TP 3 - Simple Network Management Protocol (SNMP)

Fecha de Entrega: 18/09/2023.

Objetivo: Conocer los parámetros de configuración de un agente: comunidad, vistas, acceso y valores de objetos de MIBs del sistema y familiarizarse con las operaciones soportadas por SNMP. Categorías ISO: **FCA**PS.

Bibliografía

- GORALSKI, W. 2017. Capítulo 28: "Simple Network Management Protocol (SNMP)" en *The Illustrated Network: How TCP/IP Works in a Modern Network (2nd ed)*. Morgan Kaufmann. https://www.sciencedirect.com/science/book/9780128110270
- MAURO, D., SCHMIDT. K., 2005. Capítulo 2: "SNMPv1 and SNMPv2" y Capítulo 3: "SNMPv3" en *Essential SNMP (2nd ed)*. O'Reilly Media.

Experiencia de laboratorio

1. ¿Qué podría hacer para descubrir cuales equipos de una red determinada tienen el servicio SNMP disponible? Haga una prueba en el laboratorio o en la red de su hogar y comente como llegó a éstas conclusiones.

2. Instalar el paquete `snmp` para obtener los clientes que permitirán interactuar contra agentes remotos mediante tal protocolo. Realice una captura de una consulta SNMP utilizando el utilizando el comando snmpget (consulte por ejemplo el nombre del dispositivo OID 1.3.6.1.2.1.1.5.0). Guarde la captura como "smnpget.pcapng".

Sintaxis y ejemplo de uso

```
snmpget    -v2c -c COMUNIDAD AGENTE OID
snmpwalk   -v2c -c COMUNIDAD AGENTE [OID]
snmpset    -v2c -c COMUNIDAD AGENTE OID TIPO VALOR
snmpstatus -v2c -c COMUNIDAD AGENTE

Donde:
    COMUNIDAD  es el nombre de la comunidad con la que se identificará el cliente
    AGENTE     es la dirección IP o nombre de host a quien se consultará
    OID        es el objeto a consultar (o en blanco para solicitar todo)
    TIPO       es el tipo de datos del objeto (s=string, i=integer, ...)
    VALOR      es el valor que se desea asignar al objeto
    -m ALL     hace que el comando resuelva el OID a nombre, de ser posible

$ snmpget -v2c -c public localhost iso.3.6.1.2.1.1.1.0
iso.3.6.1.2.1.1.1.0 = STRING: "Linux geopistol 3.13.0-32-generic #57-Ubuntu SMP"

$ snmpwalk -v2c -c public -m ALL 170.210.101.102 SNMPv2-MIB::sysName
SNMPv2-MIB::sysName.0 = STRING: 409-Samsung

$ snmpstatus -v2c -c public demo.pysnmp.com
[UDP: [20.163.207.223]:161->[0.0.0.0]:41875]=>[#SNMP Agent] Up: 32 days, 1:56:10.41
Interfaces: 2, Recv/Trans packets: 337109336/150884842 | IP: 0/0
```

Utilizando el cliente SNMP para monitoreo 3. Realizar consultas SNMP al dispositivo indicado por el docente.

a. Obtener los valores que indiquen el estado de la bandeja de papel y el identificador del nombre del equipo. Indicar cuales son los OID correspondientes y especificar los comandos utilizados.

b. ¿Qué otra información, que considera útil, podría ser recuperada del agente?

c. ¿Qué procedimientos y herramientas utilizó para descubrir los OID que resultan interesantes?

4. Instalar el paquete `snmp-mibs-downloader` y descargar las bases mediante la herramienta `download-mibs` . Editar el archivo `/etc/snmp/snmp.conf` y comentar la línea existente con `#` (el archivo debería contener entonces solo `# mibs :`) Repetir las consultas anteriores. ¿Qué diferencia aprecia? ¿A qué se debe?

5. Utilizar los comandos `snmpwalk` y `snmpbulkwalk` para consultar la rama `system` . Realizar una captura para cada una de las ejecuciones, medir el tiempo de ejecución de ambos comandos y contrastarlos. Recuerde que el comando `time` , antepuesto a otro, permite realizar ésta medición (`man time` para más información). Analice las diferencias. Guarde las capturas con el nombre "snmpwalk.pcapng" y "snmpbulkwalk.pcapng" respectivamente y anote las diferencias de tiempo obtenidas.

Utilizando el cliente SNMP para control

6. Habilite y deshabilite un puerto en el switch administrable provisto por el equipo docente en el laboratorio.

7. Obtenga el listado de las interfaces de red del switch y guarde la salida en un archivo denominado "tabla-switch.txt".

Recepción de TRAPS SNMP

8. En este ejercicio el docente configurará un Switch administrable para que envíe Traps SNMP a los equipos de los estudiantes.

9. Inicie una captura de tráfico filtrando por puertos 161 y 162 (`-f 'port snmp'`). Luego utilice el comando `nc` para iniciar un **servidor UDP** en escucha en el puerto correspondiente a la recepción de traps SNMP. Aguarde la recepción del Trap (lo detectará por la salida de datos binarios en pantalla). Finalice y guarde la captura con nombre "snmptrap.pcapng"

Trabajo práctico

1. ¿Qué comandos y aplicaciones necesita para poder hacer una consulta SNMP? (paquete `snmp`). En cuanto a la información que brinda un agente ⌂:

   a. ¿Cómo es posible conocer toda su información pública? Especifique los comandos que se deberían utilizar utilizados.

   b. Como es posible saber que versiones de SNMP soporta el agente.

2. ¿Qué características tienen las OID? ¿Qué es un MIB?

3. El agente que trabaja con la versión 2 o 2c del protocolo, ¿Brinda solo información a la comunidad pública? ¿Cómo es posible saberlo? Describa, con un alto nivel de abstracción, los pasos necesarios para poder acceder a dicha información.

4. A partir de la captura realizada "snmpget.pcapng", elija un mensaje SNMP en particular y describa la PDU ejemplificando con los datos de la misma. Grafique además un esquema en el que identifique los equipos involucrados y sus roles desde el punto de vista del protocolo SNMP.

5. Analice la captura realizada en la experiencia de laboratorio "snmpwalk.pcapng" "snmpbulkwalk.pcapng" ¿Qué diferencias observa entre ambas capturas? ¿Qué implicaciones tiene cada uno en el tráfico de la red y cómo explica la diferencia en el tiempo de ejecución?

6. ¿Que necesita una estación de monitoreo para poder recibir y procesar un Trap SNMP? ¿Es prudente cambiar el puerto en el que se reciben las traps?.

7. Analice la captura "snmptrap.pcapng" (puede configurar Wireshark para habilitar la resolución de OID a nombre en el menú Edit » Preferences » Name Resolution » Enable OID Resolution- Reinicie Wireshark para que cargue las MIBs existentes). A partir de la PDU correspondiente al TRAP indique: ¿qué protocolo utiliza en cada capa OSI? ¿a qué evento corresponde la trap? ¿qué información se incluye?

DESAFÍO: Instalar y configurar un servidor SNMPv3 en su sistema linux (paquete `snmpd`). Configurar el agente/servidor para que brinde a su comunidad pública únicamente información básica de su contacto. Explique brevemente qué ajustes tuvo que realizar en el archivo de configuración `/etc/snmp/snmpd.conf`.

Guía de lectura

1. ¿Qué es SNMP? ¿Que elementos contiene su arquitectura?

2. ¿Qué es un OID? ¿Cómo está compuesta?

3. ¿Que es un MIB?

4. ¿Que ventaja tiene la versión 3 protocolo SNMP respecto de las versiones anteriores?

5. ¿Qué es un Trap SNMP y cómo funciona?

6. ¿Por qué es mejor consultar mediante *bulkwalk* respecto de *walk*?

7. ¿Qué alternativas existen a SNMP?

8. ¿Qué incluye RMON?