Práctica 3: Herramienta de Gestión Nagios

Objetivos

- Instalar y configurar la herramienta de Gestión Nagios

Herramientas necesarias

- Ordenador con sistema operativo Linux (en el laboratorio se utiliza la distribución Ubuntu).
- Paquete de gestión Net-snmp. Instalar los siguientes paquetes: *snmp* y *snmpd*.
- Heramienta de Gestión Nagios
- Topología de red real o simulada en algún entorno commo GNS3

Descripción

Nagios es un sistema de monitorización de redes ampliamente utilizado, de código abierto, que vigila los equipos (hardware) y servicios (software) que se especifiquen, alertando cuando el comportamiento de los mismos no sea el deseado. Entre sus características principales figuran la monitorización de servicios de red (SMTP, POP3, HTTP, SNMP...), la monitorización de los recursos de sistemas hardware (carga del procesador, uso de los discos, memoria, estado de los puertos...), independencia de sistemas operativos, posibilidad de monitorización remota mediante túneles SSL cifrados o SSH, y la posibilidad de programar plugins específicos para nuevos sistemas.

Se trata de un software que proporciona una gran versatilidad para consultar prácticamente cualquier parámetro de interés de un sistema, y genera alertas, que pueden ser recibidas por los responsables correspondientes mediante (entre otros medios) correo electrónico y mensajes SMS, cuando estos parámetros exceden de los márgenes definidos por el administrador de red.

Llamado originalmente Netsaint, nombre que se debió cambiar por coincidencia con otra marca comercial, fue creado y es actualmente mantenido por Ethan Galstad, junto con un grupo de desarrolladores de software que mantienen también varios complementos.

Nagios fue originalmente diseñado para ser ejecutado en GNU/Linux, pero también se ejecuta bien en variantes de Unix.

Nagios está licenciado bajo la GNU General Public License Version 2 publicada por la Free Software Fundation.

Nagios permite:

- Monitorización de servicios de red (SMTP, POP3, HTTP, NNTP, ICMP, SNMP).
- Monitorización de los recursos de equipos hardware (carga del procesador, uso de los discos, logs del sistema) en varios sistemas operativos, incluso Microsoft Windows con los plugins NRPE_NT o NSClient++.
- Monitorización remota, a través de túneles SSL cifrados o SSH.
- Diseño simple de plugins, que permiten a los usuarios desarrollar sus propios chequeos de servicios dependiendo de sus necesidades, usando sus herramientas preferidas (Bash, C++, Perl, Ruby, Python, PHP, C#...).
- Chequeo de servicios paralizados.
- Posibilidad de definir la jerarquía de la red, permitiendo distinguir entre host caídos y host inaccesibles.
- Notificaciones a los contactos cuando ocurren problemas en servicios o hosts, así como cuando son resueltos (a través del correo electrónico, buscapersonas, Jabber, SMS, o cualquier método definido por el usuario junto con su correspondiente complemento).
- Posibilidad de definir manejadores de eventos que ejecuten al ocurrir un evento de un servicio o host para resoluciones de problemas proactivas.
- Rotación automática del archivo de registro.
- Soporte para implementar hosts de monitores redundantes.
- Visualización del estado de la red en tiempo real a través de interfaz web, con la posibilidad de generar informes y gráficas de comportamiento de los sistemas monitorizados, y visualización del listado de notificaciones enviadas, historial de problemas, archivos de registros, etc.

Desarrollo de la práctica

En esta práctica deberá configurarse la herramienta Nagios en una topología de red como la que se muestra en la figura siguiente:

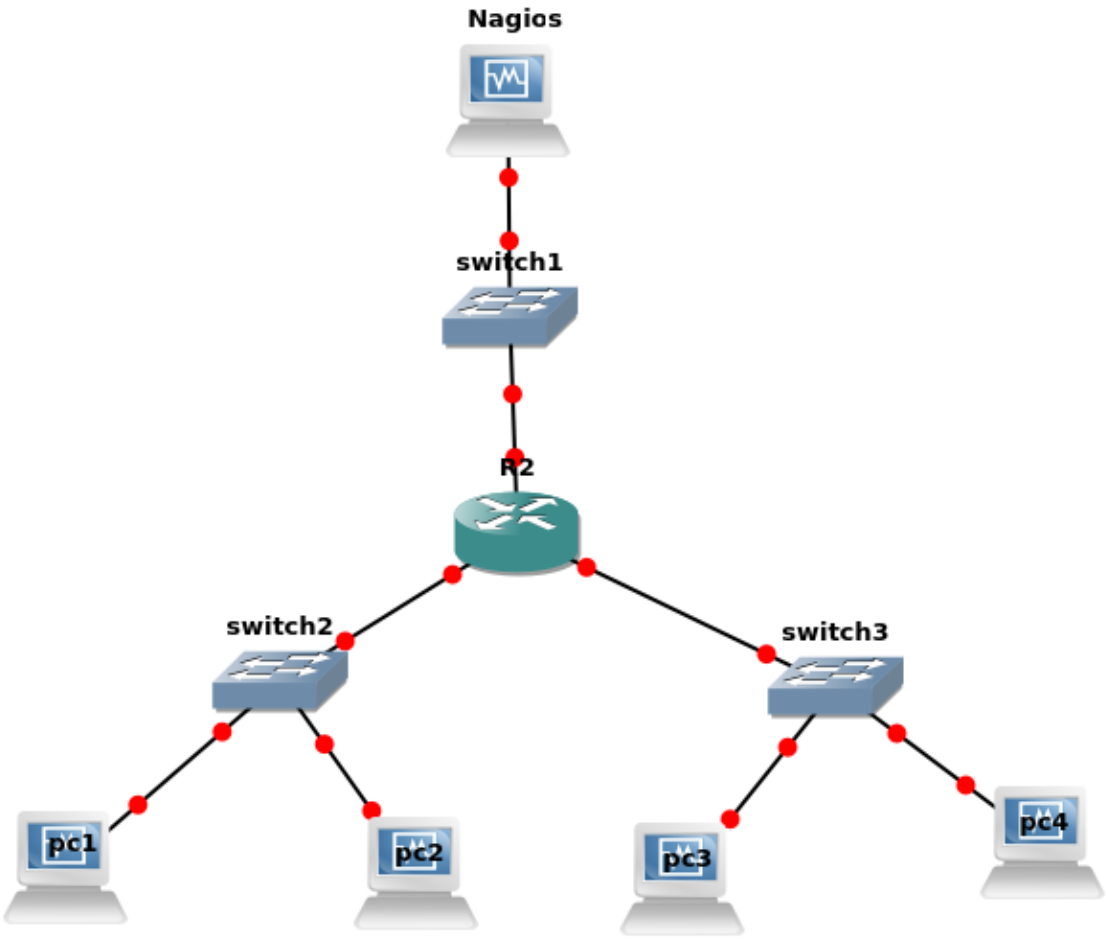

Fig.1. Topología de red

Para la realización de esta red puede utilizar GNS3 para simular el entorno. Agregue switches con capacidad de asignarles direcciones IP con el objetivo de poder ser accedidos por Nagios. Si lo prefiere puede crear una VLAN para la administración de los switches.

Se deberá cumplir con lo siguiente:

1. Monitorizar la disponibilidad de cada uno de los dispositivos que se muestran en la topología (switches, routers y pcs).
2. En los pcs se deberá monitorizar la disponibilidad de los servicios HHTP, SSH y SNMP. Pruebe además, la posibilidad de monitorizar el valor de un objeto de la MIB.

3. Asigne íconos representativos a cada uno de los equipos.
4. Apague equipos y servicios para observar el comportamiento de Nagios.

Presentación y evaluación

Esta práctica se realizará en grupos de máximo 2 estudiantes, se deberá entregar una memoria donde se explique claramente los pasos seguidos para dar solución a la práctica; por último se mostrará el funcionamiento al profesor en una sesión de laboratorio.