1º ASIR

2025

MONITORIZACIÓN DE REDES

ALEJANDRO GUERRERO VARO

PLANIFICACIÓN Y ADMINISTRACIÓN DE REDES | 1º ASIR

ÍNDICE

1. ¿Qué es SNMP y para qué se utiliza?

SNMP (Simple Network Management Protocol) es un protocolo estándar de Internet que se utiliza para **gestionar y monitorizar dispositivos de red** como routers, switches, servidores o impresoras. Su función principal es permitir que un administrador pueda **obtener información sobre el estado de estos dispositivos**, modificar ciertos parámetros y recibir alertas cuando algo no funciona correctamente. En pocas palabras, es como el "control remoto" de la red para asegurarse de que todo funcione bien.

2. Componentes

SNMP se basa en tres elementos fundamentales:

- **Gestor (Manager):** Es el equipo o software que supervisa la red. Por ejemplo, un servidor que corre Zabbix o Nagios.
- **Agente (Agent):** Es un software que corre en cada dispositivo de red y que recoge información para enviarla al gestor.
- **MIB (Management Information Base):** Es como un diccionario de datos que contiene los parámetros que se pueden consultar o modificar en los dispositivos. Cada dato tiene un identificador único llamado **OID**.

3. Funcionamiento básico: get, set, trap

- **GET:** El gestor le pide al agente un valor concreto de la MIB, por ejemplo, el tráfico actual de un puerto.
- **SET:** El gestor puede cambiar un valor en el dispositivo, por ejemplo, actualizar la configuración de un interfaz.
- **TRAP:** Es el mensaje que envía el agente al gestor de forma **automática** cuando ocurre un evento importante, como un fallo en un switch.

4. Diferencias entre SNMPv1, SNMPv2c y SNMPv3

VERSIÓN	SEGURDIAD	CARACTERÍSTICAS PRINCIPALES
V1	Comunidad de texto plano	Básica, solo lectura y escritura limitada.
V2C	Igual que v1, más rápido y con mejores operaciones	Añade soporte para bulk get, pero la seguridad sigue siendo débil.
V3	Autenticación y cifrado (MD5/SHA, DES/AES)	Es la más segura y recomendable hoy en día.

Conclusión: La seguridad de v1 y v2c es insuficiente para redes modernas porque las contraseñas viajan sin cifrar, mientras que v3 sí protege datos y contraseñas.

5. Ejemplos de OIDs relevantes

Algunos OIDs que suelen consultarse:

- **1.3.6.1.2.1.1.1.0** → Información del sistema (nombre, versión).
- **1.3.6.1.2.1.2.2.1.10** → Bytes recibidos por un interfaz.
- **1.3.6.1.2.1.2.2.1.16** → Bytes enviados por un interfaz.

6. Análisis

Software de Monitorización: Zabbix

Zabbix es un software libre que permite **monitorizar toda la red y sus servicios** de manera centralizada.

- **Instalación:** Se instala en un servidor Linux y puede monitorizar agentes en Windows, Linux y dispositivos de red.
- **Funciones principales:** Alertas automáticas, gráficos históricos, mapas de red, monitorización de SNMP, protocolos como ICMP, HTTP o TCP.
- **Evidencias:**
    - Captura de alertas configuradas para un switch mediante SNMP.
    - Gráficos del tráfico de red de un router.
    - Configuración de triggers para notificar caídas de servicio.

7. Conclusiones

- **Ventajas de SNMP:**
    - Estándar universal, fácil de implementar.
    - Permite automatizar la monitorización de toda la red.
    - Compatible con la mayoría de software de gestión.
- **Inconvenientes:**
    - Versiones antiguas no son seguras.
    - Configuración inicial puede ser compleja.
    - No siempre detecta problemas internos de aplicaciones, solo del hardware/red.
- **Por qué sigue siendo un estándar:**
    - Porque es simple, ligero y todos los fabricantes lo soportan.
    - Facilita la interoperabilidad entre dispositivos de distintos fabricantes.

- **Seguridad en entornos modernos:**
    - Solo SNMPv3 es realmente seguro.
    - En redes críticas, conviene combinarlo con VPN o firewalls para proteger los datos.

8. Opinión personal sobre qué usar en un entorno profesional:

Yo elegiría **Zabbix**, porque permite monitorizar todo tipo de dispositivos, es open source, configurable y soporta SNMPv3, lo que garantiza seguridad. Además, los gráficos y alertas me parecen muy intuitivos para un entorno profesional.