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

Objetivos

- Definir los elementos de un sistema de administración de red
- Instalar y configurar una estación de gestión
- Configurar el SNMP en un SWITCH Enterasys
- Instalar y configurar un agente de gestión
- Implementar las operaciones del protocolo de gestión de red para controlar y vigilar los agentes de gestión

Introducción teórica

The Simple Network Management Protocol es el protocolo más utilizado para la gestión de redes IP basados 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.

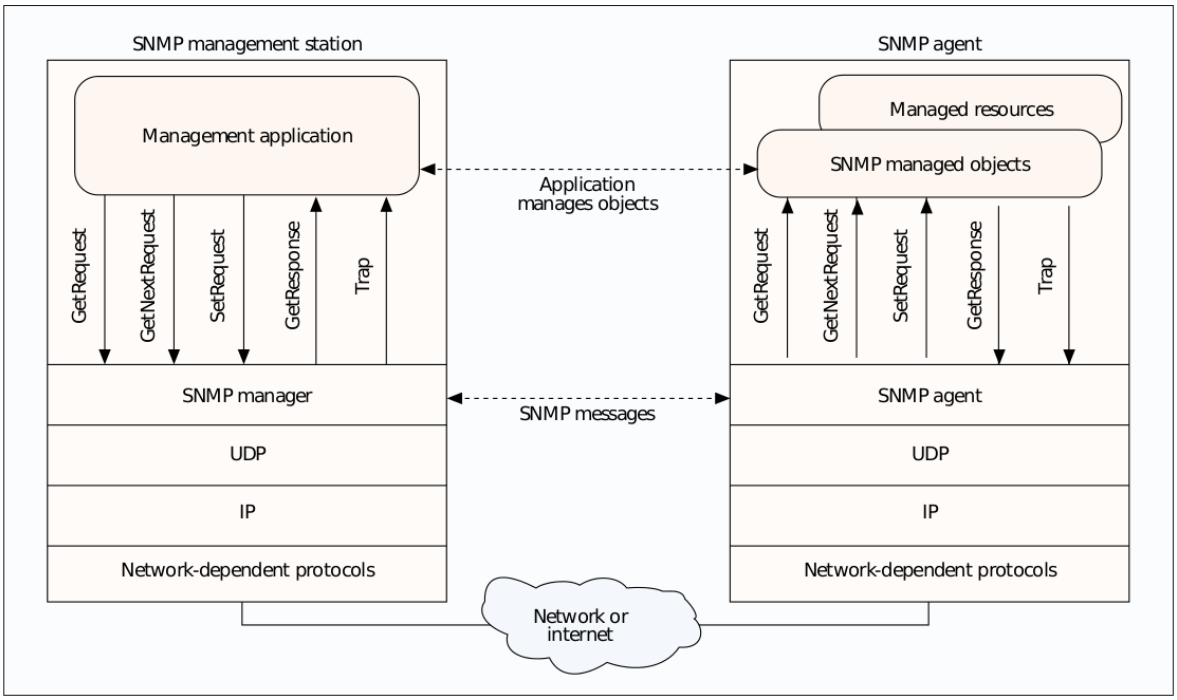
El protocolo simple de administración de red (SNMP), publicado en 1988, fue diseñado para proporcionar una fácil implementación, así como una sobrecarga baja para la gestión de redes de múltiples proveedores de routers, servidores, estaciones de trabajo y otros recursos de la red. La especificación de SNMP:

- Define un protocolo para el intercambio de información entre uno o más sistemas de gestión y un número de agentes
- Proporciona 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 independiente del proveedor más utilizado. Sin embargo, como el protocolo ganó uso generalizado, sus deficiencias se hicieron evidentes. Estos incluyen la falta de comunicación-manager-manager, la incapacidad para hacer la transferencia de datos a granel, y la falta de seguridad. Todas estas deficiencias se abordaron en SNMPv2, publicado como un conjunto de normas de Internet propuestos en 1993.

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 Instalación y Configuración de la estación de gestión

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

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

- Protocolo de Gestión de redes

Una estación de administración es típicamente un dispositivo independiente, pero puede ser una entidad implementada en un sistema compartido. En cualquier caso, la estación de gestión sirve como interfaz para el gestor de red y el sistema de gestión de red. La estación de administración 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 bases de datos de gestión 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.

Tarea 1 Instalar “Observium” en una máquina virtual

Observium es un Sistema operativo dedicado a la gestión y monitoreo de red basado en SNMP. Esta plataforma fue implementada en PHP e incluye un 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.

La plataforma se puede descargar de www.turnkeylinux.org/observium.

Se debe 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 el SWITCH del laboratorio le asigne una IP.

En un navegador, ingresar la ip asignada a Observium para consumir el servicio Web que ofrece:

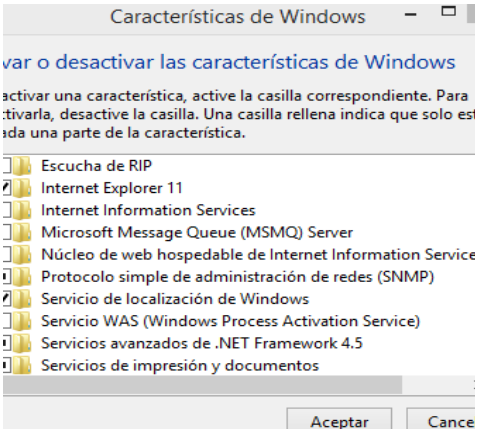
Parte 2 Instalación y configuración del agente de gestión

Otro elemento activo en el sistema de gestión de la red es el agente de gestión. Algunos dispositivos como host, bridges, routers y hubs, pueden estar equipados con el software de agente SNMP para que puedan ser monitoreados desde una estación de gestión. El agente de gestión

responde a las solicitudes de información de una estación de gestión, 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.

Para instalar y configurar un agente de gestión se debe virtualizar algún sistema operativo e instalar y configurar el SNMP en él

Tarea 1 - Activar el protocolo SNMP en Windows

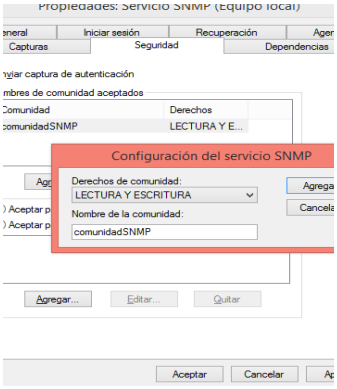


Para instalar el protocolo SNMP se debe agregar una característica de Windows, esto se logra mediante el panel de control y después en Programas y características.

En las características de Windows, buscar el Protocolo de Simple de Administración de Redes (SNMP) y activar la casilla de verificación.

Posteriormente, se deben validar que los servicios se encuentren activados. El primer servicio se llama SNMP y el segundo es captura SNMP.

Una vez activados, se debe configurar el servicio de SNMP en las herramientas de administración y supervisión. Buscar Servicio SNMP, clic derecho, propiedades, en la pestaña captura se debe agregar el nombre de la comunidad a la que pertenece el host. Por último, en la pestaña seguridad hay que agregar la comunidad y dar clic en aceptar paquetes SNMP de cualquier host.



Nota: También se deben desactivar todos los firewall y antivirus del equipo.

Tarea 2 Configurar 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

Tarea 3. Publicar los agentes en Observium

Para dar de alta un agente es necesario modificar el archivo hosts en el sistema operativo Observium. En la consola, editar el archivo /etc/hosts ; agregar la ip del agente y el hostname que se desea asignar a dicho agente.

Parte 3 Vigilancia y control de los agentes de gestión.

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:

- snmpget
- snmpgetnext
- snmpwalk
- snmptable
- snmpdelta
- snmpset
- snmpdf

- snmpnetstat
- snmpstatus
- snmptranslate
- snmptrapd (Alertas)

Ejercicio MIB

Genera el comando SNMP para contestar las siguientes preguntas. Debes consultar la información de los tres agentes (linux, windows y el Switch Enterasys)

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 el número de octetos de la interfaz que ha recibido el mayor número de octetos
6) ¿Cuál es la MAC de esa interfaz?
7) ¿Cuál es la ip de la Interfaz que ha recibido el mayor número de octetos?
8) ¿Cuántos mensajes ICMP ha recibido el agente?
9) ¿Cuántas entradas tiene la tabla de enrutamiento IP?
10) ¿Cuántos datagramas UDP ha recibido el agente?
11) ¿El agente ha recibido mensajes TCP? ¿Cuántos?
12) ¿Cuántos mensajes EGP ha recibido el agente?
13) Indica el Sistema Operativo que maneja el agente.
14) Modifica el estatus administrativo (a down) de la interfaz que ha recibido más octetos.
15) Genera una alerta para avisar cuando se reinicie el agente.
16) 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.