$\mathcal{DIFU}_{100}ci@$
Revista de Difusión Científica, Ingeniería y Tecnologías
Vol. 18, No. 1, Enero - Abril 2024
ISSN:2007-3585
Artículo arbitrado
Publicado: 30 de abril de 2024

Evaluation of a network monitoring tool, with emphasis on the verification of active equipment connection with ICMP protocol.

Evaluación de una herramienta para monitoreo de red, Teniendo énfasis en la verificación de conexión de equipo activo con protocolo ICMP

Edgar Fco. Alonzo Campos-Sánchez[1], **Remberto Sandoval-Arechiga**[1], **Víktor Iván Rodríguez-Abdalá**[1], **Salvador Ibarra-Delgado**[1], **Cristian Eduardo Boyain y Goytia Luna**[1], **Juan Manuel Pérez-Díaz**[1], **Ana Gabriela Castañeda Miranda**[1], **Oscar Osvaldo Ordaz García**[1], **Juvenal Villanueva Maldonado**[1], **J. Guadalupe Lara Cisneros**[3], **José Luis Alvarez-Flores**[2], and **José Ricardo Gómez-Rodríguez**[*1]

[1] *Universidad Autónoma de Zacatecas, Unidad Académica de Ingeniería Eléctrica,*
Posgrado en Ingeniería para la Innovación Tecnológica,
Carretera Zacatecas - Guadalajara, Kilómetro 6, Ejido la Escondida, Zacatecas, México, CP 98160.
{edgar.campos, rsandoval, abdala, sibarra, cristian.boyain, jmperez, agmiranda, oscarordazg, juvenal.villanueva, jrgrodri}@uaz.edu.mx
[2] *Universidad de Colima (UCOL), Campus Coquimatlán, Facultad de Ingeniería Mecánica y Eléctrica,*
Carretera Colima - Coquimatlan km 9, Valle de las Huertas, Colima, Colima, México, CP 28400.
alvarez_jose@ucol.mx
[3] *Universidad Autónoma de Zacatecas, Unidad Académica de Ingeniería Eléctrica,*
Carretera Zacatecas - Guadalajara, Kilómetro 6, Ejido la Escondida, Zacatecas, México, CP 98160.
jglara@uaz.edu.mx

Abstract

The network infrastructure is always growing, which demands the expansion of services causing more traffic on the active equipment, resulting in failures or degradation in the service connection to the network. This article presents the study of the Nagios Enterprise Monitoring Server (NEMS) as part of a methodology and network monitoring tool for the administrative management of the active equipment and links of the same. The study includes a review of the tool vs. commercial and open source monitoring tools, its architecture, taxonomy, properties and monitoring protocols with an emphasis on ICMP.

Keywords— Monitoring Network, Monitoring protocols, NEMS tools

Resumen

La infraestructura de red siempre está en constante crecimiento, lo que demanda la ampliación de los servicios provocando con esto un mayor tráfico en los equipos activos, teniendo como resultado fallas o degradación en el servicio de conexión a la red. En el presente artículo se presenta el estudio de el Servidor de monitorización Nagios Enterprise (NEMS) como parte de una metodología y herramienta de monitoreo de red, para la gestión administrativa del equipo activo y los enlaces de la misma. El estudio contempla la revisión de la herramienta vs herramientas de monitoreo comerciales y de código abierto, su arquitectura, taxonomía, propiedades y protocolos de monitoreo haciendo enfasis en ICMP.

Palabras clave— Monitoreo de Red, Protocolos de monitoreo, monitoreo NEMS

I. Introducción

Una definición de red de comunicación de datos, también conocida como red de computadoras, red de internet o red computacional, se define como la conexión de dos o más computadoras, que se vinculan con el objetivo de compartir archivos o recursos y lograr establecer una comunicación.

Aunque en la actualidad ya no se habla de redes de computadoras si no que ya se menciona como red de las *cosas* que se encuentran equipadas con sensores (y otras tecnologías) que les permiten transmitir y recibir datos. así pues se propone de aquí en adelante se maneje solo el termino de **redes** para referirnos a esta conexión de dos o mas "nodos".

Las redes se encuentran al servicio de industrias como: las telecomunicaciones, la bancaria, la turística, la del entretenimiento, entre muchas otras. Con el aumento del uso de las redes se han incrementado también una serie de problemas con los cuales los administradores de redes deben tratar para garantizar el buen funcionamiento de la mismas, entre dichos problemas podemos encontrar aspectos tales como:

1. asegurar que todos los equipos de red se encuentren activos,
2. evitar la congestión de la red,
3. garantizar que todos los recursos de la red se compartan de manera eficiente,
4. detectar tráfico inusual que pueda afectar el funcionamiento de la misma.

Como lo menciona *León et al* [1], con el fin de cumplir tales exigencias, se suele hacer uso de una serie de técnicas que permiten, entre otras cosas, controlar el flujo de la red, realizar la clasificación del tráfico, realizar predicciones de comportamientos futuros y detectar posibles amenazas. Estas técnicas están en constante evolución y en los últimos años han venido siendo objeto de estudios para pretender mejorar su eficacia y brindar resultados más acordes a la realidad.

En la actualidad las diferentes actividades tanto del sector industrial, comercial, gubernamental, educativo, etc., están basadas y dependen de gran manera en la **disponibilidad de la conectividad de las redes**. Es por ello que se vuelve de suma importancia garantizar el acceso de los usuarios a sus servicios de red, siempre pendientes de su correcto funcionamiento por medio de herramientas de monitoreo del equipo activo y los enlaces que la conforman.

*Autor de correspondencia

II. Marco Teórico

Una herramienta de monitoreo de red es una aplicación automatizada y/o manual que se utiliza para administrar, monitorear y evaluar la arquitectura, la infraestructura y los servicios del equipo activo de una red.

El monitoreo de red se puede definir como el proceso de revisión y análisis del tráfico de datos en una red de computadoras. Teniendo como objetivo principal garantizar que la red funcione de manera eficiente, segura y sin problemas. Este proceso implica la recopilación de datos sobre la disponibilidad de los equipos, la detección de posibles problemas y la toma de medidas correctivas cuando sea necesario.

De igual manera, como lo mencionan Birje y Bulla [2] además de Stephen, Benedict y Kuma [3] el monitoreo en la red en la nube es el proceso de revisión, control y gestión del flujo de trabajo y los procesos operativos y activos dentro de una infraestructura de red, es el uso de técnicas de administración y monitoreo de TI manuales o automatizadas para garantizar que una infraestructura o plataforma de red optimice el rendimiento de la red. Adicional, el monitoreo ayuda a administrar el rendimiento de la red, especialmente cuando los consumidores adaptan servicios de misión crítica o aplicaciones científicas.

Los sistemas de monitoreo de red actuales están perfectamente alineados con los modelos de servicios en la nube como IaaS, PaaS y SaaS. Estos sistemas ofrecen una visibilidad integral de la infraestructura, independientemente del modelo de servicio, permitiendo a las organizaciones monitorizar el rendimiento, la disponibilidad y la seguridad de sus redes en tiempo real.

En un entorno IaaS, el monitoreo se enfoca en la infraestructura virtualizada, asegurando que los recursos como servidores, almacenamiento y redes estén operando de manera óptima.

En PaaS, el monitoreo se extiende a la capa de aplicaciones y servicios, supervisando el rendimiento de las aplicaciones y las bases de datos que se ejecutan en la plataforma.

Por su parte, en SaaS, los sistemas de monitoreo garantizan la disponibilidad y el rendimiento de las aplicaciones entregadas a los usuarios finales, gestionando tanto el lado del servidor como la experiencia del usuario final. Estos sistemas son escalables, lo que les permite adaptarse a la elasticidad de los servicios en la nube, y son capaces de integrarse con herramientas de gestión de eventos y automatización para ofrecer respuestas proactivas ante posibles incidencias.

Existe tambien dos formas de obtener la información en el monitoreo, la primera y mas simple la conexión directa del dispositivo con el equipo concentrador ó las que utilizan *agentes*, que es un software o componente que se instala en un dispositivo, servidor, o nodo dentro de

una red para recopilar datos sobre el rendimiento, estado y eventos del sistema. Este agente actúa como un intermediario entre el dispositivo monitoreado y el sistema central de monitoreo, enviando información relevante como métricas de uso de CPU, memoria, actividad de red, estado de aplicaciones, y cualquier otra variable crítica. Los agentes pueden operar en tiempo real o en intervalos definidos, y su configuración puede ser ajustada para recolectar y reportar solo la información que es necesaria para el análisis y la gestión del entorno monitoreado. Su funcionamiento es esencial para la visibilidad y la proactividad en la gestión de infraestructuras de TI, ya que permite identificar y solucionar problemas antes de que afecten el rendimiento del sistema o la experiencia del usuario, para una muestra grafica los modos se muestran en la Figura 1

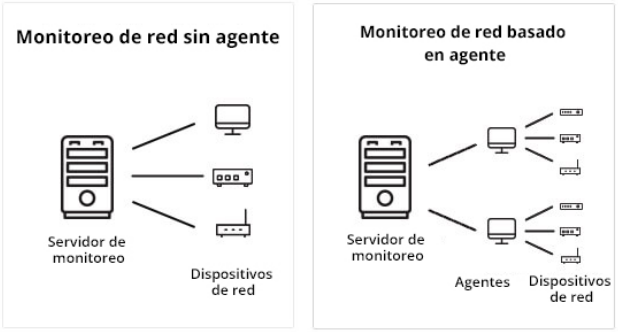

Figura 1: *Maneras de obtención de la información*

Teniendo en consideración los parrafos anteriores podemos presentar la arquitectura general de una herramienta de monitoreo de la red como se muestra en la Figura 2, de acuerdo a Birje y Bulla [2].

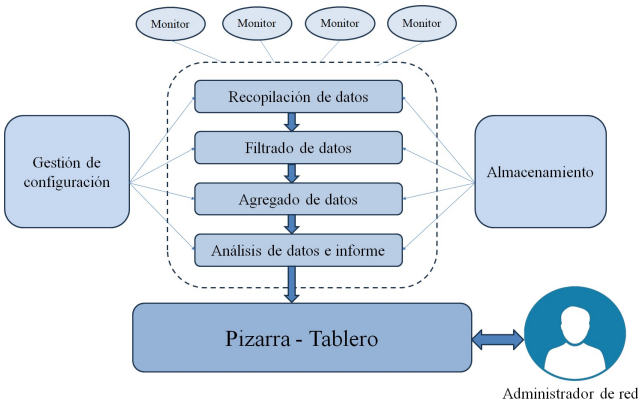

Figura 2: *Arquitectura de Herramientas de monitoreo de Red*

II.1. Protocolo ICMP

ICMP (por sus siglas en inglés, Protocolo de Mensaje de Control de Internet) surgió en la década de 1980 como parte integral del Protocolo de Internet (IP, por sus siglas en inglés) y se especificó por primera vez en el estándar RFC 792, publicado en septiembre de 1981. El desarrollo de ICMP se llevó a cabo en el contexto del crecimiento de ARPANET, la precursora de Internet, y la necesidad de contar con un protocolo que permitiera a los dispositivos de red comunicarse entre sí y reportar información de control [4].

ICMP es parte de la familia de los protocolos que trabajan en la capa de red tanto del modelo OSI como del modelo TCP/IP. ICMP desempeña un papel fundamental en la infraestructura de Internet al permitir que los dispositivos de red informen sobre errores, problemas de conectividad y otros eventos importantes. En la Figura 3 se muestran tanto sus características como sus campos principales.

Figura 3: *Mapa Mental de ICMP : caracteristicas y campos*

III. Metodología

La metodología empleada para el desarrollo del trabajo se describe esquemáticamente en la siguiente Figura 4

IV. Comparativa de NEMS con otros sistemas de Monitoreo

En la comparativa de NEMS con otros sistemas de monitoreo se presenta en las siguientes dos tablas donde en una se compara con sistemas de código abierto 5 y en la segunda se compara con sistemas de código propietario 6

V. Desarrollo

Una vez que se ha tomado la decisión de implementar NEMS (Nagios Enterprise Monitoring Server) como la

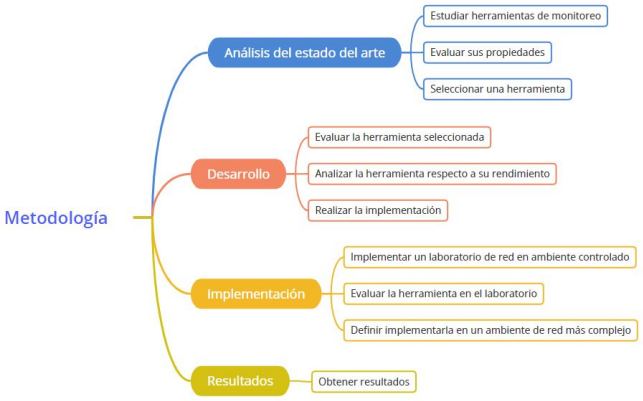

Figura 4: *Metodología empleada en este trabajo*

Herramienta de código abierto	Nivel	Propiedades																Tipo de red			
		Precisión	Adaptabilidad	Autónoma	Disponibilidad	Integralidad	Elasticidad	Extensibilidad	No intrusivo	Escalabilidad	Puntualidad	Resiliente	Confiable	Portable	Multiple Tenencia	Personalizable	Basado en Agente?	Pública	Privada	Tablero en tiempo real	
Nagios	XaaS	1		1	1		1	1	1	1		1	1	1	1	1	1	1	1	1	16
Zabbix	XaaS					1			1	1	1				1		1	1	1	1	9
Cacti	XaaS			1			1			1		1	1			1		1	1		8
Icinga	XaaS	1	1					1	1				1	1	1				1	1	9
Collected	XaaS	1		1			1		1								1	1			6
Opsview core	XaaS			1	1		1		1	1	1			1	1	1				1	10
Ganglia	XaaS			1		1				1			1		1		1		1		7
Hyperic	XaaS	1				1				1				1			1		1	1	7
Riemann	SaaS			1				1	1		1			1					1		6
cAdvisor	XaaS				1						1		1	1		1			1	1	7
Graphite	SaaS		1			1						1		1			1				5
Prometheus	SaaS	1		1		1										1			1		5

SaaS: Aplicación de monitoreo - PaaS: Plataforma de monitoreo - IaaS: Infraestructura de monitoreo - XaaS: Modelo híbrido que monitorea las tres capas

Figura 5: *Comparativa con sistemas de código abierto*

Herramienta Comercial	Nivel	Propiedades																Tipo de red o nube				
		Precisión	Autónoma	Disponibilidad	Integralidad	Elasticidad	Extensibilidad	No intrusivo	Escalabilidad	Puntualidad	Resiliente	Confiable	Portable	Multiple Tenencia	Personalizable	Basado en Agente?	Pública	Privada	Hibrida	Tablero en tiempo real	
Amazon CloudWatch	XaaS	1		1		1	1	1	1		1	1		1	1	1		1		1	13
CloudMonix	XaaS		1			1			1				1	1					1	1	7
Unified Infrastructure Management	SaaS	1	1	1	1		1		1					1			1	1		1	10
AppDynamics APM	SaaS			1						1				1		1	1				5
New Relic Cloud Monitoring	XaaS	1	1			1	1		1				1			1		1		1	9
PagerDuty	Paas		1				1		1									1		1	5
Bitnami Stacksmith	XaaS			1			1				1		1	1			1	1		1	8
Microsoft Cloud Monitoring	XaaS	1	1	1		1		1	1			1	1	1	1		1			1	12
Datadog	XaaS	1					1		1	1				1				1		1	7
Nimsoft	XaaS		1				1		1			1	1			1					6
Monitis	XaaS											1	1					1			3
RevealCloud	SaaS	1			1						1		1		1						5
LogicMonitor	SaaS	1	1				1			1		1	1	1				1	1	1	10
Cloudkick	XaaS	1			1			1					1			1		1		1	7

SaaS: Aplicación de monitoreo - PaaS: Plataforma de monitoreo - IaaS: Infraestructura de monitoreo - XaaS: Modelo híbrido que monitorea las tres capas

Figura 6: *Comparativa con sistemas de código abierto*

solución de monitoreo para la infraestructura de TI, es crucial llevar a cabo pruebas en un entorno controlado para validar su funcionalidad y eficacia en el caso de uso específico. Este paso es fundamental para asegurarse de que NEMS pueda cumplir con los requisitos de monitoreo, tanto en términos de cobertura de los elementos críticos del sistema como en la capacidad de respuesta ante incidencias. Al replicar en un entorno de prueba los escenarios operativos más relevantes, se busca verificar que NEMS no solo proporciona una supervisión precisa y en tiempo real, sino que también se integra adecuadamente con las demás herramientas y procesos de la organización, garantizando así un sistema de monitoreo robusto y funcional que pueda ser desplegado a gran escala con confianza.

Los equipos con que se desarrollo esta cama de pruebas son los que se presentan en la tabla 1, y su diagrama de topologia de interconexión se presenta en la Figura 7

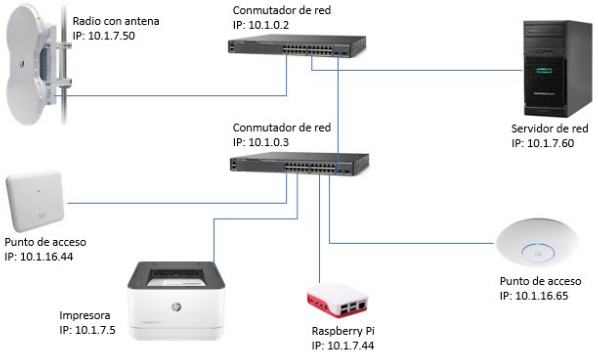

Figura 7: *Topología de Interconexión de la red de la cama de pruebas*

V.1. Alta de dispositivos

El alta de un dispositivo para el monitoreo dentro de NEMS se realiza a través de la interfaz de usuario de NEMS Configurator (NConf), encontrará esta herramienta en el menú *Configuración* de su panel NEMS. Dentro de NConf, haga clic en el enlace *Agregar* en la barra de navegación de la izquierda. Esto le presentará la pantalla Agregar dispositivo. Ingrese el nombre del dispositivo, un alias para su propia referencia y la dirección IP del dispositivo.

De acuerdo a las buenas practicas en la administración de equipo activo de red, se debe asegurar que los hosts tengan direcciones IP estáticas para que no cambien al momento de sufrir una desconexión y reconexión en la red.

A continuación, en el menú desplegable del sistema operativo en la misma pantalla, seleccione el sistema operativo de su host. Teniendo en cuenta que si no ve un tipo apropiado, también se pueden agregar sistemas operativos en *Elementos adicionales* en el menú de navegación izquierdo.

La pantalla de alta de dispositivos o anfitrión se muestra en la Figura 8

VI. Resultados

Para llevar acabo el monitoreo de hosts y servicios, NEMS utiliza plugins. Estos son componentes externos a los que Nagios les pasa información sobre lo que debe comprobarse y los límites críticos y de advertencia; una vez transmitida esta información, los plugins harán las respectivas comprobaciones y analizarán los resultados.

El resultado del chequeo de estos plugins es el estado del servicio o host monitoreado (NEMS solo recoge

Tabla 1: *Características principales de los equipos de red utilizados*

Equipo	Marca	Modelo	Característica
Conmutador	Cisco	Catalyst 2960-X	24 Puertos
Punto de Acceso	Ubiquiti	U6LR	Clientes: 200+
Servidor de red	IBM	xxxx	Procesador Intel Xeon E5-2680
Radio con antena	ubiquiti	NBE-5AC-GEN2	Enlace de hasta 450 Mbps

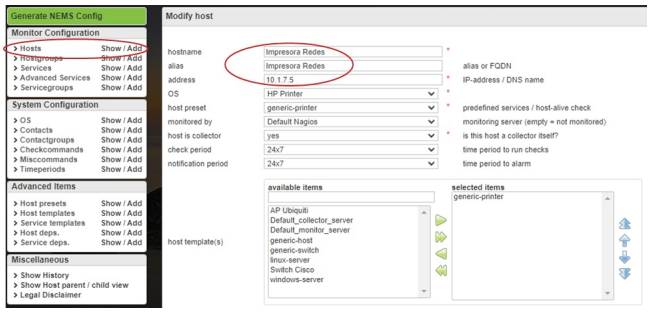

Figura 8: *Pantalla de alta de host a monitorear: nombre de dispositivo y dirección IP.*

cuatro estados: *Ok, Warning, Critical y Unknown*) e información más detallada sobre los mismos. Esto significa que, además de encontrar problemas, Nems previene a los administradores de red sobre posibles problemas mediante la detección y notificación de los estados monitoreados y definidos para cada host.

Este servidor engloba varias interfaces web de monitoreo, entre ellas:

- Nagios Core, en el que se puede hacer un seguimiento de los hosts y servicios a monitorizar en la red, acceder a alarmas y notificaciones, acceder a información específica de la Raspberry, etc.
- Nagios Nconf, a través de la cual se puede hacer cambios en la configuración adecuándola a nuestra infraestructura.
- NagVis, como lo indica [5], es un complemento de visualización para una mejor gestión de la red a través de Nagios. Crea mapas de acuerdo a las relaciones padre/hijo entre hosts de la red monitorizada por Nagios.
- Check-MK es una extensión del sistema de monitorización de Nagios que permite crear una configuración usando Python y descargar el trabajo desde Nagios Core permitiendo que más sistemas sean supervisados desde un solo servidor Nagios.

VI.1. Presentación de resultados

Para realizar la presentación de resultados, NEMS ofrece dos interfaces web, la primera es Adagios y la segunda es Nagios, dichas interfaces muestran los resultados del monitoreo de los dispositivos y servicios. Dichas interfaces ofrecen tanto una visión global del sistema, así como información más detallada y precisa de cada elemento, también recogen alertas y notificaciones que automáticamente aparecen publicadas en la interfaz.

VI.1.1. Adagios

En el panel izquierdo de la pantalla principal de Adagios, se encuentran diferentes opciones las cuales muestran el resultado visual de los dispositivos monitoreados, las opciones más relevantes son: *Status Overview, Host, Sevices y Hostgroups*.

A continuación, se describe brevemente lo que cada opción muestra como resultado del monitoreo de los dispositivos de la red implementada.

Vista Status Overview: En está vista se muestra un resumen del número de dispositivos y servicios que se están monitoreando, número de dispositivos padres en la red, así como el resumen de los problemas detectados en los servicios, la vista se muestra en la Figura 9

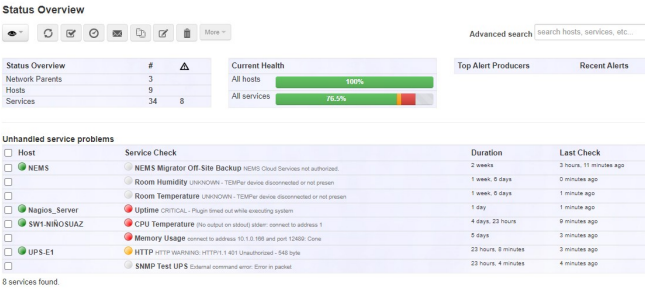

Figura 9: *Vista Overview dentro de la interface Adagios.*

Vista Hosts: Esta opción se muestra un resumen de todos los dispositivos que se están monitoreando, así como la dirección IP de cada dispositivo, desde cuando se está monitoreando, última revisión, su estado y el estado de los servicios monitoreados, la vista se muestra en la Figura 10.

Vista Services: Esta vista muestra los servicios monitoreados por dispositivo, su estatus, duración y cuando fue su última revisión, la vista se muestra en la Figura 11.

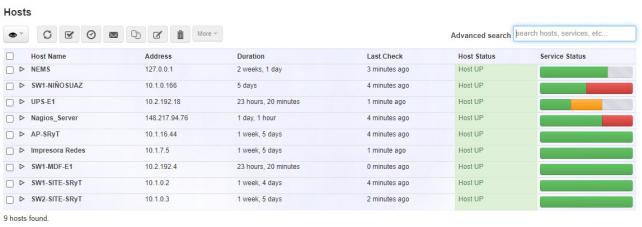

Figura 10: *Vista Host dentro de la interface Adagios.*

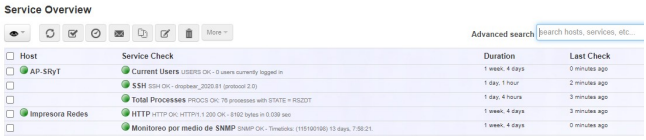

Figura 11: *Vista Service dentro de la interface Adagios.*

Vista Hostgroups: En esta vista se muestran los grupos creados, los dispositivos y servicios que pertenecen a los grupos y el estado de los servicios, la vista se muestra en la Figura 12.

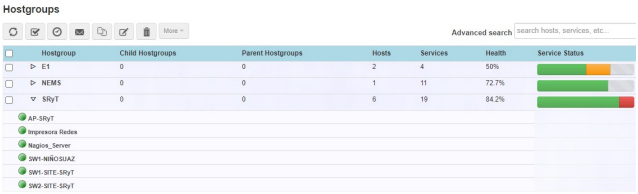

Figura 12: *Vista Hostgroups dentro de la interface Adagios.*

VI.1.2. Interface Nagios

Nagios permite tener acceso a visualizar los resultados del monitoreo de acuerdo al formato de Nagios Core tradicional, sus principales vistas son:

Vista Tactical Overview: La visión global de red configurada se puede ver en la pestaña Tactical Overview. Esta muestra información sobre los estados de dispositivos, servicios, cuántos tienen las notificaciones y los chequeos habilitados o deshabilitados. La vista se muestra en la Figura 13.

Vista Host Detail: En el apartado de Host Detail, se puede ver una lista de todos los dispositivos configurados junto con sus estados e información sobre el último chequeo, dando clic en cada uno de los dispositivos, podemos acceder a información más detallada del mismo, la vista se muestra en la Figura 14.

Vista Hostgroup Overview: En la pestaña Hostgroups, aparecen los dispositivos divididos en los diferentes

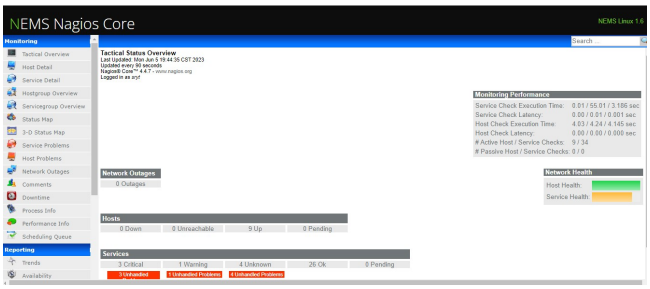

Figura 13: *Vista Tactical Overview dentro de la interface Nagios.*

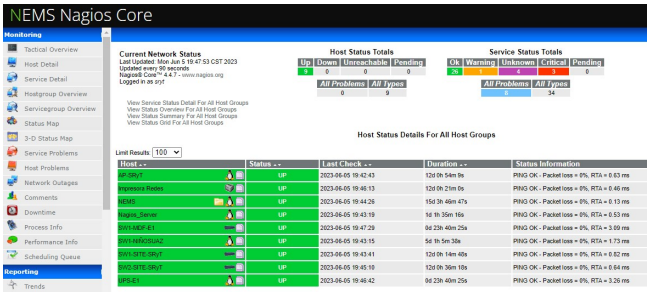

Figura 14: *Vista Host Detail dentro de la interface Nagios.*

grupos que se hayan configurado desde Nagios nConf, la vista se muestra en la Figura 15.

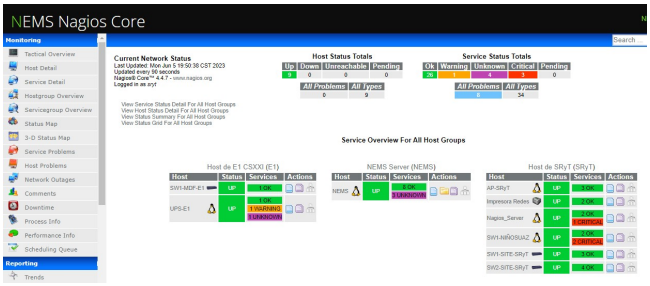

Figura 15: *Vista Hostgroup Overview dentro de la interface Nagios, muestra un listado de los hostgroups, los dispositivos que pertenecen a cada grupo y su estado.*

Vista Status Map: En esta vista aparece un mapa en el que se recogen todos los dispositivos configurados, colocando el puntero del ratón sobre cada dispositivo, aparece una pestaña con información más detallada y los servicios que cada dispositivo tiene asociado, la vista se muestra en la Figura 16.

VI.2. Interface Reportes

Una característica de Nagios Core es que se pueden generar informes y alertas. Esta interfaz web ofrece tres tipos de informes, que se describen brevemente a continuación:

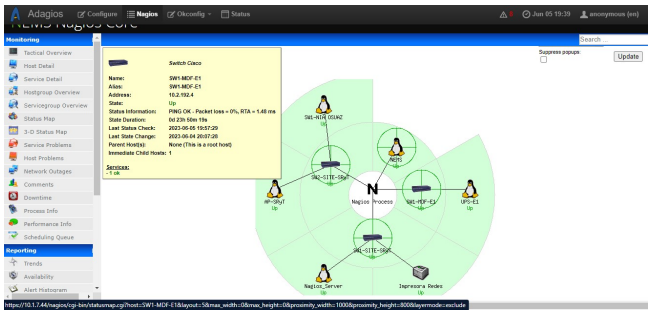

Figura 16: *Vista Status Map dentro de la interface Nagios.*

1. Trends: este informe muestra un historial de los cambios de estado que ha sufrido un dispositivo o servicio junto con la información que se ha ido obteniendo de los respectivos chequeos, la vista se muestra en la Figura 17.

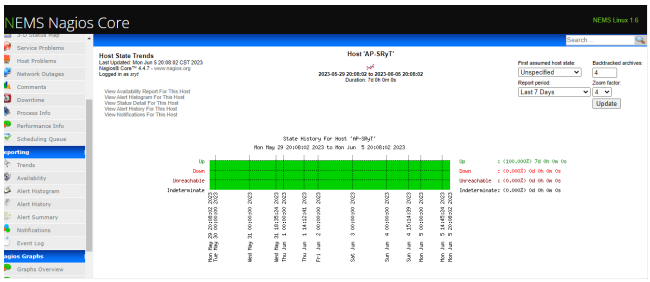

Figura 17: *Vista Trends dentro de la interface Reportes, muestra un historial de los cambios de estado que ha sufrido un dispositivo en un periodo de tiempo.*

2. Availability: este informe muestra un historial de cuánto tiempo ha estado un dispositivo en un estado determinado. Puede informar sobre un objeto o sobre varios incluyendo grupos de dispositivos o servicios, la vista se muestra en la Figura 18.

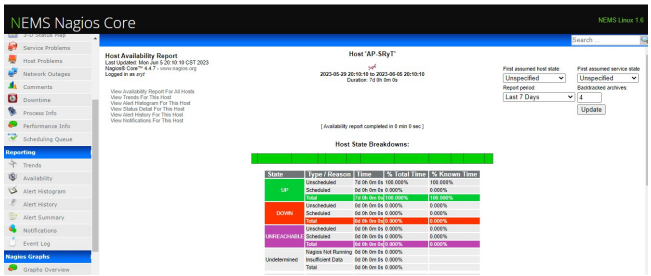

Figura 18: *Vista Availability dentro de la interface Reportes.*

3. Alert: este informe muestra el número de alertas que se han producido para un dispositivo o servicio en un periodo de tiempo. Este informe aparece en modo de histograma. También se puede obtener una lista completa con todas las alertas que se han ido registrando en el sistema, la vista se muestra en la Figura 19.

Figura 19: *Vista Alert dentro de la interface Reportes.*

VII. Rendimiento operativo de la Raspberry Pi

El rendimiento operativo de una Raspberry Pi 4 al ejecutar NEMS Linux depende de varios factores, incluyendo la carga de trabajo específica, la configuración de Nems, y otros servicios que se estén ejecutando en la Raspberry Pi.

Existen características generales como el hardware, la configuración, servicios y el almacenamiento, que pueden influir en el rendimiento operativo de una Raspberry, a continuación se describen dichas características:

Recursos del hardware: La Raspberry Pi 4 tiene mejoras significativas en comparación con modelos anteriores, con un procesador más potente, más RAM y puertos USB 3.0. Sin embargo, sigue siendo un dispositivo de recursos limitados en comparación con servidores más potentes. El rendimiento dependerá de la cantidad de hosts y servicios que se estén monitoreando.

Configuración de Nems: La configuración de Nems puede afectar el rendimiento. Si se está monitoreando una gran cantidad de hosts y servicios con verificaciones frecuentes, podría generar una carga significativa en la Raspberry Pi. Ajustar la frecuencia de verificación y optimizar la configuración de Nagios puede ayudar a mejorar el rendimiento.

Uso de recursos por otros servicios: Se ejecutan otros servicios en la Raspberry Pi, como servidores web, bases de datos u otros, esto puede afectar el rendimiento general.

Almacenamiento: El tipo y la velocidad de la tarjeta de memoria utilizada en la Raspberry Pi también pueden influir en el rendimiento. Una tarjeta de memoria rápida puede ayudar a mejorar el acceso a los datos y reducir los tiempos de carga.

Con base a lo anterior es importante monitorear el rendimiento de la Raspberry Pi mientras ejecutas NEMS Linux para identificar posibles cuellos de botella y ajustar la configuración según sea necesario.

Los resultados de la evaluación señalaron que el porcentaje promedio de utilización de la CPU se mantuvo en un 2 %, mientras que el uso de memoria se mantuvo en un 14 %. Estos hallazgos destacan la eficiencia y capacidad de respuesta del hardware utilizado, respaldando

así la idoneidad de la configuración implementada.

A continuación se muestran imágenes con el rendimiento de algunos de los componentes y características de la Raspberry, como la capacidad de memoria, archivos de proceso, así como de las aplicaciones que integran Nems. El lapso de tiempo mostrado en las imágenes corresponde a 1 mes calendario el cual se contabiliza a partir de la fecha en que se consulta el reporte.

Hasta el momento, se puede concluir que la Raspberry ha demostrado un rendimiento satisfactorio tanto en términos de procesamiento como de uso de memoria al monitorear alrededor de 900 dispositivos de red. Como parte de los próximos pasos, se contempla la expansión continua del número de dispositivos bajo monitoreo en consonancia con el crecimiento de la red. Además, se continuará evaluando el rendimiento de la Raspberry hasta alcanzar su capacidad máxima. Este proceso permitirá determinar con precisión el número máximo de dispositivos que el equipo puede monitorear de manera efectiva.

La Figura 20 muestra el nivel de actividad de procesamiento de la Raspberry al ejecutar Nems, respecto a su capacidad de memoria, para el proyecto actual la capacidad de memoria de la Raspberry es de 4 GB.

Figura 20: *Muesta el comportamiento de la capacidad de memoria de la Raspberry con el uso de Nems.*

La Figura 21 muestra el porcentaje de uso de los archivos del sistema por parte de Nems.

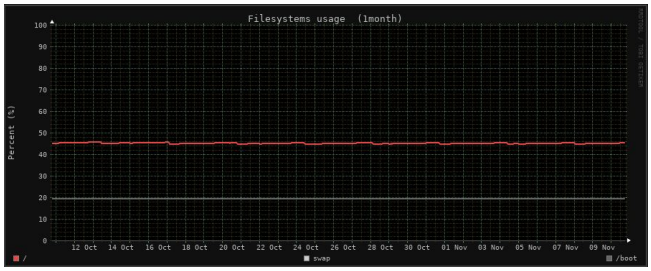

Figura 21: *Gráfica del porcentaje de uso de los archivos del sistema por parte de Nems*

La Figura 22 muestra el resumen general de los procesos y su estatus, así como el uso de CPU y memoria por parte de Nems.

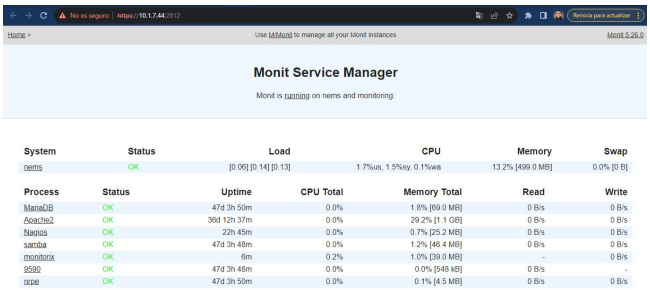

Figura 22: *Resumen general de procesos, CPU y memoria utilizados por Nems, muestra una vista rápida del estado de la Raspberry y de Nems.*

VIII. Conclusiones

El monitoreo de la red juega un papel muy importante en el apoyo a la gestión eficiente de varias áreas operativas, incluida la gestión de cuentas, la gestión de niveles de servicio acordados (SLA), el aprovisionamiento de servicios/recursos y la gestión de fallas. Ya que el monitoreo permite mantener la disponibilidad de los equipos que integran una red, a través del sensado y notificación continua que permite tomar acciones de corrección.

Para contextualizar y estudiar el monitoreo de la red, proporcionamos antecedentes y definiciones de conceptos clave, también se han mencionado las principales propiedades que deben tener las herramientas de monitoreo, los problemas que surgen de estas propiedades y las contribuciones relacionadas proporcionadas en la literatura hasta el momento. Se han descrito las principales plataformas (tanto comerciales como de código abierto) y servicios de monitoreo de red, indicando cómo se relacionan con dichas propiedades y cuestiones.

El estudio realizado permitió seleccionar la herramienta de monitoreo NEMS, y su implementación en una computadora de bajo consto, para dar respuesta al problema planteado en este proyecto.

La implementación de NEMS Linux ha demostrado ser una solución de monitoreo eficaz, ya que puede ser habilitada en hardware de bajo costo. La instalación y configuración vía WEB ayuda a la adopción del sistema de monitoreo, incluso para aquellos administradores con niveles moderados de experiencia en administración de redes, esto debido a la interfaz de usuario de NEMS Linux ofrece una experiencia intuitiva para la gestión y visualización de datos de monitoreo, esto facilita la comprensión rápida del estado de la red y la identificación de posibles problemas.

También se concluye que, la compatibilidad de NEMS Linux con una variedad de dispositivos y protocolos de red es un aspecto positivo, lo cuál permite monitorear diversos componentes de la red, desde servidores hasta dispositivos de red, contribuyendo a una visión integral

del entorno.

El monitoreo está ligado a un sistema de notificaciones y alertas integrado en NEMS Linux que mostró ser eficiente, al tener la capacidad de recibir alertas en tiempo real sobre eventos críticos lo cuál permite una respuesta proactiva ante posibles problemas antes de que afecten significativamente el rendimiento de la red.

La capacidad de personalizar los parámetros de monitoreo y adaptar el sistema según las necesidades específicas del entorno es un punto fuerte a favor de NEMS, así como la flexibilidad para ajustar umbrales y configuraciones garantiza una adaptación precisa a los requisitos particulares de la red.

Aunque la implementación fue en gran medida exitosa, se han encontrado desafíos específicos durante el proceso, se pueden identificar estos desafíos y documentar cómo se puede dar solución, puede proporcionar información valiosa para futuras mejoras o para usuarios que enfrenten problemas similares.

Finalmente, se llevó a cabo una evaluación del impacto en el rendimiento del hardware que aloja NEMS. Esta evaluación se ejecutó mediante el monitoreo de 900 dispositivos de red, abarcando tanto el tráfico local como el tráfico hacia Internet. La topología de conexión de estos dispositivos sigue un patrón de estrella distribuida en tres campus distintos.

Los resultados de la evaluación señalaron que el porcentaje promedio de utilización de la CPU se mantuvo en un 2 %, mientras que el uso de memoria se mantuvo en un 14 %. Estos hallazgos destacan la eficiencia y capacidad de respuesta del hardware utilizado, respaldando así la idoneidad de la configuración implementada.

En resumen, para tener una alta disponibilidad en la red, se necesita una herramienta de monitoreo eficiente. En este documento, se discutió desde el concepto básico de la herramienta de monitoreo hasta la implementación de una propuesta que mezcla no solo el monitoreo, sino también el uso de hardware de bajo costo que este acorde en la actualidad tecnológica, con lo cual se busca ayudar a los administradores de red a elegir la herramienta de monitoreo que mejor se adapte a sus necesidades.

IX. Trabajo futuro

Como trabajo a futuro se tiene la configuración a detalle de más protocolos de monitoreo que ayuden a explotar la herramienta, uno de estos protocolos es SNMP.

El protocolo SNMP ayuda a obtener información más detallada de los equipos activos de red monitoreados como se ilustra en la siguiente Figura 23.

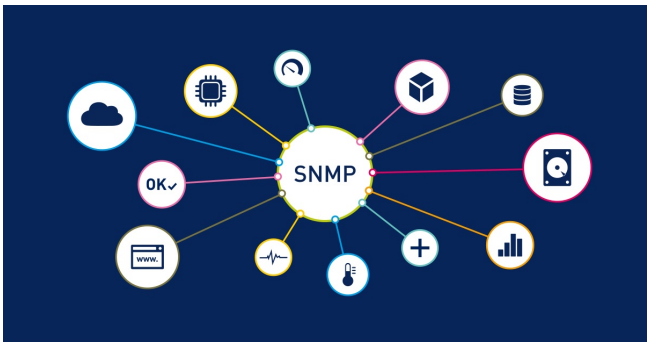

Figura 23: *Información visualizada de equipos activos de red mediante el protocolo SNMP*

Referencias

[1] Daruin Arley León et al. «Inteligencia artificial para el control de tráfico en redes de datos: Una Revisión». En: *Entre Ciencia e Ingeniería* 16.31 (2022), págs. 17-24.

[2] Mahantesh N Birje y Chetan Bulla. «Commercial and open source cloud monitoring tools: a review». En: *Advances in Decision Sciences, Image Processing, Security and Computer Vision: International Conference on Emerging Trends in Engineering (ICETE), Vol. 1*. Springer. 2020, págs. 480-490.

[3] Absa Stephen, Shajulin Benedict y RP Anto Kumar. «Monitoring IaaS using various cloud monitors». En: *Cluster Computing* 22.Suppl 5 (2019), págs. 12459-12471.

[4] Douglas E Comer. *Internetworking with TCP/IP*. Addison-Wesley Professional, 2013.

[5] Marina Cabezón Rodríguez. *Evaluación de herramientas de monitorización de redes sobre plataforma embebida*. Oct. de 2017. URL: `http://hdl.handle.net/10902/12116`.