HERRAMIENTAS DE CÓDIGO ABIERTO PARA EL MONITOREO DE REDES LAN

OPEN SOURCE TOOLS FOR LAN MONITORING

Manrique-Villafuerte Cesar Jorge

Universidad Laica Eloy Alfaro de Manabí,
Facultad de Ciencias Informáticas. Manta, Ecuador.
Correo: e1313100768@live.uleam.edu.ec

Márquez-Vélez Gricelda Mercedes

Universidad Laica Eloy Alfaro de Manabí,
Facultad de Ciencias Informáticas. Manta, Ecuador.
Correo: e1315909638@live.uleam.edu.ec

Herrera-Tapia Jorge

Docente de la Universidad Laica Eloy Alfaro de Manabí,
Facultad de Ciencias Informáticas. Manta, Ecuador.
Correo: jorge.herrera@uleam.edu.ec

RESUMEN

En el presente trabajo de investigación, se realizó el análisis de diferentes herramientas gratuitas de monitoreo de redes LAN, para poder determinar cuáles brindan los parámetros necesarios de alerta para mantener una infraestructura de red operativa y útil para los usuarios. Se llevó a cabo un análisis y comparación de cinco herramientas open source, bajo el protocolo de SNMP (Simple Network Management Protocol – Protocolo Simple de Administración de Red), el cual es el principal instrumento de comunicación entre el sistema de monitoreo y los equipos a ser monitoreados, para poder implementar un sistema de monitoreo apropiado. Luego se procedió a realizar la implementación de las herramientas escogidas, analizando el comportamiento de cada una de ellas en un entorno virtual. Por último, se realizó la evaluación y se analizó los beneficios que brinda cada una de las herramientas de monitoreo implementadas, como resultado se estableció una tabla comparativa para escoger la mejor herramienta de monitoreo de redes LAN en base a la infraestructura.

Palabras claves: Monitoreo, Open Source, Tecnologías, SNMP, Redes.

ABSTRACT

In this research work, the analysis of different free LAN network monitoring tools was carried out, in order to determine decisions that provide the necessary alert parameters to maintain an operational and useful network infrastructure for users. An analysis and comparison of five open source tools was carried out, under the SNMP protocol (Simple Network Management Protocol), which is the main communication instrument between the monitoring system and the equipment to be used. be monitored, in order to implement an appropriate monitoring system. Then we proceeded to implement the

Fecha de recepción: 15 de abril de 2021; **Fecha de aceptación:** 28 de junio de 2021; **Fecha de publicación:** 09 de julio de 2021.

chosen tools, analyzing the behavior of each of them in a virtual environment. Finally, the evaluation was carried out and the benefits provided by each of the implemented monitoring tools were analyzed, as a result a comparative table was established to choose the best LAN monitoring tool based on the infrastructure.

Keywords: Monitoring, Open Source, Technologies, SNMP, Networks.

1. INTRODUCCIÓN

La detección oportuna de fallos a través del monitoreo de red, son técnicas que tienen una gran importancia para poder brindar un buen servicio a los usuarios internos dentro de una organización. Por esa razón, la necesidad de contar con un sistema de monitoreo de red que sea capaz de notificar las fallas en la red y por supuesto mostrar el desempeño de la red mediante un análisis a través de la recolección de datos, que es esencial para la detección temprana de tomas de decisiones.

Los autores de (Villagómez Bayas, 2015) afirman que no conocer la información acerca del tráfico que atraviesa la red, que enlace está saturando el ancho de banda o que servicio está haciendo que la carga de los servidores sea elevada, esto hace imposible tener una red de telecomunicaciones óptima ya que en cualquier momento los servidores o dispositivos pueden caerse y detener servicios de vital importancia para la comunicación de la organización o empresa. Por lo cual (Junco Romero & Ravelo Padua, 2018) explica que la detección oportuna de fallas y el monitoreo de los elementos que conforman una red de computadoras son actividades de gran trascendencia para brindar un buen servicio a los usuarios. De esto se deriva la importancia de contar con herramientas capaces de notificar las fallas en la red y de mostrar su comportamiento mediante el análisis y recolección de tráfico.

(Velasco Briones & Cagua Ordoñez, 2017) indican que existen software que permite el monitoreo de la red, el cual se puede obtener por medio de licencia pagada o licencia de código abierto Por otro lado, refiriéndose a las funcionalidades de estas herramientas (Mohan, 2013) indica que el 56% de los administradores de red afirmaron que la solución actual de administración o

monitoreo de redes de su organización incluye capacidades o funciones que no usan o no necesitan.

La definición de software libre propuesta por la Free Software Foundation (Hernández, 2005), se basa en cuatro libertades básicas que cualquier programa considerado libre debe proporcionar": Libertad para emplear el programa para cualquier propósito, Libertad para poder analizar cómo funciona el programa, Libertad para redistribuir el programa y Libertad para realizar modificaciones y compartir las mejoras. El software libre se basa en cooperación y transparencia, garantizando una serie de libertades a los usuarios.

En general, el problema radica en que no existe una guía práctica para los administradores de redes, para seleccionar una herramienta de monitoreo, donde se indiquen las características y funcionalidad de cada una de estas aplicaciones. Lo que origina que estas no sean utilizadas adecuadamente, o simplemente no se las use. Por esta razón es relevante realizar un análisis de herramientas de código abierto para el monitoreo de redes, ayudando a los procesos en el área de Tecnologías de la Información (TI), donde la gestión de la tecnología adquirida se convierte en un punto vital para cualquier organización.

2. MATERIALES Y MÉTODOS

Dentro de este apartado, se detallan los métodos de investigación asociados al proyecto; los cuales guardan relación para lograr los objetivos planteados. Las metodologías escogidas para realizar este proyecto integrador y su aplicación sobre la implementación está basado métodos teóricos como PPDIOO (Preparar, Planificar, Diseñar, implementar y operar), bibliográfico y empírico (experimental) mismos que serán descritos a continuación.

2.1 Método PPDIOO

Esta metodología tiene como objetivo definir actividades mínimas que se requieran para la instalación y operación de tecnologías, se definen por las siguientes fases descritas en la siguiente figura:

Figura 1. *Ciclos de PPDIOO*

Nota. Ciclo de metodología PPDIOO. Tomada de (READER, 2020)

Fases de la metodología PPDIOO

FASE I: Preparar. Toda implementación, propuesta de solución en el área de redes, dará como efecto una mejora u optimización en las funciones del personal del área técnica, provocando efectos positivos en cualquier organización. Para el presente proyecto de investigación no habrá inversión económica directamente, ya que se dará uso de herramientas de software libre que serán implementadas en un entorno virtual.

FASE II: Planificar. A lo largo de este proceso se podrán identificar los requerimientos técnicos, cronograma de actividades y los alcances que proporcionarán las herramientas de monitoreo Nagios, OpenNMS, ICINGA, Zabbix, Cacti.

FASE III: Diseñar. La etapa de diseño se realiza con base en los requerimientos de los sistemas a utilizar para el objeto de estudio. Apoyados en la fase de planeación, se determina las características que se requieren de los servidores a implementar tanto hardware y software.

FASE IV: Implementar. Para la implementación de los laboratorios virtuales de cada de las herramientas de monitoreo de redes se realizó:

- Instalación y configuración del emulador de equipos GNS3.

- Instalación de un sistema de virtualización en VMware, una máquina virtual para el sistema de monitoreo y una máquina virtual para el envío de datos.
- Creación de un shell-script para simular el tráfico de red, utilizando los comandos: timeout; sleep; hping3.
- Instalación y configuración de cada una de las herramientas de monitoreo de redes LAN escogida para este estudio.
- Creación del ambiente de trabajo en GNS3 con las máquinas virtuales, donde se encuentra instalada cada una de las herramientas Nagios, Cacti, OpenNMS, Icinga, Zabbix y la máquina para él envió de datos.

FASE V: Operar: La fase de operación arranca una vez concluida toda la implementación del equipo en los laboratorios virtuales, tiene como objetivo monitorear todas las alertas, tráfico de red y desempeño para informar sobre futuros errores que pueden encontrar en la red.

2.2 Método Bibliográfico

Por medio de la utilización de este método de investigación, se consideraron fuentes de información primarias a los distintos artículos, estudios, informes, publicaciones, libros, ensayos y demás textos científicos; mismos que nos han brindado la sustentación teórica y técnica para la realización del presente proyecto de investigación.

2.3 Método Experimental

En cualquier tipo de investigación que lleve a cabo un enfoque experimental, el investigador emplea una o más variables de estudio, para controlar el aumento o disminución de esas variables y su efecto en las conductas observadas.

Etapas del método experimental.

PRIMERA ETAPA: Planteamiento de un problema de conocimiento: “La decisión del problema depende los intereses del investigador: comprobar teorías, descubrir o generar conocimiento o mejorar la práctica educativa. Dicho problema está relacionado con la variable dependiente. Las preguntas planteadas en la investigación deben resolverse con la aplicación de un proceso

experimental. Es fundamental revisar la bibliografía sobre el problema que se ha formulado" (Atenea Alonso, 2015).

SEGUNDA ETAPA: Formulación de hipótesis: La hipótesis es una presunta respuesta al problema, dicho de otro modo, es la sujeción de un resultado posible de la investigación experimental.

TERCERA ETAPA: Realización de un diseño adecuado a la hipótesis: "El diseño refleja la idea o esquema de trabajo del investigador, es su estructura formal. El diseño incluye diversas actividades, describe con detalle qué se debe hacer y cómo realizarlo, como por ejemplo la asignación de sujetos a los diferentes grupos experimentales y las variables implicadas" (Atenea Alonso, 2015).

CUARTA ETAPA: Recolección y análisis de datos: Para la recolección de datos es importante identificar los diferentes instrumentos o técnicas (test, cuestionarios, sistemas de observación, etc). Cada una posee ventajas y desventajas, por ende, el investigador a la hora de escoger debe tener cuenta desempeño y fiabilidad. Una vez obtenidos los datos, resultado de un plan de análisis. El análisis de datos deberá consistir en organizar y tratar la información para que se pueda describir, analizar e interpretar.

QUINTA ETAPA: Elaboración de conclusiones: Se efectúa en base a la obtención de datos obtenidos, mediante la metodología utilizada, se puede llegar a resolución llena de acuerdos o desacuerdos con otras investigaciones, consecuencias para la práctica y sugerencias para posteriores investigaciones.

3. RESULTADOS Y DISCUSIÓN

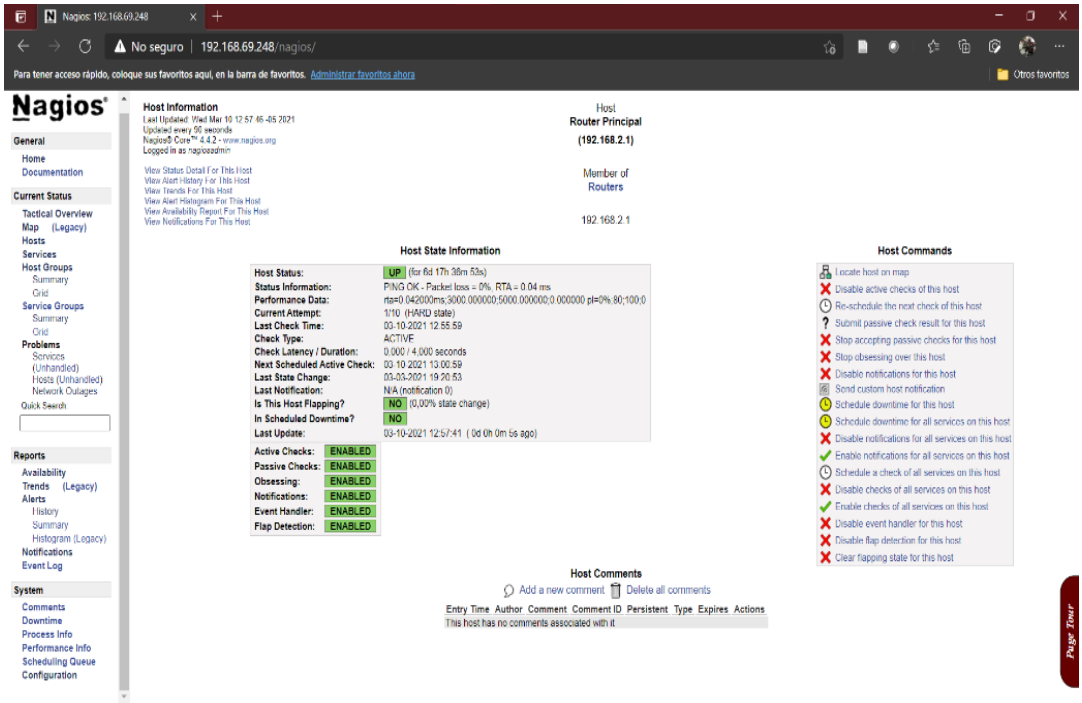
3.1 Análisis y resultados de la herramienta NAGIOS

Después de haber instalado el sistema de monitoreo Nagios, con el cual podemos estar al tanto del estado de los procesos, la memoria, CPU, ancho de banda de las interfaces de red (Solo si se instala los servicios de ancho de banda por medio de plugin). Como también el agregar nuevos host y servicios a analizar.

Luego de haber ingresado al router para ser monitoreado, se podrá observar si los servicios de este están levantados, en este caso Nagios muestra de color verde si el estado del host está operativo, como lo podemos apreciar en la figura 2, a la hora de generar reportes, Nagios nos muestra de manera visual si ha habido inconvenientes en la red en el día o la semana, esto lo podemos apreciar en el log que posee Nagios en su parte web.

Esta herramienta además nos permite configurar una serie de notificaciones las cuales nos pueden llegar a nuestros correos, donde nos indican si ha habido algún problema con nuestros sistemas de telecomunicaciones o con nuestros servidores

Figura 2. *Reporte HOST NAGIOS*



Nota: Reporte generado por Nagios. Fuentes: Autores

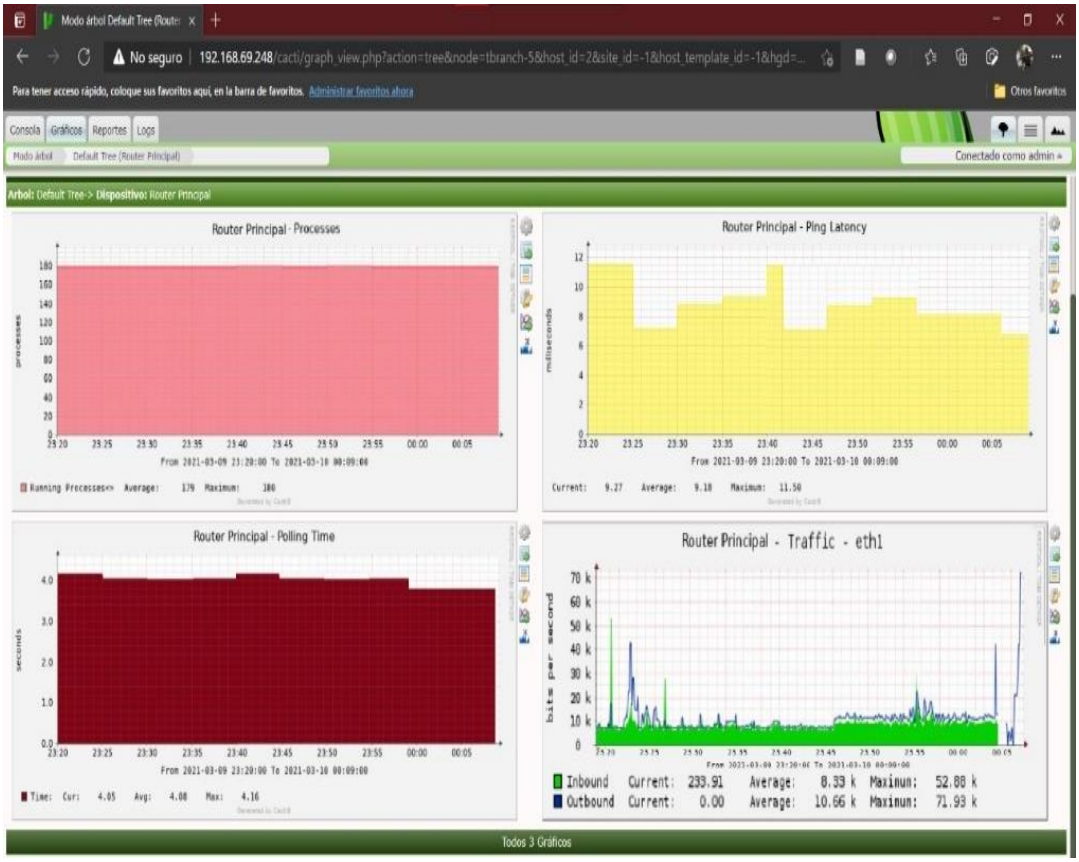
3.2 Análisis y resultados de la herramienta CACTI

Después de haber instalado el sistema de monitoreo Cacti, con el cual podemos estar al tanto del estado de los procesos, la memoria, CPU, ancho de banda de las interfaces de red. Como también el agregar nuevos host y servicios a analizar. Cacti tiene un problema en el ámbito de Fallo, ya que no llega a notificar por defecto a los usuarios de algún fallo en la red.

Como ventaja podemos aludir que este sistema de monitoreo permite la agrupación de equipos en la red, como también el medir la latencia de los equipos de telecomunicación mediante el protocolo ICMP, con el cual podremos saber si un dispositivo presente algún tipo de fallo de conectividad.

En la figura 3 podemos apreciar un reporte con gráficos que proporciona esta aplicación open source, en el cual nos muestra el consumo de memoria RAM, el CPU, la latencia del ping y el ancho de banda, todo esto en el transcurso de 1 hora. Podemos dejar constancia de que gráficamente Cacti nos muestra lo óptimo a visualizar de los servicios que hemos decido monitorear.

Figura 3. *Reporte HOST CACTI*



Nota: Reporte generado por Cacti. Fuentes: Autores

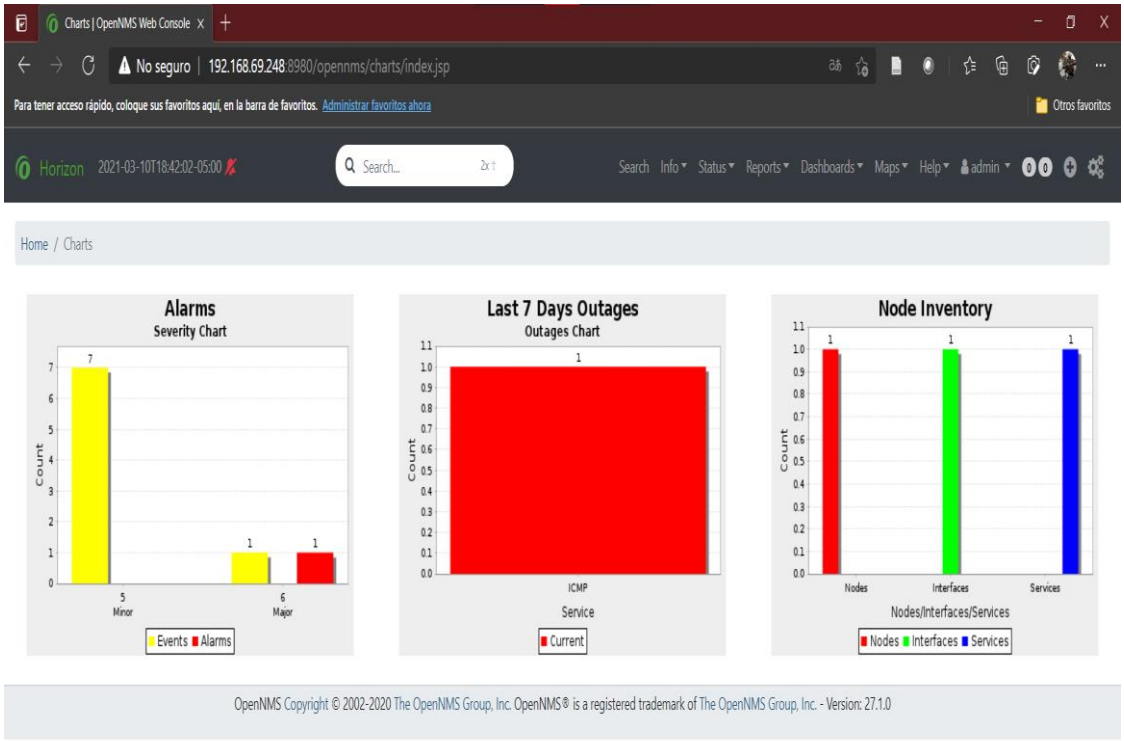
3.3 Análisis y resultados de la herramienta OpenNMS

Después de haber instalado el sistema de OpenNMS, con el cual podemos estar al tanto del estado de los procesos, la memoria, enlaces directos a características de los nodos, notificación, graficas de los procesos de las interfaces de red. Como también el agregar nuevos host y servicios a analizar.

En OpenNMS se trabaja por nodos, que vienen a ser los host o equipos que queremos monitorear. Una de las pautas que nos da OpenNMS es que está diseñado para cumplir con los aspectos del modelo FCAPS, en el cual se centra en el apartado de fallos y rendimiento.

Una de las ventajas que nos da este software es la posibilidad de agregar los equipos usando la interfaz gráfica de la web, además de ser intuitivo, en la cual solo se debe poner el grupo del nodo, la dirección ip, el nombre del nodo o en este caso, el host y si queremos desactivar la conexión snmp (La cual en casos de ingresar routers o switches deberá estar sin marcar).

Figura 4. *Reportes alertas HOST OPENNMS*



Nota: Reporte generado por OpenNMS. Fuentes: Autores

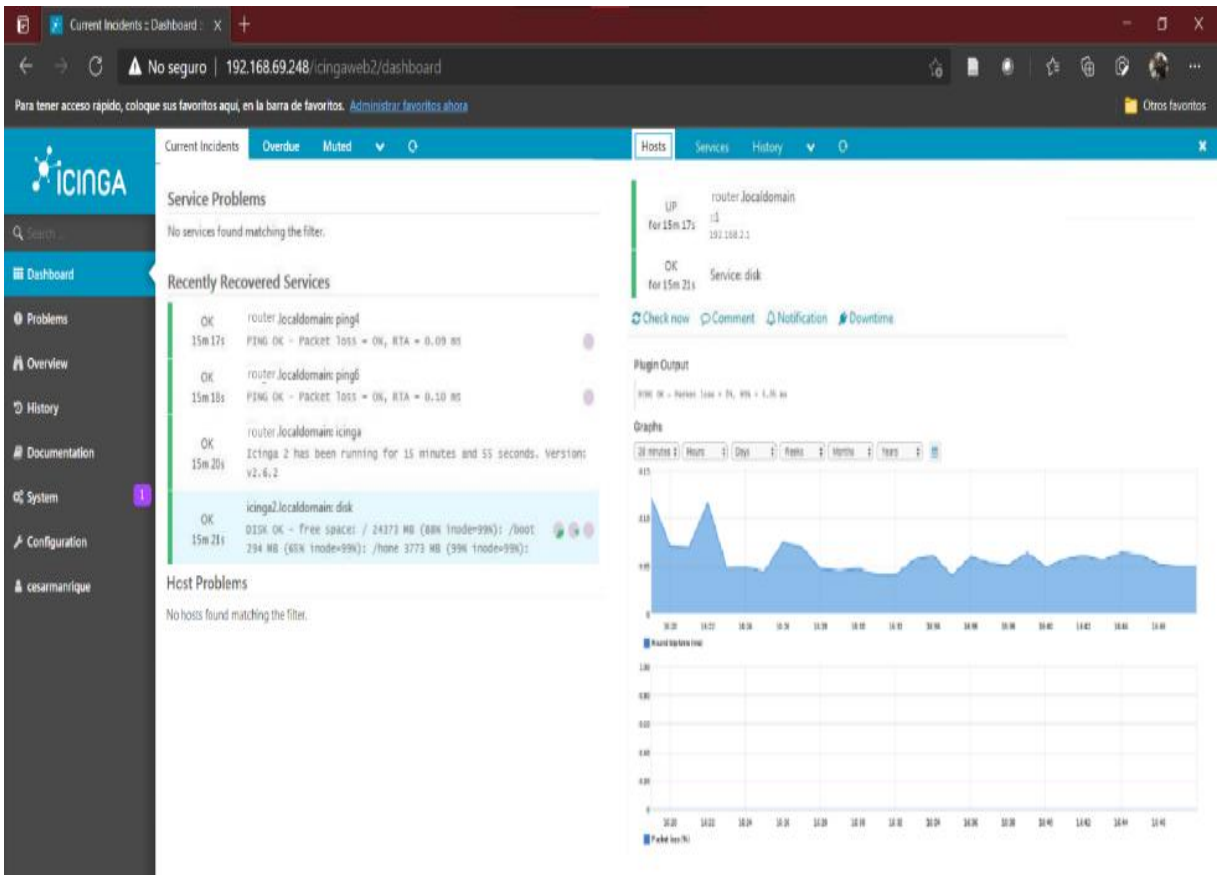
3.4 Análisis y resultados de la herramienta ICINGA

Después de haber instalado el sistema de monitoreo ICINGA, con el cual podemos supervisar la memoria, la CPU local, los procesos, el ancho de banda entre otros sin necesidad del protocolo SNMP, además de que la comunicación entre el cliente y el servidor está cifrada por TLS, con lo cual vuelve segura a

esta herramienta, cabe destacar que con ICINGA podemos supervisar casi cualquier dispositivo que tengamos en la red por medio de unos simples scripts.

La agregación de dispositivos no se la puede realizar por medio del entorno gráfico, lamentablemente se debe hacer manualmente en la terminal, muy parecido a lo que se realizaba en Nagios, al igual que agregar los servicios que se desean monitorear. Como ventaja tiene que, si se desea migrar desde Nagios a esta herramienta, no se deberá cambiar los agentes instalados en los clientes o servidores, ya que ICINGA trabaja con los mismos agentes que Nagios.

Figura 5. *Reporte HOST ICINGA*



Nota: Reporte generado por ICINGA. Fuentes: Autores

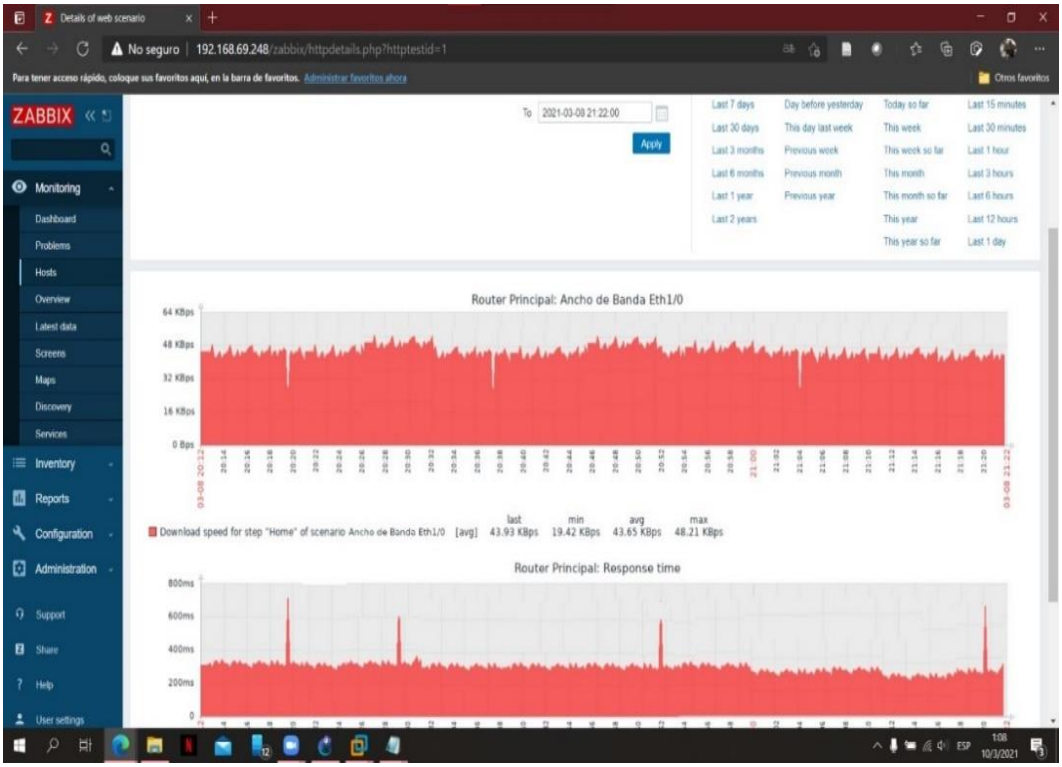
3.5 Análisis y resultados de la herramienta ZABBIX

Después de haber instalado el sistema de monitoreo ZABBIX, con el cual podemos estar al tanto del estado de los procesos, la memoria, CPU, ancho de banda de las interfaces de red. Como también el agregar nuevos host y servicios a analizar.

Esta herramienta tiene una maravillosa interfaz gráfica. Pero eso solo visualmente, intuitivamente es muy pobre, carece de ayuda en pantalla para los usuarios, lo que provoca que se deba leer mucha documentación sobre como agregar nuevos dispositivos para ser analizados, se debe seguir muchos pasos para lograr graficar un solo servicio.

Respecto a la instalación y configuración, no se aleja mucho a lo que fue la instalación de Cacti, ya que necesitan los mismos prerrequisitos para poder ser instalados, incluso se manejan con la misma base de datos, podemos inferir que Cacti y Zabbix son iguales en implementación, mas no en funcionamiento, ya que Zabbix si notifica por medio de correo electrónico cualquier tipo de fallo que ocurran con los equipos que se están monitoreando, cosa que Cacti no logra hacer.

Figura 6. *Reporte HOST ZABBIX.*



Nota: Reporte generado por Zabbix. Fuentes: Autores

3.6 Comparación de las herramientas de código abierto de monitoreo de redes LAN bajo el modelo FCAPS.

Bajo el análisis de los objetos de estudio, se recopiló información o resultados explicados en el apartado anterior respecto a cada herramienta de monitoreo

analizada. Lo que permite establecer una tabla referencial para escoger la mejor herramienta de código abierto de monitoreo de redes LAN, esto ha permitido cumplir con el objetivo general y específicos establecido en este proyecto integrador.

Para mayor comprensión se observa en la siguiente tabla el marco referencial para escoger la mejor herramienta bajo los parámetros del modelo de gestión de redes FCAPS.

Tabla 1. *Tabla Referencial.*

	Parámetros analizados del modelo FCAPS				
NOMBRE	**Fallos**	**Configuración**	**Contabilidad**	**Rendimiento**	**Seguridad**
Nagios	✔ **Si Cumple**	✔ **Si Cumple**	✔ **Si Cumple**	✔ **Si Cumple**	✔ **Si Cumple**
Opennms	✔ **Si Cumple**	✔ **Si Cumple**	✔ **Si Cumple**	X **No Cumple**	✔ **Si Cumple**
Zabbix	✔ **Si Cumple**	✔ **Si Cumple**	✔ **Si Cumple**	✔ **Si Cumple**	✔ **Si Cumple**
Icinga	✔ **Si Cumple**	X **No Cumple**	✔ **Si Cumple**	✔ **Si Cumple**	✔ **Si Cumple**
Cacti	✔ **Si Cumple**	✔ **Si Cumple**	✔ **Si Cumple**	✔ **Si Cumple**	X **No Cumple**

Nota: Tabla referencial para escoger la mejor herramienta de monitoreo open source. Fuente: Autores

Como se puede observar en la tabla 1, los únicos sistemas que cumplen con el modelo FCAPS son Nagios y Zabbix, debido a que reconocían y registraban fallos que ocurrían en las redes de telecomunicaciones; recolectan información, modifican la configuración, generan reportes y gestión cambios, parámetro en el que decae un poco ICINGA, ya que aún es una herramienta en desarrollo; reúnen las estadísticas de los usuarios, como son la utilización de disco, el tiempo del CPU y los enlaces de utilización, el rendimiento era eficiente debido

a que determinaban la eficacia de la red actual, parámetro en el cual OpenNMS falla debido a la lentitud en la ejecución de procesos y obtención de datos; Por último, respecto a la seguridad, cumplían con la autenticación, autorización y cifrado configurada en el sistema operativo, además de la control de acceso a las bases de datos, cuestión en la que Cacti decae dado a la gran cantidad de vulnerabilidades que se han encontrado en este sistema de monitoreo.

4. CONCLUSIONES

Se analizaron cinco herramientas de monitoreos de red dentro de un ambiente controlado, usando un script para generar el mismo tráfico de red para los diversos sistemas a analizar, se generaron reportes, se analizó su desempeño y su seguridad, con esto hemos llegado a la conclusión de que la mejor herramienta de monitoreo open source (código abierto) estudiados en este documento son Nagios y Zabbix, ya que cumplieron con los cinco parámetros del modelo FCAPS.

Se pudo constatar los beneficios del uso de GNS3 para la creación y virtualización de los equipos de telecomunicación como también de los servidores a usar, generando un ambiente de trabajo óptimo para realizar pruebas en tiempo real con estos dispositivos, ya que se simulaba una conexión física entre el router virtualizado, el servidor que generaba tráfico de red y el servidor donde se albergaba el sistema de monitoreo de red LAN.

Con las herramientas referentes en esta investigación que han cumplido con todas las métricas evaluadas, un administrador de red puede mantener cualquier infraestructura en óptimas condiciones, logrando prever futuros fallos en la red.

Se comparó los resultados obtenidos de las gráficas y rendimientos de los equipos monitoreados por cada una de estas aplicaciones, tomando en cuenta que algunas de estas herramientas no venían con opciones graficas de datos por defecto ni con alertas de seguridad o de errores a correos electrónicos o mensajerías de texto, como es el caso de Cacti.

Se ha establecido un marco referencial, donde se indica las herramientas que cumplen con cada parámetro del modelo FCAPS, de esta manera podemos decidir qué sistema debemos implementar si la empresa requiere un software de código libre y gratuito que cumpla con este modelo.

REFERENCIAS

Atenea Alonso, L. G. (2015). MÉTODOS DE INVESTIGACIÓN DE ENFOQUE EXPERIMENTAL. 7-8.

Cacti. (2020). Cacti. Obtenido de https://www.cacti.net/

GNS3. (2021). GNS3. Obtenido de https://docs.gns3.com/docs/

Hernández, J. (2005). Software libre: técnicamente viable, económicamente sostenible y socialmente justo. Editorial Infonomia. Barcelona. España.

ICINGA. (2020). Obtenido de https://icinga.com/

Junco Romero, G., & Rabelo Padua, S. (2018). Los recursos de red y su monitoreo. Revista Cubana de Informática Médica, 10(1), 76-83. Obtenido de: http://scielo.sld.cu/scielo.php?pid=S1684-18592018000100009&script=sci_arttext&tlng=pt

NAGIOS. (2020). Obtenido de https://www.nagios.org/

OPENNMS. (2020). Obtenido de https://www.opennms.com/

READER. (2020). Obtenido de http://reader.digitalbooks.pro/content/preview/books/37922/book/OEBPS/Text/chapter1.html

Velasco Briones, C. A., & Cagua Ordoñez, G. S. (2017). Implementación de un sistema de monitoreo de redes utilizando herramientas open source y proveer servicios de directorio a través de active directory en la facultad de Filosofía y Ciencias de la educación de la universidad de Guayaquil. Obtenido de: https://dspace.ups.edu.ec/bitstream/123456789/13474/1/UPS-GT001824.pdf

Villagómez, J. I. (2015). Servidor de control de dispositivos y servicios mediante el protocolo SNMP para la red de datos en CELEC. E.P. Unidad de negocio Hidroagoyan.

ZABBIX. (2020). Obtenido de https://www.zabbix.com/