SNMP

notes SNMP

Table des matières

1. Description

Agent SNMP

Un agent SNMP est un service réseau, construit en général sur IP et s'éxecutant sur une machine hôte, qui détient un certain nombre d'informations consultables sur le réseau, et qui est également capable d'envoyer des alertes (traps), sous certaines conditions exceptionnelles, à une machine de surveillance réseau (manager). Les informations détenues par un agent sont disposés sous la forme d'un arbre, dont les feuilles représentent les données. Chaque noeud de l'arbre est numéroté, et une information est accéssible en identifiant la feuille depuis la racine en utilisant une numérotation décimale pointée: exp: 1.6.2.3.4

Protocole SNMP (Simple Network Management Protocol)

C'est un protocole très simple qui décrit les échanges d'informations entre un agent SNMP et un manager. Dans sa version la plus simple dispose de 3 commandes:

1. une commande permet de récupérer le contenu d'une variable particulière,
2. une autre permettant de placer une valeur dans une variable
3. une autre permettant le parcours en profondeur d'une partie de l'arbre

MIB (Management infomation base)

Fichier texte nécessaire pour comprendre la nature des informations détenues pas un agent. La totalité des informations détenues pas un agent est en général segmentée en plusieurs fichiers MIB: des fichiers MIB normalisés (SNMPv2), et des fichiers MIB propres au constructeur. Les informations sont décrites de la manière suivante:

- numéro d'identification (numérotation décimale pointée)
- nom de la variable
- type
- éventuellement la liste de valeur possible de la variable avec leur signification

Les alertes susceptibles d'être envoyées par l'agent sont elles décrites par:

- numéro d'identification
- nom de l'alerte
- variables arguments de l'alerte + type

2. Implémentations

2.1. Unix (Paquetage ucd-snmp / net-snmp)

Contient un agent (snmpd), des utilitaires pour interroger un agent (snmpget, snmpset, snmpwalk..), un navigateur (tkmib) Les mibs sont placés dans un répertoire particulier

(/usr/share/snmp/mibs). Le nom du module est indiqué en entête du fichier par une ligne du type:

```
AGENTX-MIB DEFINITIONS ::= BEGIN
```

Les mibs chargés initialement sont indiquées dans la variable MIBS. Exemple:

```
SNMPv2-TC:SNMPv2-MIB:IF-MIB:IP-MIB:TCP-MIB:UDP-MIB:SNMP-VACM-MIB:
HOST-RESOURCES-MIB:NET-SNMP-AGENT-MIB:UCD-SNMP-MIB:AGENTX-MIB:
DISMAN-EVENT-MIB:LEXMARK-PVT-MIB:BRIDGE-MIB:AXIS-MIB:
WINDOWS-NT-PERFORMANCE:DHCP-MIB:DNS-MIB:
WINS-MIB:HttpServer-MIB:Printer-MIB:IBM8275-2XX-MIB:IBM8275-RC-MIB:
IBMSWITCH-MIB:LanMgr-Mib-II-MIB:NCL1135V2-MIB:NCL1170-MIB:
NCL1170-GLOBAL-MIB:NCL1170-CONFIG-MIB:NCL1170-COMMAND-MIB:
NCL1170-PER-MIB:NCL1170-ETHERNET-MIB:NCL1170-RADIO-PEERS-MIB:
NCL1170-RADIO-STATS-MIB:NCL1170-RADIO-STAT-RX-MIB:NCL1170-RADIO-STAT-TX-MIB:
NCL1170-RADIO-STAT-GEN-MIB:CISCO-MIB:CISCO-SMI:CISCO-CDP-MIB:
CISCO-FLASH-MIB:CISCO-FLASH-MIB:CISCO-IMAGE-MIB:CISCO-ISDN-MIB:
CISCO-QUEUE-MIB:CISCO-TC:CISCO-SNAPSHOT-MIB:CISCO-ENVMON-MIB:
OLD-CISCO-CHASSIS-MIB
```

2.2. Windows

L'agent SNMP livré avec windows 98/NT n'est pas très performant, mais une extension gratuite est disponible sur le net (performance mib)

3. OpenNMS

3.1. Principes

1. Découverte de nouveaux noeuds: Réalisée en envoyant successivement des paquets ICMP sur un ensemble de plages d'adresses et en examinant les réponses.
2. Détermination des aptitudes de chaques noeuds découverts
   1. en tentant des connexions sur un ensemble de ports déterminés correspondant à des services réseaux particuliers et connus.
   2. en récupérant certaines informations de l'agent SNMP: (Est-ce un routeur ou un Switch ?)

   Cette liste d'aptitude est utilisée pour regrouper les noeuds en catégories (routeur, serveurs de noms, bases de données...).
3. Surveilance régulière des noeuds, en faisant des tests sur ensemble des aptitudes découvertes pour chaque noeud.
4. Collecte d'informations via l'agent SNMP au sein de bases de données cycliques sur une période donnée (1 an) (activité processeur, disques, réseau...)
5. Enregistrement des alertes SNMP envoyés par les agents.
6. Envoi d'alertes à des utilisateurs ou des groupes d'utilisateurs particuliers sur un média donné (téléphone, email, bureau) en fonction d'évènements particuliers internes (un

service distant s'est arreté) ou externes (SNMP).

3.2. Configuration:

La configuration d'opennms est décrite en xml (à part certains qui sont des fichiers de configuration niveau java --- extension ".property") dans un ensemble de fichiers se trouvant dans le repertoire /opt/OpenNMS/etc. .

3.3. Manipulations

- Enlever un noeud de la base
  1. Derterminer le nodeid du noeud a effacer
     ```
     > select nodeid from ipinterface where ipaddr = $ipaddr
     ```
  2. Effacer toutes les interfaces
     ```
     > delete from ipinterface where nodeid = $nodeid
     ```
  3. Effacer les évènements et outages liés à ce noeud
     ```
     > delete from outages where nodeid = $nodeid
     > delete from events where nodeid = $nodeid
     > delete from snmpinterfce where nodeid = $nodeid
     > delete from ifservices where nodeid = $nodeid
     > delete from ipinterface where nodeid = $nodeid
     > delete from node where nodeid = $nodeid
     ```
  4. Effacer les fichier rrd
     ```
     > rm -rf /opt/OpenNMS/share/rrd/$nodeid
     ```

  A partir de la version 1.1, on peut enlever un noeud de la base à partir de l'application, et effacer les données rrd.
- Nettoyage de la base (niveau évènements)

3.4. Fichiers OpenNMS

datacollection-config.xml:
Configure la fréquence/durée de la collecte d'informations par SNMP et la façon (OIDs) dont sont collectées les données suivant le type de système détecté (variable sysObjectID). Balises:

<rrd>
configure la fréquence/durée des collectes
<groups>
contient un ensemble de groupe de collecte
<group>
décrit un ensemble des variables collectée: OIDs, index (si tableau), type de la variable. Cet ensemble est nommé et utilisé dans les groupes <systemDef>
<systems>

contient l'ensemble des associations system/collecte

<systemDef>

association entre un type de systeme (reconnu grâce à la variable SNMP sysObjectID) et une collecte.

capsd-configuration.xml

Décrit la façon de detecter un protocole (ip) sur une machine et configure certains services particulier: Balises:

<protocol-plugin>

décrit la manière de détecter l'activité d'un protocole en fontion d'un greffon déjà défini (ex: org.opennms.netmgt.capsd.TcpPlugin)

<smb-config>

configuration pour le plugin smb/netbios

<ip-management>

décrit les intervalles/listes d'addresses ip utilisées ou exclues de la detection de protocole.

collectd-configuration.xml

Contient l'ensemble des associations noeuds/adresses ip, collecteur (pour l'instant uniquement SNMP), et calendrier/horaire de collecte Balises:

<package>

permet de nommer l'association

<filter>

collecte uniquement si le filtre laisse passer le noeud

<service>

paramètre le collecteur

discovery-configuration.xml

Décrit les plages d'adresses ips utilisées pour detecter les machines/noeuds du réseau. Balises:

<include-range>

adresse de début/fin de la plage

<include-url>

inclut un fichier/liste d'adresses ip (une/ligne)

eventconf.xml:

Permet à opennms de reconnaitre et traduire des évènements (en général des alertes SNMP) en clair pour les transmettre sous la forme de notifications aux utilisateurs OpenNMS Balises:

<global>

configuration générale

<event-file>

permet d'inclure un fichier de descriptions (en générale dans

/opt/OpenNMS/etc/events)
<event>
décrit un évènement