redes, snmp

SNMP

SNMP Simple Network Manager Protocol es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Permite a los administradores supervisar el funcionamiento de la red, buscar y resolver sus problemas, y planear su crecimiento.

El protocolo SNMP tiene dos formas de funcionar: polling y traps. El polling consiste en lanzar consultas remotas a demanda , y los traps son mensajes que envían los dispositivos SNMP a una dirección configurada basándose en cambios o eventos. Los polling realizan operaciones síncronas de consultas y los traps funcionan de forma asíncrona.

SNMP Polling

Se lanza un chequeo contra la dirección IP de un dispositivo, para lo cual se necesita el nombre de la comunidad SNMP configurada en ese dispositivo en concreto.

El nombre de la comunidad es una cadena alfanumérica empleada como barrera de seguridad para autorizar la operación. Además se utiliza una comunidad sólo omo lectura de los parámetros y otra para escribir o cambiar dichos parámetros.

Cuando lanzamos un chequeo SNMP contra un dispositivo se obtiene un listado con una gran cantidad de información difícil de interpretar, ya que lo que muestra son unas secuencias de números que se asignan jerárquicamente y que permite identificar objetos en la red. Dichas secuencias de números, identificador de objetos, se denominan OIDs y se corresponden con un parámetro determinado de dicho dispositivo.

Para poder interpretar los datos se usan unos ficheros MIBs, exclusivos de cada dispositivo.

Estos ficheros son suministrador por el fabricante dle dispositivo, auqnue no siempre es así . Si queremos buscar un MIB de un dispositivo concreto podemos probar en Free online MIB database

```
snmpwalk –v 1 –c public 192.168.2.100
```

MIB (Management Information Base)

MIB es una Base de Información de Administración (Management Information Base, MIB) es una colección de información que está organizada jerárquicamente.

Si conocemos el OID podemos ejecutar la consulta indicando dicho código tras la dirección IP, por ejemplo

```
snmpwalk –v 1 –c public 192.168.2.100 IF-MIB::ifPhysAddress.1
```

SNMP TRAPS

Con traps no tenemos que lanzar consultas como cuando usamos polling. Con este método sólo necesitamos configurar nuestros dispositivos para enviar los trap cuando se cumplan las circunstancias especificadas, y en segundo lugar una herramienta que pueda recoger los trap SNMP recibidos.

La recepción de traps puede hacerse en Linux con ayuda del demonio snmptrapd, para instalarlo en Centos

```
yum install net-snmp-utils net-snmp-libs net-snmp
```

Instalación

Ejecutaremos el comando:

```
# apt-get install snmp snmpd
```

con lo que instalaremos tanto el cliente como el servidor SNMP. A continuación debemos cambiar algunas opciones de configuración para permitir la conexión al servidor SNMP desde otras máquinas y que puedan obtener datos.

Configuración

En primer lugar modificaremos la opción SNMPDOPTS del archivo /etc/default/snmpd:

```
 # nano /etc/default/snmpd
```

```
 SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -I -smux -p /var/run/snmpd.pid
127.0.0.1'
```

de tal forma que quede como sigue:

```
 SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -I -smux -p /var/run/snmpd.pid'
```

O ejecutar el siguiente comando:

```
 # sed -i -e "s/^\(SNMPDOPTS.*\) 127.*/\1'/" /etc/default/snmpd
```

El segundo y último archivo que debemos configurar es el situado en /etc/snmp/snmpd.conf. Buscaremos el siguiente bloque de texto:

```
# nano /etc/snmp/snmpd.conf
```

```
####
# First, map the community name (COMMUNITY) into a security name
# (local and mynetwork, depending on where the request is coming
# from):

#       sec.name  source          community
com2sec paranoid  default         public
#com2sec readonly  default         public
#com2sec readwrite default         private
```

y lo modificaremos para que quede como sigue:

```
####
# First, map the community name (COMMUNITY) into a security name
# (local and mynetwork, depending on where the request is coming
# from):

#       sec.name  source          community
#com2sec paranoid  default         public
com2sec readonly  default         public
#com2sec readwrite default         private
```

O simplemente ejecutar el siguiente comando:

```
# sed -i \
      -e 's/^\(com2sec.*paranoid.*default.*public\).*/\#\1/' \
      -e 's/^#\(com2sec.*readonly.*default.*public\).*/\1/' \
      /etc/snmp/snmpd.conf
```

A continuación debemos reiniciar el servidor SNMP para que aplique los cambios:

```
# /etc/init.d/snmpd restart
```

Por último podemos comprobar que todo funciona correctamente con el siguiente comando:

```
# snmpwalk -v 2c -c public localhost
```

```
SNMPv2-MIB::sysDescr.0 = STRING: Linux debian 2.6.18-4-686 #1 SMP Wed May 9
23:03:12 UTC 2007 i686
SNMPv2-MIB::sysObjectID.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (1339340) 3:43:13.40
[...]
IPV6-MIB::ipv6IfAdminStatus.2 = INTEGER: up(1)
IPV6-MIB::ipv6IfOperStatus.1 = INTEGER: up(1)
IPV6-MIB::ipv6IfOperStatus.2 = INTEGER: up(1)
```

SNMPWALK

Obtener información de un dispositivo

```
snmpwalk -v 2c -c <comunidad> <ip> system
```

Navegadores SNMP

- http://sourceforge.net/projects/snmpb/?source=dlp
- http://www.mg-soft.si/download.html#MIBBROWSERWIN
- http://sourceforge.net/projects/jmibbrowser/?source=recommended

Referencias

- Artículo original de →http://wiki.nutum.es/linux/nagios/centreon2/snmp?s[]=snmp
- http://es.wikipedia.org/wiki/Simple_Network_Management_Protocol
- http://www.soportejm.com.sv/kb/index.php/article/mibs
- https://blog.pandorafms.org/es/monitorizacion-snmp/

From:
https://intrusos.info/ - **LCWIKI**

Permanent link:
https://intrusos.info/doku.php?id=red:snmp&rev=1516284317

Last update: **2023/01/18 13:57**