Práctica 1: Configuración de un agente de gestión

Objetivos

- Conocer los parámetros de configuración de un agente: comunidad, vistas, acceso y valores de objetos de MIBs del sistema.
- Familiarizarse con las operaciones soportadas por SNMPv1: *snmpget, snmpgetnext, snmpset.*
- Familiarizarse con los contenidos de MIB-2.

Herramientas necesarias

- Ordenador con sistema operativo Linux (en el laboratorio se utiliza la distribución Ubuntu).
- Paquete de gestión Net-snmp. Instalar los siguientes paquetes: *snmp* y *snmpd*.

Descripción

Se supone conocimiento de comandos básicos de administración de red y de herramientas de análisis de tráfico:

- **Unix:** *ifconfig, route, netstat, ps, kill*…. (ayuda con páginas man: man comando)
- **WhireShark (Ethereal)**

Desarrollo de la práctica

Ejercicio 1.

Hacer un fichero de configuración local snmpd.conf. No es necesario pero puede basarse en el fichero de ejemplo. (Ver enlaces anexos de ejemplo y ayuda). Si le da problemas se recomienda comenzar por un fichero en blanco y escribir una configuración sencilla.

Ejemplo de configuración sencilla:

```
com2sec npublic 192.168.1.0/24 public
group gpublic v1 npublic
view todo included mib-2
access gpublic "" v1 noauth exact todo none none
```

El fichero de configuración final (mysnmpd.conf) deberá tener la siguiente configuración:

Acceso permitido a cualquier gestor que tenga una dirección IP que esté dentro del rango de la red 192.168.163.0/24.

Versión: snmp v1

Vistas:
- Una vista denominada ***todo*** donde se vea las mib-2 excepto snmp.
- Una vista denominada ***protocolos*** donde se vea interfaces, ip, snmp, icmp, tcp y udp.
- Una vista denominada ***sistema*** donde se vea system.

Acceso de comunidades:
- Comunidad ***privada*** con acceso de lectura y escritura en la vista ***sistema***.
- Comunidad ***publica*** con acceso de sólo lectura en la vista ***todo***.
- Comunidad ***adminet*** con acceso lectura y escritura en la vista ***protocolos***.

Configurar el valor de las instancias del grupo system:
- *Syscontact*
- *Syslocation*

Ejercicio 2.

Arrancar el agente (snmpd) con los ficheros de configuración locales y en el puerto 1500 (192.168.163.XX:1500).

`/usr/sbin/snmpd` (ver parámetros en la ayuda)

Se recomienda con la opción –f para que el gestor no devuelva el control al sistema, y –d para visualizar formato de los mensajes recibidos de las respuestas generadas. Si tiene problemas con el agente utilice la opción –D. El fichero de configuración local se carga con la opción –c ./mysnmpd.conf. Forzar a una dirección y puerto 192.168.163.XX:1500.

Ejemplo: `/usr/sbin/snmpd -c ./mysnmpd.conf -f -d 192.168.163.XX:1500`

Ejercicio 3.

Antes de comenzar a usar comandos para probar el agente, este ejercicio le ayudará a familiarizarse con la forma de nombrar los objetos.

En el directorio /usr/share/snmp/mibs tiene los diferentes ficheros que contienen los módulos de las MIBs que soporta el agente (declarados en ASN.1).

Mirar las páginas man (y/o el tutorial en el web) del comando *snmptranslate*. Mirar también las páginas man de *snmpcmd*, para tener información genérica válida para los diferentes comandos que se usarán.

Utilizar la opción –IR de *snmptranslate* para localizar el nombre simbólico del objeto *sysUptime* y la opción *On* valor numérico del OID.

Probar los siguientes comandos:

- `snmptranslate sysUpTime`
- `snmptranslate –IR sysUpTime`
- `snmptranslate –IR –On sysUpTime`

Utilizar *snmptranslate* para saber el nombre simbólico asignado a los OIDs siguientes:

- .1.3.6.1.2.1.1.1.0
- .1.3.6.1.2.1.2.1.0
- .1.3.6.1.2.1.3.1.0
- .1.3.6.1.2.1.4.1.0
- .1.3.6.1.2.1.5.1.0
- .1.3.6.1.2.1.6.1.0
- .1.3.6.1.2.1.7.1.0
- .1.3.6.1.2.1.11.1.0

Con este comando sabrá en qué módulos de MIBs se encuentra definido cada OID de los grupos de MIB-2.

Utilizar *snmptranslate* para visualizar el árbol (opción -Tp) del grupo system del módulo RFC1213-MIB (RFC1213-MIB::*system*). De esta forma puede conocer los OIDs accesibles dentro de cada grupo (*system*, *ip*, *udp*, …).

Ejercicio 4.

Realizar consultas con el comando *snmpget* de los objetos del grupo *system* para conocer el valor que tienen.

Ejemplo: `snmpget -v1 -c publica` 192.168.163.xx`:1500 system.1.0`

Ejercicio 5.

Cambiar el valor de *system.sysName.0* con el comando *snmpset*.

Ejercicio 6.

Comprobar qué sucede si intenta:

- Leer una instancia de una vista con una comunidad que no tiene permisos de lectura.
- Modificar una instancia de una vista con una comunidad que no tiene permisos de escritura ((p.e. *system.sysName.0*)).
- Modificar una instancia que no es de escritura, con una comunidad con la que se tiene permiso de escritura (p.e. *system.sysDescr.0*).
- Leer o modificar una instancia con una comunidad no definida.

Ejercicio 7.

Consultar la tabla de interfaces (*interfaces.ifTable*) con el comando *snmpgetnext*.

¿Qué sucede cuando llega al final de una tabla?

¿Qué sucede si usa *snmpgetnext* y llega al final de la vista definida para la comunidad que usa?

Ejercicio 8.

Abrir conexiones (ftp, telnet, http...) y consultar la tabla de conexiones abiertas con el comando *snmpwalk*: *tcp.tcpConnTable*.

Utilizar *snmptable* para consultar la tabla. Observar la diferencia.

Ejercicio 9.

Monitoriza *ip.ipInReceives.0* con el comnado *snmpdelta* y un periodo de monitorización de 5 segundos.

Ejercicio 10.

Pruebe las posibilidades de limitar el acceso con las vista, ¿Se puede definir una vista que sólo dé acceso a un objeto?

Presentación y evaluación

Cada alumno debe explicar de forma individual al profesor en clase de laboratorio cómo ha realizado la práctica y enseñarle el funcionamiento de la aplicación.

Deberá presentar una memoria al profesor con los resultados de los ejercicios y comentarios de los problemas que ha tenido.

En caso de retraso en la fecha de entrega se producirá una penalización en la nota de la práctica.

Bibliografía

- Net-SNMP: http://www.net-snmp.org/
- http://net-snmp.sourceforge.net/docs/man/snmpd.conf.html
- **Agente:** *man snmpd*
- **Configuración del agente:** *man snmpd.conf*
- **Operaciones SNMP:**
  - *man snmpget*
  - *man snmpgetnext*
  - *man snmpset*
  - *man snmpwalk*