Simple Network Management Protocol

Departamento de Sistemas Telemáticos y Computación (GSyC)

http://gsyc.urjc.es

Diciembre de 2013

SNMP: Simple Network Management Protocol

Es un protocolo del IETF para administrar dispositivos de red

- La mayoría de las redes están formadas por un número elevado de dispositivos: encaminadores, conmutadores (*switches*), servidores, estaciones de trabajo, dispositivos móviles, etc
- Necesariamente heterogéneos: distinto propósito, tamaño, fabricante... La administración tiende a complicarse
- La finalidad de SNMP es contar con un único protocolo que permita administrar uniformemente todos estos dispositivos. Típicamente de forma centralizada, o racionalmente distribuida si es necesario

- Que el protocolo esté desarrolado por el IETF (*Internet Engineering Task Force*) implica que su ámbito es el mundo IP
- Cuando decimos *administrar* queremos decir
  - *Configurar*
    Llevar el sistema a un modo de funcionamiento adecuado
  - *Monitorizar*
    Observar mediante aparatos especiales el curso de uno o varios parámetros fisiológicos o de otra naturaleza para detectar posibles anomalías (D.R.A.E.)
  - *Corregir*
    Subsanar los problemas que se produzcan, dentro de nuestros requisitos de tiempo y coste

Conceptos básicos

Los elementos fundamentales de una red que emplea SNMP son:

- Dispositivos administrados (*managed devices*). En cada uno se ejecuta un *agente*
- Administrador (*manager*). Dispositivo desde el que se administra la red. En él se ejecuta el *Network Management System*, NMS, sistema de administración de red.
- *Management Information Base*, MIB
  Base de datos de información gestionada.

Dispositivos administrados

- Ordenadores, routers, impresoras, conmutadores, teléfonos IP, cámaras de vídeo, sensores, SAI (sistemas de alimentación ininterrumpida) / UPS *Uninterruptible Power Supply*
- En cada uno se ejecuta un agente que atiende las peticiones de lectura o escritura y genera las *traps*

Administrador

- El administrador (*manager*) es el dispositivo donde se ejecuta el NMS
- *Network Management System*, NMS
  Sistema de administración de red. Cliente que se ejecuta en el administrador, que envía a los servidores peticiones de lectura y escritura y recibe las *traps*

Management Information Base

- El *Management Information Base*, MIB, *Base de datos de información gestionada* es un espacio de nombres organizado jerárquicamente en forma de árbol, que contiene la información que puede leerse y/o escribirse mediante SNMP

Cada elemento de información es un objeto, que tiene su OID. Un OID tiene dos representaciones, una numérica y otra textual
Ejemplo:
`.1.3.6.1.2.1.1.3`
`iso.org.dod.internet.mgmt.mib-2.system.sysUpTime`

Operaciones de SNMP

Lo *único* que hace SNMP es leer y escribir variables en dispositivos de red, así como enviar mensajes asíncronos
Son 4 operaciones fundamentales

- *get*
- *get-next*
- *set*
- *trap*

Esto aparentemente justifica la palabra *simple* en el nombre del protocolo. En realidad es bastante complejo, aunque no tanto como parece a primera vista.

- El uso más habitual se limita a la monitorización, sin configuración. Esto es, se usa *GetRequest* pero raramente se emplea *SetRequest*
- Aunque el protocolo está bastante extendido, cada fabricante suele centrarse en su propio mecanismo de administración remota, añadiendo SNMP como un *extra* que no siempre es tan maduro como debiera
- En Unix y Linux se usan mucho otras herramientas de monitorización como Nagios y Zabbix, que ofrecen sus propios servicios pero también incluyen SNMP

- SNMP v1. Año 1988. RFC 1065, 1066, 1067
  Muy inseguro. Contraseñas transmitidas en texto claro
- SNMP v2. Año 1993. RFC 1441, 1452
  Introduce *GetBulkRequest*
  Mejora la seguridad, pero resulta muy complicado y apenas se utiliza. En la práctica se sigue empleando una versión 2 simplificada (SNMP v2c, RFC 1901, 1908), que mantiene el envío de contraseñas en abierto
- SNMP v3. Año 2002. Incluye autenticación, confidencialidad e integridad. Rehace toda la notación, aunque mantiene funcionalidad.

Uno de los problemas de SNMP es que toda su terminología es muy peculiar y resulta confusa.
Ejemplos:

- A una contraseña la denomina *community string*
- A un sniffer le llama *probe* (sonda)

SNMP v3

- Añade seguridad a SNMP, prácticamente inexistente en versiones anteriores
  Usa criptografía simétrica. Hashes con MD5 y SHA.
- Renombra y reorganiza todos los conceptos. El mecanismo acaba siendo esencialmente el mismo, pero definido de forma más precisa
- Formalmente, ya no hay administradores y agentes. Todo son *entidades*.
  (Aunque en la práctica suele mantenerse la nomeclatura tradicional)

net-snmp

net-snmp es una implementación libre de snmp. La habitual en Unix y Linux

1. Instalar los paquetes snmp, snmpd, snmp-mibs-downloader, tkmib
2. Ejecutar `download-mibs`
   para instalar los mibs de IANA e IETF en `/usr/share/mibs`
3. Comentar (inhabilitar) la única línea que hay en `/etc/snmp/snmp.conf`

`tkmib` es un visor gráfico de MIB

Ficheros de configuración

- `snmp.conf`
  Configuración de todas la aplicaciones: Autenticación, formatos de e/s, depuración
- `snmpd.conf`
  Configuración del agente
- `snmptrapd.conf`
  Configuración del receptor de eventos

El script `snmpconf` va preguntando al usuarios los parámetros a configurar

```
snmpconf -g basic_setup
```

manejo del demonio

- `/etc/init.d/snmpd [start|stop|restart|reload|force-reload|status]`

```
$ ps -ef | grep snmpd
    root   12345     1  0   Nov 16 ?    2:35 /usr/local/bin/snmpd
$ kill -HUP 12345
```