

Key Concepts of Network Management

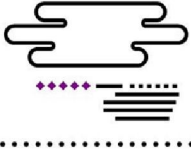
Practical Examples and Tools

Thibault Cholez

Telecom Nancy, UL

42

Nous concluons les leçons introductives à la gestion de réseaux en présentant certaines applications de gestion qui reposent sur les concepts et protocoles vus dans les précédentes leçons.



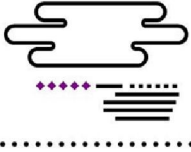
Management Applications

- SNMP is just a protocol
- Network Management operations performed by applications
- Four examples:
 - RMON
 - Net-SNMP
 - MRTG
 - Centreon
- Many others: Zenoss, Zabbix, Cacti...

43

Il convient de rappeler que SNMP est un simple protocole de transport, le format SMI et les MIBs sont une manière de structurer et d'organiser les informations de gestion. La vraie gestion du réseau, autrement dit l'intelligence, est réalisée par les applications de gestion dont dispose le gestionnaire. C'est celles-ci qui permettent réellement la visualisation et l'automatisation des activités de gestion.

Nous allons présenter brièvement quatre exemples d'applications de gestion, à savoir RMON, Net-SNMP, MRTG et Centreon, sachant que beaucoup d'autres applications existent, chacune avec ses spécificités. Certaines étant plus ou moins complètes, certaines sous licence libre et d'autres propriétaires, etc.



RMON

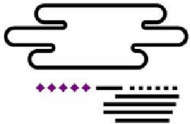
- Remote MONitoring (IETF standard)
- Many features: statistics, history, host, traffic matrix, alarms, filters, events, packet capture...
- Statistics per link (in/out): packets, octets, collisions, errors, broadcasts...
- Alarms trigger based on rising/falling thresholds

44

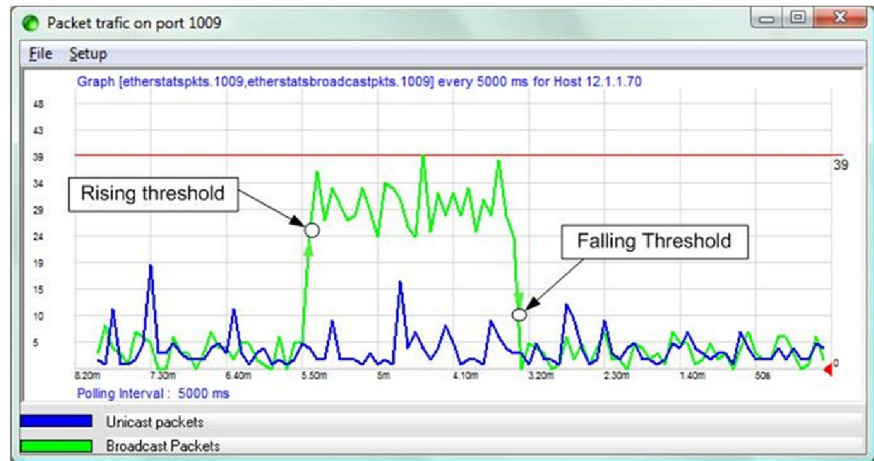
RMON signifie « Remote MONitoring ». Il s'agit d'un ensemble composé d'un gestionnaire et d'agents utilisant une MIB spécifique pour la supervision de réseau et qui est standardisée par l'IETF. Les informations essentielles pour la supervision de réseau sont ainsi toutes définies et accessibles. Cela inclut diverses statistiques, des matrices de trafic, des alarmes, des filtres, des notifications, etc.

On peut par exemple accéder à de nombreuses statistiques par lien, telles que le nombre de paquets ou d'octets transmis, le nombre de collisions, d'erreurs, etc. Et ce pour chacun des deux sens de communication. Il y a également des statistiques par hôte qui peuvent être indexées par l'adresse mac. Les alarmes sont basées sur le franchissement de seuils (qu'il s'agisse d'un seuil bas ou haut) et sont configurables.

Les agents RMON sont intelligents et incluent certains traitements sur les données de gestion, ce qui permet d'optimiser les interactions avec le gestionnaire en se limitant aux informations essentielles.

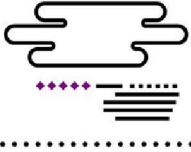


RMON



45

On peut voir ici une interface graphique tierce traçant une courbe à partir des données issues des agents RMON. En l'occurrence, on trace ici le nombre de paquets transmis en unicast et en broadcast en fonction du temps. La fréquence des mesures est établie à toutes les 5 secondes. On matérialise également deux seuils de détection: un « rising threshold » établi à 25 paquets et un « falling threshold » établi à 10 paquets.



Net-SNMP

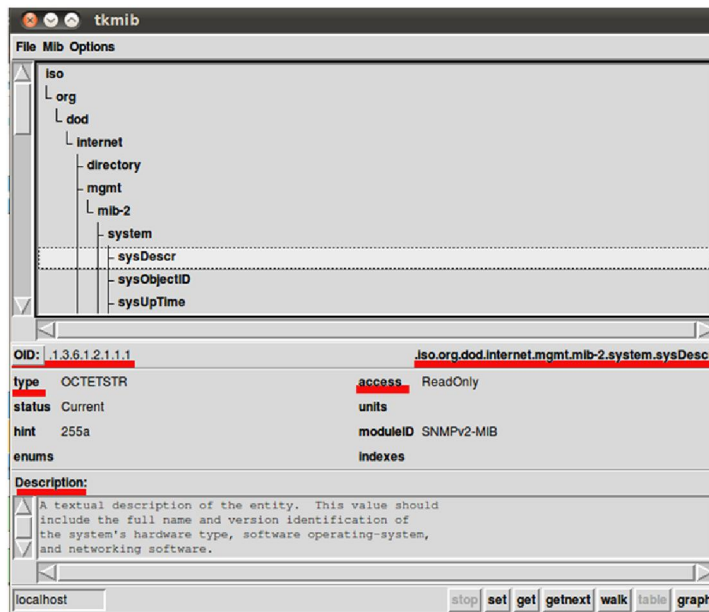
- Suite of open-source (BSD license) applications to use SNMP
- Command-line apps to monitor/configure devices using SNMP
- Graphical MIB browser
- Daemon application for receiving SNMP notification
- Agent for responding to SNMP queries
- C library to develop SNMP apps

46

Un deuxième exemple d'application est la suite d'outils Net-SNMP qui est distribuée sous licence libre. On y trouve divers outils permettant de travailler avec le protocole SNMP. Cela inclut divers exécutable en ligne de commande qui permettent d'émettre des requêtes (on a par exemple les commandes `snmpget`, `snmpgetnext`, `snmpset` dont le nom est explicite, `snmpwalk` qui permet de parcourir une MIB, `snmpstatus` qui permet d'obtenir les statistiques de base sur un agent SNMP, `snmptranslate` qui permet de convertir certains types en un format lisible par un humain, etc.)

Outre de nombreuses commandes, Net-SNMP inclut également un outil graphique pour parcourir les MIBs, un daemon pour recevoir les notifications et un agent répondant aux requêtes. La suite propose également une bibliothèque C permettant de développer de nouvelles applications, agents ou gestionnaires, reposant sur le protocole SNMP.

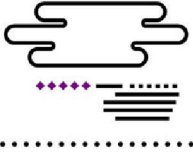
Net-SNMP



47

Nous avons ici un exemple d'une interface de visualisation de MIBs, appelé tkmib, proposée par Net-SNMP.

On y retrouve l'arbre de nommage des informations de gestion que l'on peut parcourir, l'identifiant de l'objet et le nom complet de l'objet courant, ainsi que ses principales caractéristiques, à savoir le type de l'objet, son mode d'accès, son statut et sa description textuelle.

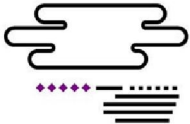


MRTG

- Open-source tool (GNU/GPL), written in Perl
- Request and gather SNMP data from network agents
- Generate graphs from data

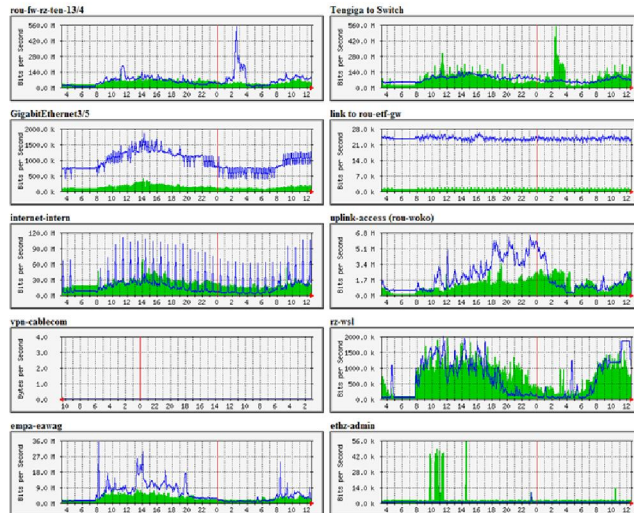
48

MRTG signifie « Multi Router Traffic Grapher ». Il s'agit d'un outil libre écrit en Perl et permettant de collecter les informations de supervision grâce à SNMP et d'en faire des graphiques au format PNG. Ces graphiques sont souvent repris dans des pages web pour créer des interfaces web de supervision.



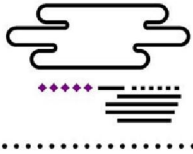
MRTG

MRTG Index Page



49

Voici un exemple de graphiques produits par MRTG.



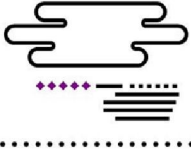
Centreon

- Powerful monitoring application (database, GUI, core engine)
- Core (fork of Nagios) and many modules are open-source (GPLv2)
- Completed with proprietary modules
- Centreon Broker can include events from many sources

50

Enfin, le dernier exemple est une application de gestion complète appelée Centreon. Centreon est constitué de plusieurs éléments, à savoir un moteur de traitement, une base de données, une interface graphique et un agrégateur qui lui permet d'inclure des données provenant de sources hétérogènes.

Le cœur de Centreon est basé sur Nagios, qui sera présenté en détail dans une leçon ultérieure. C'est une application extensible qui propose à la fois des modules open-source et d'autres propriétaires.



Centreon

- Many free functionalities
 - General view of monitoring information
 - Detailed performance graphs
 - Availability reports per device/service
 - Interface to configure managed objects
 - Configurable GUI with access control, and widgets
 - Internal logs, etc.
- And many more advanced ones
 - alerts, advanced reporting, maps, etc.

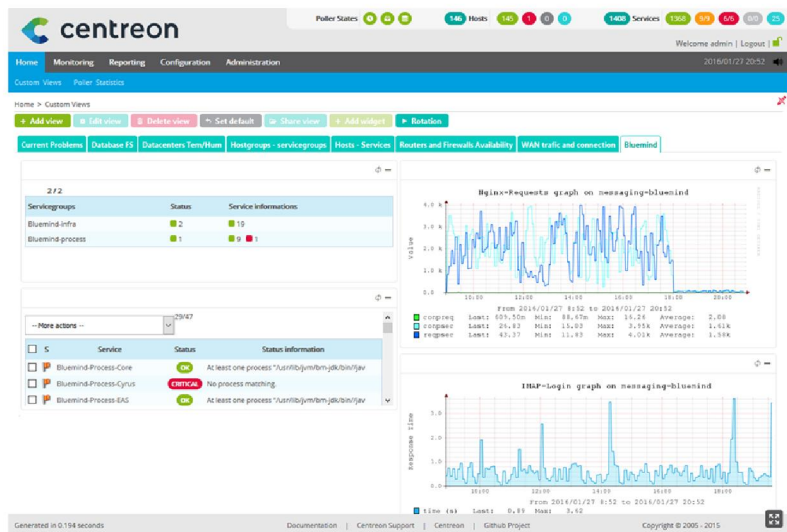
51

Parmi les fonctionnalités de la version gratuite, on trouve notamment :

- la possibilité d'avoir une vue synthétique de la supervision de son système d'informations,
- la visualisation de graphiques de performances détaillés,
- des rapports de disponibilité des ressources supervisées par équipement, par service, ou par groupe de ressources,
- une interface de configuration intuitive pour les différents objets et fichiers de configuration,
- la possibilité d'administrer complètement l'interface web et de mettre en place des accès restreints aux ressources et pages de l'interface,
- la possibilité de suivre des logs d'utilisation de la solution (logs de modifications des ressources).

Il existe d'autres fonctionnalités avancées fournies par des modules, comme la gestion des alertes, la génération de rapports personnalisés, l'intégration de cartes, etc.

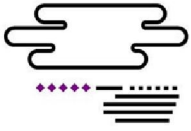
Centreon



52

Voici une illustration de Centreon. On peut y remarquer les principaux onglets indispensables pour un gestionnaire : la page d'accueil offrant une vue globale, la supervision de l'infrastructure, les rapports générés, la configuration et enfin l'administration.

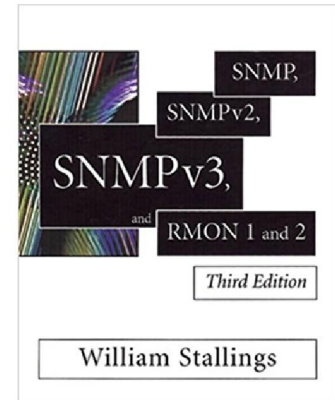
On remarque également que de nouvelles vues peuvent être facilement créées et ajoutées à la page d'accueil, afin de correspondre au mieux aux besoins du gestionnaire.



Reference Books



Essential SNMP, 2nd Edition
By Douglas Mauro, Kevin Schmidt



SNMPv3, 3rd Edition
By William Stallings

53

Pour aller plus loin, je vous conseille deux livres de référence qui vous permettront d'approfondir les concepts introduits dans ce chapitre du MOOC, à savoir:

Essential SNMP, 2nd Edition de [Douglas Mauro et Kevin Schmidt](#), et surtout *SNMPv3, 3rd Edition* de [William Stallings](#) qui a servi lors de la préparation de ces leçons.

A voir également : <https://www.simpleweb.org> où l'on peut accéder aux cours et tutoriaux de l'Université de Twente aux Pays-Bas sur la supervision de réseaux.