Taller de Gestión de Redes 2017

Taller Obligatorio

Objetivos

Este trabajo tiene los siguientes objetivos:

- Estudiar las estructuras de datos y definiciones provistos por SMI para facilitar la comprensión de las diferentes MIBs en SNMP.
- Entrenar el manejo de los comandos básicos provistos por la librería *Net-SNMP* [1], conocer el agente y los mecanismos de extensión que éste permite.
- Por último, familiarizarse con el uso de notificaciones SNMP asíncronas y su utilidad.

Para esto, se deberán responder **de forma individual** las preguntas y ejercicios planteados.

Parte 1

Preguntas

1. Explique en forma concisa la diferencia entre SMI y MIB-2.
2. Instale el software SnmpB. ¿Debería SnmpB incluír los objetos y atributos definidos por MIB-2?.
3. ¿Por qué razón cree que en SnmpB no hay objetos bajo el OID 1.3.6.1.4.1.9?

Ejercicio 1

Usted está trabajando en una empresa que fabrica impresoras multifunción complejas, y le dicen que tiene que definir la MIB para una de ellas, de manera que cuando alguien compre la impresora sepa qué variables podrá monitorizar. Escriba con una sintaxis correcta la especificación de la MIB de la impresora, que debe incluír los siguientes objetos:

1. Nombre del equipo
2. SN (Numero de serie del dispositivo)
3. Ubicación
4. Estas impresoras tienen interfaces de red cableada e inalámbrica, así que por cada una deberá definir su dirección IP/máscara.
5. Estas impresoras tienen al menos 2 bandejas para papel, y se le pueden agregar hasta 5. Para cada bandeja instalada deberá saber si tiene o no papel.
6. Nivel de tóner. Cada impresora tiene opción de tener hasta 6 cartuchos, de manera que para cada uno deberá definir si es color o negro y el nivel de carga del mismo.

Parte 2

Preguntas

Para responder a las siguientes preguntas debe instalar y configurar Net-SNMP en una máquina virtual con Linux[1].

1. ¿El agente implementa la MIB system de MIB-2 (1.3.6.1.2.1.1)?. Mediante comandos de snmp obtenga todos los valores simples para dicho agente.
2. Realizar una captura con Wireshark [2] de la ejecución del comando `snmpwalk` para consultar al agente por la OID 1.3.6.1.2.1.1. Guarde la salida en pantalla, para utilizarla en el siguiente ejercicio. ¿Qué sucede en el último paquete intercambiado? ¿Porqué termina y no continúa? ¿Cuántos

1 De ahora en mas ésta máquina virtual será referida como el agente.

paquetes SNMP fueron intercambiados entre el agente y el gestor?

3. Realice ahora una captura con Wireshark, pero ejecutando el comando `snmpbulkwalk`, para consultar al agente por la OID 1.3.6.1.2.1.1. ¿La salida en pantalla difiere de la realizada en el punto 2?[2]. En caso de ser iguales, ¿cual es el motivo de tener dos comandos que realizan la misma tarea?. Responda esta pregunta en base a la cantidad de paquetes intercambiados y analizando la captura hecha con Wireshark.

Ejercicio

Instale un servidor virtual y sobre él, un Gestor de Red (Cacti [3]). Configure el gestor para que chequee 4 variables estándar del agente y así generar gráficos de esos valores.

Deberá ser capaz de instalar, configurar y extender el agente snmp en el servidor virtual que se le asigne. El control de acceso al agente deberá ser configurado de la siguiente forma:

- Comunidad de solo lectura ROtgr2017 y comunidad lectura-escritura: RWtgr2017
- La comunidad de solo lectura se podrá usar desde cualquier equipo remoto
- La comunidad de lectura-escritura deberá ser solo permitida a una sola IP.
- La comunidad de solo lectura podrá consultar todas las OIDs del árbol.
- La comunidad de lectura-escritura solo podrá hacerlo sobre un sub-árbol.

Para extender el agente debe utilizar la directiva `pass` del archivo `snmpd.conf` para que, ante una consulta por determinada OID, ejecute un programa hecho por usted que responderá el valor asociado. Los OID por los que deberá responder les serán suministrados por el docente, y su programa de extensión deberá soportar que se haga una consulta por un valor escalar (`snmpget`) o preguntar por el siguiente elemento de la MIB (`snmpgetnext`).

Parte 3

Como administrador de una red, decide que no quiere estar al pendiente de mirar las gráficas todo el tiempo, por lo que se decide a utilizar un mecanismo asíncrono para que le reporte incidentes. Para ello deberá realizar lo siguiente:

1. Configurar el servicio de SNMP Traps en su máquina virtual agente.

2. Programar un script en el agente que deberá enviar una trap SNMP al gestor ante la aparición de un evento. Para enviar una trap será necesario utilizar el comando *snmptrap* [5]. Los eventos que generarán un trap serán definidos en conjunto con el docente.

El servicio que colecta las traps es el *snmptrapd* [4], incluído en el paquete *Net-SNMP*, resta ser configurado y puesto en ejecución.

Condiciones de entrega

El plazo para entregar es el **viernes 5 de mayo a las 23:30 horas**. La entrega se realizará a través de la plataforma EVA. El nombre del archivo debe ser obligatorio_apellido.tar.gz.

Se debe entregar un informe escrito en formato PDF con las respuestas a las preguntas y ejercicios, el cual debe reflejar el procedimiento realizado para lograr armar este pequeño proyecto. El mismo debe incluir referencias a libros, sitios web u otra información utilizada. Como anexos, debe contener las capturas solicitadas así como un txt con la ejecución y salida de los comandos solicitados. Todo el material entregado debe estar debidamente identificado.

2 Algún valor puede cambiar, por ejemplo el sysUptime, pero ignore esa diferencia.

Referencias

1. Net-SNMP http://www.net-snmp.org/
2. Wireshark https://www.wireshark.org/
3. Cacti http://www.cacti.net/
4. snmptrapd http://www.net-snmp.org/docs/man/snmptrapd.html
5. snmptrap http://www.net-snmp.org/docs/man/snmptrap.html