La supervision, la métrologie

Matthieu Herrb

Capitoul, le 3 avril 2008

Agenda

Agenda

Définition

Supervision

Action d'encadrer et de contrôler l'activité de quelqu'un qui n'a pas forcément la connaissance complète des concepts requis.

- laisse une certaine autonomie à la personne supervisée.
- nécessite d'observer et d'analyser le comportement de la personne supervisée afin de proposer des améliorations.

En informatique...

Permet de surveiller, rapporter et alerter les fonctionnements normaux et anormaux des systèmes informatiques.

Préoccupations :

- Technique : surveillance du réseau, de l'infrastructure et des machines,
- Applicative : surveillance des applications et des processus métiers.
- Contrat de service : surveillance respect des indicateurs
- Métier : surveillance des processus métiers de l'entreprise

Actions réflexes liées à cette surveillance du système
$\longrightarrow$ réactions automatisées en fonctions d'alertes définies.

Pourquoi ?

Améliorer la qualité du service :

- Détecter les anomalies à temps
- Augmenter la fiabilité des systèmes
- Communiquer avec les utilisateurs et sa hiérarchie

Concrètement

- Collecter des données, les stocker
- Créer un tableau de bord
- Générer des alarmes
- Générer des actions correctrices automatiques

Agenda

Outils pour la supervision

- briques de base :
  - collecte de données
  - stockage des données
  - représentation graphique
  - génération et transport d'alarmes
  - exécution d'actions
- colle :
  - pages web
  - génération de rapports
  - templates
  - langages de scripts
- solutions complètes

SNMP

Simple **N**etWork **M**anagement **P**rotocol
Collecte de données, remontées d'alarmes et configuration à distance.

- RFCs 1065-1067, 1155-1157, 1213, 1141, 1452, 1901-1910...
- MIB: **M**anagement **I**nformation **B**ase: défini l'arborescence des données exportées par un *agent* SNMP.
- Traps permet d'envoyer des alarmes.

Versions 1 et 2c du protocole les plus répandues :
pas de sécurité (UDP, paquets en clair, communauté 'public' partout)...
Implémentation Open Source: `http://www.net-snmp.org/`

IPMI

Intelligent **P**latform **M**anagement **I**nterface

Spécification Intel pour la gestion de plateformes matériels.
Trouvée sur de nombreux serveurs en rack.

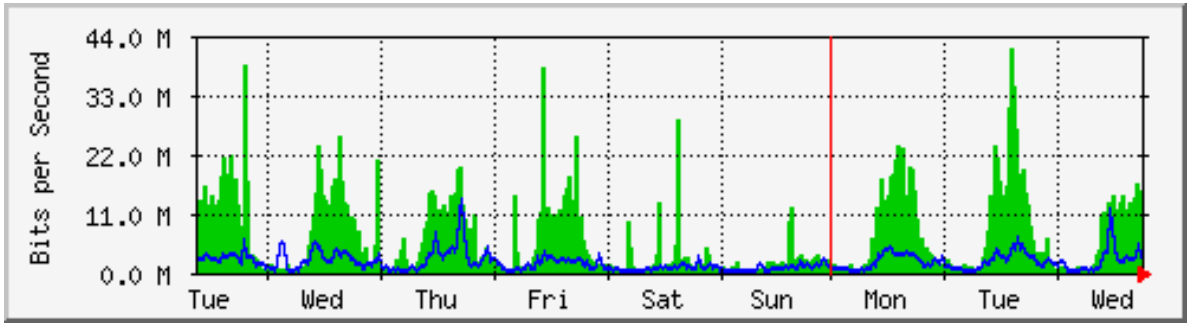
- accessible à distance
- capteurs température, ventilateurs, tensions d'alimentation...
- inventaire des composants FRU (Field Replaceable Units)
- contrôle de l'alimentation, du reboot du système.

Implémentation Open source:
`http://ipmitool.sourceforge.net/`

MRTG

MRTG MULTI ROUTER TRAFFIC GRAPHER

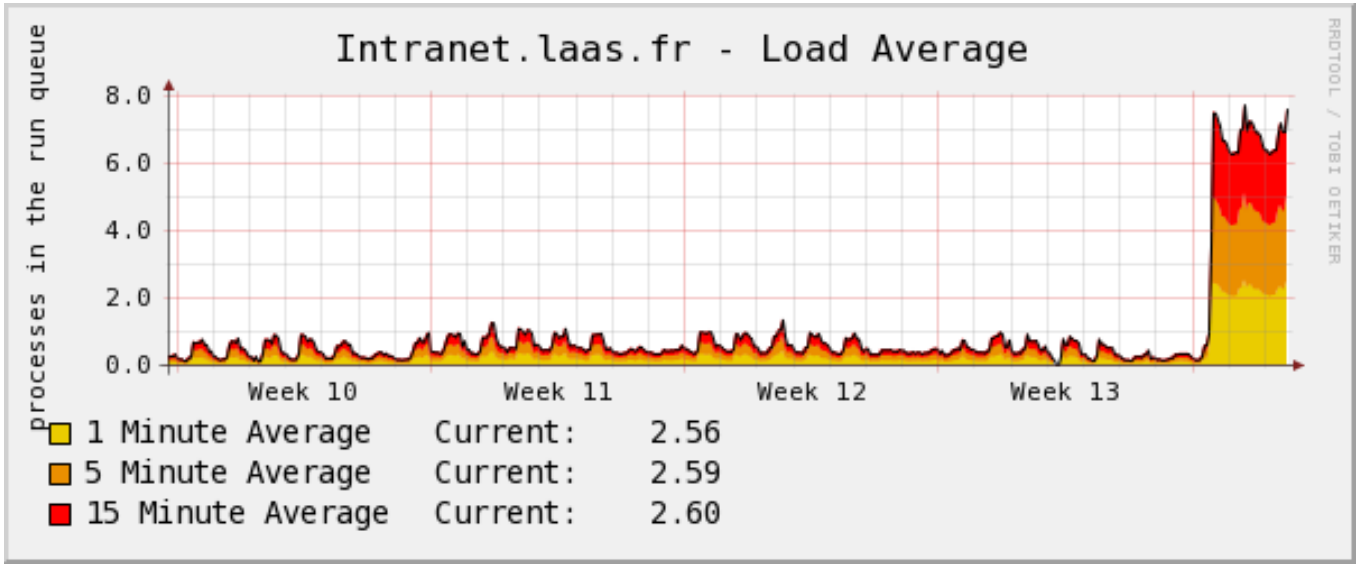
- Tracé de courbes de trafic (ou autres) en fonction du temps.
- Collecte des données par SNMP ou scripts spécifiques
- `http://oss.oetiker.ch/mrtg/`



RRDTOOL

Round **R**obin **D**atabase tool.

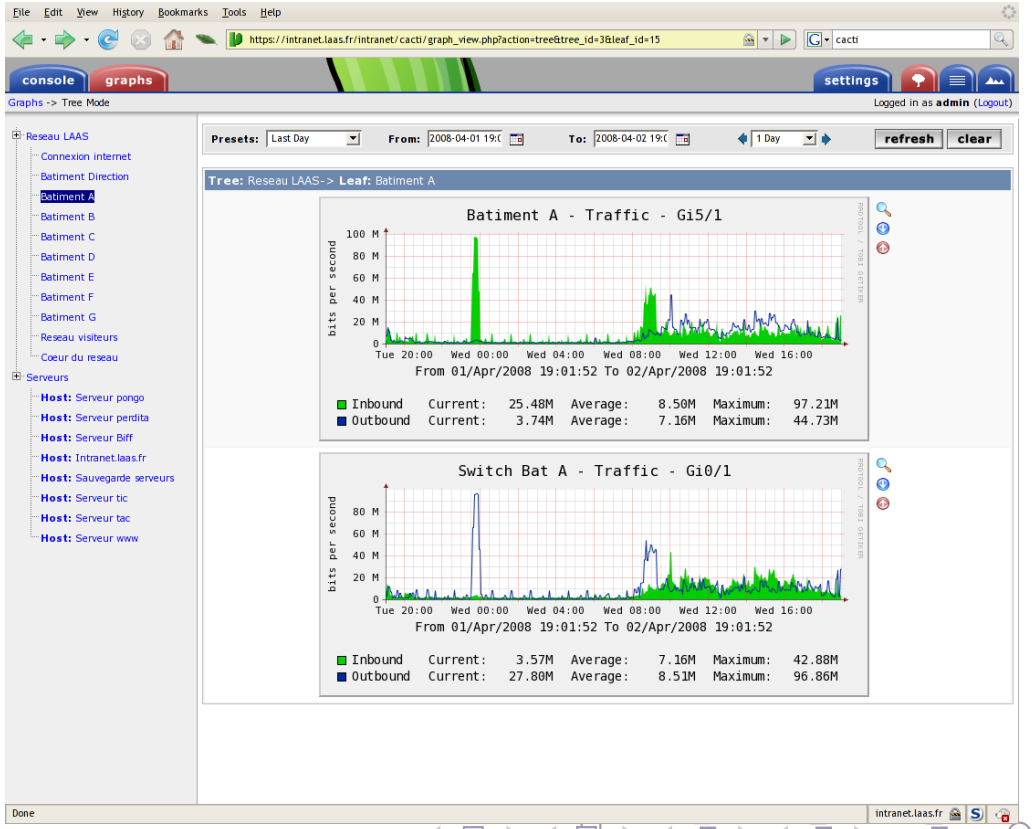
- Généralisation de MRTG:
  - Donne accès à la base de donnée «tournante»
  - Production de graphiques paramétrables et scriptables.
- Interfaces Perl, Python, Ruby, Tcl, PHP.x
- `http://oss.oetiker.ch/rrdtool/`



Cacti

Solution construite au-dessus de RRDtool pour collecter et construire des graphes.

- collecte SNMP, scripts, ...
- templates
- Interface Web
- `http://www.cacti.net/`
- Plugins



Nagios

Système complet de supervision

- Services (SMTP, IMAP, HTTP, PING, etc.)
- Ressources système (charge CPU, espace disque, utilisation mémoire)
- Génération d'alarmes en cas de problèmes
- Exécution de scripts sur évènements
- Interface Web
- Plugins
- Possibilité de fonctionnement en cluster

`http://www.nagios.org/`

Autres outils...

Collecte, Visualisation:

- ganglia `http://ganglia.info` orienté clusters, grilles

Supervision, concurrents de Nagios:

- Zabbix `http://www.zabbix.com/`
- Zenoss `http://www.zenoss.com/`

Analyse de logs, statistiques:

- awstats `http://awstats.sourceforge.net/`

Produits commerciaux : HP OpenView, IBM Tivoli, etc.

Agenda

Que superviser ?

- Quels sont les systèmes et les ports réseau à surveiller ?
- Quelle(s) informations(s) chercher ?
- Comment synthétiser efficacement un grand nombre d'infos ?
- Quelles alarmes générer ? sous quelle forme ?

$\longrightarrow$ Définir des *objectifs* et classer les indicateurs et les alarmes par rapport à ces objectifs.

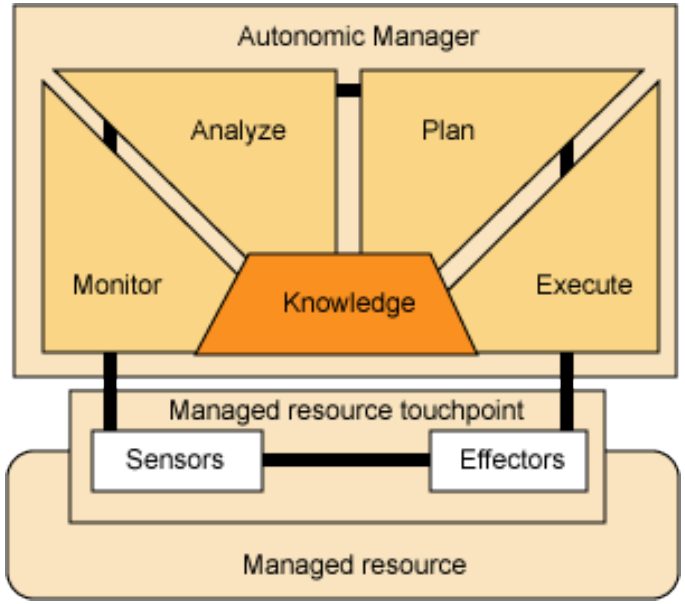
Vers les systèmes autonomiques ??

Référence aux processus biologiques d'auto-régulation du corps humain.

En informatique, concept développé par IBM et Motorola.

Quatre fonctions de base :

- self-configure
- self-protect
- self-heal
- self-optimize



Utilise des approches développées en intelligence artificielle (modélisation, apprentissage, etc.).

`http://www.usenix.org/events/lisa07/tech/`

Plan de la matinée

9h45	NAGIOS *Cedric Hillembrand (CESR)*
10h15	Statistiques d'utilisation des ressources de la plateforme GenoToul à l'INRA : GenoStats *Jean-Marc Larré & Cédric Chappert (INRA)*
10h45	**Pause**
11h15	CACTI *Nicolas Rouanet (INSA)*
11h45	Supervision réseau au CICT *Denis Mirassou (CICT)*
12h15	**Fin**

Questions ?