Práctica 1. Implementar un sistema de administración de red usando SNMP

Objetivos

- Implementar la arquitectura básica del protocolo SNMP
- Implementar la comunicación (intercambio de mensajes) entre el agente y el gestor usando SNMP.
- Implementar la persistencia de información de una manera eficiente.
- Generar reportes para controlar y vigilar los agentes.
- Implementar un modelo de administración de red.

La práctica uno se divide en tres partes. La parte uno tiene como objetivo implementar la arquitectura mínima del SNMP. La parte dos se enfoca en ejecutar una consulta SNMP usando una terminal. La parte tres contempla la implementación de un modelo de administración de red para SNMP, usando un lenguaje de programación y persistencia (óptima) de la información.

Introducción teórica

EL SNMP (*Simple Network Management Protocol)* es el protocolo más utilizado para la gestión de redes IP basadas en internet. La versión original, ahora conocido como SNMPv1, es ampliamente difundida. SNMPv2 añade funcionalidad a la versión original, pero no se ocupa de sus limitaciones de seguridad; esta norma relativamente reciente no ha alcanzado mucha aceptación. La versión SNMPv3 que conserva las mejoras funcionales de SNMPv2 y añade potentes funciones de privacidad y autenticación.

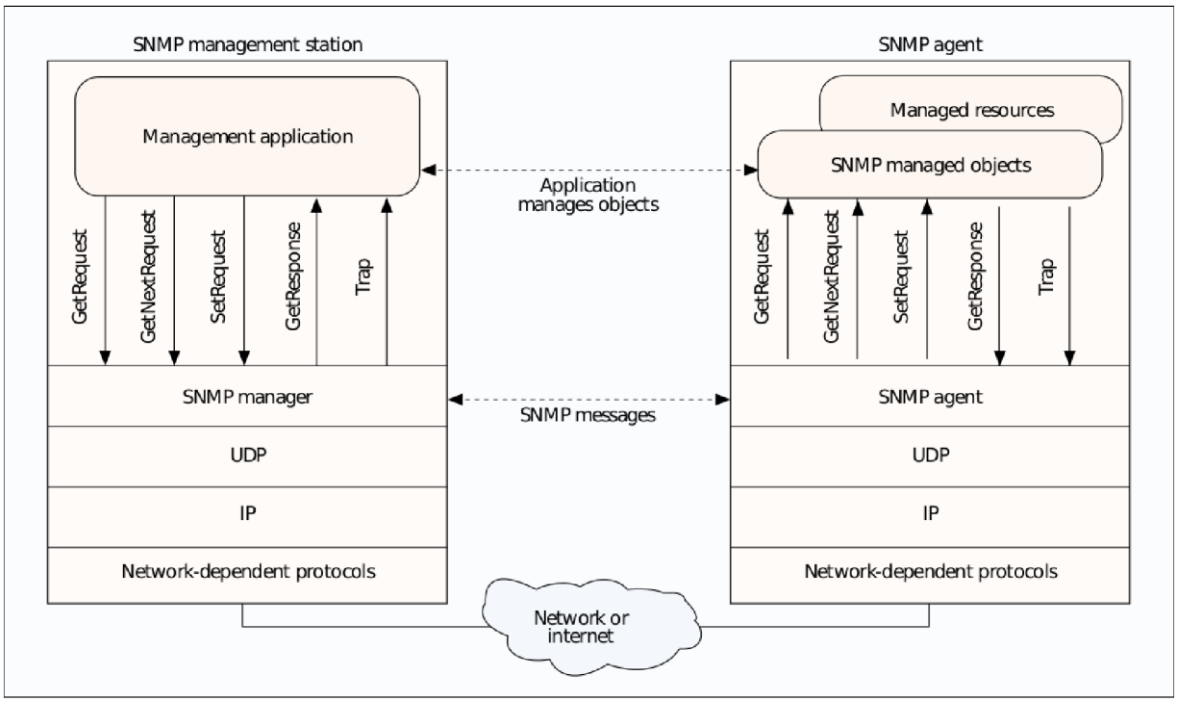
El protocolo simple de administración de red (SNMP), publicado en 1988, fue diseñado para proporcionar una implementación sencilla, así como facilitar el trabajo de gestión de redes de múltiples proveedores (enrutadores, servidores, estaciones de trabajo y otros recursos de la red). La especificación de SNMP tiene como objetivo:

- Definir un protocolo para el intercambio de información entre uno o más sistemas de gestión y un número de agentes
- Proporcionar un marco para dar formato y almacenamiento de información de gestión
- Define una serie de variables de información de gestión de propósito general, u objetos

La versión original de SNMP (ahora conocido como SNMPv1) se convirtió rápidamente en el esquema de gestión de la red más utilizado. Sin embargo, como el uso del protocolo se generalizó, se hicieron evidentes sus deficiencias. Estas incluyen la falta de comunicación-manager-manager, la incapacidad para hacer la transferencia de datos a granel, y la falta de seguridad.

SNMPv2 no ha recibido la aceptación que sus diseñadores anticiparon. Mientras que las mejoras funcionales han sido bienvenidas, los desarrolladores encontraron las modificaciones de seguridad para SNMPv2 demasiado complejas. En consecuencia, el grupo de trabajo SNMPv2 se reactivó para proporcionar una mejora de los documentos SNMPv2.

El resultado de este esfuerzo ha sido un éxito menor y un gran fracaso. El éxito de menor importancia es la mejora de los aspectos funcionales de SNMPv2. El gran fracaso radica en el área de la seguridad. El grupo de trabajo fue incapaz de resolver el problema, y surgieron dos enfoques diferentes. Con esta mejora, la parte funcional de SNMPv2 progresó de una propuesta a un estándar de Internet a partir de 1996. Luego, en 1997, empezó a trabajar en SNMPv3, lo que hace cambios funcionales menores e incorpora un nuevo enfoque de seguridad.



Parte 1 Arquitectura básica del SNMP

El modelo de administración de red que se utiliza para SNMP incluye los siguientes elementos:

- Estación de gestión
- Agente de Gestión
- base de información de gestión
- Protocolo de Gestión de redes

En las secciones se enlistan las tareas para realizar la instalación y configuración de dichos elementos

Tarea 1 Instalar la estación de gestión "Observium" en una máquina virtual

Observium es un Sistema operativo dedicado a la gestión y monitoreo de red basado en el SNMP. Esta plataforma fue implementada en PHP y soporta a un amplio rango de hardware de red y sistemas operativos incluyendo Cisco, Windows, Linux, HP, Dell, FreeBSD, Juniper, Brocade, Netscaler, NetApp y otras. Se puede descargar de www.turnkeylinux.org/observium.
Es recomendable descargar el archivo .iso para emularlo en una máquina virtual (e.g. Oracle VirtualBox).

Nota: El adaptador de red (de la máquina virtual) debe estar configurado en modo BRIDGE y permitir TODO el tráfico en modo promiscuo. Esto permite que la máquina virtual sea considerada como un nodo más de la red.

En un navegador, ingresar la IP asignada a Observium para consumir el servicio Web que ofrece. El usuario es admin y la contraseña es la indicada en la instalación.

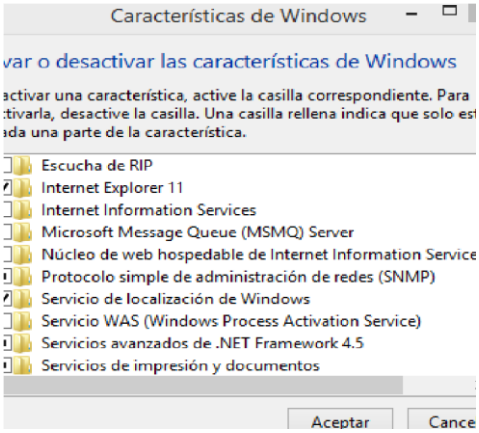
Tarea 1.1. Publicar los agentes en Observium

Observium ofrece la funcionalidad de agregar agentes. Para hacerlo, Observium solicita el hostname y la comunidad de dicho agente. Para asignar un hostname se debe modificar el archivo hosts en el sistema operativo Observium. En la consola, editar el archivo /etc/hosts; agregar la IP del agente y su hostname. La configuración de la comunidad se explica en el apartado siguiente.

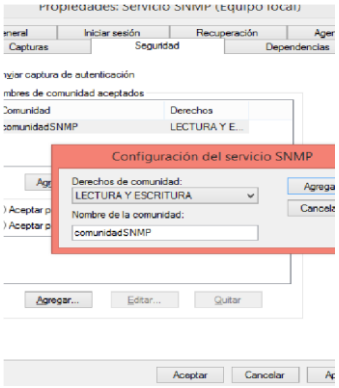
Tarea 2 Instalación y configuración de un agente

Un elemento principal del sistema de gestión de la red es el agente. Algunos dispositivos como host, bridges, routers y hubs, pueden estar equipados con el software de agente SNMP. El agente responde a las solicitudes de información de un gestor, responde a las peticiones de acciones desde la estación de gestión, y puede proporcionar de forma asíncrona a la estación de gestión información importante pero no solicitada.
A continuación se describe cómo instalar y configurar un agente para host que no están equipados con el software SNMP (Windows y Linux)

Tarea 2.1 Instalación y configuración de SNMP en Windows



Para instalar el protocolo SNMP se debe agregar una característica de Windows, esto se logra mediante el panel de control y después en Programas y características. En las características de Windows, buscar el Protocolo de Simple de Administración de Redes (SNMP) y activar la casilla de verificación.
Nota: Siempre se debe validar que los servicios (Captura SNMP y Servicio SNMP) se encuentren activos. El servicio captura SNMP se debe activar de manera manual cuando se inicie la PC.



Para configurar el SNMP en el agente, se debe buscar el Servicio SNMP y personalizarlo. Una vez localizado en los servicios locales, dar clic derecho, seleccionar las propiedades y, en la pestaña captura, se debe agregar el nombre de la comunidad que se desea asignar al host. Por último, en la pestaña seguridad hay que agregar la comunidad, dar los permisos de acceso a dicha comunidad (lectura y escritura) y habilitar la opción de aceptar paquetes SNMP de cualquier host. Nota: También se deben desactivar todos los firewall y antivirus del equipo.

Tarea 2.2 Instalación y configuración de SNMP en Linux.

1) Instalar NET-SNMP

sudo apt-get install snmpd snmp

2) configurar el archivo /etc/snmp/snmpd.conf, es recomendable crear una copia del archivo original con el comando

mv /etc/snmp/snmpd.conf /etc/snmp/snmpd.conf.bck

3) editar el archivo snmpd.conf de manera manual o usando un script de perl incluido en la instalación de NET-SNMP usando el comando:

snmpconf -r none -g basic_setup

Nota: Verificar que el archivo snmpd.conf se encuentre en la ruta correcta. El demonio SNMPD buscará el archivo de configuración snmpd.conf en la ruta /etc/snmp/snmpd.conf. Si el archivo no se encuentra en esa ubicación, no habrá respuesta a las solicitudes SNMP.

Si el archivo de configuración snmpd.conf fue modificado es importante reiniciar el servicio snmpd con el comando:

#service snmpd restart

Parte 2 Realizar solicitudes SNMP mediante consola.

Con el fin de gestionar los recursos en una red, estos recursos se representan como objetos. Cada objeto es, en esencia, una variable de datos que representa un aspecto del sistema administrado. La colección de objetos se conoce como una base de información de gestión (MIB) Las funciones MIB como una colección de puntos de acceso en el agente de la estación de gestión; el software del agente mantiene la MIB. Una estación de gestión lleva a cabo la función de control mediante la recuperación del valor de los objetos MIB. Una estación de gestión puede causar una acción que tendrá lugar en un agente o puede cambiar los ajustes de configuración de un agente mediante la modificación del valor de las variables específicas.

La estación de gestión y agentes están vinculados por un protocolo de gestión de red, lo que incluye las siguientes capacidades principales:

- GET: permite a la estación de administración para recuperar los valores de los objetos en el agente.
- SET: permite a la estación de administración para establecer los valores de los objetos en el agente
- TRAP: permite a un agente para notificar a la estación de administración de eventos significativos

Tarea 1. Operaciones SNMP

Ejecutar las siguientes operaciones SNMP para resolver el ejercicio MIB.

- snmpget
- snmpgetnext
- snmpwalk
- snmptable
- snmpset
- snmptranslate

Ejercicio MIB

Genera el comando SNMP para contestar las siguientes preguntas. Debes consultar la información de dos agentes (linux y windows)

1) ¿Cuándo fue el último reinicio (Dia, hora y minuto) de los agentes?
2) ¿Cuántas interfaces Ethernet tienen?
3) ¿Cuál es la velocidad (en MBPS) de esas interfaces?
4) ¿Cuál es la interfaz que ha recibido el mayor número de octetos?
5) Indica cuál interfaz de red ha recibido el mayor número de octetos
6) ¿Cuál es la MAC de esa interfaz?
7) ¿Cuántos mensajes ICMP ha recibido el agente?

8) ¿Cuántas entradas tiene la tabla de enrutamiento IP?
9) ¿Cuántos datagramas UDP ha recibido el agente?
10) ¿El agente ha recibido mensajes TCP? ¿Cuántos?
11) ¿Cuántos mensajes EGP ha recibido el agente?
12) Indica el Sistema Operativo que del agente.
13) Modifica el nombre del contacto o la ubicación del sistema de un agente
14) Dibuja la MIB del agente.

Tarea 2. Análisis de tráfico.

Utiliza un analizador de tráfico para monitorear la comunicación entre el agente y el gestor. Documenta los comandos básicos.

Parte 3 Implementar un modelo (versión 1) de administración de red de SNMP

En esta sección, se especifica el gestor del modelo de administración de red SNMP.

Un gestor sirve como interfaz para el administrador de red y el sistema de administración de red. El tendrá, como mínimo:

- Un conjunto de aplicaciones de gestión para el análisis de datos, recuperación de fallos, etc.
- Una interfaz por la que el administrador de la red puede supervisar y controlar la red. Es decir, la interfaz entre el usuario y las aplicaciones de gestión de red permite al usuario solicitar acciones (de vigilancia y de control) que se llevan a cabo por la estación de administración mediante la comunicación con los elementos gestionados de la red. Un protocolo por el que la estación de administración y entidades gestionadas intercambiar información de control y gestión.
- Una base de datos de la información de las MIB de todas las entidades gestionadas en la red. Es decir, la estación de gestión mantiene al menos un resumen de la información de gestión mantenido por cada uno de los elementos gestionados en la red.

Descripción de las interfaces

1) Inicio

En la pantalla de inicio, un usuario puede ver un resumen de todos los dispositivos que son monitorizados por el sistema. Debe incluir:

1. el número de dispositivos monitorizados
2. el estatus de conexión cada dispositivo (up or down).
3. el número de interfaces de red que están disponibles (de cada dispositivo)
4. el estatus de cada interfaz, si esta activa (up) o inactiva (down)

2) Agregar agente

El sistema de administración podrá agregar múltiples agentes y monitorizarlos de manera concurrente. Para agregar un agente, se debe indicar hostname, versión SNMP, puerto SNMP y comunidad. La información debe ser permanente, es decir, el sistema debe recordar los agentes agregados.

3) eliminar agente

El sistema debe eliminar cualquier agente, así como la información generada por el mismo.

4) Estado de Dispositivo

El estado de un dispositivo indica la información principal del agente: el nombre del host, IP, nombre, versión y logo del sistema operativo, el número de interfaces de red, el tiempo de actividad desde el último reinicio, la ubicación física y la información de contacto del administrador. También es posible visualizar el comportamiento del dispositivo mediante gráficas.

4.1) Gráficas de dispositivos

El sistema debe mostrar el resultado del monitoreo en tiempo real, usando gráficas. En ellas se debe describir el comportamiento de algunos objetos de la MIB. Cada equipo debe elegir 5 objetos MIB y generar la gráfica correspondiente. La información debe ser adquirida en tiempo real usando SNMP. La persistencia de información debe ser óptima pensando en información de alto rendimiento. A continuación, se muestra un listado de las posibles alternativas:

1. Tráfico de interfaz (entrada y salida)
2. Estadísticas de paquetes Ipv4 (entrada y salida)
3. Estadísticas ICMP (entrada y salida)
4. Estadísticas IP (entrada y salida)
5. Estadísticas de paquetes SNMP (entrada y salida)
6. Conexiones TCP establecidas
7. Segmentos TCP (entrada y salida)
8. Estadísticas TCP (entrada y salida)
9. Datagramas UCP (entrada y salida)
10. Errores UDP (entrada y salida)
11. Respuestas PING (entrada y salida)
12. Respuestas SNMP (entrada y salida)
13. Uso del sistema de archivos