Supervision réseau

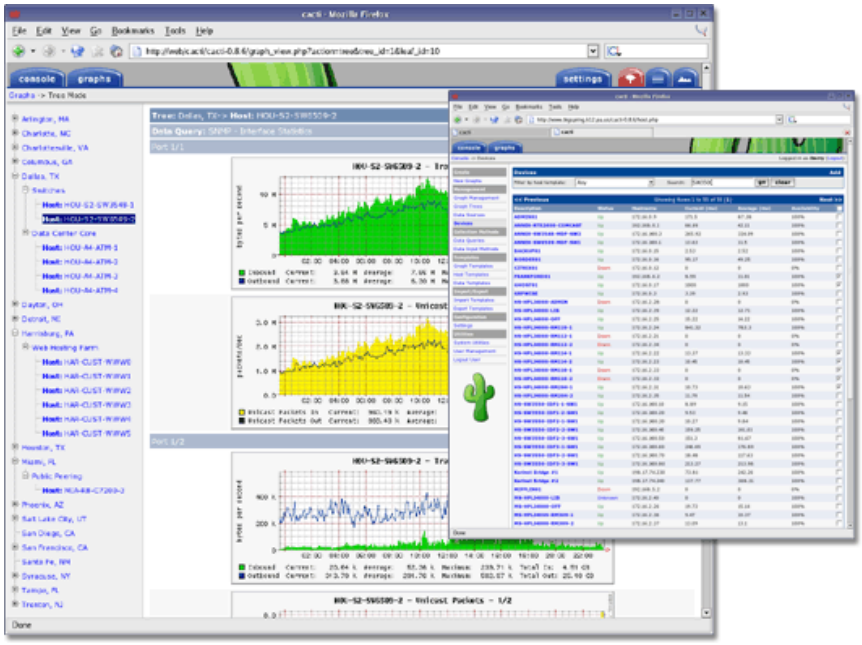


Table des matières

I- Introduction

La supervision réseau (ou monitoring) comprend un ensemble de protocoles, matériels et logiciels informatiques permettant de suivre à distance l'activité d'un réseau informatique. Ces solutions permettent également de cartographier le réseau.

La supervision est particulièrement adaptée pour des réseaux de plus de 50 machines et pour les prestataires de services.

Le principe général est le suivant :
- Des agents (ou sondes) sont placés sur les équipements à surveiller
- Un ou plusieurs serveurs centralisent les informations pour les afficher de manière cohérente aux techniciens ou aux administrateurs.

Il convient de distinguer la supervision qui utilise des technologies quasi temps réel de la gestion de parc informatique qui utilise des technologies moins dynamiques (inventaires de machines, gestion des stocks, ...).

II- Types de surveillance et actions liées

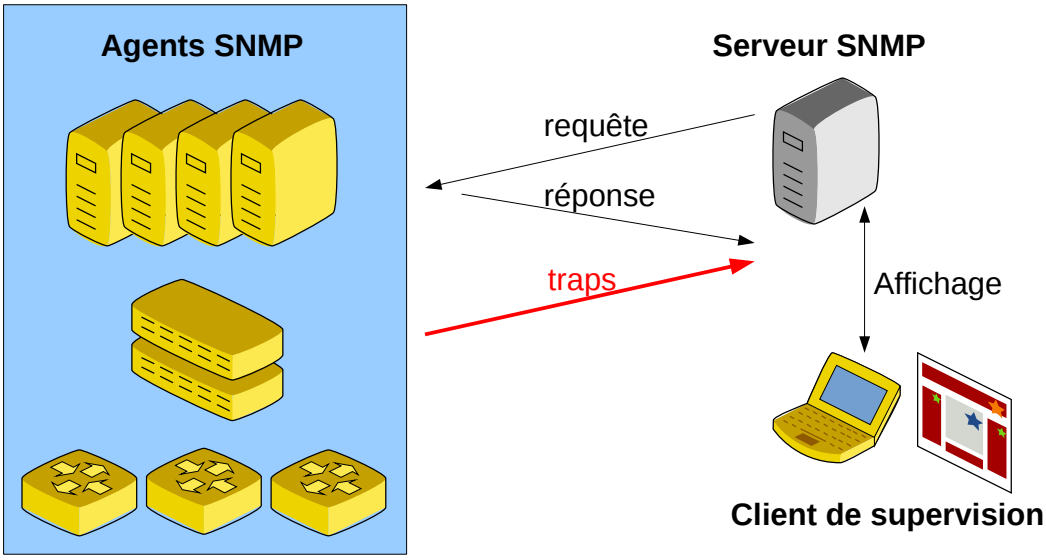
Globalement, les outils de supervision sont utilisés pour la surveillance :
- Matérielle (activité d'un équipement, charge, ...)
- Réseau (débit, latence, taux d'erreur, QoS, protocoles, sécurité ...)
- Système (logs, performances, intégrité)
- Applicative (performances, modifications de configuration, analyse)

Les actions liées aux événements peuvent être :
- Un enregistrement dans un journal
- Un tracé graphique
- Une alerte (mail, SMS, ...)
- Une exécution de script pour automatiser les tâches à faire.

III- Protocoles

SNMP

SNMP est le protocole incontournable de la supervision. C'est un protocole de niveau applicatif. Il sait analyser les informations de tous les niveaux (physiques, réseaux, services, systèmes). Toutes les plateformes peuvent installer le service SNMP (Windows, Linux, Cisco, HP, ...) mais aucune ne l'active par défaut pour raison de sécurité.



Protocole

Les agents de supervision communiquent avec le serveur de trois manière :

- Requête SNMP (du serveur vers l'agent)
- Réponse SNMP (de l'agent vers le serveur)
- Alarme (ou trap) envoyée de l'agent vers le serveur quand un problème arrive.

Communautés

SNMP fonctionne par communauté : Une communauté est un groupe d'agents.

Côté agents :

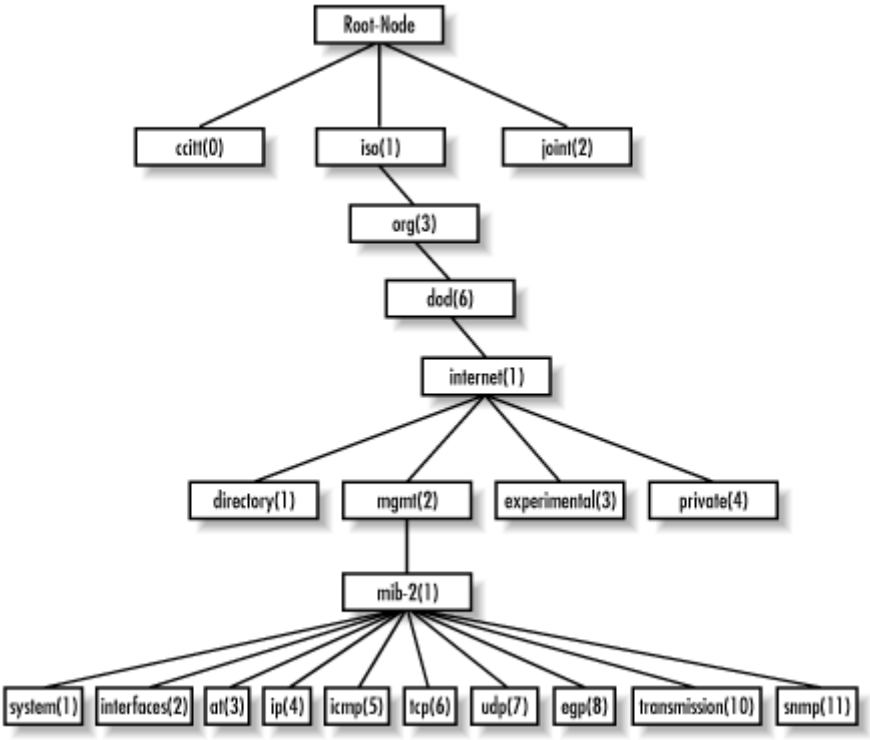
- On créé une communauté publique (souvent nommée **public**) accessible à tous en lecture seule
- On créé une communauté privée (avec un nom quelconque) accessible en lecture/écriture mais protégée par un mot de passe.

Côté serveur, on ajoute les hôtes et on indique les éléments de la MIB à surveiller.

MIB (Management Information Base)

Le protocole spécifie une base de données qui stocke des attributs classées dans un arbre. La MIB utilisée peut-être normalisée (ex : Mib II) ou spécifique.

Exemple partiel de MIB :



Exemple : Requête pour connaître le nom de la zone d'un serveur DNS :
iso.internet.internet.internet.mgmt.mib-2.dns.dnsServMIB.dnsServMIBObjects.
dnsServZone.dnsServZoneTable.dnsServZoneEntry.dnsServZoneName
1.3.6.1.2.1.32.1.1.4.1.1.1

Une liste des MIBs et de leurs objets est présente ici :
http://www.simpleweb.org/ietf/mibs/

Versions :

SNMPv1 n'est plus utilisé aujourd'hui car il est très peu performant dans les échanges de trames. Le standard est la version 2c.
La version 3 apporte la notion de sécurité et de chiffrement mais n'était pas supportée par tous les équipements jusqu'à maintenant.

Sur le sujet :

http://irp.nain-t.net/doku.php/215snmp:start
http://www.frameip.com/snmp/

Solutions applicatives

Pour simplifier le travail de supervision et ne pas être dépendant du protocole SNMP, les logiciels de supervisions développent souvent un protocole ou un agent particulier pour leur solution (agent zabbix, NRPE pour Nagios, etc.).

ICMP

ICMP est le protocole associé à IP (niveau 3) qui permet le dépannage et la surveillance et la détection de problèmes du niveau 3.
Il est utilisé par certains systèmes de supervision d'équipements réseau.
C'est un protocole très simple qui envoie un code d'erreur en cas de problème.

Pour les supervisions systèmes et applicatives, ICMP ne peut être efficace car il est limité au niveau 3.

Autres protocoles

Intel a créé un protocole permettant de gérer la partie matérielle. Ce protocole est assez répandu, il s'appelle IPMI.
Intel présente cette technologie ici :
http://www.intel.com/design/servers/ipmi/ani/index.htm

IV- Solutions de supervision

Il existe de très nombreuses solution de supervision existantes. Le monde du logiciel libre est particulièrement actif dans ce domaine.

Solutions libres les plus connues :

Le site monitoring-fr et son wiki http://wiki.monitoring-fr.org/ expose les solutions libres les plus abouties et donne des tutoriaux pour les configurer.

Parmi ces solutions, les plus utilisée sont :

- Nagios
- Centreon
- Shinken
- Zabbix
- Cacti (graphes)
- Eyes of Network

Solutions propriétaires pour grandes entreprises :

- HP Open View
- IBM Tivoli monitoring
- Microsoft System Center

Solutions propriétaires pour PME :

- PRTG
- Netcrunch

Solutions propriétaires SaaS (cloud) :

- Netvigie
- RG Vision
- Satelliz