.

Sommaire

Introduction 1

Présentation réseau VDH

Partie 1: L'outil ntop

Installation de ntop

Compatibilité 4

Mise en place 4

Fonctionnement de ntop

Vue d'ensemble de ntop 5

Description des rubriques du menu 6

Plugins et configuration avancée 13

Partie 2: L'outil Oreon-Nagios

Installation de Oreon-Nagios

Compatibilité 16

Mise en Place 16

Fonctionnement de Oreon-Nagios

Vue d'ensemble de Oreon-Nagios 19

Description de l'outil Oreon-Nagios 20

Conclusion 28

Annexes

Configuration d'un routeur/switch Cisco 29

Architecture du réseau VDH

Glossaire 32

Introduction:

De nos jours, le besoin de surveiller les réseaux informatiques, les ressources réseaux, les
et les postes clients devient grandissant pour des entreprises d'une certaine taille. Or, le
des investissements, parfois prohibitif, dans un système de management de réseaux (net
management system, NMS) freine l'emploi de cet outil.
Dans le cadre du monde de l'Open source*, les solutions sont nombreuses et de bonne qu
Le but de ce stage a donc été de fournir un comparatif et une présentation des différents
produits NMS existants sous GNU/Linux.

Présentation de l'entreprise :

L'entreprise qui m'a accueilli pendant deux mois et demi est la Ville du Havre. J'ai été ass
service « Informatique et Télécommunications » et plus précisément dans la branche « Ré
et Systèmes » (Fig.1). Mon tuteur a été M. Alain Frémont(Ingénieur réseau)pendant près d
mois et demi et M. Jean-Luc Thorel (Responsable sur service « Réseaux et Systèmes ») po
second mois.

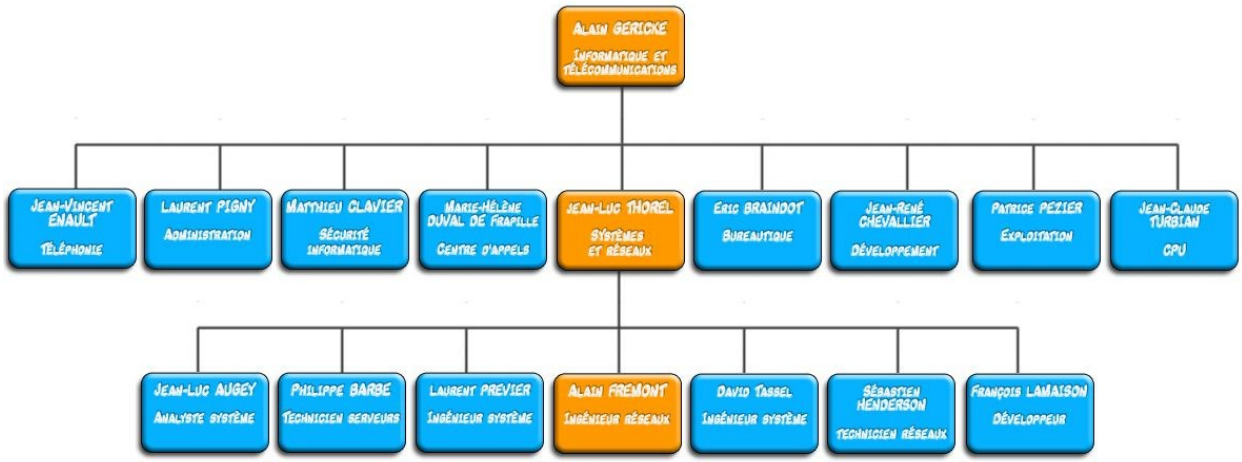


Figure 1 – Organigramme du service

Ce service n'est pas à proprement parler un « service » mais un syndicat, en effet ce synd
gère pas seulement le parc informatique de la Ville du Havre mais également l'infrastruct
informatique de plusieurs villes de la Communauté de l'agglomération Havraise (CODAH)
que des villes extérieurs comme Bolbec et Dieppe. Le « Syndicat Inter-collectivité pour la
Gestion et le Développement d'un Centre Informatique » (SIGDCI) a pour rôle la mise en p
des serveurs centraux (Oracle, WEB...), l'installation de l'infrastructure (routeurs, switches
liaisons lasers, cuivres, BLR...), l'exploitation du parc informatique (installation, assistance
formation, développement...).
La ville du Havre possède un réseau très important de plus de 2100 postes clients et 40 s
inter-connectés par 177 switchs et 184 routeurs (cf. annexe pour une vue d'ensemble de
l'architecture du réseau de la ville du Havre). Les besoins d'une telle entreprise sont donc

et nombreux. Dans le cadre du stage, mon objectif a été dans un premier temps de cherc
outil capable de fournir une vue d'ensemble de ce réseau en donnant à l'administrateur r
les caractéristiques du trafic réseau (hôtes, protocoles...)
Mon tuteur de stage avait déjà mené des recherches sur ce type d'outil et il m'a donc orie
vers les produits suivants: Nagios, cacti, ntop, mrtg... Seuls trois ont retenu mon attentior
par leur facilité d'utilisation, leurs fonctionnalité et leur gratuité. En effet, les produits rete
sont tous open source et correspondent tous aux besoins énoncés précédemment. Le pre
outil est Cacti conçu pour l'analyse de trames SNMP* et la création de graphiques suite à
l'exploitation des trames.
Le second programme est ntop, ce dossier inclut une introduction à ntop.
Le troisième produit est Nagios, une introduction à Nagios (en association avec Oreon) se
également proposée dans ce dossier.

Présentation de l'ou ntop.

ntop (pour Network TOP) est un outil de supervision réseau conçu pour l'observation et l
résolution de problème d'un réseau. C'est une application open source développée par Lu
durant ses études portant sur le réseau à l'université de Pisa (Italie).
La première version de ce logiciel a vu le jour en 1998, la dernière version est la vers. 3.2
d'octobre 2005. Ce programme a pour objectif de produire des informations et des graphi
sur le trafic d'un réseau (comme pourrait le faire la commande unix « top » avec les proce
ntop n'est pas seulement un analyseur TCP/IP, il s'appuie sur une librairie nommée « libpc
lui permettant d'être un analyseur hybride couche 2/couche 3.

Il capture et analyse les trames* d'une interface donnée et permet d'observer une majeu
des caractéristiques du trafic (entrant et sortant) grâce à deux modes de fonctionnement
interface web et un mode texte. L'application ntop est normalement compatible avec tout
plateformes Linux et Unix.
Dans le cadre du stage, ntop a été mis en place sous l'OS* GNU/Linux Debian vers. 3.1 Sa

Nous traiterons donc dans ce dossier de présentation de ntop:
-dans une première partie: l'installation de l'application ntop
-dans une seconde partie: les différentes possibilités de l'application

Présentation de l'ou Nagios

Nagios est une application de monitoring (surveillance) de réseau en temps réel, elle perm
savoir à tout moment le statut des hôtes et des services spécifiés par l'utilisateur. Nagios
charge également de l'envoi d'alertes suite à une panne ou un dysfonctionnement du rés
Nagios permet entre autre:

- La surveillance des services de réseaux (SMTP, POP3, HTTP, NNTP, PING, etc.)
- La surveillance des ressources des hôtes (charge processeur, utilisation du disque,
- Parallélisation de la vérification des services.
- Notifications (alertes) des contacts quand un hôte ou un service a un problème et e

résolu
- Interface web, pour voir l'état actuel du réseau, les notifications et l'historique des problèmes, fichiers log, etc.

Nagios a été conçu pour fonctionner sous Linux, mais des versions win32, MacOS... sont également disponibles. Dans le cadre du stage, nagios a été mis en place sous l'OS* GNU Debian vers. 3.1 Sarge.

Malgré sa puissance et ses fonctionnalités, Nagios n'est pas exempt de défaut. En effet, c logiciel possède l'inconvénient d'être assez difficile à mettre en place et à configurer. L'aj d'hôte et de services n'est pas une tâche aisée car celle-ci doit être faite à la main à l'aid fichiers de configuration. Heureusement, ces tâches fastidieuses peuvent se voir granden allégées grâce à Oreon.

Présentation de l'o

Le projet Oreon est une solution de supervision Open Source basée sur nagios. L'objectif projet est de proposer une nouvelle interface à Nagios, et de lui apporter des fonctionnali nouvelles. Oreon peut s'installer aussi bien dans le cadre d'un déploiement de solution de supervision réseau, que sur un Nagios déjà existant.
Lors de mon stage, Nagios a d'abord été mis en place afin de voir les possibilités offertes logiciel. La configuration de Nagios étant trop fastidieuse, la solution Oreon a été mise en afin d'obtenir plus de facilité dans la configuration.

Remarque: à titre d'information, Oreon est un projet créé et soutenu depuis 2ans par des étudiants parisiens de l'EPITECH.

I.1./ L'outil ntop

a) Compatibilité

Le logiciel ntop est compilable sous toute plateformes Unix. Il existe cependant des paque
pour les OS suivants:
-Linux (Debian, RedHat, Slackware, SuSe...)
-Solaris
-*BSD
-MacOS X
-Win32 (Windows 95 et suivants...)

b) mise en place

Dans cette partie, nous allons traiter de l'installation de ntop sous Debian.
La meilleure façon d'installer le produit ntop est d'utiliser la commande « apt-get ». En plu
trouver, de télécharger et d'installer la dernière version stable du paquet*, la commande
get »permet également d'installer les dépendances* du paquet.
La commande « apt-get » permettra également de mettre à jour et de supprimer des paq
Recherche des paquets ntop à l'aide de la commande « apt-cache search ntop » :

```
sigtestlinux3:/home# apt-cache search ntop
darkstat - a network traffic analyzer
diveintopython - A free Python book for experienced programmers
fpdns - remotely determine DNS server version
ntop - display network usage in top-like format
printop - Graphical interface to the LPRng print system.
python-roman - A module for generating/analyzing Roman numerals
sntop - A curses-based utility that polls hosts to determine connectivity
sigtestlinux3:/home#
```

Une fois le paquet trouvé, il nous suffit d'installer ntop et sa dépendance avec la comman
« apt-get install ntop » :

```
sigtestlinux3:/home# apt-get install ntop
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Les NOUVEAUX paquets suivants seront installés :
  ntop
0 mis à jour, 1 nouvellement installés, 0 à enlever
Inst ntop[5.8.4-8sarge3] (5.8.3-8sarge4 Debian:3.1r2/stable)
sigtestlinux3:/home#
```

ntop est alors installé mais pas encore fonctionnel. Il nous faut tout d'abord définir le mot
passe de l'administrateur avec la commande « ntop -A <password> » ou « ntop --set-adm
password <password>, une fois cette opération effectuée, il est possible de lancer ntop a
script suivant « /etc/init.d/ntop start »

```
sigtestlinux3:/home# ntop -A password
sigtestlinux3:/home# /etc/init.d/ntop start
daemon starting...
ntop
sigtestlinux3:/home#
```

Grâce à ce script, nous demandons ici à ntop de se lancer en mode « démon », c'est à dir
ntop s'exécute en tâche de fond afin de récupérer les données du réseau constamment. D
plus,nous demandons à ntop de fournir un log dans le répertoire syslog (qui nous permett
comprendre les erreurs d'exécution du programme) , enfin nous demandons à ntop de lan
son serveur web (qui va permettre la présentation des résultats) rappelons que ntop intèg
propre serveur web et donc qu'il ne nécessite pas de serveur externe (tel que Apache par
exemple).

Remarque: Il est possible de vérifier le bon fonctionnement de ntop à l'aide de la comman
« ps -ef | grep ntop »:

```
sigtestlinux3:/home# ps -ef |grep ntop
ntop -d -L -u ntop -P /var/lib/ntop --skip-version-check -a
/var/log/ntop/access.log -i eth0 -O /var/log/ntop/ -p
/var/lib/ntop/protocol.list
grep ntop
sigtestlinux3:/home#
```

Voilà donc qui conclue cette partie sur l'installation de ntop, passons donc au fonctionnem
de cet outil.

I.2./ Fonctionnement de ntop

a) Vue d'ensemble de ntop

De base, ntop délivre à un administrateur réseau une grande quantité d'informations sur
réseau. Cependant, les réseaux étant de plus en plus importants et comportant souvent p
sous-réseaux (c'est le cas du réseau VDH) il est préférable d'utiliser ntop en tant que colle
de NetFlow* envoyé par un routeur et/ou un switch (Fig.1).

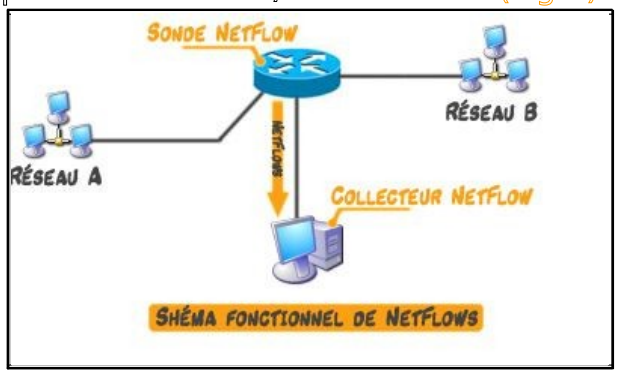


Figure 1 – Fonctionnement de NetFlow

Cette opération permet d'avoir les informations sur l'ensemble des réseaux et sous-réseau
visibles par les sources (switch ou routeur jouant dans ce cas le rôle de sonde NetFlow).
Remarque: se référer à l'annexe « Architecture du réseau VDH » pour l'emplacement de la
sonde NetFlow au sein du réseau Ville du Havre.
Les résultats peuvent être visionnés soit via le mode ligne de commande soit via le l'inter
web accessible par défaut via l'adresse suivante: http://nom_hote:3000/ (Fig.2 - 1)

La page de lancement de ntop est la suivante, elle comporte deux parties : le menu et so
menu situés dans la partie supérieure (Fig.2-2) et la fenêtre de navigation située dans la
inférieure (Fig.2-3):

Figure 2 - Page d'accueil de ntop

b) Description des différentes rubriques du menu

Rubrique « About »:

- About//What's ntop? : renvoie à la page de lancement de ntop qui donne une brève description des fonctionnalités du logiciel.
- About//Configuration : permet de voir la configuration de ntop comportant des informations avec entre autres:
  la version du programme, son processID, la date d'installation, la version de l'OS hô
  l'adresse du serveur web, l'adresse du serveur web sécurisé (si l'option est activée)
  mémoire allouée à ntop et de nombreuses statistiques...

- About//Credits : notes des développeurs et historique du programme ntop.

- About//Man page : manuel de ntop (également disponible avec la saisie de la commande man ntop en mode ligne de commande)

Rubrique « Summary »:

- Summary//Traffic : donne les informations concernant :

- les statistiques globales du trafic (Fig.3-1)
- les proportions des paquets émis en Unicast/Broadcast/Multicast* (Fig.3-2)

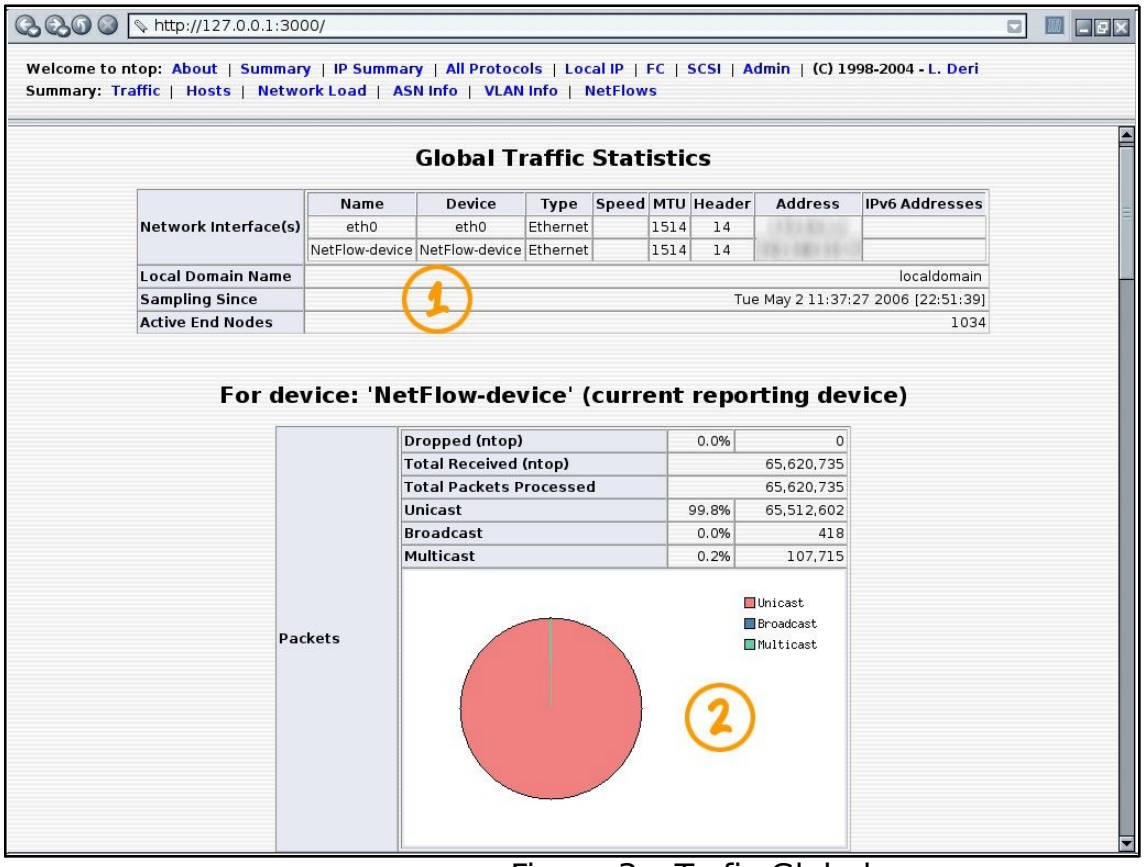


Figure 3 – Trafic Global

- les proportions des protocoles de la couche transport* : TCP/UDP/ICMP
- les proportions des protocoles de la couche application* (Fig.4-3)(http, nbios, mail, ssh, sql...) Remarquenous verrons qu'il est possible de spécifier les protocoles que nous souhaitons voir apparaître(cf. I.2.c.)
- la distribution des ports TCP/UDP* utilisés durant la dernière minute.

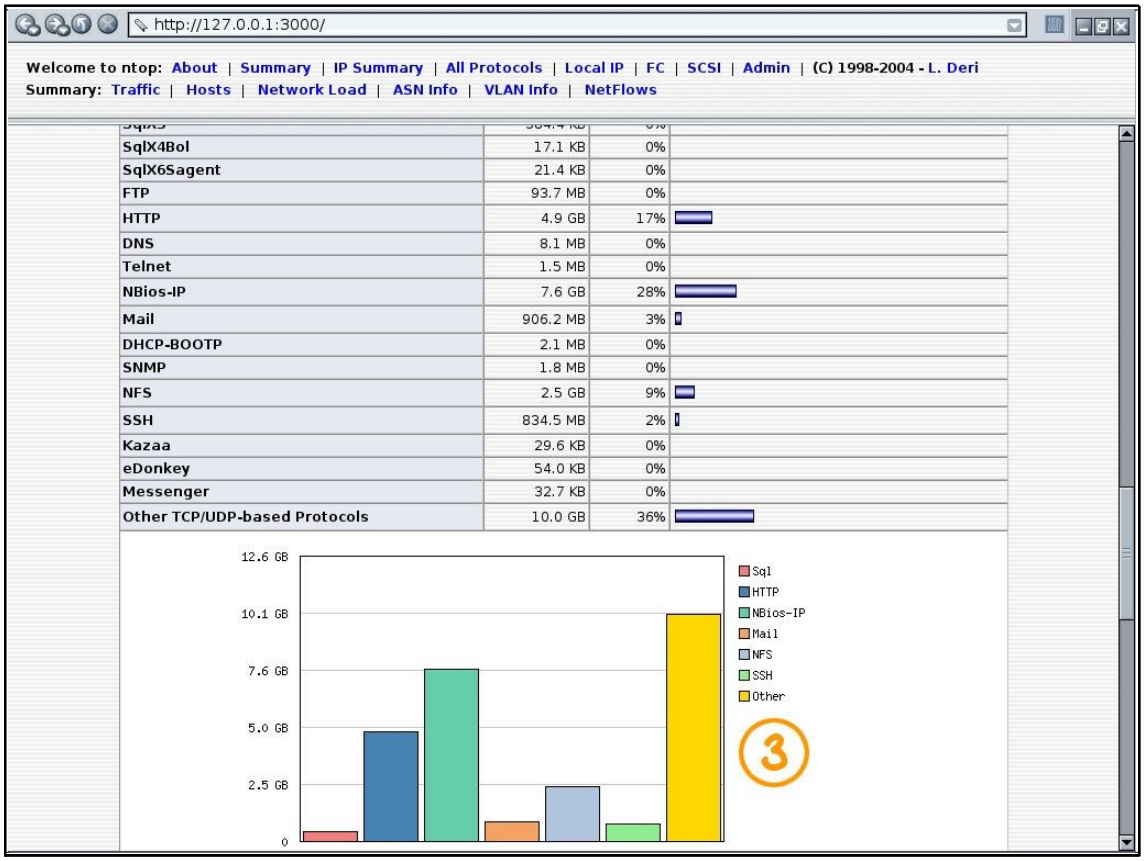
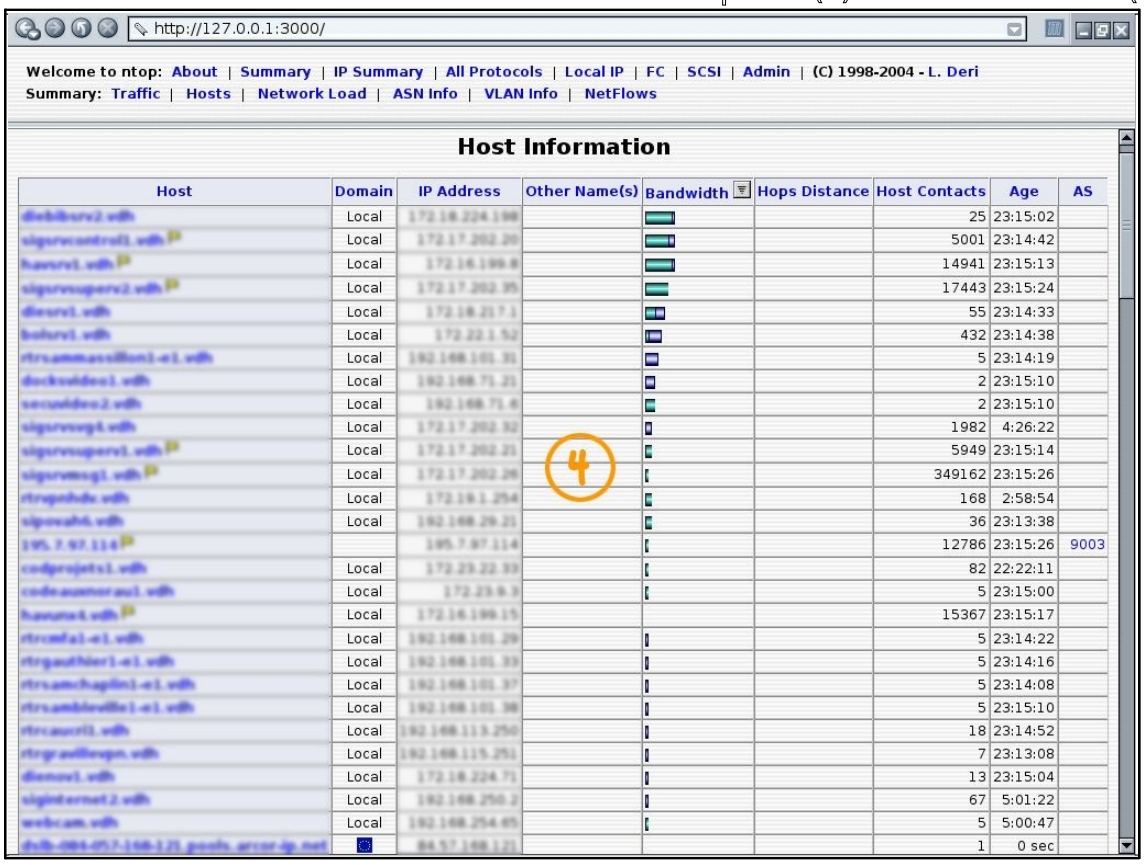


Figure 4 – protocoles IP

- Summary//Hosts : donne une liste de tous les hôtes (locaux et distants) qui effectue des transactions via les réseaux monitorés par le(s) sondes NetFlow (Fig.5-4):



Remarque: Il est possible sur toutes les pages où le nom ou l'adresse d'un hôte est d'obtenir des informations sur cet hôte juste en cliquant dessus, on accède alors au informations qui lui sont propres: son adresse IP, son domaine, son adresse MAC, l'O vendeur, le total des données échangées (Fig.7-1), les graphiques sur son activité a cours du temps (Fig.6-4)(si le plugin* rrd-plugin est activé cf. I.2.c)
Cette page permet également d'obtenir les statistiques de l'hôte au cours de la der journée avec des graphiques (Fig.7-2), les protocoles qu'utilisent l'hôte, les dernière adresses contactées, (Fig.7-3) et enfin les ports concernés.

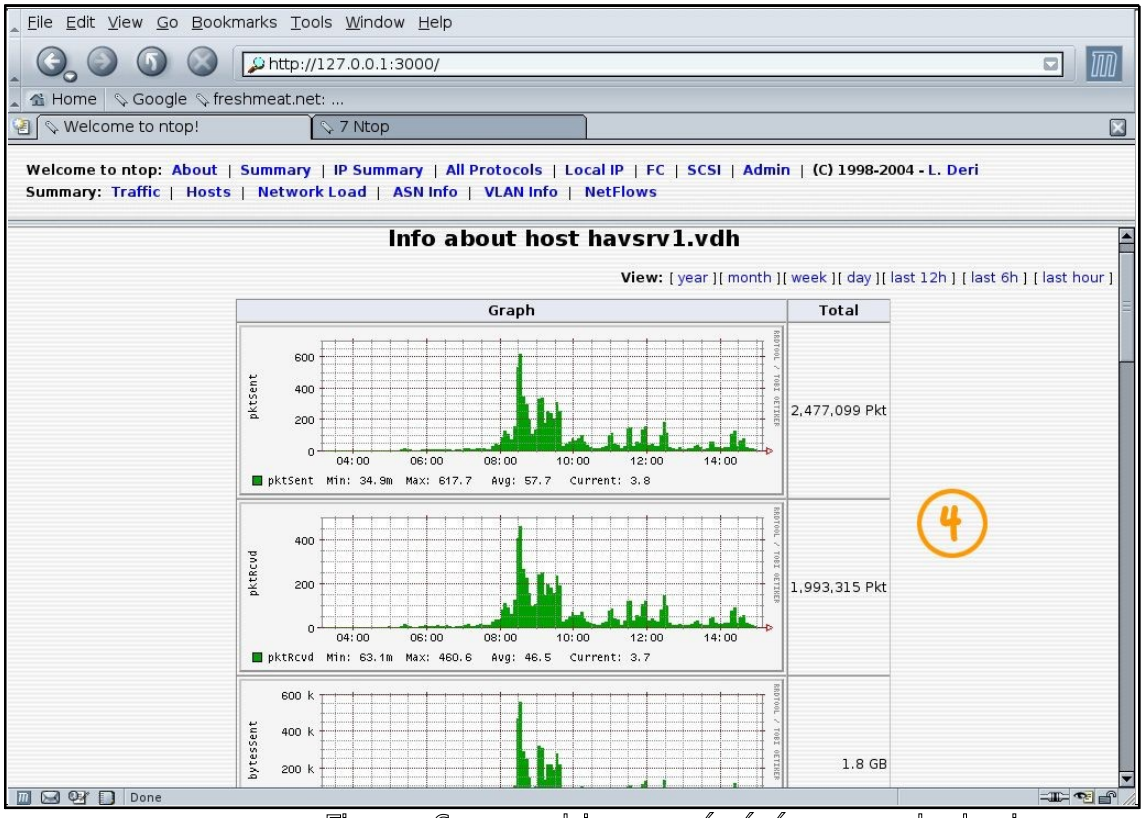


Figure 6 – graphiques générés par rrd_plugin

Welcome to ntop: About | Summary | IP Summary | All Protocols | Local IP | FC | SCSI | Admin | (C) 1998-2004 - L. Deri
Summary: Traffic | Hosts | Network Load | ASN Info | VLAN Info | NetFlows

Info about [redacted]

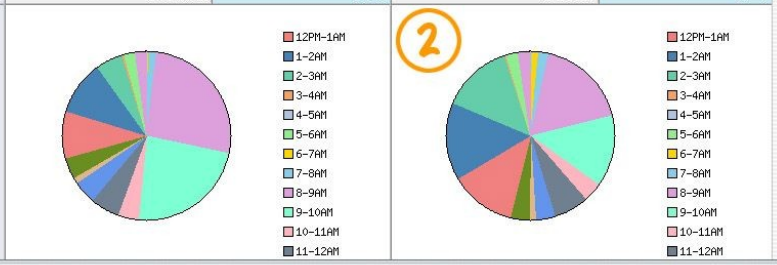
IP Address	[redacted] Local [unicast]
First/Last Seen	Tue May 2 11:37:33 2006 - Wed May 3 11:50:53 2006 [1 day 0:13:20]
Domain	vdh
Host Location	Remote (outside specified/local subnet)
Total Data Sent	2.4 GB/4,169,603 Pkts/0 Retran. Pkts [0%]
Broadcast Pkts Sent	0 Pkts
Data Sent Stats	Local 2.1 % / Rem 97.9 %
IP vs. Non-IP Sent	IP 100 % / Non-IP 0 %
Total Data Rcvd	397.0 MB/3,623,455 Pkts/0 Retran. Pkts [0%]
Data Rcvd Stats	Local 4.2 % / Rem 95.8 %
IP vs. Non-IP Rcvd	IP 100 % / Non-IP 0 %
Sent vs. Rcvd Pkts	Sent 53.5 % / Rcvd 46.5 %
Sent vs. Rcvd Data	Sent 86.0 % / Rcvd 14.0 %
Historical Data	[ ]
Host Healthness (Risk Flags)	1. Suspicious activities: too many host contacts

1

Host Traffic Stats

Time	Tot. Traffic Sent	% Traffic Sent	Tot. Traffic Rcvd	% Traffic Rcvd
11 AM	137.2 MB	5.7 %	26.5 MB	6.8 %
10 AM	98.3 MB	4.1 %	14.7 MB	3.8 %
9 AM	562.8 MB	23.6 %	55.0 MB	14.1 %
8 AM	631.6 MB	26.4 %	68.4 MB	17.6 %
7 AM	36.5 MB	1.5 %	7.6 MB	2.0 %
6 AM	9.3 MB	0.4 %	4.8 MB	1.2 %
5 AM	9.5 MB	0.4 %	2.8 MB	0.7 %
4 AM	801.8 KB	0.0 %	174.3 KB	0.0 %
3 AM	11.3 KB	0.0 %	15.5 KB	0.0 %
2 AM	11.2 KB	0.0 %	15.3 KB	0.0 %
1 AM	11.4 KB	0.0 %	15.5 KB	0.0 %
12 AM	11.2 KB	0.0 %	15.3 KB	0.0 %
11 PM	913.0 KB	0.0 %	124.9 KB	0.0 %
10 PM	748.4 KB	0.0 %	75.8 KB	0.0 %
9 PM	11.5 KB	0.0 %	15.5 KB	0.0 %
8 PM	58.5 MB	2.4 %	8.8 MB	2.3 %
7 PM	2.2 MB	0.1 %	436.8 KB	0.1 %
6 PM	7.8 MB	0.3 %	1.7 MB	0.4 %
5 PM	129.0 MB	5.4 %	53.6 MB	13.8 %
4 PM	247.8 MB	10.4 %	59.2 MB	15.2 %
3 PM	222.9 MB	9.3 %	49.4 MB	12.7 %
2 PM	94.0 MB	3.9 %	14.9 MB	3.8 %
1 PM	32.0 MB	1.3 %	6.2 MB	1.6 %
12 PM	106.9 MB	4.5 %	14.4 MB	3.7 %

Total



2

Last Contacted Peers

Sent To	IP Address	Received From	IP Address
192.168.29.10	192.168.29.10	192.168.29.10	192.168.29.10
172.23.22.25	172.23.22.25	172.23.22.25	172.23.22.25
172.23.22.21	172.23.22.21	172.23.22.21	172.23.22.21
192.168.26.12	192.168.26.12	192.168.26.12	192.168.26.12
172.23.22.4	172.23.22.4	172.23.22.4	172.23.22.4
192.168.35.2	192.168.35.2	192.168.35.2	192.168.35.2
172.23.22.37	172.23.22.37	172.23.22.37	172.23.22.37
172.23.22.30	172.23.22.30	172.23.22.30	172.23.22.30
Total Contacts	8069	Total Contacts	8262

3

TCP/UDP Service/Port Usage

IP Service	Port	# Client Sess.	Last Client Peer	# Server Sess.	Last Server Peer
www	80			90/11.6 KB	172.23.22.8

Fig.7

- Summary//Network Load : uniquement disponible lorsque l'écoute est faite via le po ethernet.

- Summary//ASN Info : donne des informations concernant les ASN contactés par les hôtes avec leurs numéros de système autonome et les volume échangés.

- Summary//VLAN Info : uniquement disponible si la sonde NetFlow qui fournit les informations à ntop est un switch de couche 3 intégrant les VLAN.

Rubrique « IP Summary »:

- IP Summary//Traffic : donne des informations sur les protocoles IP utilisés et sur les volumes échangés par les hôtes. (Fig.8-1)

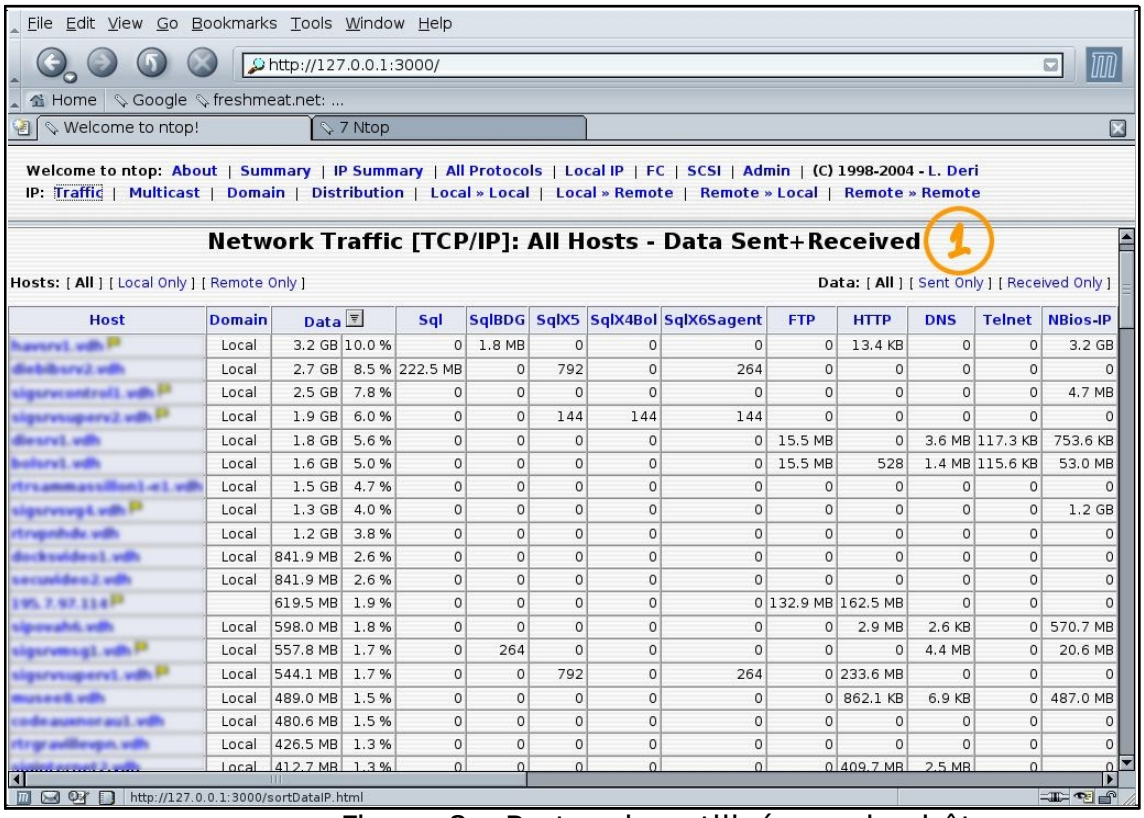
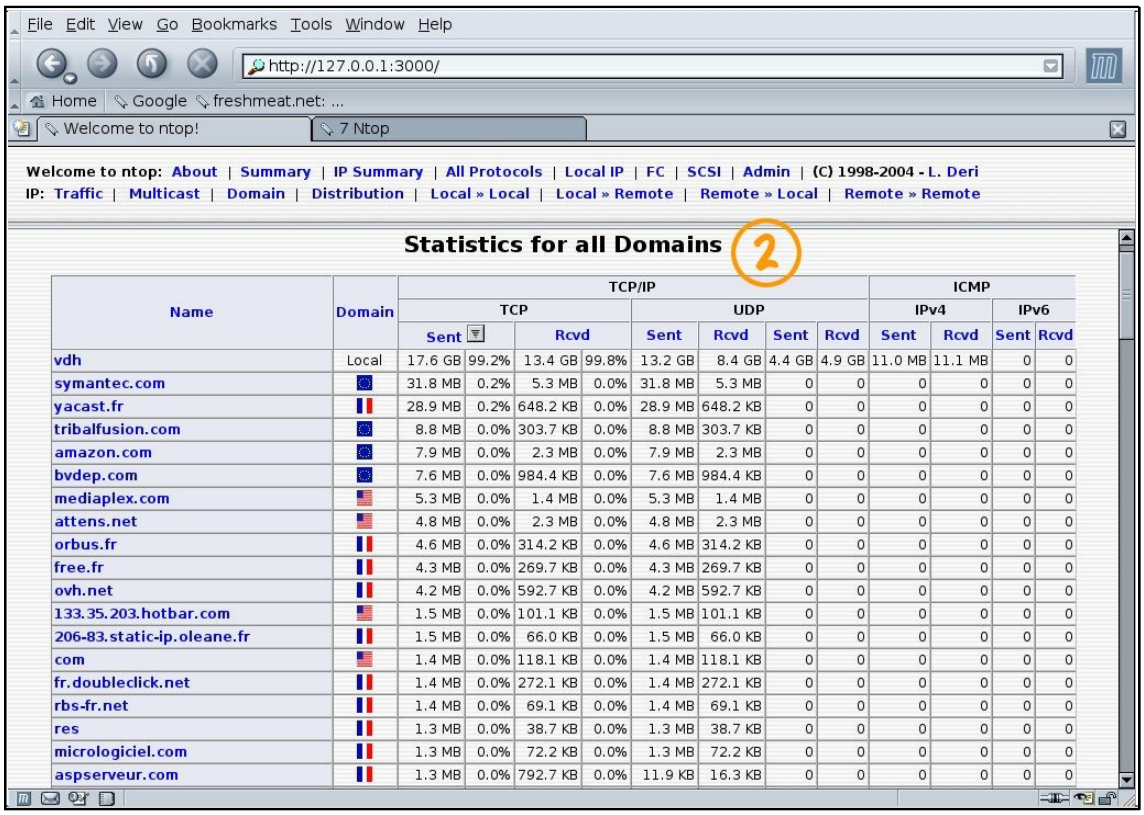


Figure 8 – Protocoles utilisés par les hôtes

- IP Summary//Multicast : fournit une liste des hôtes effectuant du multicast.

- IP Summary//Domain : fournit une liste des noms de domaines ainsi que les volume échangés par ces domaines. (Fig.9-2)



Name	Domain	TCP/IP								ICMP			
		TCP				UDP				IPv4		IPv6	
		Sent		Rcvd		Sent	Rcvd	Sent	Rcvd	Sent	Rcvd	Sent	Rcvd
vdh	Local	17.6 GB	99.2%	13.4 GB	99.8%	13.2 GB	8.4 GB	4.4 GB	4.9 GB	11.0 MB	11.1 MB	0	0
symantec.com		31.8 MB	0.2%	5.3 MB	0.0%	31.8 MB	5.3 MB	0	0	0	0	0	0
yacast.fr		28.9 MB	0.2%	648.2 KB	0.0%	28.9 MB	648.2 KB	0	0	0	0	0	0
tribalfusion.com		8.8 MB	0.0%	303.7 KB	0.0%	8.8 MB	303.7 KB	0	0	0	0	0	0
amazon.com		7.9 MB	0.0%	2.3 MB	0.0%	7.9 MB	2.3 MB	0	0	0	0	0	0
bvdep.com		7.6 MB	0.0%	984.4 KB	0.0%	7.6 MB	984.4 KB	0	0	0	0	0	0
mediaplex.com		5.3 MB	0.0%	1.4 MB	0.0%	5.3 MB	1.4 MB	0	0	0	0	0	0
attens.net		4.8 MB	0.0%	2.3 MB	0.0%	4.8 MB	2.3 MB	0	0	0	0	0	0
orbus.fr		4.6 MB	0.0%	314.2 KB	0.0%	4.6 MB	314.2 KB	0	0	0	0	0	0
free.fr		4.3 MB	0.0%	269.7 KB	0.0%	4.3 MB	269.7 KB	0	0	0	0	0	0
ovh.net		4.2 MB	0.0%	592.7 KB	0.0%	4.2 MB	592.7 KB	0	0	0	0	0	0
133.35.203.hotbar.com		1.5 MB	0.0%	101.1 KB	0.0%	1.5 MB	101.1 KB	0	0	0	0	0	0
206-83.static-ip.oleane.fr		1.5 MB	0.0%	66.0 KB	0.0%	1.5 MB	66.0 KB	0	0	0	0	0	0
com		1.4 MB	0.0%	118.1 KB	0.0%	1.4 MB	118.1 KB	0	0	0	0	0	0
fr.doubleclick.net		1.4 MB	0.0%	272.1 KB	0.0%	1.4 MB	272.1 KB	0	0	0	0	0	0
rbs-fr.net		1.4 MB	0.0%	69.1 KB	0.0%	1.4 MB	69.1 KB	0	0	0	0	0	0
res		1.3 MB	0.0%	38.7 KB	0.0%	1.3 MB	38.7 KB	0	0	0	0	0	0
micrologiciel.com		1.3 MB	0.0%	72.2 KB	0.0%	1.3 MB	72.2 KB	0	0	0	0	0	0
aspserveur.com		1.3 MB	0.0%	792.7 KB	0.0%	11.9 KB	16.3 KB	0	0	0	0	0	0

Figure 9 – Domaines

- IP Summary//Distribution : permet de voir sous forme graphique la part de trafic ent face au trafic sortant.

- IP Summary//Local>>Remote : permet de voir en détails les hôtes qui émettent du sortant.

- IP Summary//Remote>>Local : permet de voir en détails les hôtes qui émettent du entrant.

Rubrique « All Protocols »:

- All Protocols//Traffic : donne des informations sur les protocoles de couche 3 (réseau utilisés et sur les volumes échangés par les hôtes.

- All Protocols//Throughput : donne des informations sur le débit utilisé par les hôtes avec le débit courant, le débit moyen et le maximum observé.

- All Protocols//Activity : donne des informations sur le trafic mesurés pour chaque hô selon l'heure de la journée. (Fig.10-1)

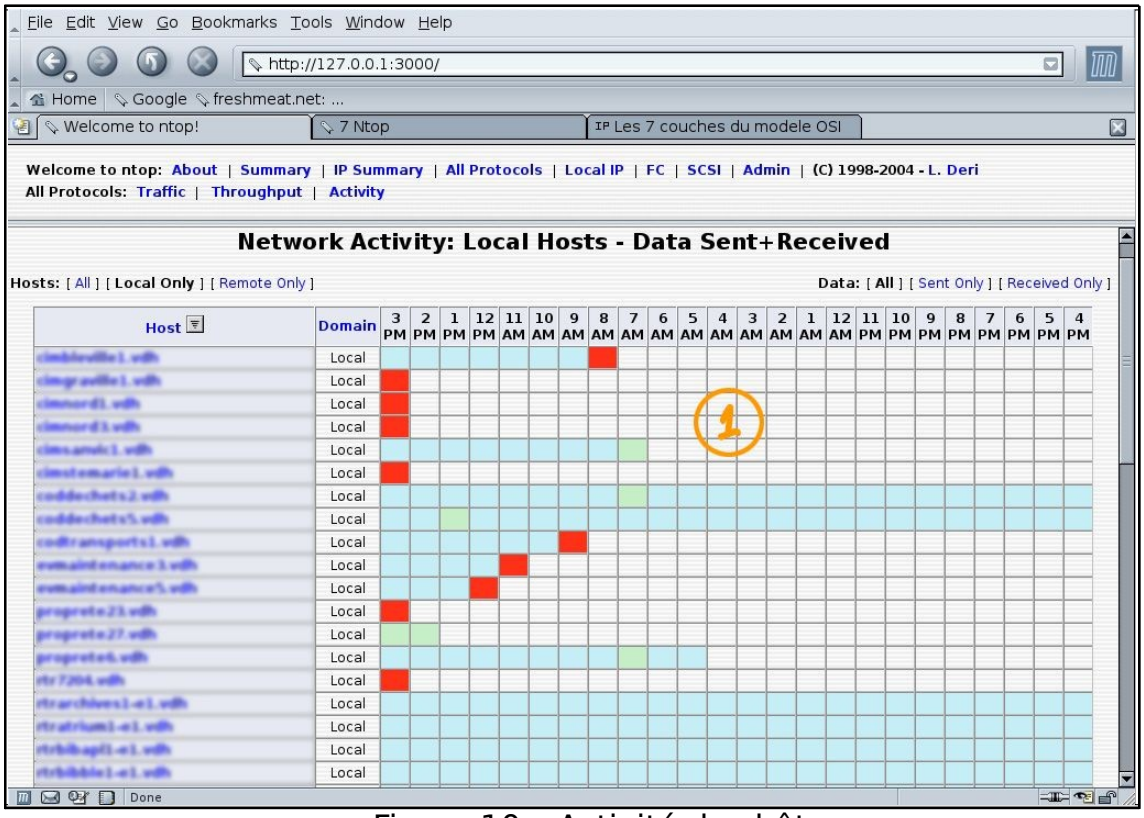


Figure 10 – Activité des hôtes

Rubrique « Local IP »:

- Local IP//Ports used : donne une liste des services/ports utilisés par les serveurs et l clients locaux.

- Local IP//Local Matrix: fournit une liste des 6machines locales qui ont reçu ou envoy plus de trafic à travers le du réseau.

c) Plugins et configuration avancée

Dans cette partie, nous allons traiter des moyens mis en place lors du stage pour amélior résultats et aller plus loin dans la configuration de ntop pour se rapprocher au mieux des de l'utilisateur:

a. Plugins

Le lancement et la configuration des plugins se fait via le menu Admin//Plugins.
Dans le cadre du stage, le nombre de réseaux et de sous réseaux étant trop important po utiliser ntop en standard (écoute du réseau avec la carte ethernet), il nous a fallu paramé ntop pour une utilisation en tant que collecteur de NetFlow.
Pour ce faire, il a fallu dans un premier temps configurer le plugin. Cette configuration du plugin se fait en cliquant sur le nom du plugin (Fig.11-1)
L'activation du plugin se fait en cliquant sur 'active' (Fig.11-2)

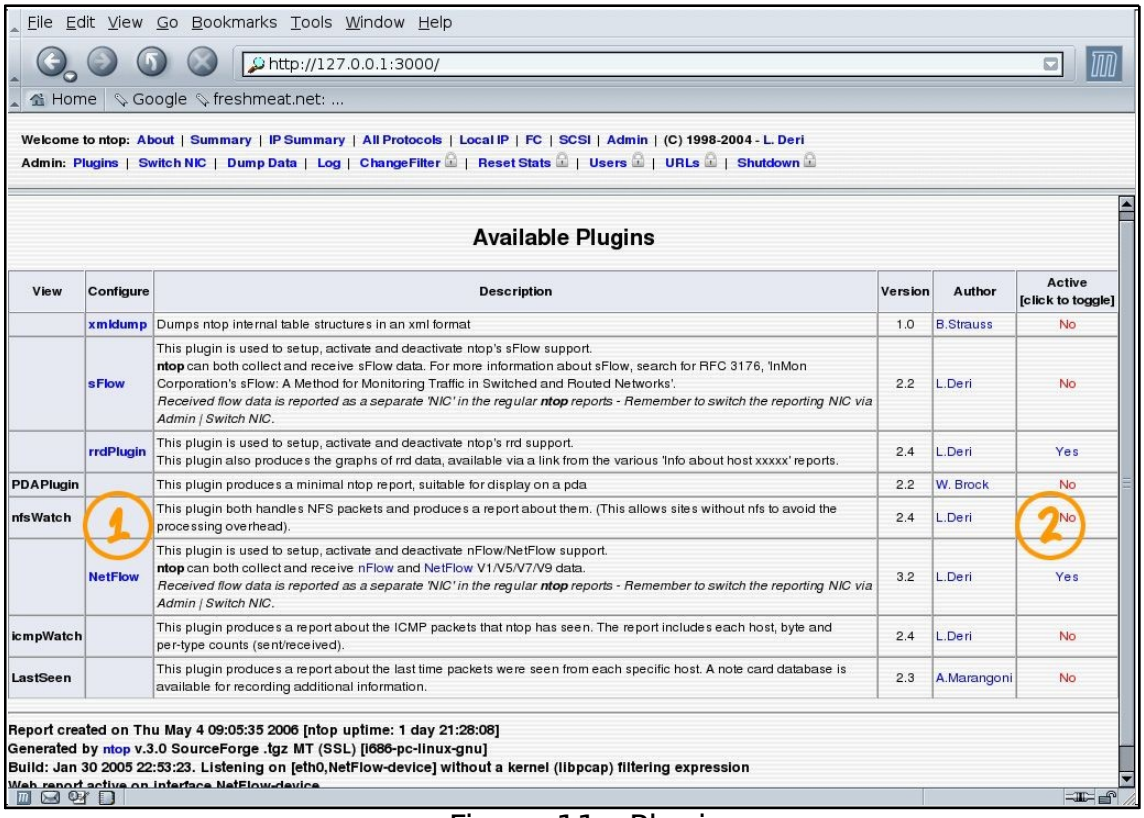


Figure 11 - Plugins

Les informations à renseigner sont les suivantes:

- Port de collecte NetFlow : par défaut 2055 mais n'importe quelle valeur peut être employé lors de la configuration de la sonde NetFlow. (cf. annexe)
- Adresse du réseau où se situe la sonde NetFlow : par exemple 192.168.0.0/24 cette information permet de savoir quelles adresses sont locales et quelles adresses sont distantes.
- Format des NetFlow : permet de spécifier comment va être interpréter la trame Net (défaut= no aggregation).
- Filtrage : permet de spécifier les adresses des sondes à exclure et à inclure pour la des NetFlows.
- Debug: permet d'activer ou de désactiver le debugage dans le log standard de ntop disponible dans le menu Admin//Log

La partie « Flow Statistics » permet de consulter le nombre de flows émis, traités, la versi flows... Une fois le plugin NetFlow configuré et activé, il reste à changer l'interface d'écou le menu Admin//Switch NIC et sélectionner alors l'interface nommée « NetFlow-device ».

De la même façon, il a été nécessaire pour le stage de mettre en place un suivi graphique l'activité des hôtes. Pour ce faire, il nous a fallu paramétrer et activer le plugin « rrdPlugin configuration et les informations à renseigner sont:

- Dump Interval : permet de spécifier l'interval de temps avant que la sauvegarde soi de façon permanente (en secondes).
- Dump Hours : idem (en heures).
- Dump Days : idem (en jours).

- Dump Months : idem (en mois)
- Hosts Filter : permet de spécifier si la sauvegarde doit porter sur tous les hôtes ou seulement sur certains d'entre eux. (défaut=any)

b. Configuration avancée

Pour les besoins du stage, il a fallu dans un premier temps configurer ntop pour qu'il joue de collecteur NetFlow. Puis dans un second temps, adapter ntop au besoin de l'entreprise effet, ntop possède par défaut une liste de protocoles par défaut avec lequel il créé ses g cependant l'entreprise utilisant des protocoles spécifiques non pris en compte par défaut, a fallu modifié la liste de protocoles. La mise en place de la nouvelle liste de protocoles s la manière suivante:

- Créer le fichier contenant la liste des protocoles nommé protocol.list dans le réperto /var/lib/ntop/ de la manière suivante: <nom_protocol>=<numéro_port>|<nom_serv La syntaxe est disponible dans la man page.

```
sigtestlinux3:/# cd /var/lib/ntop
sigtestlinux3:/var/lib/ntop# touch protocol.list
sigtestlinux3:/var/lib/ntop# vi protocol.list
Sql=1521
SqlBDG=1522
SqlX5=1525
FTP=ftp|ftp-data
HTTP=http|www|https|3128
DNS=name|domain
Telnet=telnet|login
NBios-IP=netbios-ns|netbios-dgm|netbios-ssn
Mail=pop-2|pop-3|pop3|kpop|smtp|imap|imap2
DHCP-BOOTP=67-68
SNMP=snmp|snmp-trap
NNTP=nntp
NFS=mount|pcnfs|bwnfs|nfsd|nfsd-status
X11=6000-6010
SSH=22
Gnutella=6346|6347|6348
Kazaa=1214
eDonkey=4661-4665
Messenger=1863|5000|5001|5190-5193
sigtestlinux3:/var/lib/ntop#
```

- Activer les options de démarrage de ntop, pour cela modifier le fichier /etc/default/n

```
sigtestlinux3:/home# vi /etc/default/ntop
# This file will normally include the debconf template but you can disable
# that and use this file only.

./var/lib/ntop/init.cfg
GETOPT= "-p /var/lib/ntop/protocol.list"
sigtestlinux3:/home#
```

- Une fois effectuer cette opération, relancer ntop grâce à la commande « ntop restar

```
sigtestlinux3:/home# cd /etc/init.d
sigtestlinux3:/home# ntop restart
Stopping daemon...
Starting daemon...
ntop
sigtestlinux3:/home#
```

ntop tiendra alors compte des protocoles situés dans protocol.list.
Voilà qui conclue cette partie sur la configuration avancée de ntop.

II.1./ Installation de Oreon-Nagios

a) Compatibilité

Nagios a été prévu à l'origine pour fonctionner et être compilé sous Linux, toutefois il dev
fonctionner également sous les autres Linux. La communauté Oreon a effectué les tests s
distributions suivantes: RedHat, Mandriva, SuSe, Debian, Gentoo, Ubuntu...

b) Mise en place

Malgré la disponibilité de Nagios sous la forme de paquet. L'installation du programme n'e
aisée car celle-ci nécessite l'installation d'un serveur LAMP*. En effet, Nagios dispose d'ur
interface web basé sur l'association PHP/MySQL mais ne possède pas de serveur intégré e
nécessite donc l'installation d'un serveur http (de préférence apache). Nous verrons donc
cette partie l'installation du couple Oreon-Nagios sur une machine tournant sous Debian:

- Installation du serveur web: Apache dans sa version 2
  Remarque: comme pour l'installation de ntop, la commande pour l'installation de paquet « apt-get » a été utilisée. Rappelons qu'il est possible de mettre à jour la list paquets disponibles à l'aide de la commande « apt-update ». Installation de apache de sa dépendance avec la commande « apt-get install apache2 »

```
sigtestlinux3:/home# apt-get install apache2
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Les NOUVEAUX paquets suivants seront installés :
  apache2   apache2-common
[...]
sigtestlinux3:/home#
```

- Installation des premiers paquets nécessaire à la compilation (gcc et g++) et à l'installation (sudo et make) des paquets Oreon et Nagios.

```
sigtestlinux3:/home# apt-get install gcc make sudo g++
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Les NOUVEAUX paquets suivants seront installés :
  gcc  make  sudo  g++
[...]
sigtestlinux3:/home#
```

- Installation de la base de données MySQL dans sa version 4.1

```
sigtestlinux3:/home# apt-get install mysql-server-4.1
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Les NOUVEAUX paquets suivants seront installés :
  mysql-server-4.1 mysql-common files
[...]
sigtestlinux3:/home#
```

- Installation des composants PHP4
  Remarque: La version 5.x de PHP n'est supporté qu'à partir de la version 1.3 d'Oreo
  (version non stable à l'heure où je rédige ces lignes)

```
sigtestlinux3:/home# apt-get install php4 php4-gd php4-cgi php4-mysql php4-snmp libapache2-mo
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Les NOUVEAUX paquets suivants seront installés :
  php4  php4-gd  php4-cgi  php4-mysql  php4-snmp  libapache2-mod-php4
[...]
sigtestlinux3:/home#
```

- Installation de Nagios
  Pour installer Nagios, il existe deux méthodes: soit télécharger les codes sources et
  compiler grâce au paquetage Oreon, soit utiliser la commande « apt-get ». L'avanta
  la première méthode est d'être totalement automatisée cependant cette méthode
  possède aussi le défaut de ne pas installer l'interface web de Nagios mais uniquem
  celle de Oreon.

  - Méthode 1: installation via le paquetage Oreon

    Le paquetage est disponible sur le site officiel du projet Oreon sous forme d'u
    tarball à l'adresse suivante: http://www.oreon-project.org
    Reste à décompresser l'archive et lancer le script d'installation

```
sigtestlinux3:/tmp# tar xzf install_nagios_by_oreon-v0.3.tar.gz && cd install_nagios_by_oreon
sigtestlinux3:/tmp/install_nagios_by_oreon-v0.3# ./install
```

    Le script propose alors d'installer les utilitaires nécessaire à Nagios (rrdtool, n
    snmp, gd...)
    Remarque: une erreur s'est glissé dans le script de lancement situé dans
    /etc/init.d/nagios, à la ligne commençant par « su -l », supprimer le -l.

  - Méthode 2: installation via la commande « apt-get »

    Comme pour ntop, un paquetage Debian Nagios existe:

```
sigtestlinux3:/# apt-get install nagios-text nagios-plugins
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Les NOUVEAUX paquets suivants seront installés :
  nagios-text  nagios-plugins  nagios-common
[...]
sigtestlinux3:/#
```

    reste à installer les utilitaires nécessaire à Nagios:

```
sigtestlinux3:/# apt-get install lib-gd rrdtool
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Les NOUVEAUX paquets suivants seront installés :
  nagios-text  nagios-plugins  nagios-common
[...]
sigtestlinux3:/#
```

- Installation de Oreon
  L'installation de Oreon se fait après celle de Nagios puisque Oreon est une interface améliorée basée sur Nagios et que ce produit ne peut fonctionner sans la base Nag
  L'installation se fait sous la forme d'un script téléchargable à l'adresse suivante:
  http://www.oreon-project.org/download-oreon-fr.html
  Remarque: à l'heure où je rédige ces lignes, la dernière version stable est la 1.2.2
  Reste à décompresser l'archive et à lancer le script d'installation:

```
sigtestlinux3:/tmp# tar xzf oreon-1.2.2.tar.gz && cd oreon-1.2.2
sigtestlinux3:/tmp/oreon-1.2.2# install_nagios_by_oreon-v0.3# ./install
```

  Enfin, il ne reste plus qu'à installer les paquets optionnels à Oreon
  - Installation de nmap: outil qui permettra de découvrir de nouveaux hôtes dan Oreon

```
sigtestlinux3:/# apt-get install nmap
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Les NOUVEAUX paquets suivants seront installés :
  nmap
[...]
sigtestlinux3:/#
```

  - Installation des composantes graphiques d'Oreon:

```
sigtestlinux3:/# apt-get install librrds-perl libgd-gd2-perl wget
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Les NOUVEAUX paquets suivants seront installés :
  librrds-perl libgd-gd2-perl wget
[...]
sigtestlinux3:/#
```

  - Installation des composants qui seront utilisés par les sondes écrites en perl

```
sigtestlinux3:/# apt-get install libnet-snmp-perl
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Les NOUVEAUX paquets suivants seront installés :
  libnet-snmp-perl
[...]
sigtestlinux3:/#
```

  - Finition:
    supprimer le fichier oreon.conf du dossier apache2 car il utilise le même alias

```
sigtestlinux3:/# rm /etc/apache/conf.d/oreon.conf
sigtestlinux3:/#
```

    Redémarrage des services Oreon-Nagios

```
sigtestlinux3:/# cd /etc/init.d
sigtestlinux3:/etc/init.d# apache2 restart
sigtestlinux3:/etc/init.d# mysql restart
sigtestlinux3:/etc/init.d# ./nagios restart
```

    Dès lors, l'interface web Oreon est accessible à l'adresse: http://IPserverOreon/oreon avec IPServerOreon=adresse IP ou hostname du serveur Oreon. Si ce n'est pas le cas, vérifier que Nagios est bien actif grâce commande « ps-ef | grep nagios ».

- Installation « Web Setup » de Oreon
  Au premier lancement d'Oreon, un assistant d'installation permet de finaliser l'installation d'Oreon:

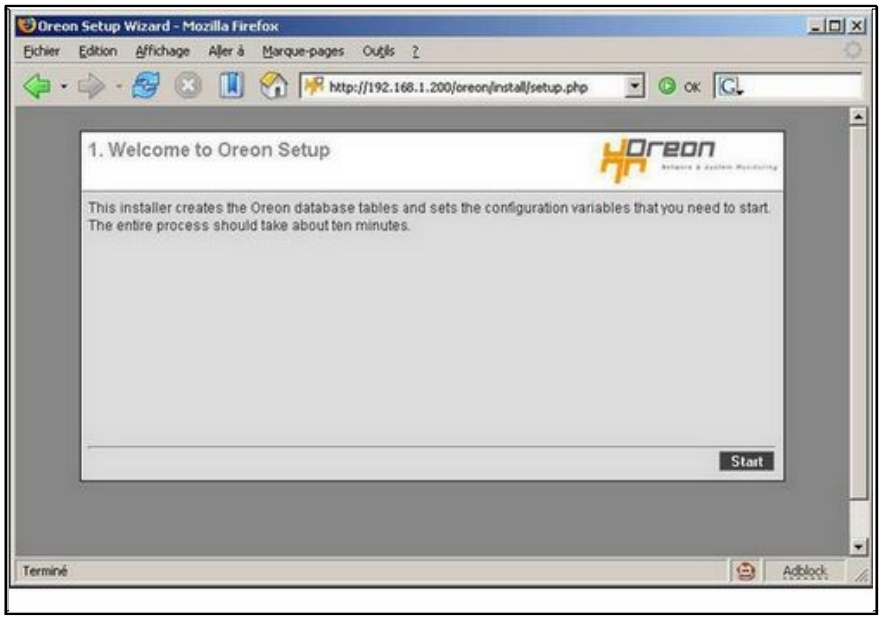


Figure 1 – Web setup de Oreon

  Suivre les instructions pour finaliser l'installation de Oreon et son intégration à MyS

- A la fin de cette installation, la suppression du répertoire d'installation de Oreon po une raison de sécurité

```
sigtestlinux3:/# rm -Rf /usr/local/oreon/install
sigtestlinux3:/#
```

Voilà qui clôture donc la partie sur l'installation de Oreon-Nagios.

II.2./ Fonctionnement de Oreon-Nagios

a) Vue d'ensemble de Oreon-Nagios

Dans un premier temps, il est indispensable de remarquer que Oreon-Nagios n'offre en rie même services que ntop. En effet, ntop fournit des informations quand au trafic et aux protocoles utilisés par les hôtes d'un réseau informatique. Cependant ntop n'indique en ri statut des hôtes, leurs disponibilité, les problèmes rencontrés sur les ressources réseaux. ce type de besoin qu'intervient le couple Oreon-Nagios, le rôle de ce produit sera donc de fournir à l'administrateur un rapport sur l'ensemble des ressources de son réseau.
Ces deux outils ne sont en aucun cas redondants mais plutôt complémentaire.
Comme on a pu le dire précédemment, les services offerts par ntop et Oreon-Nagios sont différents, leurs mode de fonctionnement l'est également. Effectivement, l'interrogation d équipements du réseau s'effectue grâce à des requêtes ICMP et des requêtes SNMP afin d les rapports le plus complet possible. Les équipements pouvant être intégrés à Oreon-Nag

sont tous les équipements qui possèdent une adresse IP fixe. Il sera préférable que les périphériques supportent le protocole SNMP afin d'offrir des rapports plus détaillés. La possibilité d'utiliser des agents de surveillance sur les serveurs comme par exemple NS_c également possible et pris en charge par Oreon-Nagios.

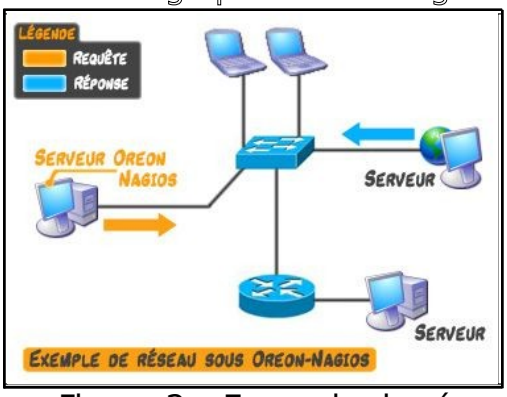


Figure 2 – Exemple de réseau

Dans le cas de la figure 2, nous avons installé Oreon-Nagios sur un serveur Oreon-Nagios. fois le paramétrage effectué, le serveur va alors s'assurer de l'activité des ressources du r (switchs, routeurs, firewalls, serveurs, postes clients, etc.) en envoyant des requêtes ICMP (ping*), l'hôte interrogé va alors répondre. Il sera également possible, dans un second ter selon les besoins de l'administrateur qu'Oreon-Nagios se charge d'interroger les machines des critères définis par l'administrateur (charge processeur, occupation des disques, trafic des interfaces, etc.) L'outil Oreon-Nagios permet donc à l'administrateur réseau de connaî temps réel l'état de son réseau et les problèmes rencontrés.

b) Description de l'outil Oreon-Nagios

L'interface web de Oreon-Nagios est accessible à l'adresse http://nom_hote/oreon. On arri alors sur la page d'identification. Reste à se loguer (le login par défaut étant 'Admin'). La p d'accueil permet d'avoir un compte rendu de l'état du réseau (Fig.3).

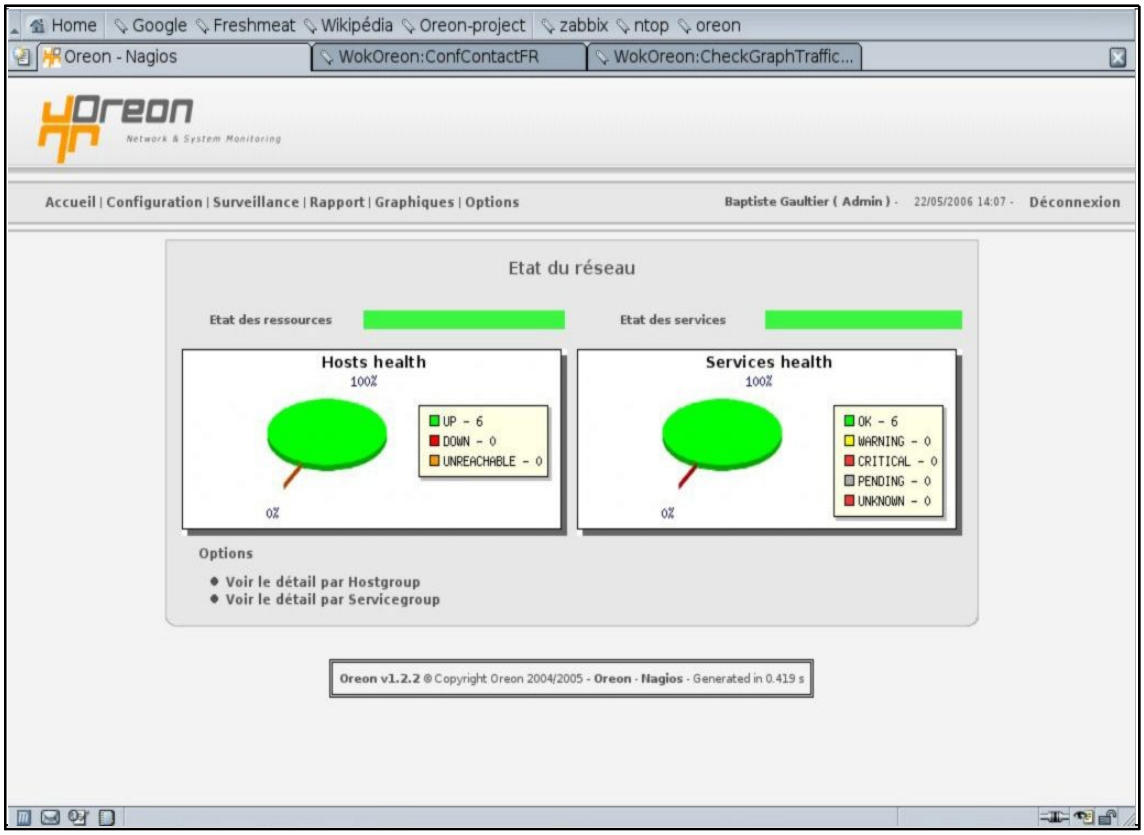


Figure 3 – Page d'accueil Oreon-Nagios

Les autres pages de Oreon-Nagios sont décomposé en 3 parties. La barre de menu situé e
permet de naviguer entre les différents sous-menu (Fig.4-1). La partie de droite présente
différents sous-menu (Fig.4-2) la partie centrale est réservé à la fenêtre de navigation(Fig

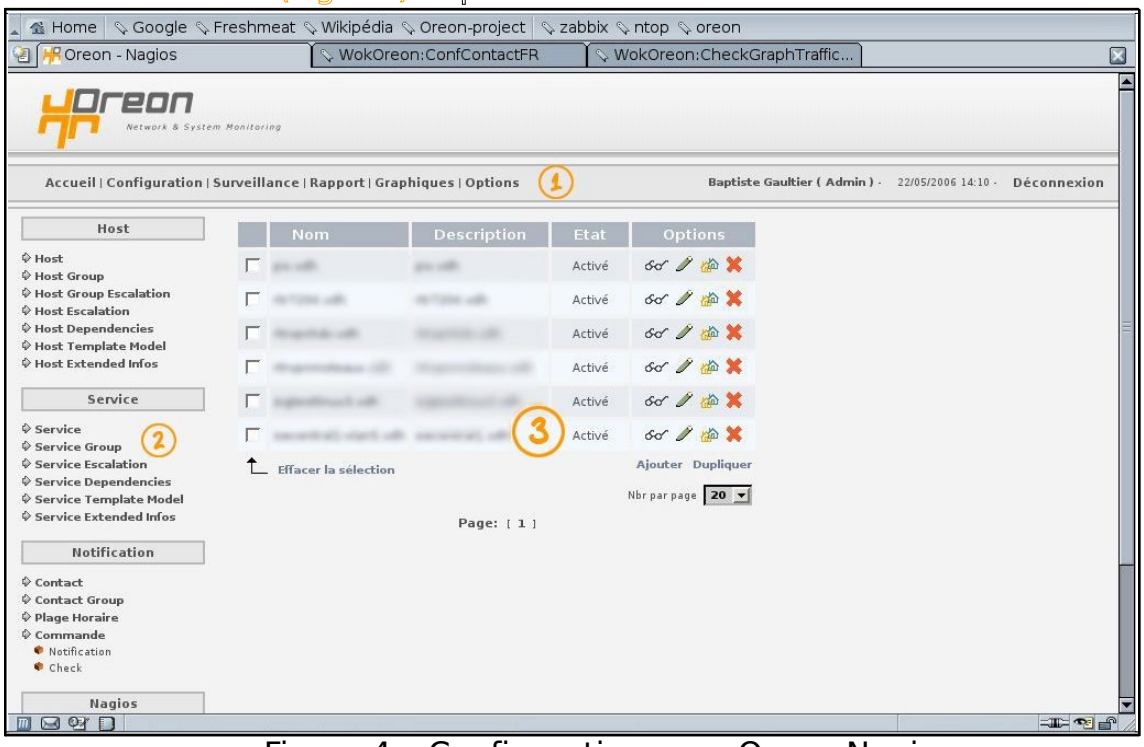


Figure 4 – Configuration sous Oreon-Nagios

La première chose à faire suite à l'installation de Oreon-Nagios est de générer les sondes
permettront l'envoie de requêtes vers les hôtes. La génération des sondes se fait via le m

« Options//Sondes » puis clic sur « Générer ».

Venons-en maintenant aux premières actions de configuration à mener suite à l'installatio
Oreon-Nagios.

- Options//Général : Permet de configurer les options générales de Oreon-Nagios, les
  répertoires d'installation, la communauté et la version de SNMP utilisé pour la collec
  d'informations, etc.
  Remarque:La vérification des droits des répertoires est indispensable au bon
  fonctionnement du programme!

- Options//Langue : permet de modifier la langue du programme (chose appréciable
  puisque l'interface Oreon est entièrement traduite en français)

- Options//Nagios.cfg : permet de vérifier et configurer le fichier de nagios.cfg

Une fois ces générations et vérifications effectuées, la configuration de la supervision (Co
Host, Service) peut débuter:

1. Configuration des contacts

Les tâches d'un administrateur réseau étant nombreuses, il est impossible à l'administrat
réseau de rester devant son logiciel de supervision à attendre les pannes. Il faut donc que
l'administrateur puisse être informé en cas de panne ou de problèmes sur son réseau. C'e
rôle de la notification d'erreur implémentée dans Oreon-Nagios. La notification d'erreur
permet à toute personne enregistrée en tant que contact d'être informés par mail(ou autr
problèmes rencontrés sur le réseau.

2. Configuration des hôtes

Tout d'abord, pour effectuer ces actions, il faut être logué en Admin sans restrictions.
L'ajout d'« hosts » permet d'ajouter à la base Nagios les ressources réseau comme les sw
routeurs, serveurs, postes, imprimantes, etc. Dès lors, l'administrateur pourra observer l
de chacun des hôtes ajoutés. De plus, l'administrateur pourra avoir plus d'informations su
hôtes grâce à l'ajout de services (IV.b.3.).
L'ensemble des actions qui vont suivre se feront via le menu « Configuration/ »

- Configuration//Host : permet de voir les hôtes enregistrés dans la base. (Fig.5-1)
  Reste alors à renseigner les champs, (Fig.5-2) les descriptions des champs sont fou
  ci-dessous.

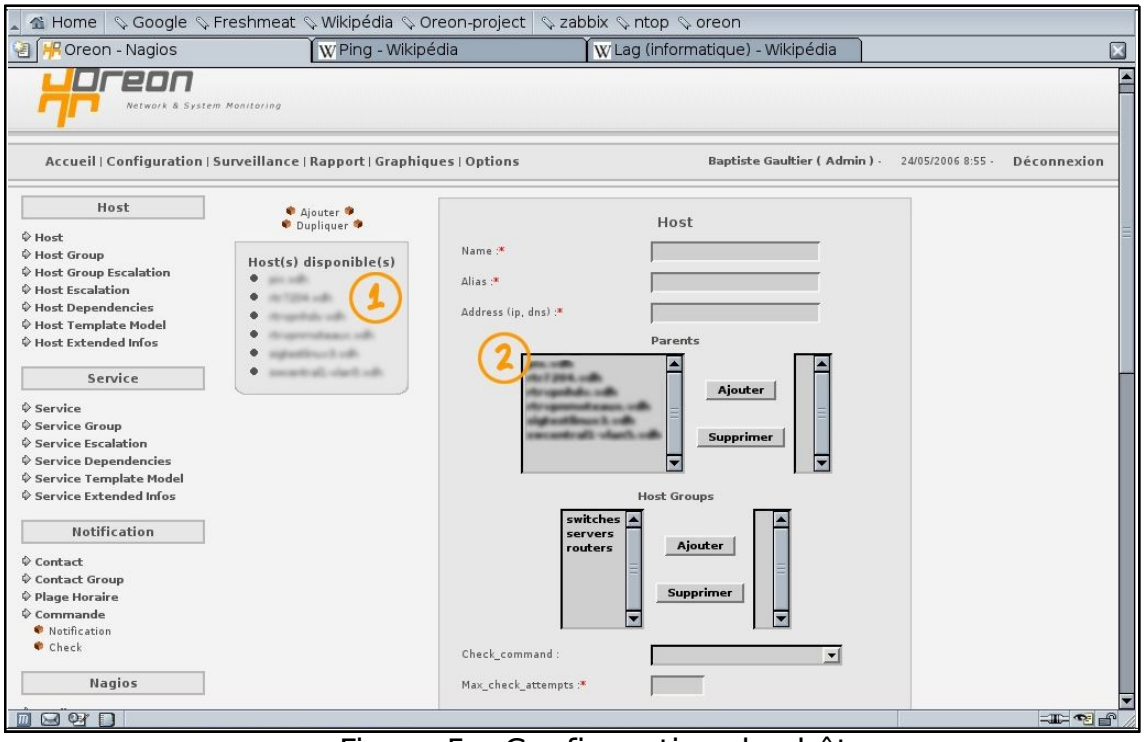


Figure 5 – Configuration des hôtes

CHAMPS	DESCRIPTION
Name	C'est le nom court qui permet d'identifier l'hôte. Il est utilisé dans les groupes d'hôtes et les définitions de service pour fa référence à cet hôte particulier. Les hôtes peuvent être associés à de multiples services (qui sont supervisés). Si elle est dans le bon contexte, la macro $HOSTNAME$ contient ce nom court.
Alias	C'est un nom long ou une description de l'hôte permettant de l'identifier plus facilement. Si elle est utilisée dans le bon contexte, la macro $HOSTALIAS$ contient cet alias/description.
Adresse	Cette directive définit l'adresse de l'hôte. C'est normalement une adresse IP. Il est possible d'utiliser un FQDN (Fully Qualified Domain Name, nom de domaine complet) pour identifier l'hôte, mais si l service DNS* n'est pas actif, cela peut poser des problèmes. Si elle est utilisée dans le bon contexte, la macro $HOSTADI contient cette adresse. Remarque: si vous ne spécifiez pas une directive d' adresse dans la définition d'un hôte, le nom s employé comme adresse. Si le DNS tombe, tous les contrôles de service échoueront puisque les plugins seront incapable résoudre les noms.
Parents	Cette directive définit une liste de noms courts d'hôtes "parents" de cet hôte, séparés par des virgules. Les hôtes parents généralement des routeurs, des commutateurs, des firewalls, etc. se trouvant entre l'hôte de supervision et les hôtes dis routeur, le commutateur, etc. le plus proche de l'hôte distant est considéré comme le parent de cette hôte. Si cet hôte est sur le même segment que l'hôte de supervision (sans routeur intermédiaire, etc.), il est considéré comme sur le réseau local et n'aura pas d'hôte parent. Laissez cette valeur vide si l'hôte n'a pas d'hôte parent (c.a.d s'il est sur l segment que l'hôte de Nagios). L'ordre dans lequel sont déclarés les parents n'a pas d'influence sur la façon dont la supervision se déroule.
Host Groups	Cette directive définit le (ou les) groupe(s) d'appartenance de cet hôte. Si le groupe n'apparaît pas, il faudra le créer par la suite et rajouter cet hôte.
Check_Command	Cette directive définit le nom court de la commande à utiliser pour déterminer si l'hôte est hors service ou non. Typiquen cette commande lance un "ping" vers l'hôte pour voir si il est "vivant". La commande doit retourner un état OK (0) sinon Nagios supposera que cet hôte est hors service. Si vous laissez cet arg vide, l'hôte ne sera pas contrôlé - Nagios supposera que l'hôte est toujours en fonctionnement. Ceci est utile pour superv des imprimantes ou autres périphériques qui sont éteints fréquemment. Le temps d'exécution maximal de cette comma déterminé par la variable host_check_timeout.
Max_check_attempts	Cette directive définit le nombre de fois ou Nagios relancera la commande de contrôle de l'hôte si celle-ci retourne un ét différent de OK. Positionner cette valeur à 1 fera que Nagios générera une alerte sans re-contrôler l'hôte. Note : si vous n voulez pas contrôler l'état de l'hôte, vous devez quand même mettre une valeur supérieure ou égale à 1. Pour ne pas eff contrôle de l'hôte, laissez simplement vide l'option <host_check_command>.
Check_enable	Cette directive définit si, oui ou non, les contrôles sont activés pour cet hôte. Valeurs: 0 = contrôles désactivés, 1 = cor

d	activés.
Event_handler_enabled	Cette directive définit si, oui ou non, le gestionnaire d'évènements est activé pour cet hôte. Valeurs: 0 = gestionnaire d'évènements désactivé, 1 = gestionnaire d'évènements activé.
Event_handler	Cette directive définit le nom court de la commande à chaque fois qu'un changement de l'état de l'hôte est détecté (c-à-chaque fois qu'il est hors service ou qu'il se rétablit). Lisez la documentation sur les gestionnaires d'événements pour de explications détaillées sur la façon d'écrire des scripts de gestion d'événements. Le temps d'exécution maximal de cette commande est déterminé par la variable event_handler_timeout.
Low_flap_threshold	Cette directive définit le seuil bas de la détection d'oscillation pour cet hôte. Si vous fixez cette directive à 1, la valeur fix directive globale (au niveau de Nagios) low_host_flap_threshold sera utilisé à la place.
High_flap_threshold	Cette directive définit le seuil haut de la détection d'oscillation pour cet hôte.Si vous fixez cette directive à 1, la valeur fix directive globale (au niveau de Nagios) high_host_flap_threshold sera utilisé à la place.
Flap_detection_enabled	Cette directive définit si, oui ou non, la détection d 'oscillation est activée pour cet hôte. Valeurs: 0 = détection d'oscillat désactivée, 1 = détection d'oscillation activée.
Process_perf_data	Cette directive définit si, oui ou non, le traitement des données liées à la performance du contrôle est activé pour cet hô Valeurs: 0 = traitement désactivé, 1 = traitement activé.
Retain_status_information	Cette directive définit si, oui ou non, les informations liées au statut de l'hôte sont mémorisées, entre les (re)démarrages Nagios, pour cet hôte. Valeurs: 0 = mémorisation désactivée, 1 = mémorisation activée. Ceci n'est utile que si vous avez mémorisation des états, avec la directive adéquate Value: 0 = mémorisation des états désactivée , 1 = mémorisation de activée.
Retain_nonstatus_information	Cette directive définit si, oui ou non, les informations non liées au statut de l'hôte sont mémorisées, entre les (re)démarr Nagios, pour cet hôte. Valeurs: 0 = mémorisation désactivée, 1 = mémorisation activée. Ceci n'est utile que si vous avez mémorisation des états, avec la directive adéquate.
Notification_interval	Cette directive définit le nombre d'"unités de temps" à patienter avant de re-notifier un contact que l'hôte est toujours h service ou inaccessible. Si vous n'avez pas modifié la valeur par défaut de la directive interval_length, qui est de 60 par nombre exprime des minutes. Si vous mettez cette valeur à 0, Nagios ne re-notifiera pas les contacts à propos des probl cet hôte - une seule notification sera émise.
Notification_period	Cette directive définit le nom court de la période durant laquelle les notifications d'événements concernant cet hôte peu être émises vers les contacts. Si un hôte est hors service, inaccessible, ou se rétablit en dehors de la période de notificat aucune notification ne sera envoyée.
Notification_options	Cette directive définit quand les notifications pour cet hôte doivent être envoyées. Les options valides sont une combina d'une ou plusieurs des valeurs suivantes : : d = envoi de la notification pour un état DOWN, u = envoi de la notification p état UNREACHABLE , et r = envoi de la notification pour le retour à la normale (état OK). Si vous spécifiez la valeur n (no aucune notification ne sera envoyée. Exemple: avec les valeurs d,r dans ce champ, les notifications seront envoyées quand l'hôte sera DOWN et quand il sorti état pour un état OK.
Notifications_enabled	Cette directive définit si , oui ou non, les notifications sont activées pour cet hôte. valeurs: 0 = notifications désactivées, notifications activées.
Stalking_options	Cette directive définit pour quel état de l'hôte le "suivi précis" est activé. Les options valides sont une combinaison d'une plusieurs des valeurs suivantes: o = suivi sur les états UP, d = suivi sur les états DOWN , et u = suivi sur les états UNREA
Etat	Cette directive permet d'activer ou désactiver le surveillance de cet hôte.
Comment	Cette directive permet d'ajouter des informations complémentaire pour l'hôte.

Remarque: seuls les champs suivis d'un astérisques sont à remplir obligatoire

- Une fois le configuration terminée, clic sur « Sauvegarder ».
- Il sera dès lors possible de voir, modifier, dupliquer et supprimer un hôte grâc menu Configuration//Hosts/Options

Remarque: Les modifications ne sont prises en compte qu'après le redémarrage de Nagios accessible dans le menu Configuration//Nagios/Appliquer. Puis clic sur « Générer » puis sur « Redémarrer ».

- Configuration//Host Group : Permet d'ajouter des groupes d'hôtes, les champs à rem

lors de la création d'un groupe d'hôte sont les suivants:

CHAMPS	DESCRIPTION
Nom	Cette directive définit le nom court qui identifie le groupe d'hôtes.
Alias	Cette directive définit un nom long ou une description permettant d'identifier plus facilement le groupe d'hôtes. Elle sert à permettre une identification plus facile d'un groupe d'hôtes.
Host	C'est une liste de noms courts d'hôtes à inclure dans ce groupe.
Contact Group(s)	C'est une liste de noms courts de groupes de contact à notifier en cas de problème (ou de rétablissement) concernant un hôte quelconque de ce groupe. Les groupes de contacts sont séparés par des virgules.
Etat	Cette directive permet d'activer ou désactiver ce groupe d'hôtes.
Comment	Ce champ permet d'ajouter des informations complémentaires.

- Une fois le configuration terminée, clic sur « Sauvegarder ».
- Il sera dès lors possible de voir, modifier, dupliquer et supprimer un hôte grâc menu Configuration//Host Group/Options.

Remarque: Les modifications ne sont prises en compte qu'après le redémarrage de Nagios accessible dans le menu Configuration//Nagios/Appliquer. Puis clic sur « Générer » puis sur « Redémarrer ».

3. Configuration des services

Les services permettent d'effectuer des requêtes sur les ressources réseaux afin d'obteni amples informations sur ces ressources. Par exemple, il est possible d'effectuer des requê un routeur donné afin de connaître le trafic entrant ou sortant d'une interface.
Avant la configuration, vérifier que les machines à analyser sont bien configurées avec le protocole SNMP.

Remarque: il est possible de vérifier le bon fonctionnement d'une machine avec SNMP grâ commande « snmpwalk » par exemple. Cette commande permet de communiquer avec u entité réseau en utilisant les requêtes SNMP GETNEXT.

```
sigtestlinux3:/# snmpwalk -Os -c public -v 1 sigtestlinux3
sysDescr.0 = STRING: Linux sigtestlinux3 2.4.27-2-386 #1 Wed Aug 17 09:33:35 UTC 2005 i686
sysObjectID.0 = OID: netSnmpAgentOIDs.10
sysUpTime.0 = Timeticks: (41104755) 4 days, 18:10:47.55
sysName.0 = STRING: sigtestlinux3
[...]
sigtestlinux3:/#
```

- Configuration//Service : permet d'ajouter de nouveaux services, les champs à rense sont décrits dans le tableau ci-dessous.

CHAMPS	DESCRIPTION
HostGroup name	Permet de définir à quel Groupe d'hôte le service va s'appliquer.

Host name	Permet de définir à quel hôte le service va s'appliquer.
Utiliser un modèle de template	Cette directive permet de définir un template de service à utiliser pour définir le service en cours.
Description	C'est un nom long ou une description du service permettant de l'identifier plus facilement.
Is Volatile	Cette directive permet de définir si le service sera éphémère ou pas.
Service Groups	Permet de définir le groupe auquel appartient le service
Check_command	Cette directive définit le nom court de la commande à utiliser pour le service. Par exemple: check_graph_traffic
Check_command_arguments	Permet d'entrer les paramètres de la commande entrée précédemment, par exemple: $USER1$/check_graph_traffic.pl -H 192.168.2.65 -C public -v 1 -i 2
Max_check_attempts	Cette directive définit le nombre de fois ou Nagios relancera la commande de contrôle de l'hôte si celle-ci retourne un différent de OK. Positionner cette valeur à 1 fera que Nagios générera une alerte sans re-contrôler l'hôte. Note : si vou voulez pas contrôler l'état de l'hôte, vous devez quand même mettre une valeur supérieure ou égale à 1. Pour ne pas le contrôle de l'hôte, laissez simplement vide l'option <host_check_command>.
Normal_check_interval	Permet de définir la période séparant deux lancement du service. Cette période doit être exprimée en minute.
Retry_check_interval	Permet de définir la période séparant deux tentatives du service si la commande de contrôle précédente retourne un différent de OK. Cette période doit être exprimée en minute.
Check_enabled	Cette directive définit si, oui ou non, les contrôles sont activés pour cet hôte. Valeurs: 0 = contrôles désactivés, 1 = co activés.
Check_period	Cette directive définit les horaires pendant lesquels les commandes de contrôles vont être effectué, par exemple 24x7 que les contrôles auront lieu 7J/7, 24h/24
Parallelize_check	Permet de définir si le service peut être effectué de manière parallèle avec d'autres.
Obsess_over_service	Permet de définir si oui ou non, la fin du service doit être notifiée.
Check_freshness	Permet de définir si oui ou non le service doit rafraîchir son contenu.
Freshness_threshold	Définit la période de rafraîchissement du contenu du service.
Event_handler	Cette directive définit le nom court de la commande à chaque fois qu'un changement de l'état de l'hôte est détecté (c chaque fois qu'il est hors service ou qu'il se rétablit). Lisez la documentation sur les gestionnaires d'événements pour explications détaillées sur la façon d'écrire des scripts de gestion d'événements. Le temps d'exécution maximal de cet commande est déterminé par la variable event_handler_timeout.
Event_handler_enabled	Cette directive définit si, oui ou non, le gestionnaire d'évènements est activé pour cet hôte. Valeurs: 0 = gestionnaire d'évènements désactivé, 1 = gestionnaire d'évènements activé.
Low_flap_threshold	Cette directive définit le seuil bas de la détection d'oscillation pour cet hôte. Si vous fixez cette directive à 1, la valeur la directive globale (au niveau de Nagios) low_host_flap_threshold sera utilisé à la place.
High_flap_threshold	Cette directive définit le seuil haut de la détection d'oscillation pour cet hôte. si vous fixez cette directive à 1, la valeu par la directive globale (au niveau de Nagios) high_host_flap_threshold sera utilisé à la place.
Flap_detection_enabled	Cette directive définit si, oui ou non, la détection d 'oscillation est activée pour cet hôte. Valeurs: 0 = détection d'oscil désactivée, 1 = détection d'oscillation activée.
Process_perf_data	Cette directive définit si, oui ou non, le traitement des données liées à la performance du contrôle est activé pour ce s Valeurs: 0 = traitement désactivé, 1 = traitement activé.
Retain_status_information	Cette directive définit si, oui ou non, les informations liées au statut de l'hôte sont mémorisées, entre les (re)démarrag Nagios, pour ce service. Valeurs: 0 = mémorisation désactivée, 1 = mémorisation activée. Ceci n'est utile que si vous activé la mémorisation des états, avec la directive adéquate Value: 0 = mémorisation des états désactivée , 1 = mém des états activée.
Retain_nonstatus_information	Cette directive définit si, oui ou non, les informations non liées au statut du service sont mémorisées, entre les (re)démarrages de Nagios, pour ce service. Valeurs: 0 = mémorisation désactivée, 1 = mémorisation activée. Ceci n'e que si vous avez activé la mémorisation des états, avec la directive adéquate.
Notification_interval	Cette directive définit le nombre d'« unités de temps » à patienter avant de re-notifier un contact que le service est to hors service ou inaccessible. Si vous n'avez pas modifié la valeur par défaut de la directive interval_length, qui est de défaut, ce nombre exprime des minutes. Si vous mettez cette valeur à 0, Nagios ne re-notifiera pas les contacts à prop problèmes de ce service - une seule notification sera émise.

Notification_period	Cette directive définit le nom court de la période durant laquelle les notifications d'événements concernant ce service peuvent être émises vers les contacts. Si un service ne peut être effectué, renvoit un statut qui n'est pas OK, ou se ré dehors de la période de notification, aucune notification ne sera envoyée.
Notification_options	Cette directive définit quand les notifications pour cet hôte doivent être envoyées. Les options valides sont une combi d'une ou plusieurs des valeurs suivantes : d = envoi de la notification pour un état DOWN, u = envoi de la notificatio un état UNREACHABLE , et r = envoi de la notification pour le retour à la normale (état OK). Si vous spécifiez la valeur (none), aucune notification ne sera envoyée. Exemple: avec les valeurs d,r dans ce champ, les notifications seront envoyées quand l'hôte sera DOWN et quand il s cet état pour un état OK.
Notifications_enabled	Cette directive définit si , oui ou non, les notifications sont activées pour ce service. valeurs: 0 = notifications désactiv notifications activées.
Stalking_options	Cette directive définit pour quel état de l'hôte le "suivi précis" est activé. Les options valides sont une combinaison d'u plusieurs des valeurs suivantes: o = suivi sur les états UP, d = suivi sur les états DOWN , et u = suivi sur les états UNREACHABLE.
Etat	Cette directive permet d'activer ou désactiver le surveillance de ce service.
Comment	Cette directive permet d'ajouter des informations complémentaire pour le service.

Remarque: Les modifications ne sont prises en compte qu'après le redémarrage de Nagios accessible dans le menu Configuration/Nagios/Appliquer. Puis clic sur « Générer » puis sur « Redémarrer ».

Voilà qui cloture la partie sur l'utilisation de Oreon-Nagios. De nombreuses informations s également disponibles sur http://oreon-project.org et http://nagios-contribs.org. Toutes ce pages ont été écrites et traduites par la communauté française Oreon-Nagios et sont don disponibles en français. De nombreuses informations sont également disponible en anglai l'adresse suivante: http://www.nagios.org.

Conclusion

Ce stage m'a beaucoup apporté, tant sur le plan personnel que professionne
m'a permis de mieux comprendre et d'appréhender l'organisation d'une gran
entreprise, les contraintes et les missions d'une structure telle que le SIGDC
stage m'a également permis d'apprendre considérablement sur le monde lib
sa philosophie et sa culture, sur sa puissance d'organisation grâce aux
communautés, et enfin sur les alternatives qu'il apporte aux solutions
commerciales. Au cours de ces deux mois, j'ai pu appréhender des sujets va
comme la création graphique, les routeurs cisco, le script linux... Ce stage m
également formé sur le travail d'équipe, l'aspect formatif et l'aide que le trav
d'équipe propose mais également les contraintes de ce type de travail. En
conclusion , je suis très satisfait de ce stage qui a ajouté une dimension
professionnelle au travail à l'IUT ainsi qu'un apport personnel crucial pour ma
poursuite d'étude.

Annexes

Configuration d'un routeur Cisco ou d'un switch Cisco (IOS 12.3) pour l'envoi de NetFlows

- Tout d'abord vérifier que la fonction routage est bien activé
  Après avoir configuré le routage IP, il faut utilisé les commandes suivantes en commençant par le mode de configuration global:

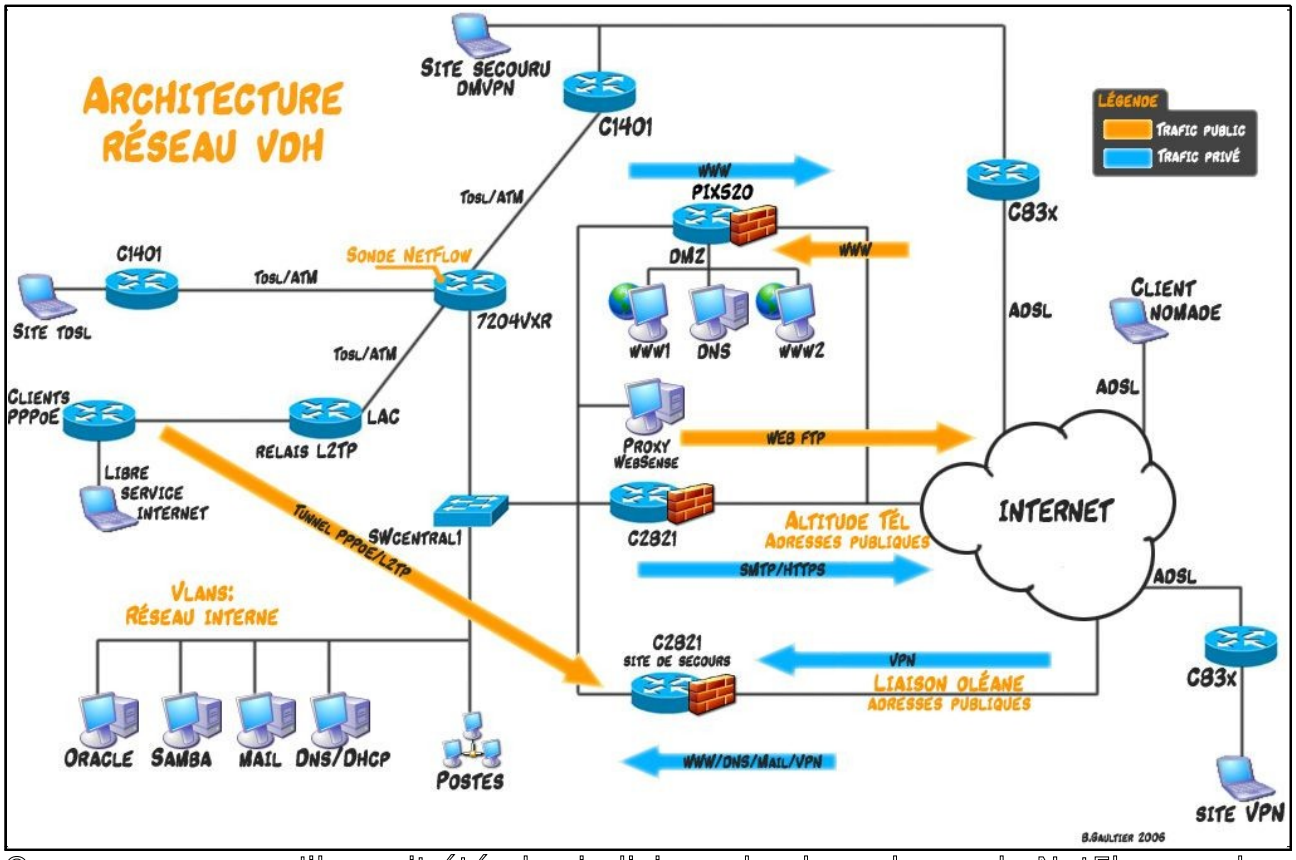
```
interface numero_interface|port
ip flow egress
ip flow ingress
ip flow-export destination ip port_udp
ip flow-export version
```

  Remarque:
  La commande « ip route-cache egress/ingress » permet d'activer NetFlow en entrar
  en sortant ou les deux.
  La commande « ip flow-export » permet d'activer l'envoi de NetFlow sur l'adresse IP
  collecteur ainsi que sur le port de son choix (par défaut=2055) et enfin de préciser
  version de Netflow utilisé.

- Il est également possible de visualiser et de vider les statistiques NetFlow à l'aide d
  commandes respectives « show ip cache flow » et « clear ip flow stats ».

```
show ip cache flow
clear ip flow stats
```

Vue d'ensemble du réseau VDH avec emplacement de la sonde NetFlow:



On remarquera qu'il aurait été plus judicieux de placer la sonde NetFlow sur le switch Swc cependant le modèle du switch ne permettant pas l'exportation des NetFlow, la sonde a é activé sur le routeur Cisco 7204VXR pourvu de la fonction d'exportation de NetFlow.

Script awk d'analyse de log:
Ce script a pour but de fournir à l'administarteur réseau un rapport quotidien sur les conn
VPN (Virtual Private Network). Schéma fonctionnel du script:

Contenu du script AnalyseVPN.sh (remarque: ce listing n'est pas complet et ne contient q
code important):

```
#!/bin/bash
########################################
# Script analyseVPN.sh par B.Gaultier 2006  #
########################################

#Déclaration des variables d'environnement
DIR=./tmp
DIR_log=../log

#Création du fichier rapport_rtrvpn.txt
echo "Rapport des VPN pour le rtrvpn:" > $DIR/rapport_rtrvpn.txt
echo "" >> $DIR/rapport_rtrvpn.txt
echo "" >> $DIR/rapport_rtrvpn.txt

        #Création du fichier contenant les infos UP
        awk 'BEGIN { printf ("") }
        /tunnel is UP/ {print $NF}' $DIR_log/rtrvpn.log.0|sort|uniq -c|sort -n|awk 'BEGIN { printf ("") }
        // {print $2,"UP:  ",$1}' > hosts_up

        #Création du fichier contenant les infos DOWN
        awk 'BEGIN { printf ("") }
        /tunnel is DOWN/ {print $NF}' $DIR_log/rtrvpn.log.0|sort|uniq -c|sort -n|awk 'BEGIN { printf ("") }
        // {print $2,"DOWN",$1}' > hosts_down

        cat hosts_up hosts_down|sort -r|less >> $DIR/rapport_rtrvpn.txt

        #mise en page
        echo "" >> $DIR/rapport_rtrvpn.txt
        echo "" >> $DIR/rapport_rtrvpn.txt
        echo "Listes des erreurs de reconnexions:" >> $DIR/rapport_rtrvpn.txt
        echo "" >> $DIR/rapport_rtrvpn.txt

                #Regarde si les reconnexions sont toutes immédiates et indique la liste des erreurs de reconnexions
                diff --ignore-blank-lines down up|awk 'BEGIN { printf ("") }
                // {print $2}'|sort|uniq -c|less >> $DIR/rapport_rtrvpn.txt

#envoie du rapport par mail
mailliste="prenom.nom@ville-lehavre.fr"
cat $DIR/rapport_rtrvpn.txt|mail -s "Rapport VPN" $mailliste
```

Glossaire

Broadcast: Le broadcast est un terme anglais (en français on utilise le terme diffusion) définissant une diffusion de données à un ensemble d'ordinateurs connectés à un réseau informatique. Les protocoles de communications réseau prévoient une méthode simple po diffuser des données à plusieurs machines en même temps. Au contraire d'une communic « Point à Point » (unicast, cf. glossaire), il est possible d'adresser des paquets de données ensemble de machines d'un même réseau uniquement par des adresses spécifiques qui s interceptées par toutes les machines du réseau ou sous-réseau.
Pour une diffusion de données moins générale, on utilisera les adresses « Multicast »(cf. glossaire).

Couche application: La couche application est la 7ème couche du modèle OSI. Elle est l'interface utilisateur logiciel et fait parvenir les requêtes à la couche de présentation. Elle permet d'exploiter les services du système.

Couche transport: La couche transport est la 4ème couche du modèle OSI. Cette couche permet d'établir une communication de bout en bout. Elle gère la segmentation et le réassemblag données, le multiplexage et le démultiplexage, le contrôle de flux ainsi que la détection d et la reprise sur erreur.

Dépendance: Une dépendance logicielle se conçoit dans le cadre d'une intégration de pac glossaire) logiciel en vue de construire un agrégat logiciel. Une dépendance exprime des relations entre paquets.

DNS: Le Domain Name System (ou DNS, système de noms de domaine) est un système permettant d'établir une correspondance entre une adresse IP et un nom de domaine et, généralement, de trouver une information à partir d'un nom de domaine.

LAMP: LAMP est un acronyme informatique permettant de désigner facilement la réunion ces logiciels libres sur une même plate-forme :

- « Linux », le système d'exploitation
- « Apache », le serveur web
- « MySQL », le serveur de base de données
- « Perl », « PHP » ou « Python », les langages de script.

Multicast: On entend par multicast le fait de communiquer simultanément avec un groupe d'ordinateurs identifiés par une adresse spécifique (adresse de groupe). L'avantage de ce par rapport au classique unicast devient évident quand on veut diffuser de la vidéo. En st on envoie une image autant de fois que l'on a de connexions simultanées : perte de temp

ressources du serveur et surtout de bande passante. Alors qu'en multicast le paquet n'est qu'une seule fois, et sera routé vers toutes les machines du groupe de diffusion.

NetFlow: NetFlow est le nom d'un protocole propriétaire conçu pour la collecte d'informati sur le trafic IP. Les routeurs Cisco avec cette fonctionnalité envoit des paquets UDP qui so collectés par un collecteur NetFlow (ntop possède cette fonction).

Open Source: Le terme Open Source définit une licence de logiciel obéissant à une définition très précise établie par l'Open Source Initiative, et dont voici les principaux critères néces

- Libre redistribution
- Code source disponible
- Travaux dérivés possibles

OS: OS pour Operating System, en français Système d'exploitation , un OS est un ensemb programmes responsables de la liaison entre les ressources matérielles d'un ordinateur et applications de l'utilisateur (traitement de texte, jeu vidéo...). Il assure le démarrage de l'ordinateur, et fournit aux programmes applicatifs des interfaces standardisées pour les périphériques.

Paquet: Un paquetage ou paquet logiciel (en anglais package) désigne une archive comp les fichiers informatiques, les informations et procédures nécessaires à l'installation d'un sur un système d'exploitation au sein d'un agrégat logiciel, en s'assurant de la cohérence fonctionnelle du système ainsi modifié.

Ping: (acronyme de Packet INternet Groper) est le nom d'une commande permettant d'envoyer une requête ICMP à une autre machine. Si la machine ne répond pas il se peut l'on ne puisse pas communiquer avec elle. Cette commande réseau de base permet d'obt informations et en particulier le temps de réponse de la machine à travers le réseau et au est l'état de la connexion avec cette machine (renvoi code d'erreur correspondant).

Plugin: un plugin, ou plug-in, de l'anglais to plug in (brancher), parfois traduit en module externe, module enfichable, module d'extension, greffon ou plugiciel, est un logiciel tiers venant se greffer à un logiciel principal afin de lui apporter de nouvelles fonctionnalités. L logiciel principal fixe un standard d'échange d'informations auquel ses conformes se conforment.
Le module n'est généralement pas conçu pour fonctionner seul mais avec un autre progra

SNMP: Simple Network Management Protocol ou « protocole simple de gestion de réseau français, est un protocole de communication qui permet aux administrateurs réseaux de g les équipements du réseau et de diagnostiquer les problèmes de réseau.

TCP: Transmission Control Protocol ou « protocole de contrôle de transmissions », est un protocole de transport fiable, en mode connecté en opposition au protocol non-connecté U (cf. Glossaire).

Trame: une trame est un paquet d'information véhiculé au travers d'un support physique (cuivre, fibre optique, etc.). Une trame est composée d'un préambule, puis des informatio que l'on veut transmettre, et d'un postambule.

UDP: User Datagram Protocol (ou UDP, protocole de datagramme utilisateur) est un des principaux protocoles de télécommunication utilisé par Internet. Il fait partie de la couche transport.

Le rôle de ce protocole est de permettre la transmission de paquets (aussi appelés datag de manière très simple entre deux entités, chacune étant définie par une adresse IP et ur numéro de port (pour différencier différents utilisateurs sur la même machine). Contrairer au protocole TCP, il travaille en mode non-connecté : il n'y a pas de moyen de vérifier si t les paquets envoyés sont bien arrivés à destination et ni dans quel ordre. C'est pour cela souvent décrit comme étant un protocole non-fiable. Par contre, pour un datagramme UD donné, l'exactitude du contenu des données est assuré grâce à une somme de contrôle (checksum).

Unicast: Le terme unicast définit une connexion réseau point à point. On entend par unica fait de communiquer entre deux ordinateurs identifiés chacun par une adresse réseau uni Les paquets de données sont routés sur le réseau suivant l'adresse du destinataire encap la trame transmise. Normalement, seul le destinataire intercepte et décode le paquet qui adressé.