UNIVERSIDAD AUTÓNOMA DE ZACATECAS

EVALUACIÓN DE NEMS COMO HERRAMIENTA PARA LA VERIFICACIÓN DE CONEXIÓN DEL EQUIPO ACTIVO EN UNA RED

Edgar Fco. Alonzo Campos Sánchez

Tesis de Maestría

presentada a la Unidad Académica de Ingeniería Eléctrica

de acuerdo a los requerimientos de la Universidad para obtener el título de

MAESTRO EN INGENIERÍA PARA LA INNOVACIÓN TECNOLÓGICA

Directores de tesis:

Dr. José Ricardo Gómez Rodriguez, Dr. Remberto Sandoval Aréchiga y Dr. Cristian Eduardo Boyaín y Goytia Luna

UNIDAD ACADÉMICA DE INGENIERÍA ELÉCTRICA

Zacatecas, Zac., 2024

Zacatecas, Zac.

18 de julio de 2024

C. Edgar Fco. Alonzo Campos Sánchez

PRESENTE

At'n: Dr. Víktor Iván Rodríguez Abdalá
Responsable de MIIT

Los abajo firmantes, miembros del comité tutorial designado por la Maestría en Ingeniería para la Innovación Tecnológica de la Universidad Autónoma de Zacatecas "Francisco García Salinas" para la evaluación del trabajo de tesis titulado: **"Evaluación de NEMS como herramienta para la verificación de conexión del equipo activo en una red"**, desarrollado bajo la dirección del Dr. José Ricardo Gómez Rodríguez, manifiestan que después de haber revisado el trabajo y que habiendo sido atendidas todas las correcciones indicadas por este comité, se **AUTORIZA** para proceder a su impresión y empastado.

COMITÉ TUTORIAL

Dr. José Ricardo Gómez Rodríguez
Director

Dr. Remberto Sandoval Aréchiga
Co-director

Dr. Cristian Eduardo Boyain y Goytia Luna
Co-director

Dr. Víktor Iván Rodríguez Abdalá
Sinodal

Dr. Oscar Osvaldo Ordaz García
Sinodal

c.c.p. Responsable de Maestría en Ingeniería para la Innovación Tecnológica

Asunto: **Cesión de derechos**
Zacatecas, Zac.

18 de julio de 2024

A QUIEN CORRESPONDA

PRESENTE

El que suscribe C. **Edgar Fco. Alonzo Campos Sánchez** estudiante de la *Maestría en Ingeniería para la Innovación Tecnológica* con matrícula **92302164**, adscrito a la *Unidad Académica de Ingeniería Eléctrica*, manifesta que es el **autor intelectual** del presente trabajo de tesis titulado: **Evaluación de NEMS como herramienta para la verificación de conexión del equipo activo en una red** bajo la dirección del *Dr. José Ricardo Gómez Rodríguez* y cede los derechos a la *Universidad Autónoma de Zacatecas "Francisco García Salinas"* para la divulgación total o parcial con fines académicos y de investigación.

A T E N T A M E N T E.

Edgar Fco. Alonzo Campos Sánchez

Carta de similitud núm. 664/IyP
Zacatecas, Zacatecas 25/junio/2024

Dr. Viktor Iván Rodríguez Abdalá
Responsable de la MIIT – UAZ Presente

Estimado Dr. Rodríguez,

Después de saludarlo, sirva el presente oficio para notificar que el documento

"Evaluación de nems como herramienta para la verificación de conexión del equipo activo en una red"
de Edgar Fco. Alonzo Campos Sánchez

Fue analizado con el software Copyleaks, con la intención de detectar similitudes; el resultado en cuestión fue

20.8 % de similitud

De acuerdo a lo anterior, el porcentaje se considera **ACEPTABLE** de acuerdo a los estándares internacionales.

Atentamente
"Somos Arte, Ciencia y Desarrollo Cultural"

Dr. Carlos Francisco Bautista Capetillo
Coordinador de Investigación y Posgrado
Universidad Autónoma de Zacatecas

RESUMEN

En la actualidad las telecomunicaciones es un área que constantemente desarrolla innovaciones, particularmente en las redes de datos (conocidas como redes), dichas innovaciones han permitido a las instituciones tanto públicas como privadas usar las redes para brindar comunicación e interconexión a sus integrantes.

La infraestructura de red está constantemente en crecimiento, lo que demanda la ampliación de los servicios de la misma provocando con esto un mayor tráfico en los equipos activos, teniendo como resultado fallas o degradación en el servicio de red.

Teniendo en consideración la temática referente a las fallas o degradación en el servicio de red, se presenta el estudio de algunas metodologías y herramientas de monitoreo de red, las cuales permiten una mejor gestión administrativa del equipo activo y los enlaces de red.

El estudio contempla la revisión de herramientas de monitoreo comerciales y de código abierto, su arquitectura, taxonomía, propiedades y protocolos de monitoreo de red que interactúan con las herramientas de monitoreo.

Derivado del estudio se seleccionó la herramienta de monitoreo de red de nombre comercial **NEMS** la cual se evaluó en una cama de pruebas con equipos de red conectados en un ambiente controlado. Debido a que NEMS está diseñado para ejecutarse en computadoras de bajo costo, la herramienta se instaló para su evaluación en una Raspberry Pi.

La herramienta analizada presentó varios aspectos importantes a tomar en cuenta: 1) Presenta una interfaz amigable y con un avance significativo en su usabilidad, ya que se pueden realizar las configuraciones en un ambiente totalmente gráfico, 2) presenta la posibilidad de realizar configuraciones desde un enfoque descendente grupo-nodos, 3) presenta la posibilidad de presentación del monitoreo en diferentes modalidades o vistas.

Aunado a estos aspectos se encontró que la herramienta, al ser desplegada en una computadora de bajo costo y bajo consumo energético, puede ser ubicada en cualquier espacio de los centros de datos o de la red a monitorear. Incluso en sus gráficas de consumo y desempeño, este dispositivo es capaz de monitorear una gran cantidad de dispositivos.

DEDICATORIA

Así como toda acción tiene una reacción con la misma fuerza pero en sentido contrario, todo esfuerzo tiene su resultado, es por eso que quiero dedicar la finalización de este posgrado, Maestría en Ingeniería para la Innovación Tecnológica, a mis padres, quienes con su ejemplo y esfuerzo de siempre salir adelante a pesar de las adversidades, me han dado la fuerza física y mental para terminar con éxito el posgrado y no claudicar en el intento.

A mí madre quien con su don de siempre ayudar y siempre dar lo mejor de ella, me inculcó valores y el tener fe ciega en nuestras creencias.

A mí padre quien con su fortaleza física y su hambre de conocimiento, me inculcó que jamás hay que rendirse ante las adversidades de la vida y el desear aprender cada día cosas nuevas.

A ellos les agradezco inifinitamente y les dedico este logro.

Agradecimientos

Por este medio agradezco infinitamente a mi esposa Norma, mi hija Emma Zirel Karina, mi hijo Edgar Jesús Alonzo y a mi hijo Juan Fernando Emmanuel por comprender, tolerar y aceptar el tiempo que no les dediqué debido a los dos años de estudio del posgrado y que, a pesar de todo me han brindado su apoyo.

A mis padres y hermanos por alentarme a seguir estudiando y brindarme su apoyo incondicional.

A mis compañeros de generación por contribuir con su apoyo, tips, momentos de alegrías y sobre todo por su amistad.

Al Posgrado en Ingeniería para la Innovación Tecnológica de la Universidad Autónoma de Zacatecas por la oportunidad de investigar nuevas herramientas de monitoreo de red, así como a mí asesor el Dr. José Ricardo Gómez Rodríguez por siempre encausarme a ser un mejor profesional.

Al Sistema Nacional de Posgrados (SNP) del Consejo Nacional de Humanidades, Ciencia y Tecnología (CONAHCYT) por su apoyo económico a través de la convocatoria "Becas Nacionales (Tradicional) 2021-2023".

Contenido General

Pág.

Lista de figuras

Figura Pág.

Figura Pág.

Lista de tablas

Nomenclatura

LAN *Local Área Network* (Red de Área Local).

MAN *Metropolitan Area Network* (Red de Área Metropolitana).

WAN *Wide Area Network* (Red de Área Amplia).

IT *Information technology* (Tecnologías de la Información).

MIB *Management Information Base* (Base de Información de Gestión).

$SNMP$ *Simple Network Management Protocol* (Protocolo Simple de Gestión de Red).

$IETF$ *Internet Engineering Task Force* (Grupo de Trabajo de Ingeniería de Internet).

AI *Artificial Intelligence* (Inteligencia Artificial).

$NIST$ *National Institute of Standards and Technology* (Instituto Nacional de Estándares y Tecnología).

SLA *Service Level Agreement* (Acuerdo de Nivel de Servicio).

$NEMS$ *Nagios Enterprise Monitoring Server* (Servidor de Monitoreo Empresarial Nagios).

$SMTP$ *Simple Mail Transfer Protocol* (Protocolo Simple de Transferencia de Correo).

$POP3$ *Post Office Protocol* (Protocolo de Oficina de Correos).

$HTTP$ *Hypertext Transfer Protocol* (Protocolo de Transferencia de Hipertexto).

$PING$	*Packet Internet Groper* (Buscador de Paquetes de Internet).
CPU	*Central Processing Unit* (Unidad Central de Procesamiento).
SSH	*Secure Shell* (Acceso Remoto Seguro).

Glosario

Agente: Un software que se ejecuta en dispositivos de red y que proporciona información al servidor de monitoreo, como SNMP agentes.

Alerta - Notificación: Una notificación generada por el sistema de monitoreo cuando se supera un umbral predefinido, indicando un posible problema.

Disponibilidad de red: Es un indicador medido en tiempo, el cual muestra la disponibilidad de una red, generalmente expresado como un porcentaje.

Escalamiento: La capacidad de agregar o quitar recursos de monitoreo según sea necesario para adaptarse al crecimiento de la red.

Herramienta de monitoreo de una red: Es una herramienta automatizada y manual que se utiliza para administrar, monitorear y evaluar la arquitectura, la infraestructura y el servicio de computación en la red.

Monitoreo de red: Es 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.

Nagios: Una plataforma de código abierto ampliamente utilizada para el monitoreo de redes y sistemas. NEMS Linux se basa en Nagios.

NEMS Linux: Nagios Enterprise Monitoring Server es una distribución de Linux basada en Nagios que facilita la implementación de un sistema de monitoreo de red.

Servicios de misión crítica: Los servicios o sistemas de misión crítica son las aplicaciones que son esenciales para el funcionamiento de una actividad en una empresa, organización o gobierno.

Capítulo 1

Introducción

1.1. Planteamiento del problema

En la última década, se ha sido testigo de un significativo aumento en la cantidad de dispositivos y equipos interconectados a las redes de telecomunicaciones de área local (LAN, por sus siglas en inglés), metropolitana (MAN, por sus siglas en Inglés) y global (WAN, por sus siglas en inglés). Este crecimiento exponencial ha llevado a que la probabilidad de falla en los servicios de red sea mayor, generando como consecuencia la necesidad de estar preparados para brindar una respuesta en el menor tiempo posible y resolver los problemas presentados por los usuarios. En este contexto, resulta de vital importancia la habilidad para identificar de manera precisa cuándo, dónde y por qué se produjo la falla en la red.

Por lo anterior se vuelve de suma importancia **contar con una herramienta que ayude a visualizar el funcionamiento de la red de comunicación de datos** o en su caso permita dar respuesta a: ¿cuál es el problema?, ¿dónde se presenta el problema?, ¿cómo se hizo el problema?, ¿cuándo ocurrió el problema?.

1.2. Hipótesis

Una herramienta avanzada de monitoreo de red permite la detección de fallas de conectividad, y además ofrece la capacidad de informar de manera precisa la ubicación exacta de dichas fallas, mejorando así la capacidad de respuesta y la eficacia en la resolución de problemas de red.

1.3. Justificación

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

En los últimos tiempos las redes han tomado gran importancia en el diario vivir de los seres humanos. Dichas redes son usadas en una gran cantidad de campos tales como: industria de las telecomunicaciones, industria bancaria, industria turística, industria del entretenimiento, entre muchas otras. Sin embargo, con el aumento del uso de las redes se ha incrementado también una serie de problemas con los cuales los administradores de red deben tratar para garantizar el buen funcionamiento de la mismas, entre dichos problemas se puede encontrar aspectos tales como: asegurar que todos los equipos de red se encuentren activos, evitar la congestión de la red, garantizar que todos los recursos de la red se compartan de manera eficiente entre los usuarios y las aplicaciones, además de detectar tráfico inusual que pueda afectar el funcionamiento de la misma.

Como lo menciona León et al. (2022), 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.

El monitoreo de una LAN es esencial para garantizar un rendimiento óptimo, identificando posibles problemas y mantener la seguridad. Además, los modelos de servicio: Infraestructura como Servicio IaaS (por sus siglas en inglés), Plataforma como Servicio PaaS (por sus siglas en inglés) y Software como Servicio SaaS (por sus siglas en inglés) son enfoques comunes en el cómputo en la nube.

El monitoreo de una LAN y el cómputo en la nube son dos aspectos cruciales para garantizar el rendimiento, la disponibilidad y la seguridad de los sistemas informáticos en una organización.

Existen herramientas comunes para el monitoreo de una LAN y la gestión en la nube, es importante ajustar las herramientas y estrategias de monitoreo según las necesidades específicas de cada entorno. La combinación de herramientas de entorno local y en la nube proporciona una visión completa de la infraestructura y facilita la identificación y resolución de problemas.

A continuación, se describen algunos trabajos que utilizan técnicas, modelos y sistemas que ayudan a la administración de las redes.

1. Un primer trabajo titulado **Monitoreo de IaaS usando varios monitores en la nube**, corresponde a Stephen, Benedict y Kumar (2019), que en resumen indica que:

   En el cómputo en la nube, el desempeño de la infraestructura como servicio es crítico debido a los múltiples usos que se le dan a la infraestructura en las distintas áreas de una organización. Los proveedores de la nube garantizan que los recursos estarán disponibles las 24 horas. Recientemente, los usuarios de la nube han aumentado rápidamente; por lo tanto, los proveedores también han aumentado, aumentando básicamente la complejidad de la infraestructura. Esta compleja infraestructura debe asignarse adecuadamente a los usuarios y se debe notificar a los usuarios la disponibilidad de recursos. Por lo tanto, el seguimiento constante de estos recursos es fundamental.

   En este análisis, se miden y tabulan la comparación de varias herramientas de monitoreo en términos de parámetros. A modo de comparación, las instancias de la nube de Amazon se monitorean con tres herramientas de monitoreo diferentes: el monitoreo de CloudWatch, el monitor de nube de tiempo de actividad IDERA y el administrador de aplicaciones ManageEngine. Los parámetros de IaaS son utilización de CPU, entrada de red, salida de red, lectura de disco, escritura de disco, tiempo de respuesta y uso de memoria. Además de las instancias de Amazon, también se monitorean servidores como Tomcat y bases de datos como PostgreSQL y también se analizan sus parámetros de rendimiento. La transferencia de datos de la red también es alta usando Cloudwatch.

   Como conclusiones de la investigación se tiene:

   Para analizar el rendimiento de IaaS en la nube, el acuerdo de nivel de servicio (por sus siglas en ingles SLA) firmado entre el proveedor y el cliente juega un papel importante.

En nuestra contribución a la investigación se ha tomado la disponibilidad como la métrica principal y se ha llevado a cabo el análisis. Aquí, la herramienta de monitoreo de la nube ManageEngine muestra la disponibilidad en porcentaje, mientras que las otras herramientas CloudWatch e Idera no lo hacen. Pero muestran los parámetros de cálculo como la utilización de la CPU, la entrada y salida de la red, la lectura y escritura del disco, etc. Cuando no hay disponibilidad de recursos, el usuario y el proveedor pueden concluir que se trata de una violación del acuerdo. El cómputo en la nube es una utilidad informática en la que se puede imponer una penalización al proveedor, ya que garantiza una disponibilidad del 99.9 %. Como se menciona en las conclusiones del artículo citado, esta investigación ahora se centra únicamente en los servicios web de Amazon y en el futuro se ampliará a varios proveedores de servicios y se podrán tabular los detalles de su disponibilidad.

2. Un segundo trabajo titulado **La definición del NIST de computación en la nube** corresponde a Mell y Grance (2011), quien propone lo siguiente:

   El cómputo en la nube es un paradigma en evolución. La definición del Instituto Nacional de Estándares y Tecnología NIST (por sus siglas en inglés) caracteriza aspectos importantes del cómputo en la nube y pretende servir como medio para realizar comparaciones amplias de servicios en la nube y estrategias de implementación, y proporcionar una base para la discusión desde qué es la computación en la nube hasta cómo utilizarla mejor. Los modelos de servicio e implementación definidos forman una taxonomía simple que no pretende prescribir ni restringir ningún método particular de implementación, prestación de servicios u operación comercial.

   La definición del NIST de cómputo en la nube es: un modelo para permitir el acceso a la red ubicuo, conveniente y bajo demanda a un conjunto compartido de recursos informáticos configurables (por ejemplo: redes, servidores, almacenamiento, aplicaciones y servicios) que se pueden aprovisionar y liberar rápidamente con un mínimo esfuerzo de gestión o interacción del proveedor de servicios. Este modelo de nube se compone de cinco características esenciales, tres modelos de servicio y cuatro modelos de implementación.

Modelos de servicio:

Software como servicio (SaaS, por sus siglas en inglés): La capacidad proporcionada al consumidor es utilizar las aplicaciones del proveedor que se ejecutan en una infraestructura de nube. Se puede acceder a las aplicaciones desde varios dispositivos cliente a través de una interfaz de cliente ligero, como un navegador web (por ejemplo, correo electrónico basado en web), o una interfaz de programa. El consumidor no gestiona ni controla la infraestructura de la nube subyacente, incluida la red, los servidores, los sistemas operativos, el almacenamiento o incluso las capacidades de las aplicaciones individuales, con la posible excepción de ajustes limitados de configuración de aplicaciones específicas del usuario.

Plataforma como servicio (PaaS, por sus siglas en inglés): La capacidad proporcionada al consumidor es implementar en la infraestructura de la nube aplicaciones creadas o adquiridas por el consumidor creadas utilizando lenguajes de programación, bibliotecas, servicios y herramientas respaldados por el proveedor. El consumidor no administra ni controla la infraestructura de la nube subyacente, incluida la red, los servidores, los sistemas operativos o el almacenamiento, pero tiene control sobre las aplicaciones implementadas y posiblemente los ajustes de configuración para el entorno de alojamiento de aplicaciones.

Infraestructura como servicio (IaaS, por sus siglas en inglés): La capacidad proporcionada al consumidor es proporcionar procesamiento, almacenamiento, redes y otros recursos informáticos fundamentales donde el consumidor puede implementar y ejecutar software arbitrario, que puede incluir sistemas operativos y aplicaciones. El consumidor no gestiona ni controla la infraestructura de la nube subyacente, pero tiene control sobre los sistemas operativos, el almacenamiento y las aplicaciones implementadas; y posiblemente control limitado de componentes de red seleccionados (por ejemplo, firewalls de host).

Modelos de implementación:

Nube privada: La infraestructura de la nube se proporciona para uso exclusivo de una única organización que comprende múltiples consumidores (por ejemplo, unidades de negocio). Puede ser propiedad de la organización, un tercero o una combinación de ellos, administrarlo y operarlo, y puede existir dentro o fuera de las instalaciones.

Nube comunitaria: La infraestructura de la nube se proporciona para uso exclusivo de una comunidad específica de consumidores de organizaciones que tienen inquietudes compartidas (por ejemplo: misión, requisitos de seguridad, políticas y consideraciones de cumplimiento). Puede ser propiedad de, administrada y operada por una o más organizaciones de la comunidad, un tercero o alguna combinación de ellos, y puede existir dentro o fuera de las instalaciones.

Nube pública: La infraestructura de la nube está preparada para uso abierto por parte del público en general. Puede ser propiedad de, administrada y operada por una organización empresarial, académica o gubernamental, o alguna combinación de ellas. Existe en las instalaciones del proveedor de la nube.

Nube híbrida: La infraestructura de nube es una composición de dos o más infraestructuras de nube distintas (privada, comunitaria o pública) que siguen siendo entidades únicas, pero están unidas por una tecnología estandarizada o patentada que permite la portabilidad de datos y aplicaciones (por ejemplo, explosión de nube para equilibrio de carga entre nubes).

3. Un tercer trabajo titulado **Cloud monitoring: A survey** corresponde a Aceto et al. (2013), quienes realizan un estudio sobre el monitoreo en la nube y que se resume a continuación:

   Hoy en día, el cómputo en la nube se utiliza ampliamente para brindar servicios a través de Internet por razones tanto técnicas como económicas. El número de servicios basados en la nube ha aumentado rápida y fuertemente en los últimos años, al igual que la complejidad de las infraestructuras detrás de estos servicios. Para operar y gestionar adecuadamente infraestructuras tan complejas, se necesita constantemente una supervisión eficiente.

   Como se menciona en las conclusiones del artículo citado, muchos trabajos en la literatura han estudiado las propiedades, características, tecnologías subyacentes (por ejemplo, virtualización), seguridad y privacidad de la nube. Sin embargo, hasta donde se ha investigado, estas encuestas carecen de un análisis detallado del monitoreo de la nube. Para llenar este vacío, en este documento se proporcionó una encuesta sobre el monitoreo de la nube. Se analizaron las motivaciones para el monitoreo de la nube, brindando también definiciones y

antecedentes para las siguientes contribuciones. Luego, se analizó y discutió cuidadosamente las propiedades de un sistema de monitoreo para la nube, los problemas que surgen de dichas propiedades y cómo se han abordado dichos problemas en la literatura. También se describen las plataformas actuales, tanto comerciales como de código abierto, y los servicios de monitoreo de la nube, subrayando cómo se relacionan con las propiedades y problemas identificados anteriormente. Finalmente, se identificaron temas abiertos, principales desafíos y direcciones futuras en el campo del monitoreo de la nube.

El cómputo en la nube se ha convertido rápidamente en un paradigma ampliamente adoptado para la prestación de servicios a través de Internet. Esto se debe a una serie de razones técnicas, que incluyen: mejora de la eficiencia energética, optimización de la utilización de recursos de hardware y software, elasticidad, aislamiento del rendimiento, flexibilidad y esquema de servicio bajo demanda. Además de estos beneficios técnicos, la literatura ha demostrado cómo el modelo de computación en la nube proporciona varios beneficios económicos, incluidos gastos operativos y de capital mínimos. Por todas estas razones, el número de organizaciones que adoptan soluciones en la nube y de suscriptores que acceden a servicios en la nube ha aumentado rápidamente, superando los optimistas planes iniciales, al igual que la complejidad de los sistemas en la nube.

Los servicios en la nube son bajo demanda, elásticos y escalables y, por lo tanto, un sistema en la nube necesita las siguientes características principales: disponibilidad, concurrencia, equilibrio de carga dinámico, independencia de las aplicaciones en ejecución, seguridad e intensidad. Para proporcionar estas características, se implementan y operan en los sistemas de computación en la nube técnicas avanzadas de virtualización, enfoques de programación sólidos y dinámicos, medidas de seguridad avanzadas y mecanismos de recuperación ante desastres.

Los centros de datos para cómputo en la nube siguen creciendo tanto en recursos de hardware como en volumen de tráfico, haciendo cada vez más compleja la operación y gestión de estos. En este escenario, se requieren actividades de monitoreo precisas y detalladas para operar eficientemente estas plataformas y gestionar su creciente complejidad.

En la literatura existe una gran cantidad de trabajos que proponen estudios y taxonomías de cómputo en la nube en general, de tecnologías de virtualización, y de seguridad en la nube. Sin embargo, hasta donde se ha investigado, no existen encuestas específicas sobre plataformas, técnicas y herramientas para monitorear infraestructuras, servicios y aplicaciones en la nube. Esto es lo que se define como monitoreo de la nube.

En este artículo, se proporcionó un estudio del monitoreo de la computación en la nube, de acuerdo a la siguiente metodología.

a) Selección de una taxonomía bien conocida de los términos y roles en el campo del cómputo enn la nube para la contextualización de las contribuciones que brindamos en este artículo. Para ello se utilizó el trabajo NIST.

b) Después de analizar la literatura en el campo de cómputo en la nube, utilizando las definiciones propuestas por NIST, se proporcionó una taxonomía de dos ejes para el monitoreo de cómputo en la nube:

- Un eje es para las diversas motivaciones para monitorear el cómputo en la nube;
- El otro eje se expande aún más en tres dimensiones: capa, nivel de abstracción, pruebas y métricas.

c) Gracias a los resultados del paso anterior, se analizaron varios trabajos de investigación para derivar las principales propiedades de los sistemas de monitoreo de la nube, los problemas asociados con dichas propiedades y las contribuciones en la literatura sobre estas propiedades y problemas. Además, se analizaron una serie de plataformas comerciales y de código abierto y una serie de servicios para el monitoreo de la nube, evidenciando también su relación con las propiedades y cuestiones discutidas anteriormente.

d) Los pasos anteriores proporcionan las directrices para atender los problemas abiertos y las direcciones futuras en el campo del monitoreo de la nube.

Este artículo proporciona contribuciones de interés para la comunidad investigadora, analizando la literatura y arrojando luz sobre los temas de investigación actuales y futuros sobre el monitoreo de la nube.

Con base a las investigaciones realizadas y descritas por los distintos autores se llega a la conclusión que es de vital importancia realizar un correcto control de la congestión y tráfico de la red, así como garantizar una alta disponibilidad de la misma y la integridad de los equipos activos que la integran apoyándose de diferentes técnicas o metodologías aplicables como lo son: políticas, metodologías y sistemas o herramientas de monitoreo.

1.4. Objetivos

1.4.1. Objetivo general

Evaluar NEMS y diversas herramientas de monitoreo de equipo activo de red, desde la documentación oficial del desarrollador o fabricante, incluyendo tanto soluciones comerciales como aquellas de código abierto. Este análisis permitirá seleccionar una herramienta de monitoreo idónea para establecer un sistema de monitoreo en la red que sea eficiente y llegar a su implementación.

1.4.2. Objetivos particulares

Para el cumplimiento del objetivo general se trazaron los siguientes objetivos particulares:

- Realizar una evaluación de NEMS en relación con las herramientas comerciales y de código abierto disponibles en el mercado para monitoreo de redes, desde la documentación oficial.
- Desplegar NEMS en una computadora de bajo costo con el objetivo de evaluar su desempeño en una cama de pruebas bajo condiciones controladas.
- Integrar NEMS en una red para su implementación efectiva en un escenario de uso real.

1.5. Alcances y limitaciones

Alcance: El monitoreo de equipo activo de red se puede realizar gracias a diferentes protocolos y en diferentes capas haciendo referencia al modelo de referencia OSI (por sus siglas en inglés). En esté estudio se propone realizar el monitoreo con el protocolo ICMP (por sus siglas en inglés) de la capa de red.

Limitaciones: No se incluye el monitoreo de enlaces de red con tráfico a Internet.

1.6. Metodología

La metodología empleada en el desarrollo del proyecto se presenta esquemáticamente en la Figura 1.1, destacando los siguientes puntos clave:

Análisis del estado del arte: Se llevó a cabo un análisis exhaustivo de diversas herramientas de monitoreo de red. La elección de la mejor herramienta se basó en los resultados obtenidos durante este análisis.

Desarrollo propuesto: La herramienta seleccionada se sometió a una evaluación detallada, analizando su rendimiento y requisitos técnicos de implementación. Esta fase permitió definir su implementación en un entorno de red controlado.

Implementación: Con base en la evaluación, pruebas y resultados obtenidos, se consideró la posibilidad de implementar la herramienta de monitoreo en un ambiente de red más complejo.

Resultados: Se definen conforme a la evaluación y pruebas realizadas con la herramienta seleccionada. La métrica utilizada para la evaluación fue la disponibilidad de los dispositivos, siguiendo la metodología del Estándar ANSI/TIA-942-2005.

Aunque existen diversas tecnologías, herramientas y enfoques disponibles para abordar la problemática, es esencial llevar a cabo un análisis exhaustivo de la literatura actual, también conocido como marco de referencia. Este análisis se abordará detalladamente en el próximo capítulo.

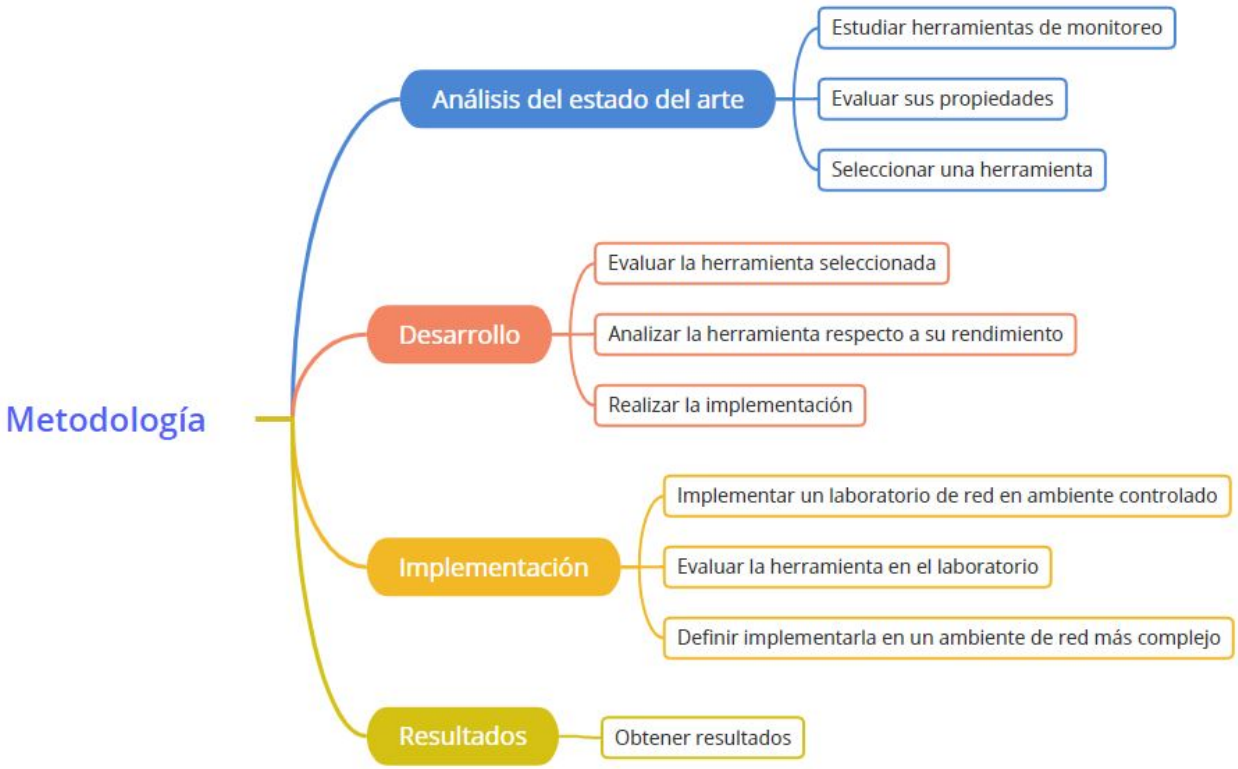

Figura 1.1 Metodología: análisis, desarrollo, implementación y resultados

.

Capítulo 2

Marco Teórico

2.1. Introducción

En el marco teórico se describe a grandes rasgos las características principales de una herramienta de monitoreo de red, así como del hardware y protocolos utilizados por dichas herramientas, y que se ve conceptualmente en la Figura 2.1

Figura 2.1 Mapa mental de una herramienta de monitoreo.

El monitoreo de una red es esencial para garantizar un rendimiento óptimo, identificando posibles problemas y mantener la seguridad. Además, los modelos de servicio IaaS, PaaS y SaaS son enfoques comunes en el cómputo en la nube

En IaaS, donde se proporciona infraestructura virtualizada, es crucial monitorear la red para garantizar el rendimiento y la disponibilidad de las máquinas virtuales, almacenamiento y redes.

Herramientas de monitoreo como Nagios, Zabbix o prometheus son útiles para supervisar conectividad, uso de ancho de banda, latencia y otros aspectos de la red.

En PaaS, la atención se centra en la plataforma y los servicios proporcionados. El monitoreo debe incluir el estado de los servicios de aplicaciones y bases de datos en la plataforma. Herramientas como: New Relic, AppDynamics o Azure Monitor pueden ser utilizadas para medir el rendimiento de las aplicaciones, identificar cuellos de botella y monitorear la integración entre servicios.

En SaaS, el monitoreo de red se enfoca en garantizar la disponibilidad y el rendimiento de la aplicación. Se deben supervisar aspectos como latencia, velocidad de carga y disponibilidad de la aplicación desde diferentes ubicaciones. Herramientas como: Dynatrace, SolarWinds o Pingdom son útiles para monitorear la experiencia del usuario final y garantizar un rendimiento óptimo de la aplicación.

En relación con el monitoreo de una LAN, estos modelos de servicio pueden utilizarse de diversas maneras. Por ejemplo, los servicios en la nube (IaaS, PaaS, SaaS) pueden ser implementados y utilizados a través de una LAN para facilitar la conectividad y la comunicación entre los dispositivos locales y los recursos en la nube. Esto permite a las organizaciones aprovechar la flexibilidad y escalabilidad de la nube mientras mantienen una LAN para sus necesidades específicas.

Monitorear la disponibilidad y el rendimiento de la red asegura que los usuarios tengan acceso a los recursos de manera eficiente, el monitoreo de la red en busca de posibles amenazas de seguridad y actividades sospechosas ayuda a proteger los datos y mantener la integridad del sistema. La escalabilidad de la infraestructura es necesaria para manejar cargas de trabajo crecientes, así como el implementar sistemas de registro para rastrear eventos y detectar problemas, facilita la solución de los mismos. La automatización de alertas ayuda a abordar problemas antes de que afecten significativamente el rendimiento de la red.

El monitoreo continuo de la red es esencial para garantizar la eficiencia operativa, la seguridad y la entrega confiable de servicios, independientemente del modelo de servicio adoptado.

De acuerdo con Mell y Grance (2011), una red de computadoras en la nube, es un "modelo para permitir un acceso de red conveniente y bajo demanda a un conjunto compartido de recursos informáticos configurables, que se pueden aprovisionar y liberar rápidamente con un mínimo esfuerzo de administración o interacción con el proveedor de servicios".

Según lo indica Birje y Bulla (2020), no todas las redes brindan el mismo servicio y son adecuadas para todos. Varios modelos, tipos y servicios han evolucionado para ayudar a ofrecer la solución adecuada a las necesidades del cliente. Los diferentes tipos de despliegues en redes locales son: *pública, privada e híbrida.* Hay tres grandes categorías principales de modelos de servicios de red: IaaS, PaaS y SaaS.

La gran demanda de uso que han tenido las redes LAN, MAN y WAN en la última década, ha provocado que existan fallas en los tres niveles de red. Por lo que es de suma importancia contar con una herramienta que permita: *visualizar el buen funcionamiento de la red o en su caso la detección de errores*.

Existen plataformas que intentan resolver la necesidad de visualizar el estado de una red con diferentes métodos y métricas, las cuales se ajustan a diferentes necesidades o tipos de redes de datos en específico, el análisis de dichas ofertas permitiría seleccionar la adecuada para la red que está bajo análisis.

2.2. ¿Qué es una herramientas de monitoreo de red?

Una herramienta de monitoreo de red es una aplicación automatizada y 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 (2020) y Stephen, Benedict y Kumar (2019) 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.

Las herramientas de monitoreo de la red, como lo mencionan Alhamazani et al. (2015) y Aceto et al. (2013) ayudan a realizar operaciones fluidas en la red, como contabilidad y facturación, y demás actividades administrativas.

2.3. Arquitectura general del modelo de monitoreo en una red

El enfoque multi-agente para la arquitectura de una herramienta de monitoreo en la LAN o en la nube. La herramienta de monitoreo en la LAN o en la nube tiene cinco funciones importantes: recopilación de datos, filtrado de datos, agregación de datos, análisis de datos y toma de decisiones. Los múltiples agentes se inyectan en varias partes de la LAN o nube para realizar dichas funciones. La arquitectura general de la herramienta de monitoreo de la LAN o en la nube se muestra en la Figura 2.2, de acuerdo a Birje y Bulla (2020).

2.4. Propiedades de las herramientas de monitoreo de red

Las propiedades de las herramientas de monitoreo de una red como lo menciona Aceto et al. (2013). La herramienta de monitoreo de red debe admitir las propiedades que se listan en la Tabla 2.1, para mejorar el rendimiento de la herramienta.

2.5. Herramientas comerciales de monitoreo de red

En esta sección, se describen brevemente las herramientas comerciales de monitoreo de red más populares que simplifican la tarea de administración para el administrador de la red, según Birje y Bulla (2020).

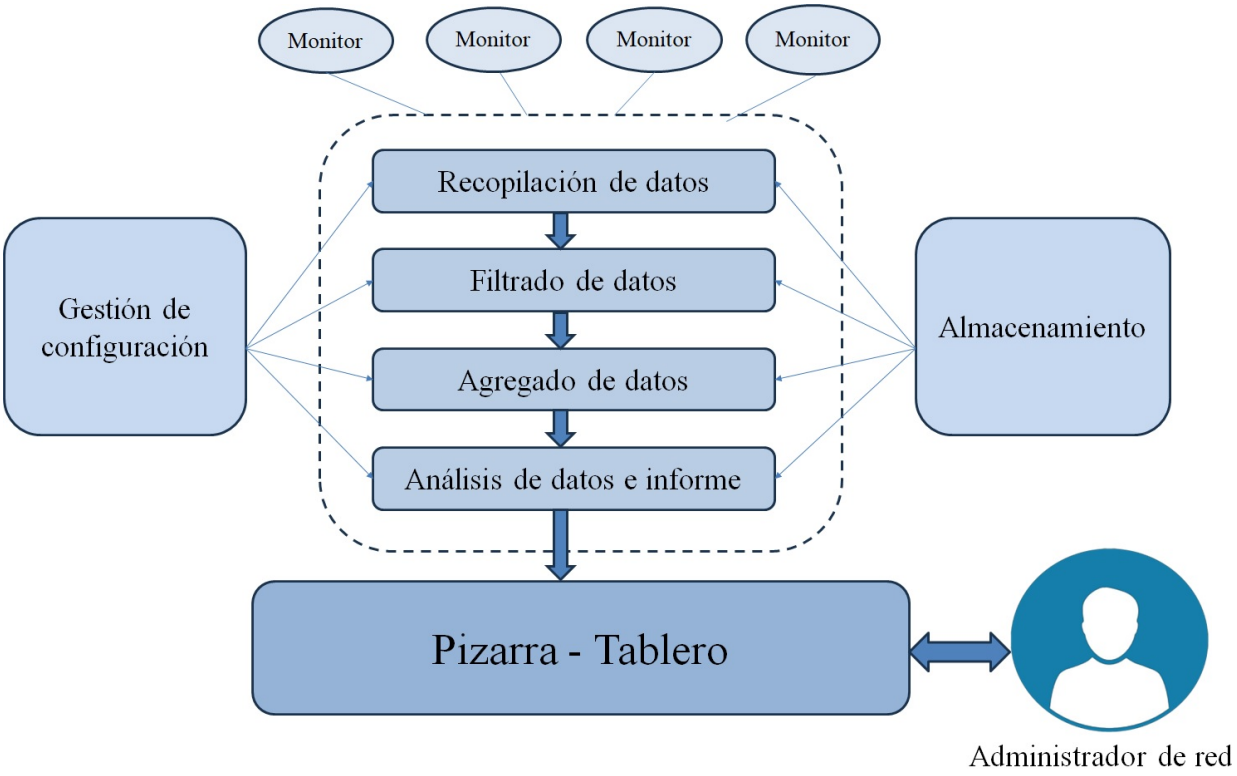

Figura 2.2 Arquitectura de una herramienta de monitoreo de red.

1. Amazon CloudWatch: Es un servicio de monitoreo creado para una variedad de usuarios, como desarrolladores, operadores de sistemas, ingenieros de confiabilidad del sitio y administradores de TI. Ofrece datos, información y conocimientos procesables para monitorear las aplicaciones, saber y responder a los cambios de rendimiento en todo el sistema, así como mejorar la utilización de recursos, como lo indica Amazon (2023) y Elasticsearch (2023).

2. CloudMonix: Es una solución mejorada de supervisión y automatización de la red en la nube para Microsoft Azure Cloud. El panel de monitoreo en vivo de CloudMonix permite a los administradores de Azure Cloud comprender de antemano los recursos de la nube, informarse con señales sobre precauciones y exclusiones y organizar actividades de recuperación y restauración automatizadas, como lo indican Netreo (2023) y Al-Ayyoub et al. (2016).

Tabla 2.1 Propiedades de una herramienta de monitoreo de red.

Propiedad	Definición
Precisión	Indicar medidas precisas que se acerquen lo más posible a los valores reales
Adopción	Adopte y admita la naturaleza dinámica de una red local o en la nube
Autonomía	Gestiona sus recursos de forma automática sin interacciones humanas
Disponibilidad	Disponible todo el tiempo para todos los usuarios de la red
Integralidad	Admite recursos heterogéneos, varios tipos de datos y múltiples inquilinos
Elasticidad	El tamaño de la red aumenta y disminuye dinámicamente en función al uso
Extensibilidad	Extender el recurso/servicio según los nuevos requisitos del usuario
No Intrusivo	Adoptar modificaciones significativas como los cambios en los requisitos
Escalabilidad	Funcionalidad al agregar un gran número de usuarios y organizaciones
Puntualidad	Responder dentro del límite de tiempo
Resiliente	Funcionalidad de servicios cuando la red cambia según los nuevos requisitos
Confiable	Realice la tarea requerida en cualquier momento
Portable	Entorno de red incorporado con plataformas y servicios heterogéneos
Tenencia múltiple	Concurrente en el suministro de datos a los usuarios
Personalización	Personalizable para todas la operaciones de red y necesidades del usuario

3. CA Unified Infrastructure Management (CA UIM): Proporciona una única solución basada en análisis para la gestión y el control proactivo, y efectivo de las modernas infraestructuras de red híbrida. Es la solución de monitoreo de TI que adoptó técnicas de inteligencia artificial para proporcionar informes analíticos inteligentes, amplia cobertura y una arquitectura extensible y portátil, como lo indica Broadcom (2019).

4. AppDynamics APM: Es una herramienta de monitoreo de inteligencia de aplicaciones que monitorea la comprensión operativa, el rendimiento de la aplicación, la experiencia del usuario y la influencia comercial de las aplicaciones de software. Gestiona el rendimiento de aplicaciones y ayuda a mapear la aplicación automáticamente, como lo indica AppDynamics (2023).

5. New Relic Cloud Monitoring: La aplicación se utiliza para monitorear la infraestructura y la aplicación de red en la nube dinámica de manera inteligente. Supervisa las aplicaciones en un solo lugar, lo que ayuda a ver las tasas de error, la carga de la página, las transacciones lentas y la lista de servidores en ejecución, como lo indica New (2008).

6. PagerDuty: Tiene más libertad para personalizar las métricas y el mecanismo de alerta, como lo indica PagerDuty (2023).

7. Bitnami Stacksmith: Es una entrega personalizada fácil e independiente con un objetivo único, es decir, hacer que sea modesto comenzar con los servicios de AWS desde la línea de comandos. Emplea un algoritmo de inteligencia artificial para mejorar el rendimiento de las actividades en la red, como lo indica Bitnami (2023).

8. Microsoft Cloud Monitoring: Se logra tener más visibilidad y control en la red híbrida, con seguridad y administración de operaciones sencillas. Es un grupo de servicios basados en la nube para manejar la configuración local y en la nube desde un solo lugar, como lo indica Microsoft (2023).

9. Datadog: Ayuda a monitorear eventos y métricas de rendimiento para organizaciones de TI y desarrolladores. La herramienta admite propiedades de escalabilidad y funciona de manera eficiente incluso si aumenta el tamaño de los datos. La herramienta ayuda en consolas personalizables en tiempo real con pantallas de corte y señales, por etiquetas, caracteres, etc., como lo indica DataDog (2023).

10. Nimsoft: Admite el monitoreo de múltiples capas y monitorea los recursos de la red virtual y física. Nimsoft les permite a sus consumidores ver y monitorear los recursos que se alojan en diferentes infraestructuras en la red, como lo indica Nimsoft (2010).

11. Monitis: Es una herramienta de monitoreo en la nube basada en múltiples agentes. Los agentes se instalan en la red antes del firewall. El agente recopila todos los datos de los dispositivos de red mediante complementos, como lo indica US Website (2022).

12. RevealCloud: Se utiliza para monitorear diferentes tipos de redes en la nube. Los consumidores pueden monitorear a través de diferentes capas de la red, como lo indica TechTarget (2023).

13. LogicMonitor: También ayuda a los consumidores a monitorear las diferentes capas de la red en la nube como IaaS, PaaS, SaaS. Los protocolos SSL (por sus siglas en inglés) y

SNMP (por sus siglas en inglés) se utilizan para fines de comunicación, como lo indica Logic-Inc (2023).

14. Cloudkick: Se utiliza para monitorear y administrar instancias de servidor que se ejecutan en la nube de Amazon EC2 y otros proveedores de nube mediante una única interfaz combinada. En cada instancia se instalan agentes pequeños y de baja sobrecarga que recopilan diferentes métricas de la CPU, la memoria y la red, como lo indica Kick (0015).

2.6. Herramientas de monitoreo de código abierto

Como lo indica Birje y Bulla (2020), las herramientas de monitoreo de código abierto pueden ofrecer una serie de ventajas en la parte económica sobre las opciones nativas de los proveedores de la red. En esta sección, se analiza brevemente las herramientas de monitoreo de la red de código abierto más utilizadas. Algunas de las principales se describen a continuación:

1. Nagios: Monitorea todo tipo de componentes de la red como protocolos de red, sistemas operativos, métricas de rendimiento del sistema, aplicaciones, servidor web, servicios web, sitio web, etc. Nagios proporciona un alto nivel de rendimiento al consumir menos recursos del servidor utilizando un motor de monitorización de 4 núcleos, como lo indica Nagios (2023).

2. Zabbix: Es un marco de monitoreo de nivel empresarial diseñado para monitorear aplicaciones, plataforma e infraestructura en la red y base de datos. Es una herramienta de monitoreo basada en agentes donde se instalan múltiples agentes en el servidor y el cliente para recopilar, filtrar y analizar los datos, como lo indica Zabbix (2001).

3. Cacti: Es una herramienta de monitoreo que se puede instalar en varios sistemas operativos como Linux o Windows OS y conectarse a RRDTool que se utiliza para generar varios tipos de gráficos relacionados con datos de red relevantes. Funciona con SNMP y presenta las estadísticas de la red en un formato fácil de entender, como lo indica Cacti (2004).

4. Icinga: Es el marco de monitoreo que monitorea todos los sistemas disponibles en la red, que alerta al usuario de muchas maneras y proporciona una base de datos para sus informes de SLA, como lo indica Icinga (2009).

5. Collected: Es una herramienta de monitoreo que monitorea varios componentes como recursos del sistema, redes, sensores, bases de datos, aplicaciones y servicios, etc. esta es una herramienta de monitoreo basada en agentes escrita en lenguaje C y se puede desplegar en plataformas Linux y Mac, como lo indica Collec (2023).

6. Opsview core: Es una herramienta de monitoreo de red empresarial que ofrece una licencia gratuita para usar Opsview Monitor, limitada a 25 dispositivos monitoreados. Supervisa la infraestructura de TI física y virtual de múltiples inquilinos con alta disponibilidad y una gran función de tablero, como lo indica Opsview (2010).

7. Ganglia: Es una herramienta de supervisión distribuida y escalable para sistemas informáticos de alto rendimiento como el cómputo en red y en la nube. Ganglia monitorea las aplicaciones, la plataforma y la infraestructura de red, como lo indica Birje y Bulla (2020).

8. Hyperic: Es la supervisión de aplicaciones y la gestión del rendimiento para infraestructuras de TI físicas, virtuales y en la nube. Detecta recursos automáticamente y recopila métricas de disponibilidad, utilización y rendimiento, como lo indica Communications IDG (2007).

9. Riemann: Proporciona una herramienta unificada y sencilla para monitorear aplicaciones distribuidas e infraestructura de TI. Permite a los desarrolladores definir varios tipos de eventos para monitorear, así como flujos que generan alertas cuando ocurre un tipo particular de evento, como lo indica Kyle y Ritschard (2023).

10. cAdvisor: Container Advisor, fue una de las primeras herramientas de monitoreo de código abierto creadas para aplicaciones en contenedores como grid y cómputo en la nube. No monitorea toda la aplicación que se ejecuta en la nube, sino solo aquellos componentes que están instalados en contenedores, como lo indica Prometheus (2014a).

11. Elasticsearch: Es un motor de búsqueda Restful de código abierto construido sobre Apache Lucene y lanzado bajo una licencia de Apache. Proporciona una solución de monitoreo escalable y multi-inquilino y realiza búsquedas en tiempo real para administrar la nube de manera efectiva, como lo indica Elasticsearch (2023).

12. Graphite: Es una herramienta popular de código abierto para monitorear aplicaciones, plataformas e infraestructura en la red. No recopila datos ni los almacena de manera persistente, pero las empresas pueden integrar Graphite con una variedad de otras herramientas, incluido Riemann, para realizar actividades de monitoreo, como lo indica Graphite (2005).

13. Prometheus: Es uno de los sistemas de monitoreo robustos más populares. Supervisa varias capas de la red como SaaS, PaaS e IaaS. Proporciona altas opciones de personalización y un motor de visualización nativo que también ayuda a integrar herramientas de terceros, como lo indica Prometheus (2014b).

De acuerdo al análisis realizado de las diferentes herramientas de monitoreo de red tanto comerciales y de código abierto se creó una clasificación que contiene tanto sus propiedades, así como la taxonomía de una herramienta de monitoreo.

2.7. Clasificación de herramientas de monitoreo de red

La clasificación de las herramientas de monitoreo de red. Se consideran las propiedades del sistema de monitoreo de la red y los tipos de red. Algunas herramientas de monitoreo están diseñadas e implementadas para un tipo de red específico, la clasificación contiene cinco partes: propiedades de la herramienta de monitoreo, el tipo de red, modelo de monitoreo basado en agente o sin agente, pizarra o tablero y el modelo de servicio, según lo comenta Birje y Bulla (2020). La taxonomía o clasificación de una herramienta de monitoreo de red describe conceptualmente en la Figura 2.3

Las matrices comparativas de las figuras 2.4 y 2.5 listan las herramientas de monitoreo de red de código abierto y comerciales respectivamente, dichas matrices nos muestran la comparativa entre de las propiedades de cada herramienta para así ayudarnos a elegir la mas competitiva.

2.8. Equipo activo de red

El equipo activo de red que se utilizará para llevar acabo la implementación de un laboratorio de red en ambiente controlado. A continuación se lista el equipo de red a utilizar:

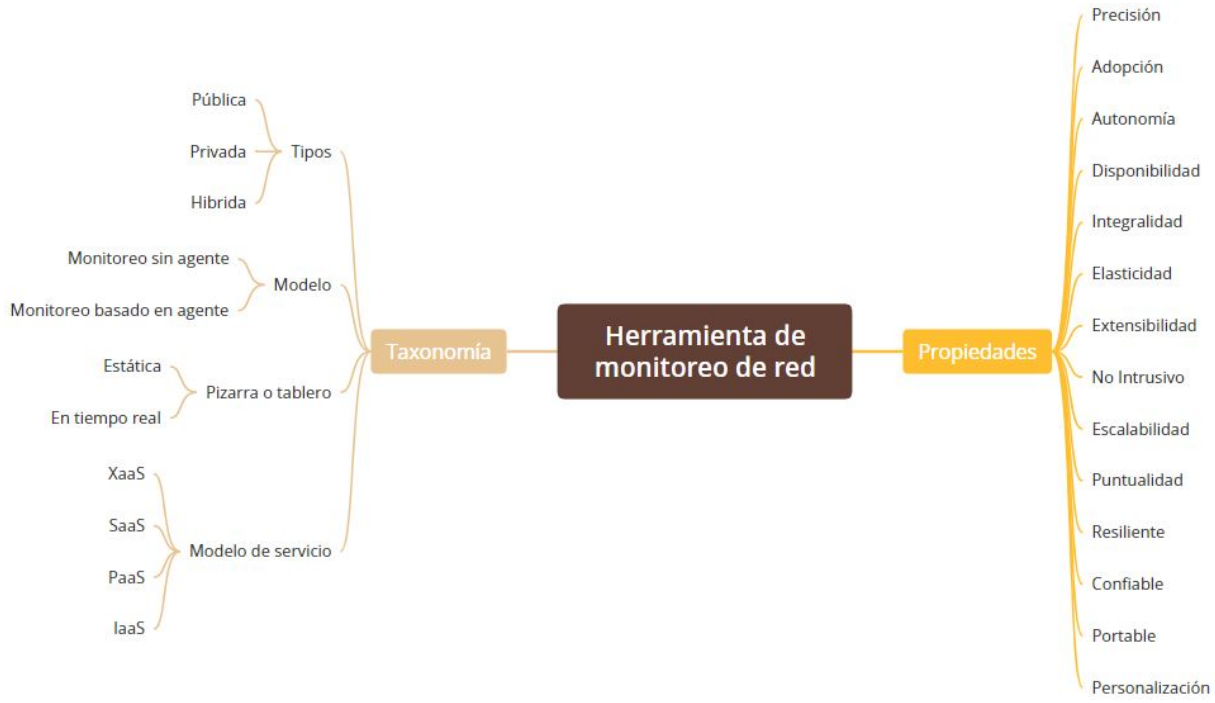

Figura 2.3 Taxonomía o clasificación de una herramienta de monitoreo de red.

Herramienta de código abierto	Nivel	Propiedades															Basado en Agente?	Tipo de red		Tablero en tiempo real	
		Precisión	Adaptabilidad	Autónoma	Disponibilidad	Integralidad	Elasticidad	Extensibilidad	No Intrusivo	Escalabilidad	Puntualidad	Resiliente	Confiable	Portable	Multiple Tenencia	Personalizable		Pública	Privada		
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 2.4 Herramientas de código abierto de monitoreo de red.

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	Híbrida	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 2.5 Herramientas comerciales de monitoreo de red.

Conmutador o switch de red: El switch de red es pieza fundamental dentro del esquema de red y cualquier problema o falla que se presenta en el switch impacta directamente en la conectividad de los usuarios a la red, por esta razón es de vital importancia su monitoreo.

Punto de Acceso: En la actualidad la movilidad dentro de una red de datos es indispensable y esta característica la otorgan los puntos de acceso por lo que su monitoreo es indispensable para así, garantizar un servicio continuo de acceso a la red de los usuarios.

Servidor de red: Gran parte de los servicios que se utilizan en una red por parte de los usuarios se ejecutan en un servidor de red. Mantener el correcto funcionamiento de los mismos, así como su monitoreo dentro de la red, ayuda a garantizar que las actividades que realizan los usuarios se mantengan sin interrupciones.

Radio con antena: Para poder brindar la conexión de red en áreas que por sus características no es factible realizar la conexión por un medio físico, se implementa un enlace de red punto a punto por medio de radio con antena, dicho en lace debe mantenerse activa para no afectar el acceso a la red, de ahí la importancia de mantener su monitoreo dentro de la red.

2.9. Protocolos de monitoreo de red

Los protocolos de monitoreo de red son fundamentales para recopilar información sobre el rendimiento, la disponibilidad, la seguridad de los dispositivos y servicios de red. A continuación se describe brevemente los protocolos de monitoreo de red más comunes, sus funciones y beneficios. En la Figura 2.6 se muestra un mapa conceptual de dichos protocolos.

Figura 2.6 Principales protocolos de monitoreo de red.

2.9.1. 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, como lo menciona Comer (2013).

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 como se muestra en la Figura 2.7

Una descripción esquemática de ICMP se muestra en la Figura 2.8

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. Aquí hay algunas de las principales características por las que se desarrolló ICMP:

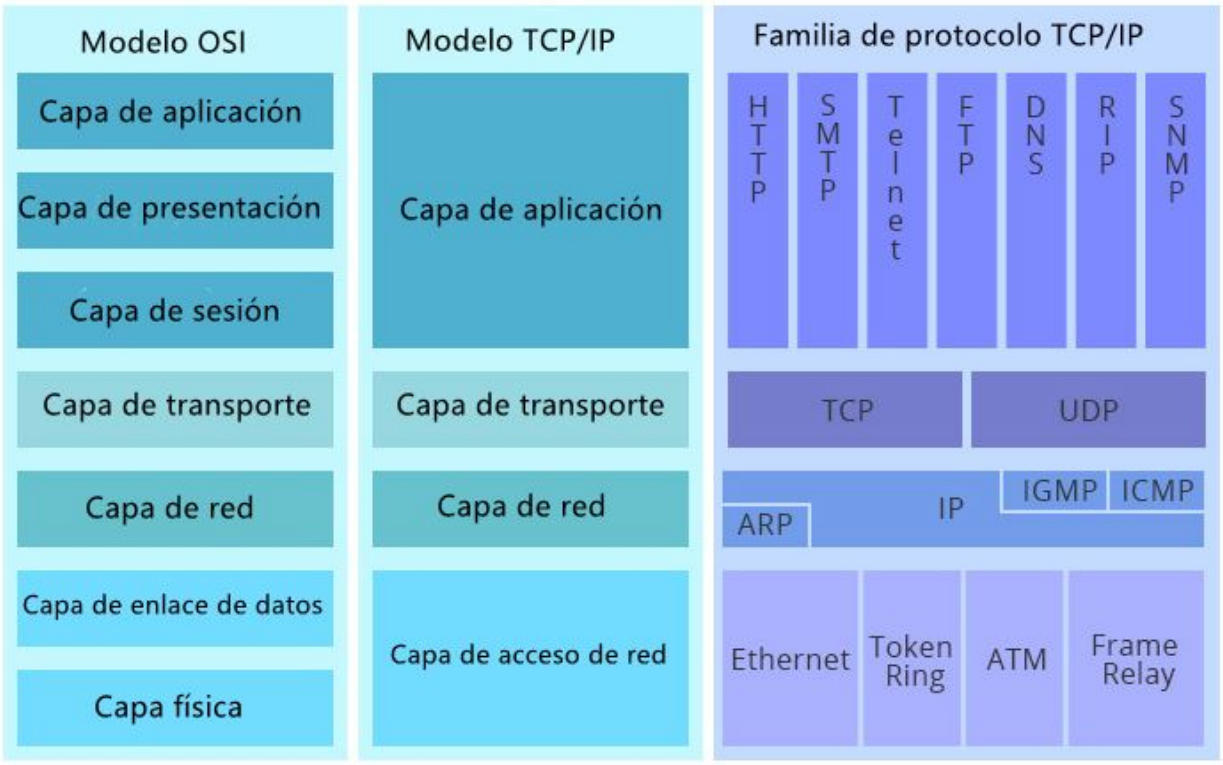

Figura 2.7 Familia de protocolos de los Modelos OSI y TCP/IP.

- **Detección de errores en la comunicación IP:** Informa sobre errores en la entrega de paquetes IP, como cuando un host de destino no está disponible o cuando se alcanza el límite de tiempo de espera (time-out) para la entrega de un paquete.

- **Gestión de rutas y redirección:** Proporciona información sobre rutas y redirección de tráfico. Por ejemplo, un router puede enviar un mensaje ICMP de redirección a un host si determina que hay una ruta más eficiente para alcanzar su destino.

- **Control de congestión:** Los ruteadores pueden enviar mensajes ICMP de congestión cuando están experimentando una carga excesiva para que los dispositivos ajusten su tasa de envío de paquetes.

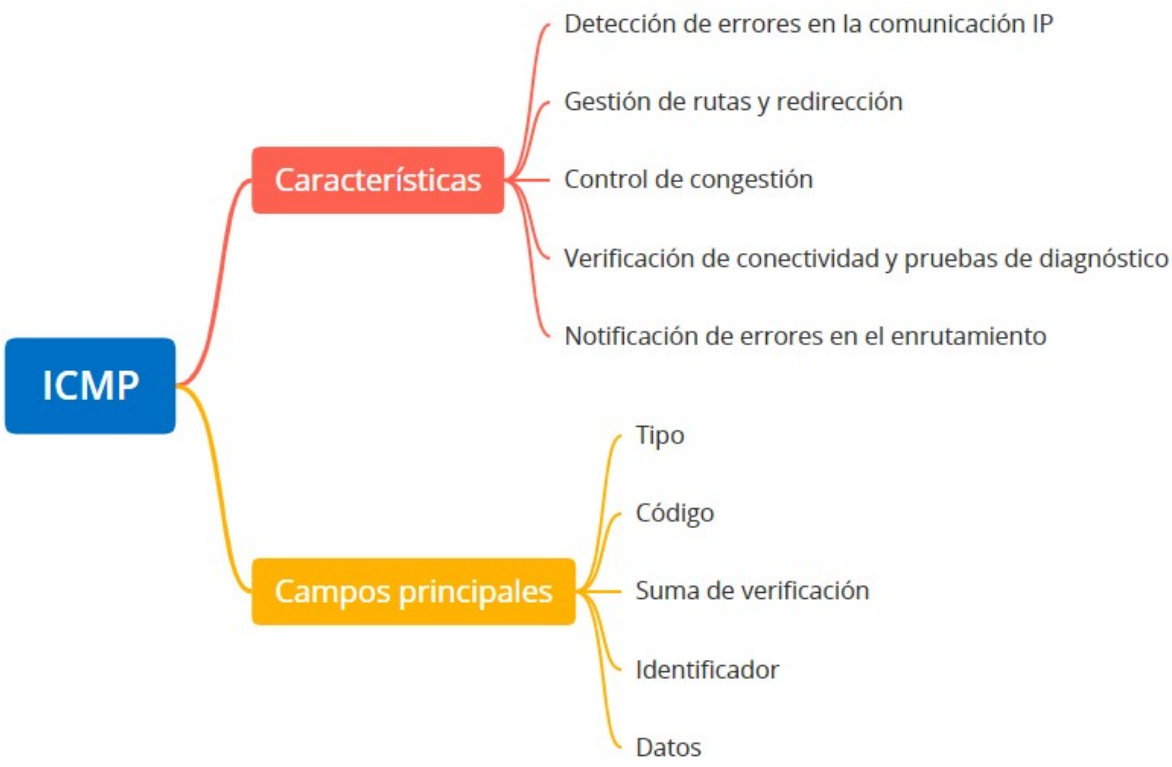

Figura 2.8 ICMP.

- **Verificación de conectividad y pruebas de diagnóstico:** Se utiliza ampliamente para realizar pruebas de diagnóstico en la red, como el comando "ping". El comando "ping", envía paquetes ICMP de solicitud y recibe respuestas para verificar si un dispositivo remoto está disponible y mide la latencia de la comunicación.
- **Notificación de errores en el enrutamiento:** Notifica a los dispositivos sobre problemas en la topología de red, como cuando una ruta no está disponible o cuando un dispositivo de destino es inaccesible.

ICMP se diseñó para mejorar la confiabilidad y la eficiencia de las comunicaciones en las redes basadas en IP, al proporcionar un conjunto de mensajes, así como funciones para el control de errores, para la gestión de rutas y la realización de pruebas de diagnóstico. Es una parte esencial de la infraestructura de Internet y juega un papel clave en la operación y el mantenimiento de las redes

IP en todo el mundo. Un paquete ICMP consta de varios campos que permiten transmitir información esencial sobre la comunicación de red y los mensajes de control. Los campos principales se muestran en la Figura 2.9, los cuales incluyen:

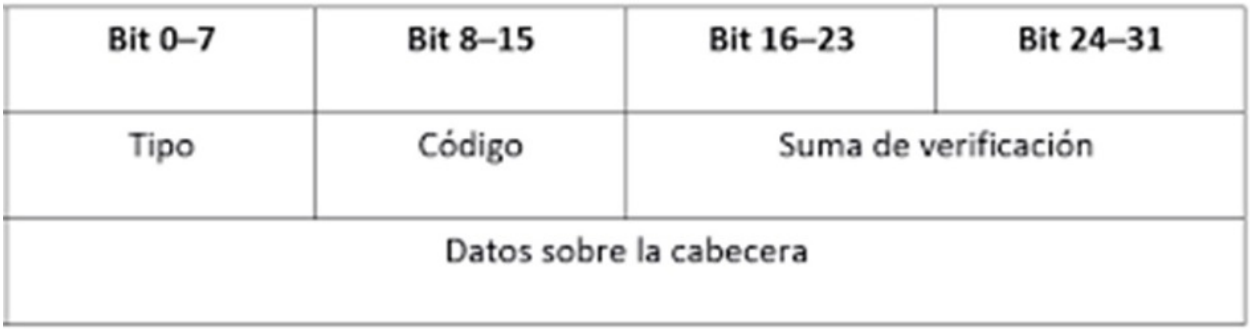

Figura 2.9 Campos principales de un paquete ICMP.

1. **Tipo:** Este campo especifica el tipo de mensaje ICMP y determina la función del paquete. Algunos ejemplos de tipos de mensajes ICMP comunes incluyen Echo Request (solicitud de eco), Echo Reply (respuesta de eco), Destination Unreachable (destino inaccesible), Time Exceeded (tiempo excedido) y Redirect (redirección), entre otros.

2. **Código:** El campo de código se utiliza en conjunto con el campo de tipo y proporciona información adicional sobre el tipo de mensaje ICMP. El valor del código puede variar según el tipo de mensaje.

3. **Suma de verificación:** Este campo se utiliza para verificar la integridad del paquete ICMP. La suma de verificación se calcula sobre el contenido del paquete y se utiliza para detectar errores de transmisión.

4. **Identificador y Número de Secuencia:** Estos campos se utilizan en los mensajes ICMP de solicitud y respuesta de eco (como los utilizados por el comando "ping"). El identificador y el número de secuencia permiten que el emisor y el receptor asocien solicitudes y respuestas correspondientes.

5. **Datos:** El campo de datos contiene información adicional específica del tipo de mensaje ICMP. La longitud y el contenido de este campo pueden variar según el tipo de mensaje ICMP.

Las herramientas de monitoreo de red, puede utilizar ICMP de varias maneras para llevar a cabo la supervisión de dispositivos y servicios. Aquí hay algunas formas en las que se puede utilizar:

- **Ping ICMP:** Las herramientas de monitoreo pueden realizar pruebas de ping ICMP regulares a dispositivos y servidores para verificar su disponibilidad y latencia. Esto se hace enviando paquetes ICMP Echo Request (solicitud de eco) y esperando respuestas ICMP Echo Reply (respuesta de eco). Si un dispositivo no responde a las solicitud de ping o lo hace con demasiada intermitencia, se pueden generar alertas para informar sobre problemas de disponibilidad.

- **Monitoreo de dispositivos:** Se puede configurar la herramienta de monitoreo para supervisar dispositivos específicos mediante pruebas de ping ICMP. Si un dispositivo no responde al ping, la herramienta de monitoreo puede considerarlo como no disponible y generar alertas en consecuencia.

- **Detección de problemas de red:** La supervisión de ICMP también puede utilizarse para detectar problemas en la red, como altas tasas de latencia. La herramienta de monitoreo puede generar alertas si detecta condiciones anómalas en las respuestas a las pruebas de ping.

2.9.2. SNMP

Protocolo Simple de Administración de Red (SNMP, por sus siglas e inglés):

Función: Es un protocolo utilizado para recopilar información de dispositivos de red y administrarlos. Permite la supervisión de dispositivos como ruteadores, switches, servidores, impresoras y otros componentes de red.

Beneficios: Proporciona una forma estandarizada de monitorear y administrar dispositivos de red, lo que simplifica la tarea de gestionar redes grandes y heterogéneas.

SNMP opera en el nivel de aplicación del modelo de referencia OSI y se basa en el intercambio de mensajes entre un administrador de red (que realiza solicitudes) y agentes SNMP (que residen en los dispositivos de red y responden a las solicitudes). Estos mensajes SNMP contienen información sobre el estado y el rendimiento de los dispositivos de red.

2.9.3. Netflow

Función: Es un protocolo que proporciona información sobre el tráfico de red, incluyendo datos sobre el flujo de paquetes, el origen y el destino de las comunicaciones, y la cantidad de datos transferidos.

Beneficios: Es utilizado para el monitoreo del tráfico de red, la detección de intrusiones y la planificación de capacidad. Permite a los administradores de red comprender cómo se utiliza la red y tomar decisiones informadas.

2.9.4. Protocolo HTTP/HTTPS

Estos protocolos se utilizan para establecer una conexión entre el cliente y un servidor web. Se pueden utilizar para supervisar el rendimiento, la disponibilidad y los tiempos de respuesta de sitios web y servicios en línea.

Estos son solo algunos de los protocolos y herramientas comunes utilizados en el monitoreo de red. Cada uno tiene sus propias funciones, beneficios, y a menudo se utilizan en conjunto para proporcionar una visión completa del estado de la red, para garantizar su funcionamiento eficiente y seguro.

Cada uno de los protocolos mencionados tienen sus propias ventajas y desventajas, y se utilizan para propósitos diferentes en el ámbito de las redes de computadoras. A continuación, se mencionan algunas ventajas y desventajas de cada uno:

ICMP:

Ventajas:

- Es fundamental para el funcionamiento de la red, ya que se utiliza para enviar mensajes de error y control.

- Permite verificar la conectividad y el estado de la red a través de herramientas como el comando "ping".

Desventajas:

- Puede ser utilizado para ataques de denegación de servicio (DoS, por sus siglas en inglés) debido a la posibilidad de inundación de mensajes ICMP.

SNMP:
Ventajas:

- Proporciona una interfaz estándar para monitorear y gestionar dispositivos de red.
- Facilita la supervisión proactiva de la red y la identificación de problemas antes de que afecten el rendimiento.

Desventajas:

- Puede presentar riesgos de seguridad si no se configura correctamente, ya que la información de gestión puede ser sensible.

NetFlow:
Ventajas:

- Permite la recopilación de información detallada sobre el tráfico de red, incluidos datos sobre origen y destino, tipos de servicios.
- Facilita la identificación de patrones de tráfico y la detección de amenazas de seguridad.

Desventajas:

- Puede requerir un mayor consumo de recursos para realizar un seguimiento detallado del tráfico, lo que puede afectar el rendimiento en entornos muy activos.

HTTP/HTTPS:
Ventajas:

- Es el protocolo utilizado para la transferencia de datos en la red mundial WWW (por sus siglas en inglés (World Wide Web)).
- Facilita la comunicación entre clientes y servidores web.

Desventajas:

- No está diseñado específicamente para la gestión de red o la transferencia eficiente de grandes cantidades de datos.

En resumen, la elección de un protocolo depende del propósito específico y de los requisitos de la aplicación. Por ejemplo, SNMP se utiliza para la gestión de red, NetFlow es útil para el análisis detallado del tráfico, ICMP es esencial para la resolución de problemas de conectividad, y HTTP es fundamental para la comunicación en la web.

Algunas razones principales por las que ICMP es utilizado para el monitoreo de redes son:

- Disponibilidad: Está presente en la mayoría de los dispositivos de red y sistemas operativos. Su uso está estandarizado en IP, lo que significa que es ampliamente compatible y está disponible en una variedad de dispositivos y sistemas.
- Funciones de diagnóstico: Incluye mensajes de diagnóstico, como los mensajes de eco (ping), que son útiles para verificar la conectividad entre dispositivos y medir la latencia de la red. El comando ping es una herramienta comúnmente utilizada para verificar la accesibilidad de un dispositivo en una red.
- Monitoreo rápido: Es ligero y no impone una carga significativa en la red. Los mensajes ICMP son relativamente simples y rápidos de procesar, lo que los hace adecuados para tareas de monitoreo y diagnóstico rápidas.
- Identificación de problemas de red: Es posible identificar problemas en la red, como pérdida de paquetes, latencia excesiva o problemas de enrutamiento. Esto facilita la detección y resolución de problemas de conectividad.

- Eficiencia en ancho de banda: Generalmente utiliza menos ancho de banda en comparación con otros protocolos de monitoreo, lo que lo hace adecuado para redes donde la eficiencia del ancho de banda es crucial.

Con base a lo anterior y tomando en cuenta el alcance definido se optó por utilizar ICMP en la herramienta de monitoreo ya que permite verificar la conectividad del equipo activo que integra una red.

Derivado de evaluar las herramientas de monitoreo de código abierto mostradas en la matriz comparativa de la Figura 2.4, se define utilizar Nagios, al analizar las opciones de Nagios existentes, se encuentra la aplicación Servidor de Monitoreo Empresarial Nagios (NEMS, por sus siglas en inglés) la cual se puede implementar en computadoras de bajo costo como es el caso de las Raspberry.

2.10. NEMS para Raspberry Pi

Como se menciona en Robbie y Marshall (2020), NEMS es el servidor de supervisión empresarial de Nagios para computadoras integradas en una placa única, sin necesidad de archivos de configuración de Nagios. NEMS Linux es una imagen de Nagios Core moderna, preconfigurada, personalizada y diseñada para ejecutarse en micro-computadora de bajo costo, como Raspberry Pi y PINE64. En esencia, NEMS es una implementación ligera de Debian Buster optimizada para el rendimiento y la confiabilidad en su uso.

NEMS Linux representa un enfoque actualizado para el monitoreo de activos de red, dejando atrás la necesidad de utilizar secuencias de comandos antiguas de Nagios. Aunque los scripts siguen siendo parte del sistema, los administradores ya no tienen que interactuar directamente con ellos. Todo el proceso de control, configuración y supervisión se realiza de manera intuitiva a través de un navegador web, con la comodidad de recibir notificaciones por correo electrónico, Telegram o Pushover sobre todas las actividades operativas desde el primer momento. Además, NEMS Linux ofrece una API JSON para una integración más fluida, una pantalla de TV diseñada para la visualización de los dispositivos monitoreados y muchas otras características.

NEMS Linux ha evolucionado hasta integrar Nagios como su motor de monitoreo, además de una interfaz de configuración web. Esto lo convierte en una herramienta de monitoreo altamente eficaz y disponible en la actualidad. El desarrollo de NEMS ha continuado avanzando, permitiendo su implementación en plataformas como Raspberry Pi.

En la Figura 2.10 se muestra un mapa conceptual de la estructura de NEMS

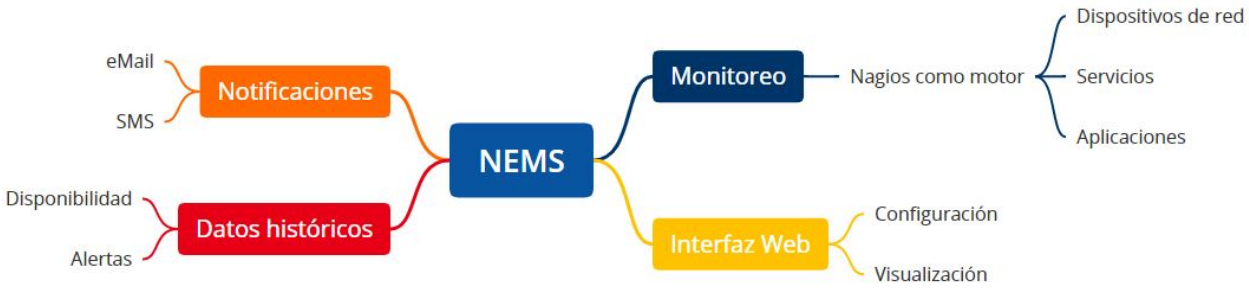

Figura 2.10 Mapa conceptual de la estructura de NEMS Linux: monitoreo, interfaz web, notificaciones.

2.10.1. Propiedades de NEMS

De acuerdo a Robbie y Marshall (2020), ya se ha mencionado la interfaz de configuración web y las mejoras que NEMS Linux aporta a la experiencia de Nagios. Esos son los puntos clave que hacen que NEMS se eficaz. A continuación se describen una pequeña selección de características adicionales.

Migrador NEMS

El menú Migrator permite hacer una copia de seguridad de toda su configuración de NEMS (equipo activo de red, servicios, comprobaciones, configuraciones del sistema, etc.) a través de un conjunto de programas que trabajan juntos para permitir a los clientes acceder a espacios de archivos del servidor mediante los protocolos SMB (por sus siglas en inglés, Server Message Block) y CIFS (por sus siglas en inglés, Common Internet Filesystem). Las copias de seguridad se pueden cifrar y solo el administrador conoce la clave de descifrado. Si el dispositivo falla, puede restaurar la imagen en una nueva tarjeta de memoria SD (por sus siglas en inglés, Digital Segura), restaurar

la copia de seguridad de Migrator y estar en funcionamiento en menos de cinco minutos con todas sus configuraciones intactas. Migrator también permite la transición de una plataforma a otra. Por ejemplo, si se configuró un servidor NEMS Linux en una Raspberry Pi 3, se puede mover fácilmente a una Máquina Virtual o incluso a otra computadora de bajo costo.

Otra ventaja que Migrator trae a la mesa es una ruta de actualización más simple: a medida que se presentan nuevas versiones importantes de NEMS Linux, puede restaurar la nueva imagen de NEMS, importar su copia de seguridad y estar en la última versión de NEMS en solo minutos con su configuración intacta.

Notificaciones de registro.

Servicio NEMS Check-In, este servicio opcional (deshabilitado de forma predeterminada) se conectará con el servidor de servicios en la nube de NEMS cada cierto tiempo, el cual es definido por el administrador de la red. Si el servidor NEMS no se registra, recibirá un correo electrónico advirtiéndole que su servidor NEMS dejó de responder.

Configuración NEMS mediante NConf

NEMS Configurator (NConf) es lo que hace posible la configuración de Nagios basada en navegador. Esta versión personalizada de la antigua herramienta de configuración de NConf aporta una interfaz sofisticada a la arquitectura moderna de NEMS. Toda su configuración de Nagios se realiza a través de esta interfaz: desde agregar equipo activo de red hasta configurar sus controles de servicio, modificar comandos de configuración y monitoreo. Todo se hace a través de un sistema intuitivo basado en un navegador, el cual permitirá dejar de lado las configuraciones a través de archivos .cfg de Nagios.

Herramienta de configuración del sistema

Hablando de eliminar los archivos de configuración de Nagios, varias opciones de configuración de Nagios se han movido a una herramienta llamada Herramienta de configuración del sistema NEMS, también conocida como SST. Elementos como la configuración del servidor SMTP, las credenciales de usuario del dominio y otros valores predeterminados forman parte de esta interfaz.

2.10.2. Hardware Raspberry Pi 4 Modelo B

Una Raspberry Pi es una pequeña computadora que tiene un tamaño similar a una tarjeta de crédito y que se utiliza para construir proyectos de electrónica, lanzada en 2012 por la Fundación Raspberry Pi con el propósito de hacer más accesible la informática, presenta su propio sistema operativo, Raspbian, basado en Debian. Además, es compatible con otros sistemas operativos. El modelo más reciente, Raspberry Pi 4 Model B, ofrece mejoras significativas en velocidad de procesamiento, rendimiento multimedia, memoria y conectividad respecto a modelos anteriores, manteniendo la compatibilidad y eficiencia energética. Para los usuarios finales, este modelo brinda un rendimiento de escritorio comparable a sistemas de PC x86 de nivel básico, de acuerdo a Raspberry (2023).

Las características clave de este producto incluyen un procesador de cuatro núcleos de 64 bits de alto rendimiento, compatibilidad con dos pantallas a resoluciones de hasta 4K a través de un par de puertos micro-HDMI, decodificación de vídeo por hardware de hasta 4K, hasta 8 GB de RAM, doble LAN inalámbrica de banda 2.4/5.0 GHz, Bluetooth 5.0, Giga bit Ethernet, USB 3.0 y capacidad de alimentación a través de Ethernet (por sus siglas en inglés, PoE).

De forma esquemática una Raspberry se define de acuerdo a la figura 2.11

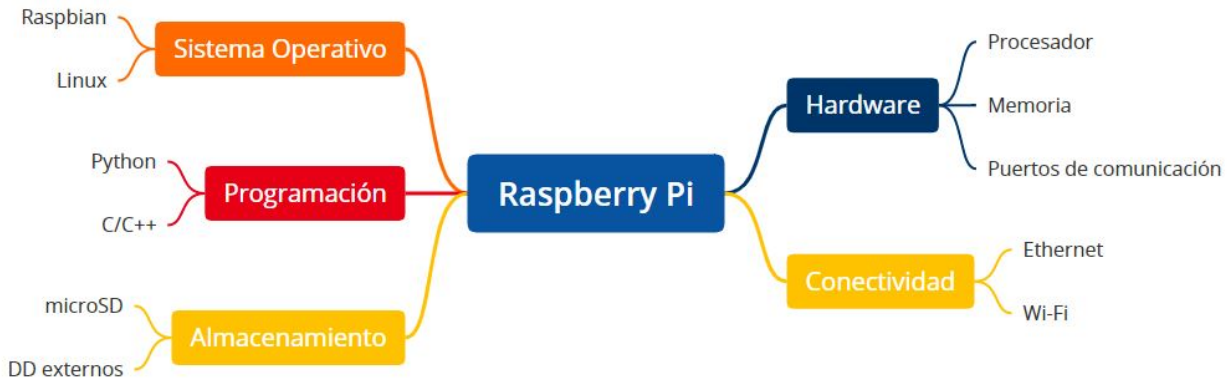

Figura 2.11 Mapa conceptual Raspberry Pi: hardware, sistema operativo, almacenamiento.

.

Sistema operativo Raspberry Pi

Raspberry Pi OS es un sistema operativo gratuito basado en Debian, optimizado para el hardware Raspberry Pi y es el sistema operativo recomendado para uso normal en una Raspberry Pi. El sistema operativo viene con más de 35,000 paquetes: software pre-compilado incluido en un formato agradable para una fácil instalación en su Raspberry Pi.

El sistema operativo Raspberry Pi se encuentra en desarrollo activo, con énfasis en mejorar la estabilidad y el rendimiento de tantos paquetes Debian como sea posible en Raspberry Pi.

Capítulo 3

Desarrollo

3.1. Introducción

Basándose en el análisis de las herramientas de monitoreo, se realizó la selección de la herramienta de monitoreo de equipo activo de red que mejor se adapte a las necesidades de la red, tomando en cuenta las distintas propiedades de cada una, así también se describe el proceso de instalación, configuración y puesta a punto de la herramienta seleccionada.

3.2. Arquitectura del equipo activo de red a monitorear

Se presenta la arquitectura de red que se diseño para tener un laboratorio de ambiente controlado, dicha arquitectura se muestra en la Figura 3.1

En la Tabla 3.1, se presenta un resumen de las características principales de los equipos de red utilizados en la implementación del laboratorio de red en ambiente controlado.

La información completa de cada uno de los equipos de red se encuentra en su hoja de datos que se incluyen en el Apéndice A.

Tabla 3.1 Características principales de los equipos de red utilizados en el laboratorio controlado.

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

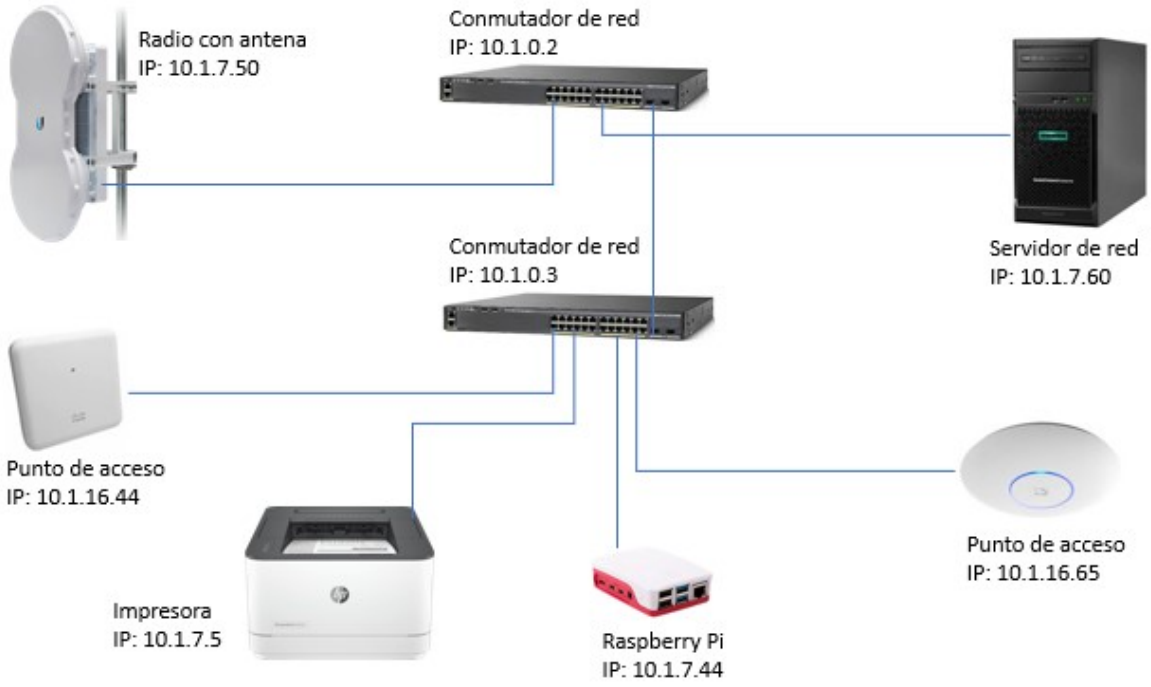

Figura 3.1 Arquitectura de red del equipo activo de la cama de pruebas.

3.3. Selección de la herramienta de monitoreo

Derivado de analizar las propiedades que integran las múltiples herramientas de monitoreo que existen en el mercado, tanto comerciales y de código abierto, se determinó que la herramienta que cumple con la mayor cantidad de puntos evaluados a favor es Nagios.

Algunos de los puntos analizados y por los cuales se seleccionó Nagios son:

Monitoreo: Permite monitorear varios aspectos de la red, para el caso de estudio los dispositivos que integran la red.

Escalabilidad: Asegura que la herramienta pueda crecer con las necesidades a medida que la red evoluciona.

Protocolos de red compatibles: Asegura que la herramienta sea compatible con varios protocolos de red.

Interfaz intuitiva: Cuenta con una interfaz web para la configuración y la interpretación de los datos.

Alertas y notificaciones: La capacidad de recibir alertas en tiempo real es crucial para abordar problemas antes de que afecten a los usuarios.

Historial y registro: Un registro histórico permite analizar tendencias y comportamientos a lo largo del tiempo.

Costo: Al ser una herramienta de código abierto, su implementación tiene un bajo costo ya que solo se invierte en el hardware.

Al enfocarse en las diferentes opciones que brinda Nagios para el monitoreo de red, se encontró que NEMS Linux, es una herramienta de monitoreo de equipo activo, servicios, protocolos y demás servicios de red y la cual será utilizada para implementar un sistema de monitoreo de red y probado en un ambiente controlado, según los alcances definidos en este proyecto.

3.4. NEMS para Raspberry Pi

NEMS Linux, es una distribución de Linux diseñada específicamente para la monitorización de sistemas y redes a través de Nagios, que es una popular plataforma de monitoreo de código abierto. NEMS Linux está basado en la distribución Raspbian.

NEMS Linux proporciona una interfaz web a través de la cual se configura y gestionan los parámetros de monitoreo, ver informes y recibir notificaciones.

A continuación se describe paso a paso lo necesario para realizar la instalación, configuración y puesta a punto de NEMS

3.5. Instalación de NEMS en una Raspberry Pi

Para llevar a cabo una instalación correcta, es esencial seguir las instrucciones proporcionadas por Robbie y Marshall (2020), las cuales detallan los requisitos que se describen en el Apéndice B.

3.6. Configuración y puesta a punto de NEMS

3.6.1. Inicialización

En términos generales, la inicialización es el único momento en el que necesitará interactuar directamente con la terminal de Linux en un servidor NEMS. Durante este proceso, se generan certificados autofirmados para garantizar que cada usuario de NEMS Linux disponga de uno único, se configura la zona horaria, se crea la cuenta de administrador de Nagios y la cuenta de Linux, entre otras tareas. Para inicializar el servidor NEMS Linux, simplemente conéctese al servidor a través de SSH en el puerto 22 predeterminado utilizando las siguientes credenciales:

Username: nemsadmin
Password: nemsadmin

Una vez conectado, escriba: sudo nems-init

Se pedirá que ingrese la contraseña nuevamente. Siga las indicaciones.
agregar Pantalla de inicialización de NEMS.

3.6.2. Conexión al servidor NEMS

Con el servidor NEMS Linux en funcionamiento, puede acceder a todo su conjunto de funciones a través de su navegador web. Simplemente acceda a https://nems.local/ o puede usar alternativamente la dirección IP del servidor NEMS desde cualquier navegador WEB.

3.6.3. Configuración de SMTP para notificaciones por correo electrónico de NEMS

Acceda a la Herramienta de configuración del sistema NEMS (SST) desde el menú Configuración de su panel NEMS. Esta herramienta basada en navegador WEB, elimina la necesidad de usar

el archivo *resource.cfg* tradicional de Nagios para configurar su correo electrónico y otras configuraciones. En el panel de configuración seleccione la opción de Notificaciones y capture los datos de su servidor SMTP, así como la cuenta de correo a la que se harán las notificaciones.

3.6.4. Monitoreo de una computadora Linux en la red

Un Host en NEMS Linux es cualquier dispositivo de red que desee monitorear. Esto puede ser una computadora o un switch de red; puede ser un enrutador o una impresora. Las opciones son realmente infinitas, y si bien NEMS Linux se puede descargar y usar de forma gratuita, un solo servidor NEMS puede manejar fácilmente cientos de hosts.

Agregar un anfitrión

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 3.2

3.6.5. Generar configuración NEMS: Realice cambios en vivo

En el Configurador de NEMS (NConf), se configuran todos sus comandos de verificación y configuraciones de notificación. Pero hasta que genere la configuración, los cambios que se realicen no estarán realmente habilitados en su servidor NEMS en ejecución.

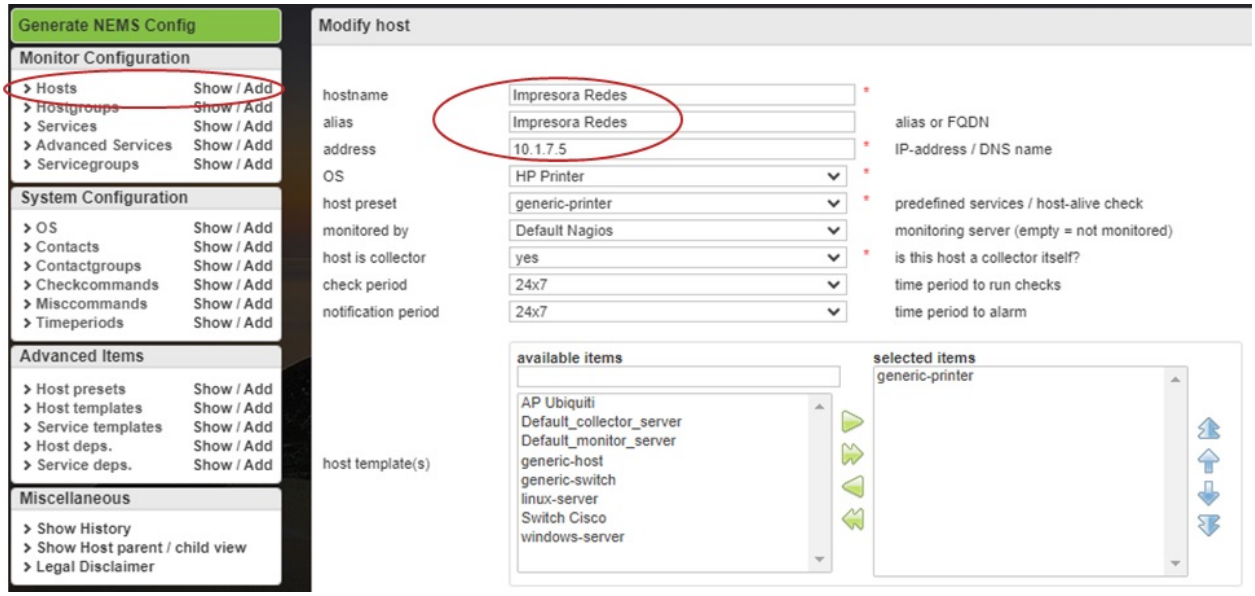

Figura 3.2 Pantalla de alta de host a monitorear: nombre de dispositivo y dirección IP.

Para realizar los cambios en vivo, presione el enlace Generar configuración de NEMS en la barra de navegación de la izquierda. Se deben visualizar 0 errores. Si se visualizan errores, revisar dónde está el error, realizar los cambios necesarios y volver a intentarlo.

Si todo sale bien, presione Implementar configuración en el servidor NEMS y los cambios se activarán instantáneamente con la implementación de Nagios en el servidor NEMS.

3.6.6. Comprensión de las definiciones de notificación

Antes de configurar sus primeros comandos de verificación, deberá comprender qué significan las opciones de notificación de un solo caracter. Si no se establecen correctamente los ajustes de notificación, es posible que no se generen notificaciones o que se envíe un exceso de notificaciones. La configuración de las notificaciones se realiza en la opción de contactos y los campos de notificación como se indica en la Figura 3.3

Configuración de notificaciones del anfitrión

Se pueden utilizar los siguientes parámetros *d,u,r,f,s,n*, de los cuales, estas son las definiciones:

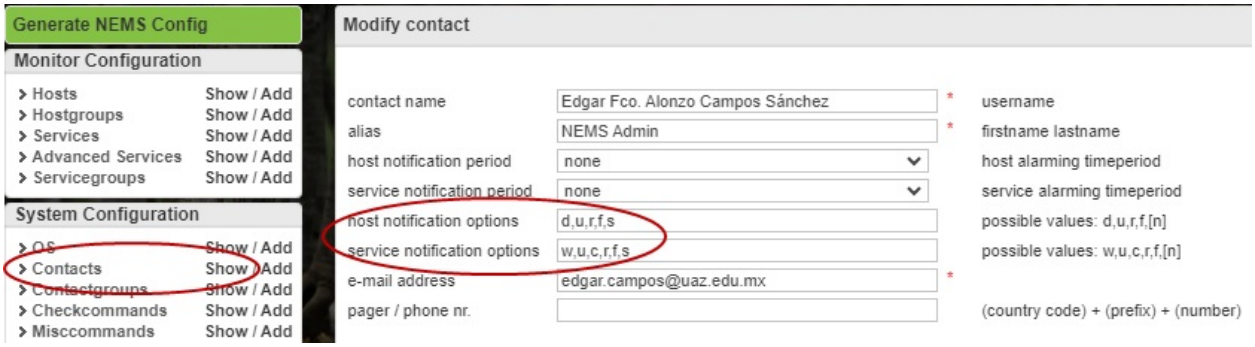

Figura 3.3 Pantalla de alta del tipo de notificación configurada por equipo.

d Notificar si el host está caído.

u Notificar si el host es inalcanzable (por ejemplo, Internet caído).

r Notificar sobre la recuperación.

f Notificar si el host está aleteando (arriba/abajo/arriba/abajo).

s Notificar si un tiempo de inactividad programado del servicio comienza o finaliza.

n Nunca notificar.

Configuración de notificación de servicio

Se pueden utilizar los siguientes parámetros *w,u,c,r,f,n*, de los cuales, estas son las definiciones:

w Notificar si está en estado de advertencia.

u Notificar si se encuentra en un estado desconocido.

c Notificar si está en estado crítico.

r Notificar si se recupera de un mal estado anterior.

f Notificar si el servicio está oscilando (arriba/abajo/arriba/abajo).

n Nunca notificar.

Capítulo 4

Resultados

4.1. Monitoreo de equipo activo de red en ambiente controlado

NEMS es una imagen de Nagios 4 que permite monitorear redes y que está específicamente diseñada para funcionar sobre una computadora de bajo costo RaspberryPi. El objetivo de Nagios es detectar cualquier equipo, servicio o sistema que no esté funcionando correctamente para que la solución del problema se haga lo más rápido posible y que los usuarios de la red sean los menos partícipes posibles del problema detectado.

Como lo indica Cabezón Rodríguez (2017), entre sus múltiples funciones y propiedades detectadas, como parte de la evaluación, tenemos las siguientes:

- Supervisión de servicios de red (SMTP, POP3, HTTP, PING, etc.).
- Supervisión de los recursos del dispositivo (carga del procesador, uso del disco, etc.).
- Plugin de diseño simple que permite a los usuarios desarrollar fácilmente sus propios controles de servicio.
- Controles de servicios y hosts paralelos. Se pueden supervisar diferentes servicios, tanto del mismo dispositivo como de dispositivos diferentes, al mismo tiempo.
- Capacidad para definir la jerarquía del dispositivo de red utilizando dispositivos "padres", permitiendo la detección entre dispositivos que están inactivos y aquellos que son inaccesibles.

- Notificaciones de contacto cuando se producen problemas de servicio o de dispositivo y se resuelven (mediante correo electrónico u otro método definido por el usuario).

- Interfaz web opcional para ver el estado actual de la red, la notificación y el historial de problemas, el archivo de registro, etc.

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 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 Cabezón Rodríguez (2017), 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.

Para realizar pruebas de evaluación de la herramienta y poder obtener resultados derivados de la implementación de NEMS, se construyó una cama de pruebas con equipo de red en ambiente controlado el cual consta de los equipos que se ilustran en las siguientes Figuras 4.1, 4.2, 4.3 y los cuales se definieron en el Capítulo 3 de este documento.

Figura 4.1 Interconexión de equipos en la cama de pruebas de red en ambiente controlado: conmutador de red, punto de acceso y Raspberry.

Figura 4.2 Cama de pruebas de red en ambiente controlado.

4.2. 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.

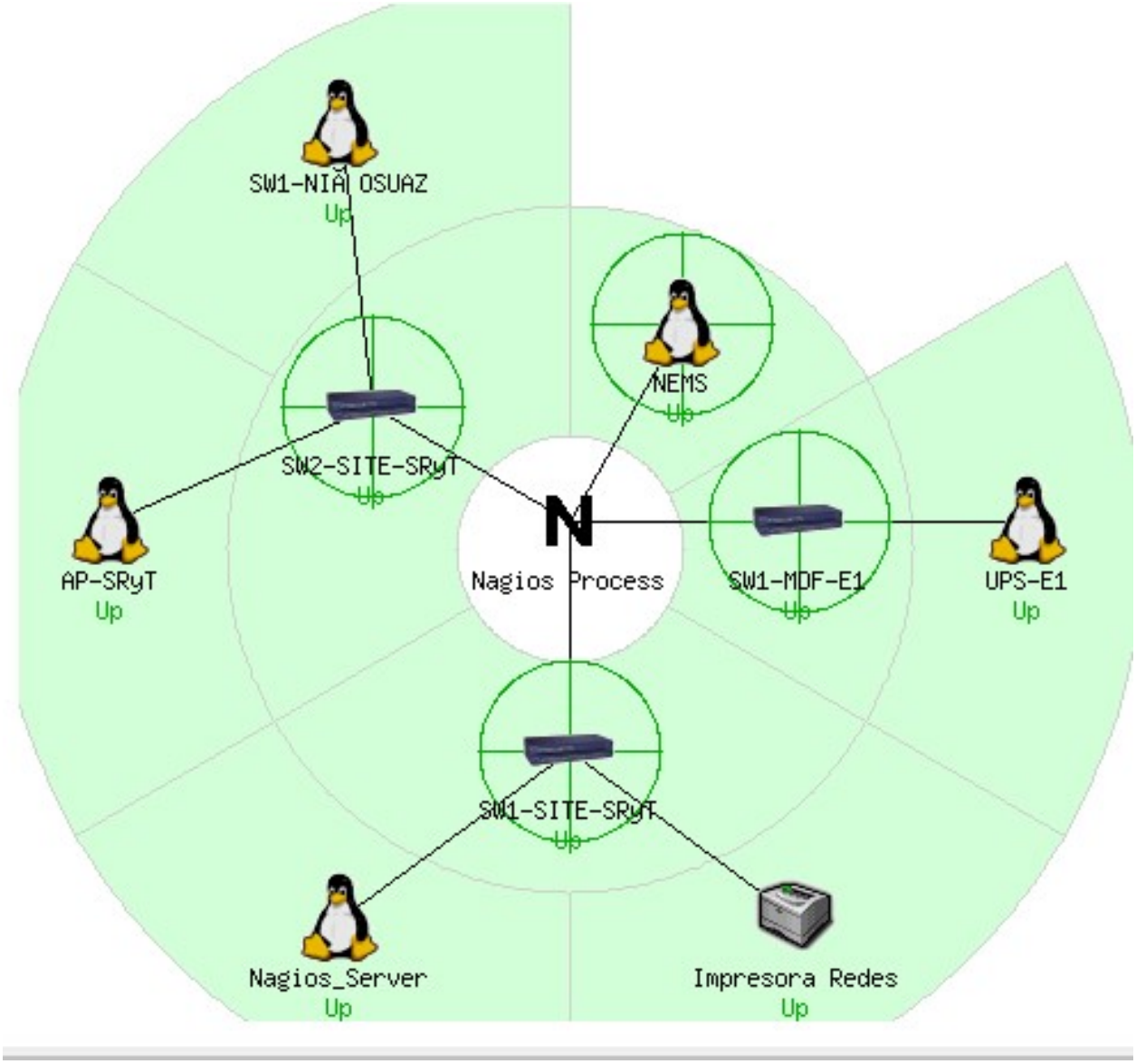

Figura 4.3 Mapa de equipos de red utilizados en la cama de pruebas en ambiente controlado.

4.2.1. Interface 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 4.4

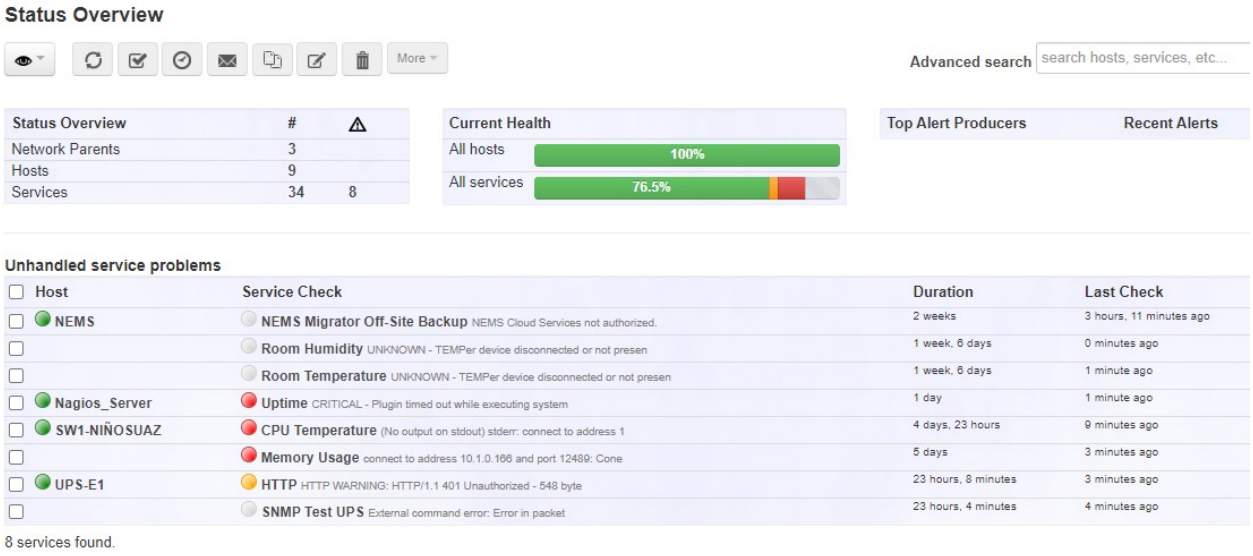

Figura 4.4 Vista Overview dentro de la interface Adagios.

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 4.5.

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 4.6.

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 4.7.

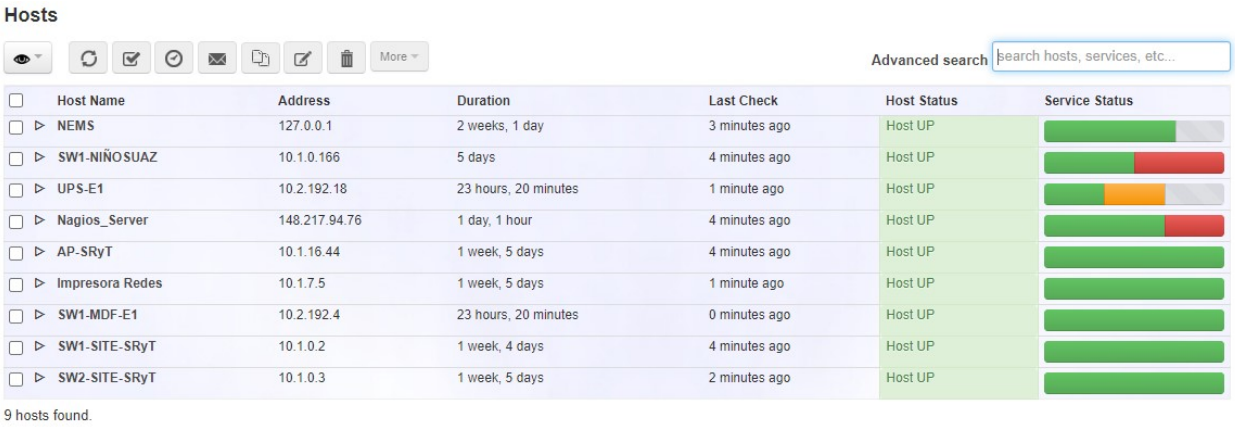

Figura 4.5 Vista Host dentro de la interface Adagios.

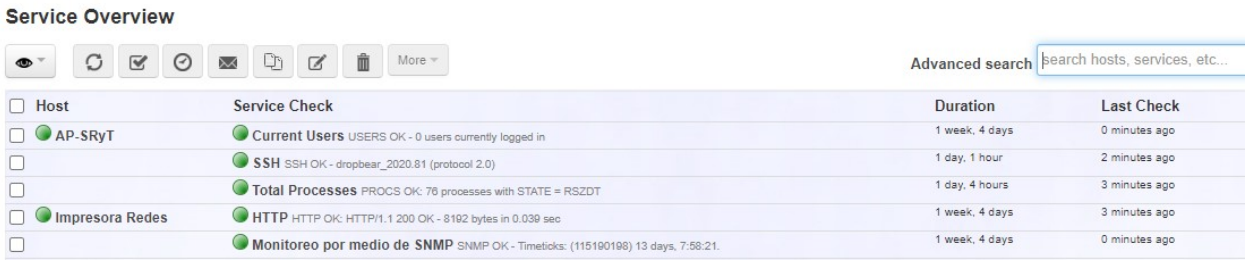

Figura 4.6 Vista Service dentro de la interface Adagios.

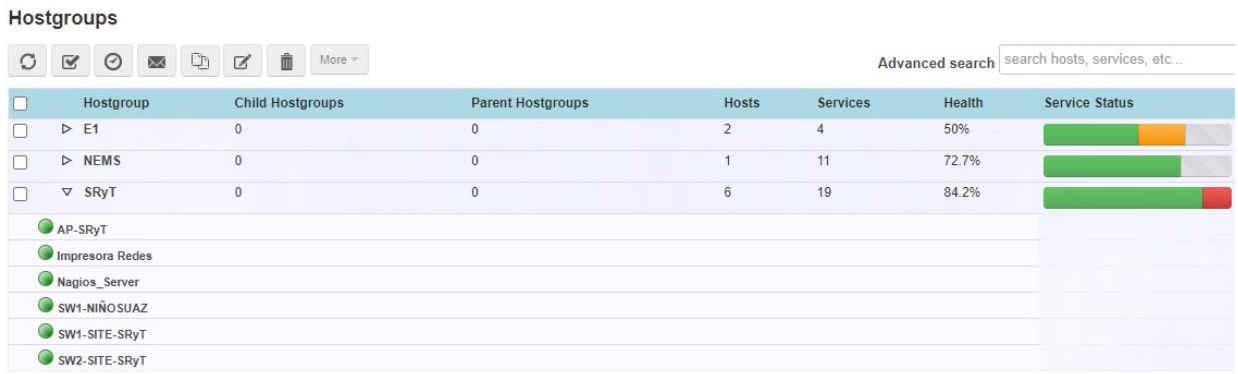

Figura 4.7 Vista Hostgroups dentro de la interface Adagios.

4.2.2. 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 4.8.

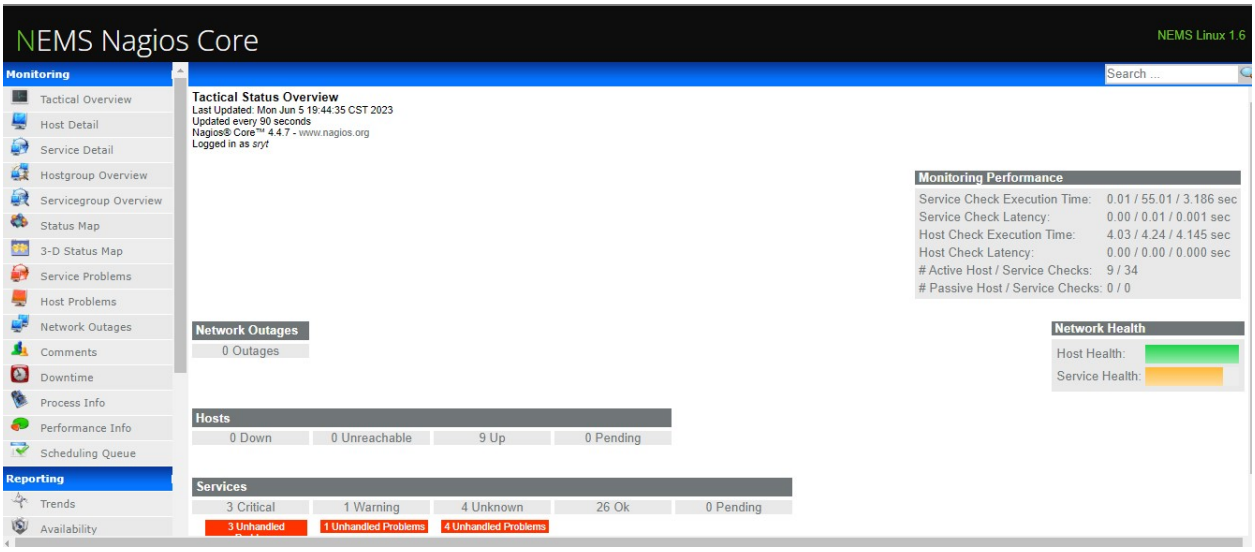

Figura 4.8 Vista Tactical Overview dentro de la interface Nagios.

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 4.9.

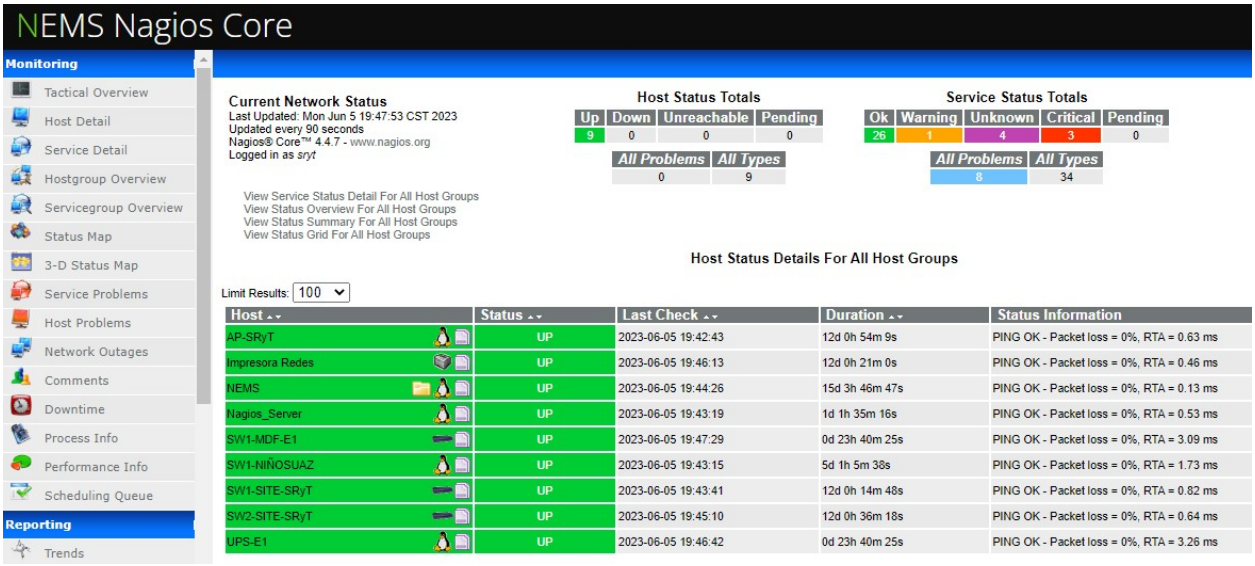

Figura 4.9 Vista Host Detail dentro de la interface Nagios.

Vista Hostgroup Overview: En la pestaña Hostgroups, aparecen los dispositivos divididos en los diferentes grupos que se hayan configurado desde Nagios nConf, la vista se muestra en la Figura 4.10.

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 4.11.

4.2.3. 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:

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 4.12.

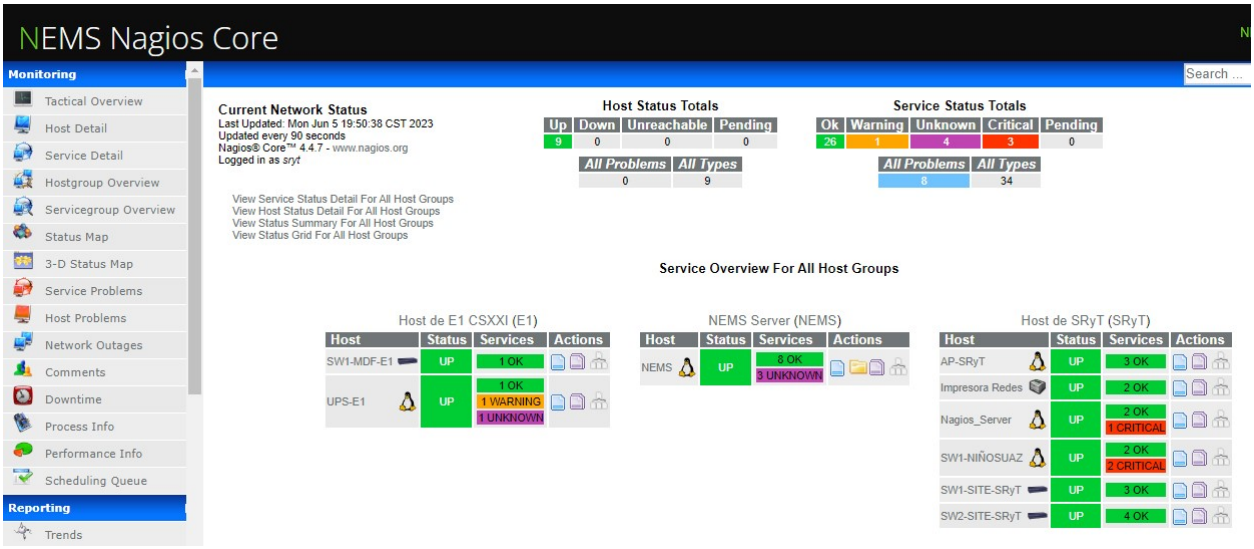

Figura 4.10 Vista Hostgroup Overview dentro de la interface Nagios, muestra un listado de los hostgroups, los dispositivos que pertenecen a cada grupo y su estado.

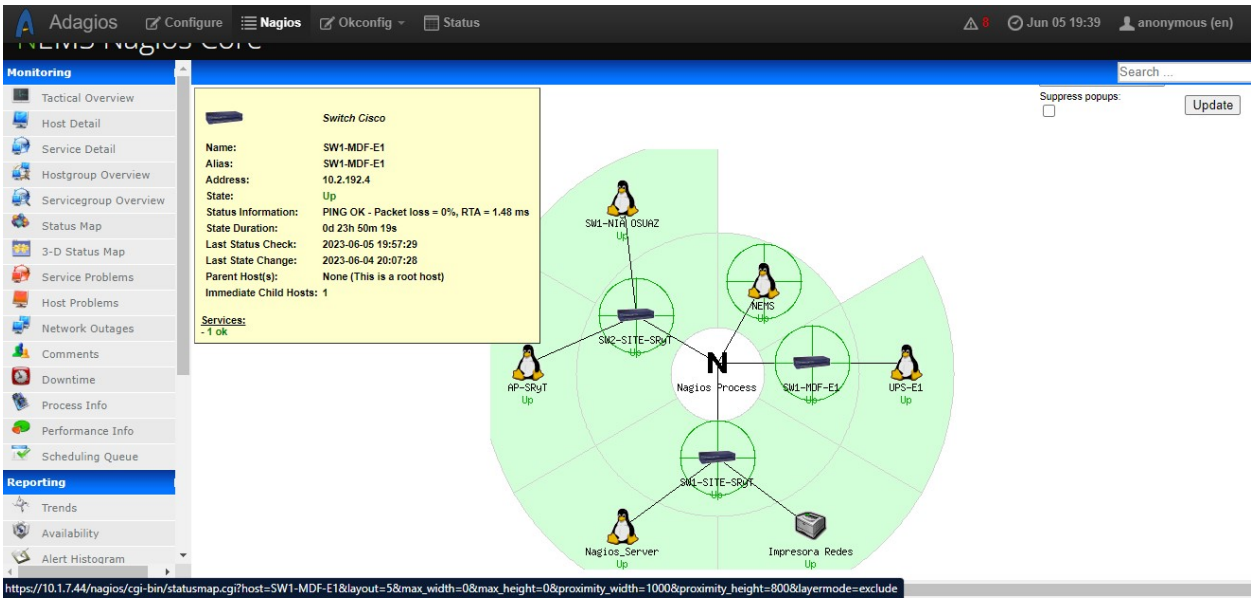

Figura 4.11 Vista Status Map dentro de la interface Nagios.

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 4.13.

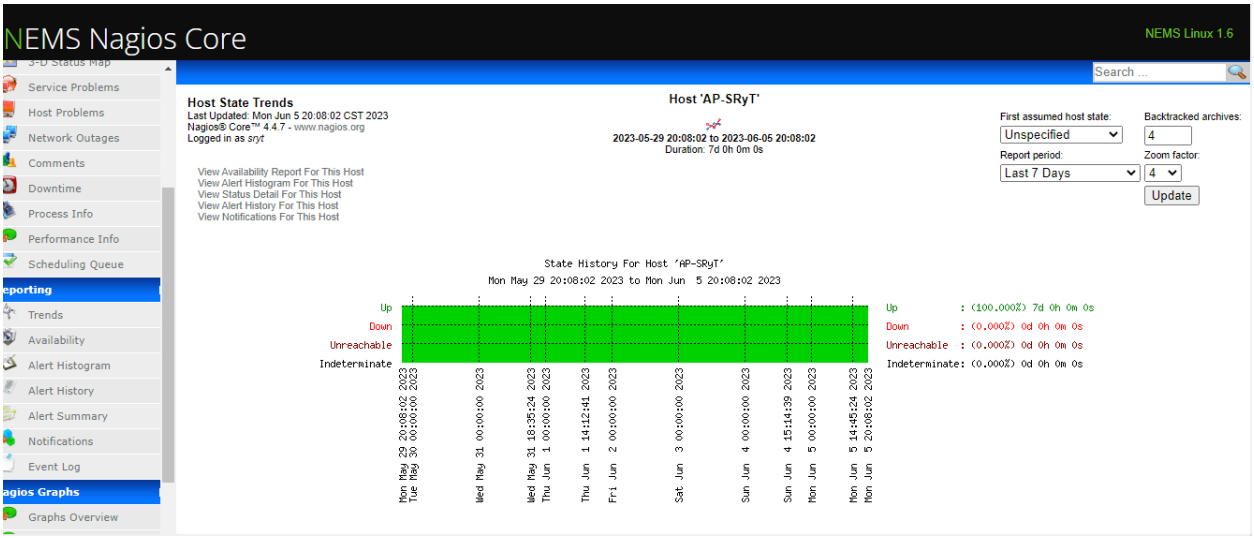

Figura 4.12 Vista Trends dentro de la interface Reportes, muestra un historial de los cambios de estado que ha sufrido un dispositivo en un periodo de tiempo.

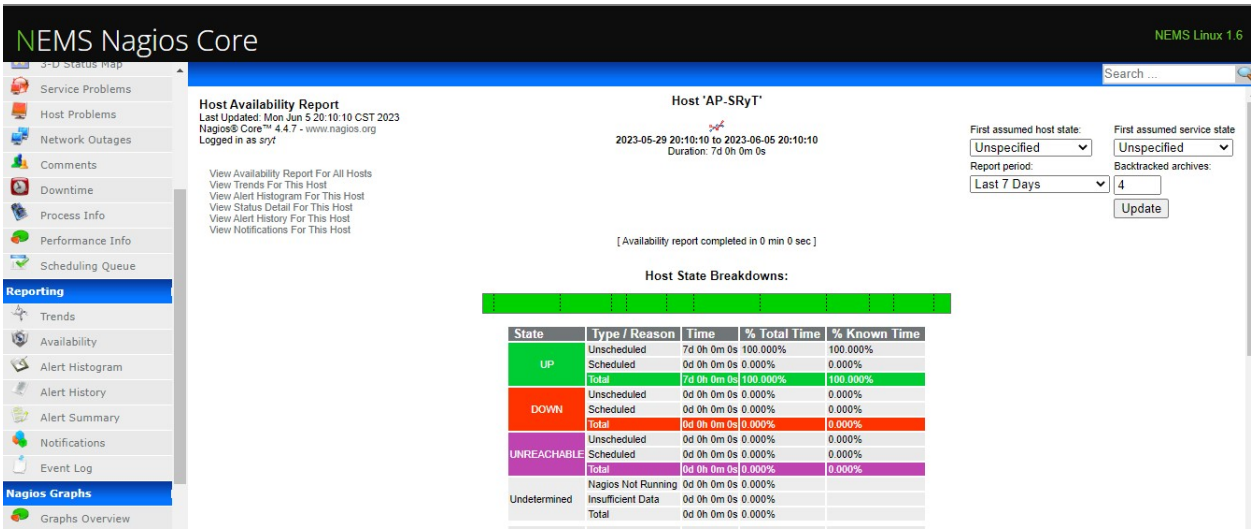

Figura 4.13 Vista Availability dentro de la interface Reportes.

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 4.14.

Figura 4.14 Vista Alert dentro de la interface Reportes.

4.2.4. Mapa general de una red institucional educativa

Después de realizar las pruebas de red en ambiente controlado y el análisis de los resultados obtenidos, se pidió autorización para implementar la herramienta Nems en un ambiente de red más complejo por lo que se comenzó con el monitoreo de diferentes equipos activos de red que integran la red de los diferentes campus de la Universidad Autónoma de Zacatecas. En la Figura 4.15 se muestra el mapa general de los dispositivos monitoreados hasta ahora con NEMS.

En la Figura 4.15, se visualiza como está dividida la red en diferentes estrellas, las cuales integran los equipos activos de red que forman la red LAN de cada Unidad Académica y cada Campus que integran a la Universidad

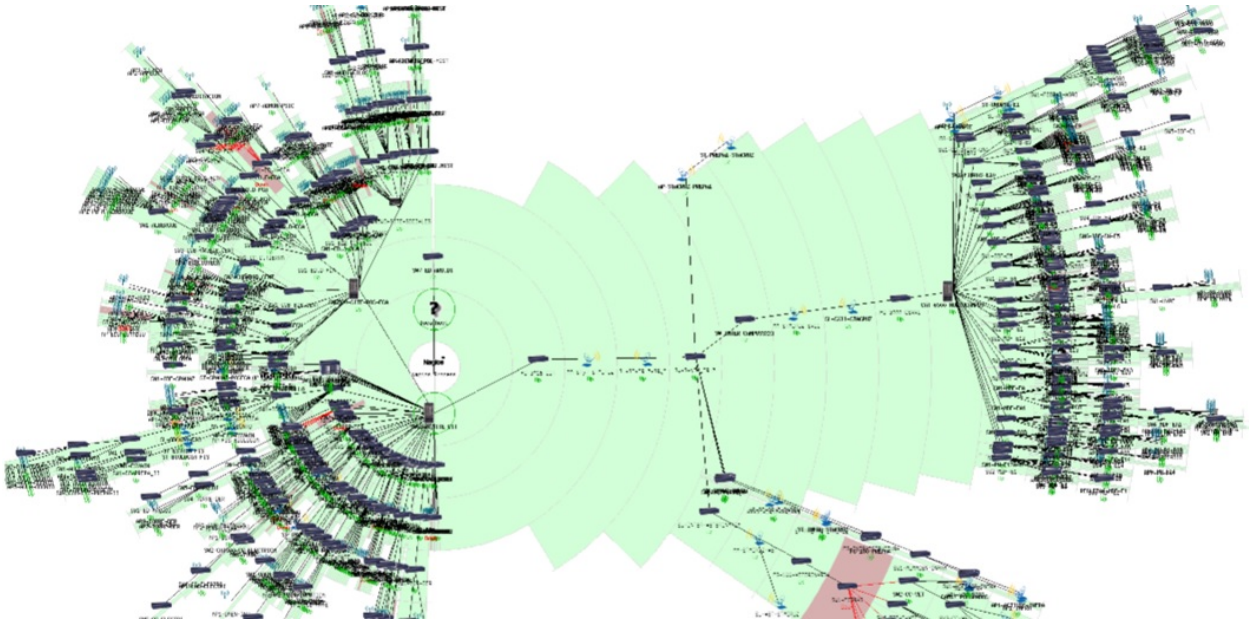

Figura 4.15 Mapa general de la red de la Universidad Autónoma de Zacatecas.

4.3. Análisis de los resultados

De acuerdo a los resultados obtenidos se puede comparar tanto la forma de presentar como la manera de administrar los dispositivos monitoreados en NEMS con respecto a Nagios, donde todo movimiento se tiene que realizar por medio de comandos a través de una consola Linux

El monitoreo de dispositivos a través de NEMS ofrece una gran ventaja respecto a otras herramientas de monitoreo ya que NEMS incluye el monitoreo de servicios como:

- Temperatura del CPU.
- Memoria usada.
- Nivel de procesamiento.
- Usuarios conectados.
- Conexiónes SSH.
- Conexión HTTP.

Dichos servicios se visualizan seleccionando los dispositivos en la vista de Adagios como se muestra en la Figura 4.16.

Figura 4.16 Vista de servicios monitoreados por host.

4.4. 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 4.17 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.

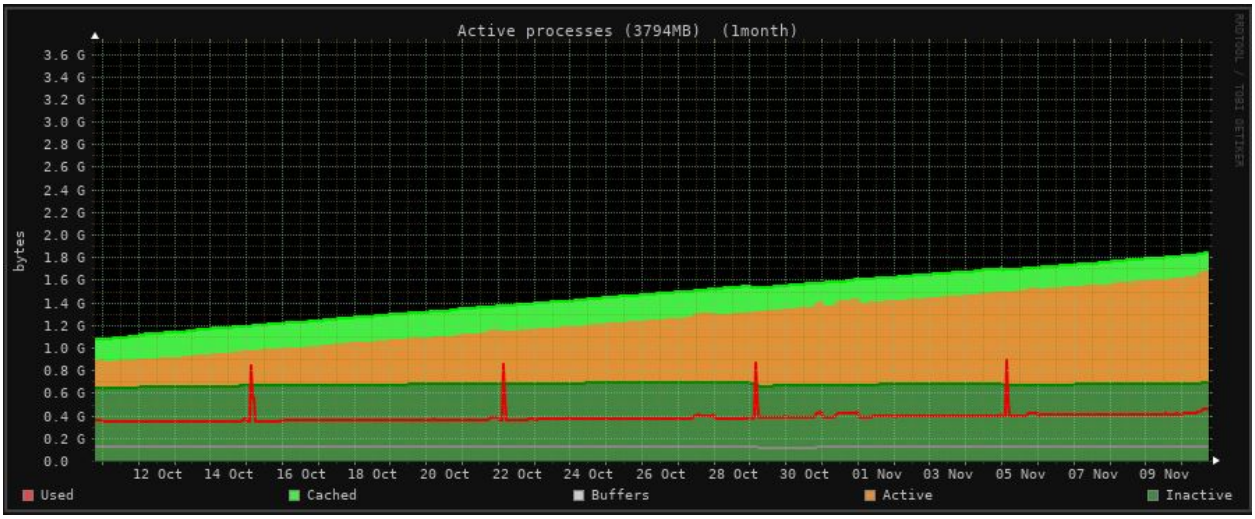

Figura 4.17 Muesta el comportamiento de la capacidad de memoria de la Raspberry con el uso de Nems.

La Figura 4.18 muestra el porcentaje de uso de los archivos del sistema por parte de Nems.

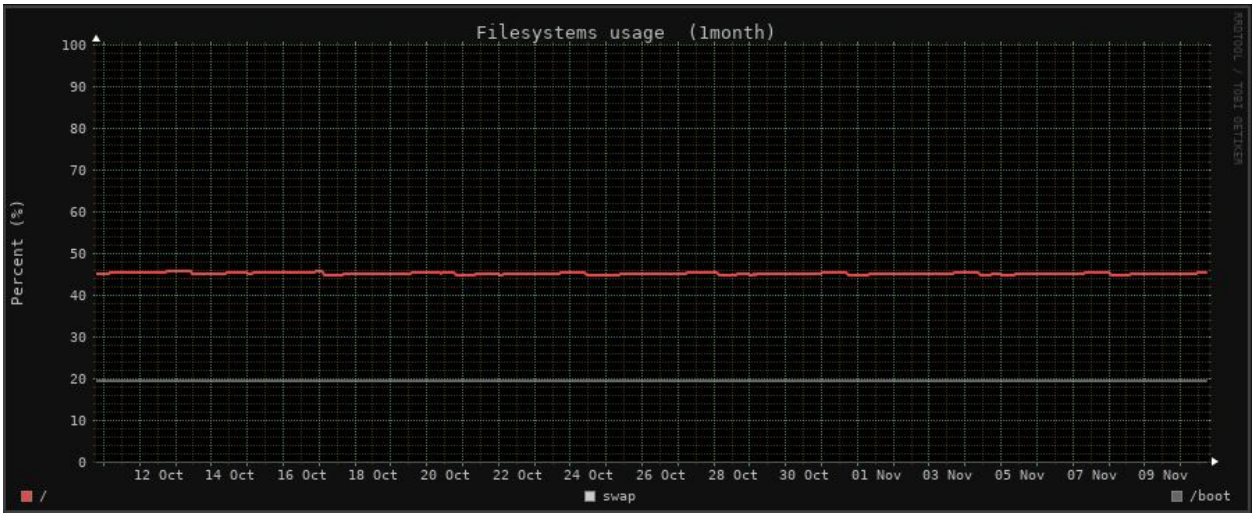

Figura 4.18 Gráfica del porcentaje de uso de los archivos del sistema por parte de Nems

La Figura 4.19 muestra el resumen general de los procesos y su estatus, así como el uso de CPU y memoria por parte de Nems.

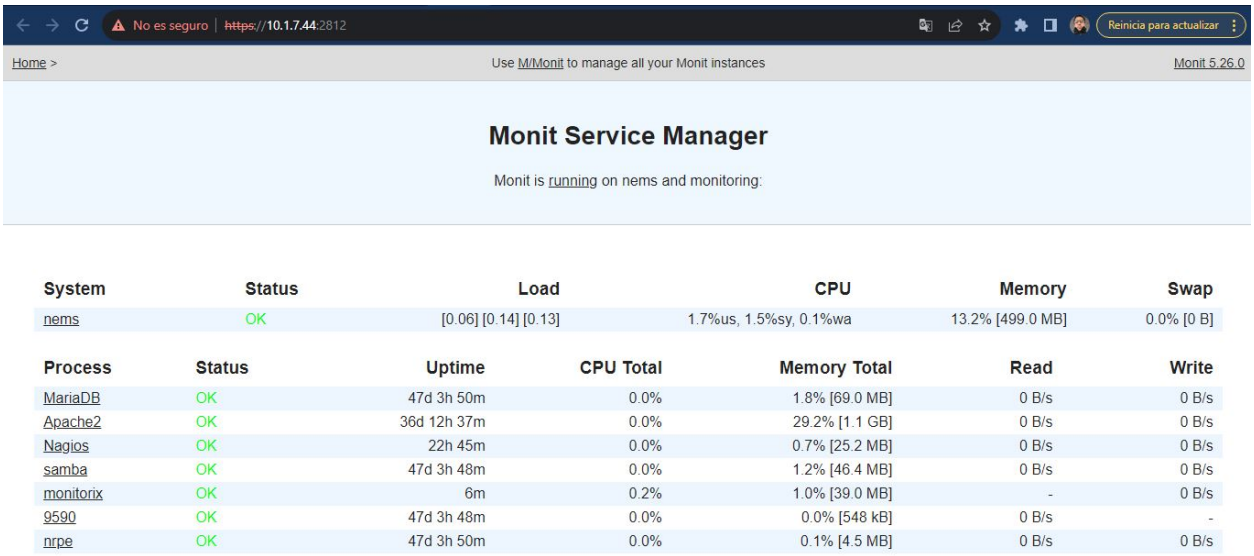

Figura 4.19 Resumen general de procesos, CPU y memoria utilizados por Nems, muestra una vista rápida del estado de la Raspberry y de Nems.

Capítulo 5

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.

5.1. 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 5.1.

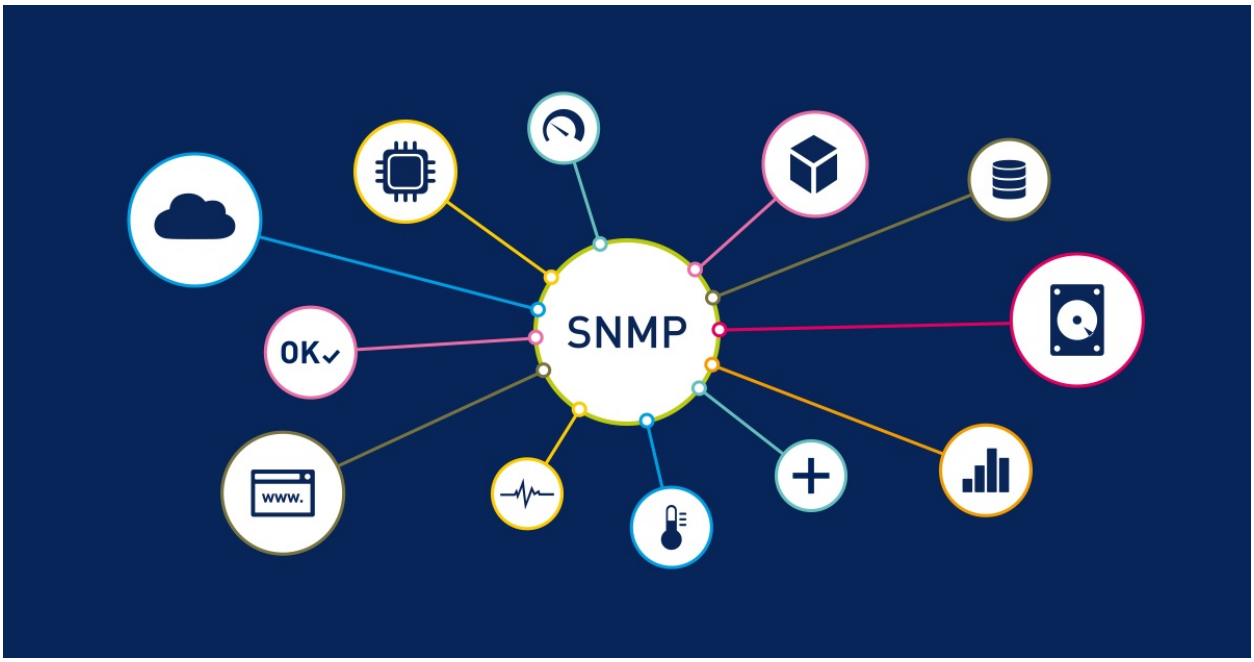

Figura 5.1 Información visualizada de equipos activos de red mediante el protocolo SNMP

Los tres conceptos fundamentales de SNMP son MIB(siglas en inglés de Management Information Base), agente y gestor. El gestor y el agente se comunican mediante dicho protocolo. La estación gestora sirve como interfaz entre el gestor humano y el sistema de gestión de red, envía peticiones a los agentes para que estos les manden información. Los dispositivos de red (ruteadores, switches, etc.) pueden tener instalados agentes SNMP y éstos responden a las órdenes de las estaciones gestoras y de forma asíncrona envían información importante no solicitada.

La información de gestión SNMP se recoge en bases de datos llamadas MIBs. Las MIBs se encuentran en los dispositivos gestionados y forman un conjunto de puntos de acceso a los dispositivos desde la estación gestora. Los recursos a monitorizar en la red se encuentran representados en la MIB como objetos y estos objetos están ordenados de forma jerárquica sobre una estructura de árbol. Cada objeto lleva asociado un identificador de objeto único OID (pos sus siglas en inglés). Las operaciones SNMP se realizan sobre los objetos de la MIB. Hay tres tipos de operaciones, las cuales se describen brevemente a continuación:

- Get: la estación gestora extrae el valor de un objeto del agente.
- Set: la estación gestora fija el valor de un objeto del agente.
- Trap: el agente notifica a la estación gestora eventos significativos.

Para que se pueda realizar el monitoreo de dispositivos de red, se debe asegurar previamente, que éstos cuenten con el protocolo SNMP configurado. En caso de que no cuenten con el protocolo activado, se puede configurar de una manera muy básica:

Para entrar en la configuración del router, se hace a través de una sesión telnet como se muestra en la Figura 5.2.

```
telnet 192.168.110.1
RI> enable
RI# configure terminal
RI(config)#snmp-server community public ro
RI(config)#end
```

Figura 5.2 Comando para activar el protocolo SNMP en switch Cisco

Referencias bibliográficas

Aceto, Giuseppe et al. (2013). «Cloud monitoring: A survey». En: *Computer Networks* 57(9), págs. 2093-2115.

Alhamazani, Khalid et al. (2015). «An overview of the commercial cloud monitoring tools: research dimensions, design issues, and state-of-the-art». En: *Computing* 97, págs. 357-377.

Amazon, Web Services (2023). «Amazon CloudWatch: User Guide». En: URL: `https://docs.aws.amazon.com/AmazonCloudWatch/latest/%20monitoring/acw-ug.pdf`.

Ampratwum, Isaac (2020). «An intelligent traffic classification based optimized routing in SDN-IoT: A machine learning approach». Tesis doct. Université d'Ottawa/University of Ottawa.

App-Dynamics (2023). «AppDynamics Documentation». En: URL: `https://docs.appdynamics.com/`.

Arcilla, Magdalena et al. (2007). «Una propuesta organizativa de los procesos de SD y SS en ITIL». En: *REICIS. Revista Española de Innovación, Calidad e Ingeniería del Software* 3(2), págs. 6-20.

Al-Ayyoub, Mahmoud et al. (2016). «Towards improving resource management in cloud systems using a multi-agent framework». En: *International Journal of Cloud Computing* 5(1-2), págs. 112-133.

Bauset-Carbonell, María-Carmen y Manuel Rodens-Adam (2013). «Gestión de los servicios de tecnologías de la información: modelo de aporte de valor basado en ITIL e ISO/IEC 20000». En: *Profesional de la información* 22(1), págs. 54-61.

Birje, Mahantesh N y Chetan Bulla (2020). «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, págs. 480-490.

Bitnami (2023). «Loved by Developers Trusted by Ops». En: URL: https://bitnami.com/.

Blake, Steven et al. (1998). *An architecture for differentiated services*. Inf. téc.

Broadcom, Inc (2019). «Broadcom Inc. Connecting Everything». En: URL: https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/unified-communications-monitor/4-3-3.html.

Cabezón Rodríguez, Marina (oct. de 2017). *Evaluación de herramientas de monitorización de redes sobre plataforma embebida*. URL: http://hdl.handle.net/10902/12116.

Cacti, Group (2004). «What is Cacti?» En: URL: https://www.cacti.net/info/cacti.

CAGUA, Christian, Johanna A NAVARRO y Ernesto LOJAN (2018). «Modelo de gestión estratégica de los servicios de tecnologías de la información». En: *Revista Espacios* 39(18).

Chávez Zambrano, Gema Katherine y Lady Geomar Tuárez Anchundia (2016). «Propuesta de red de datos para la gestión de los servicios de red en el campus politécnico de la Espam MFL». B.S. thesis. Calceta: Espam.

Collec (2023). «Documentation». En: URL: https://collectd.org/documentation.shtml.

Comer, Douglas E (2013). *Internetworking with TCP/IP*. Addison-Wesley Professional.

Communications IDG, Barry Nance (2007). «Hyperic HQ Reviews». En: URL: https://www.networkworld.com/article/2291083/hyperic-hq.html.

DataDog (2023). «Monitoring in the Cloud eBook». En: URL: https://www.datadoghq.com/resources/monitoring-in-the-cloud-ebook/.

Elasticsearch (2023). «Document APIs». En: URL: https://www.elastic.co/guide/en/elasticsearch/reference/current/docs.html.

Graphite, Geology.com (2005). «What is Graphite?» En: URL: https://geology.com/minerals/graphite.shtml.

Icinga, GmbH (2009). «Why Monitoring?» En: URL: https://icinga.com/products/.

Kick (15). En: URL: https://aws.amazon.com/es/blogs/aws/.

Kyle, Kingsbury y Pierre-Yves Ritschard (2023). «Riemann - A network monitoring system». En: URL: http://riemann.io/.

Larrocha, Elena Ruiz et al. (2010). «Filling the gap of Information Security Management inside ITIL®: proposals for posgraduate students». En: *IEEE EDUCON 2010 Conference*. IEEE, págs. 907-912.

León, Daruin Arley et al. (2022). «Inteligencia artificial para el control de tráfico en redes de datos: Una Revisión». En: *Entre Ciencia e Ingeniería* 16(31), págs. 17-24.

Li, Wei y Andrew W Moore (2007). «A machine learning approach for efficient traffic classification». En: *2007 15th International symposium on modeling, analysis, and simulation of computer and telecommunication systems*. IEEE, págs. 310-317.

Logic-Inc (2023). «Performance Monitoring for Complex IT». En: URL: https://www.logicmonitor.com/platform.

Mell, Peter y Timothy Grance (sep. de 2011). *The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology*. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

Microsoft, Azure (2023). «Azure Monitor». En: URL: https://azure.microsoft.com/en-in/products/monitor/.

Millán Naveas, Ginno y Manuel Vargas Guzmán (2020). «Un algoritmo de control de flujo para redes de computadoras de alta velocidad». En: *Ingeniare. Revista chilena de ingeniería* 28(1), págs. 24-30.

Nagios, Enterprises (2023). «Nagios Core». En: URL: https://www.nagios.com/solutions/aws-monitoring/ (visitado 29-06-2023).

Netreo (2023). «Cloud Monitoring Solutions». En: URL: https://www.netreo.com/solutions/cloud-monitoring/.

New, Relic (2008). «New Relic Deliver more perfect software». En: URL: https://newrelic.com/.

Nguyen, Giang et al. (2020). «Deep learning for proactive network monitoring and security protection». En: *IEEE Access* 8, págs. 19696-19716.

Nimsoft (2010). «Getting Started Guide Nimsoft Monitor». En: URL: https://support.nimsoft.com/downloads/server50/SLM.pdf.

Opsview, Ltd (2010). «Opsview - Enterprise IT Infrastructure Monitoring». En: URL: https://www.opsview.com/.

PagerDuty (2023). «Introduction». En: URL: https://developer.pagerduty.com/docs/ZG9jOjQ2NDA2-introduction.

PAILIACHO, Verónica M et al. (2019). «Modelo de gestión de disponibilidad de la infraestructura tecnológica. Un enfoque desde ITIL». En: *Revista Espacios* 40(35).

Peña Casanova, Mónica et al. (2018). «Sistema para detección y aislamiento de fallas». En: *Revista Cubana de Ciencias Informáticas* 12(2), págs. 58-73.

Prometheus, Authors (2014a). «MONITORING DOCKER CONTAINER METRICS USING CADVISOR». En: URL: https://prometheus.io/docs/guides/cadvisor/.

Prometheus, Authors (2014b). «Prometheus - Monitoring system y time series database». En: URL: https://prometheus.io/.

Quintero Gómez, Luisa Fernanda (2015). «Modelo basado en ITIL para la Gestión de los Servicios de TI en la Cooperativa de Caficultores de Manizales». En.

Raspberry (2023). «Raspberry Pi Documentation». En: URL: https://www.raspberrypi.com/documentation/.

Robbie, Ferguson y Bill Marshall (ene. de 2020). *Welcome to NEMS Linux — NEMS Linux Documentation 1.6 documentation*. docs.nemslinux.com. URL: https://docs.nemslinux.com/en/latest (visitado 20-04-2023).

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

TechTarget (2023). «SearchWindowsServer Information, News and Tips from TechTarget». En: URL: https://www.techtarget.com/searchwindowsserver/.

US Website, TeamViewer (2022). «Centralized remote monitoring». En: URL: https://www.teamviewer.com/en/products/remote/solutions/remote-management/ (visitado 29-06-2023).

Villamizar, Miguel Ángel PÉREZ (2018). «Aplicación de la metodología ITIL para impulsar la gestión de TI en empresas del Norte de Santander (Colombia): revisión del estado del arte». En: *Espacios* 39(09), pág. 17.

Vinayakumar, R, KP Soman y Prabaharan Poornachandran (2017). «Applying deep learning approaches for network traffic prediction». En: *2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*. IEEE, págs. 2353-2358.

Zabbix, LLC (ene. de 2001). *Zabbix cloud images*. www.zabbix.com. URL: https://www.zabbix.com/cloud_images (visitado 29-06-2023).

Apéndice A: Hoja de datos del equipo activo de red

Conmutador o switch de red.

https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-x-series-swi
datasheet_c78-728232.html

Radio con antena

https://dl.ubnt.com/datasheets/nanobeam/NanoBeam_DS.pdf

Punto de acceso

https://dl.ubnt.com/datasheets/unifi/UniFi_AP_DS.pdf

https://www.cisco.com/c/en/us/products/collateral/wireless/aironet-2800-series-access
datasheet-c78-736497.html

Raspberry Pi 4 Model B

https://datasheets.raspberrypi.com/rpi4/raspberry-pi-4-datasheet.pdf

Apéndice B: Instalación y documentación NEMS

B.1. Instalación de NEMS en una Raspberry Pi

De acuerdo a las especificaciones de Robbie y Marshall (2020) para lograr una correcta instalación, es necesario seguir las siguientes instrucciones tomando en cuenta los requerimientos indicados a continuación.

B.1.1. Software y hardware necesario

- Raspberry Pi 3 Modelo B o superior modelo RPi.
- Tarjeta MicroSD rápida de 16 GB o superior o unidad flash USB.
- Una fuente de alimentación para la Raspberry Pi, preferiblemente conectada a un UPS.
- Un cable de red ethernet.

B.1.2. Instalar NEMS Linux en MicroSD

Para poder realizar la correcta instalación de NEMS en una tarjeta de memoria microSD es necesario realizar lo siguiente:

1. Descargue en la computadora la última versión de NEMS Linux desde https://nemslinux.com/
2. Instale en la computadora la aplicación Raspberry Pi Imager desde https://www.raspberrypi.com/software/
3. Haga clic en Elegir sistema operativo
4. Haga clic en Elegir personalizado en la parte inferior de la lista
5. Busque la copia descargada de NEMS Linux
6. Haga clic en Elegir almacenamiento

7. Inserte la tarjeta MicroSD o unidad flash USB
8. Seleccione cuidadosamente la tarjeta MicroSD o unidad flash USB
9. Haga clic en Escribir

El proceso se muestra en la Figura B.1

Figura B.1 Proceso de carga de NEMS a tarjeta mSD.

B.1.3. Primer arranque

Para lograr el primer arranque de la aplicación NEMS es necesario realizar lo siguiente:

1. Inserte la tarjeta MicroSD o la unidad flash USB que contiene NEMS Linux a la Raspberry Pi.

2. Conecte el puerto Gigabit Ethernet de la Raspberry Pi a la red mediante un cable Ethernet.

3. Encienda la Raspberry Pi para iniciar el servidor NEMS.

4. Espere aproximadamente 5 minutos para realizar las operaciones de primer arranque.

5. Durante la operación de primer arranque, el sistema de archivos se redimensionará automáticamente a la capacidad de su almacenamiento y el servidor NEMS se reiniciará.

Una vez completadas las operaciones de primer arranque, visite https://nems.local/ en su navegador web. Si la resolución de nombres no funciona, pruebe con la dirección IP de su dispositivo NEMS, que puede encontrar en la tabla de direcciones de DHCP.

La pantalla de inicio se muestra en la Figura B.2

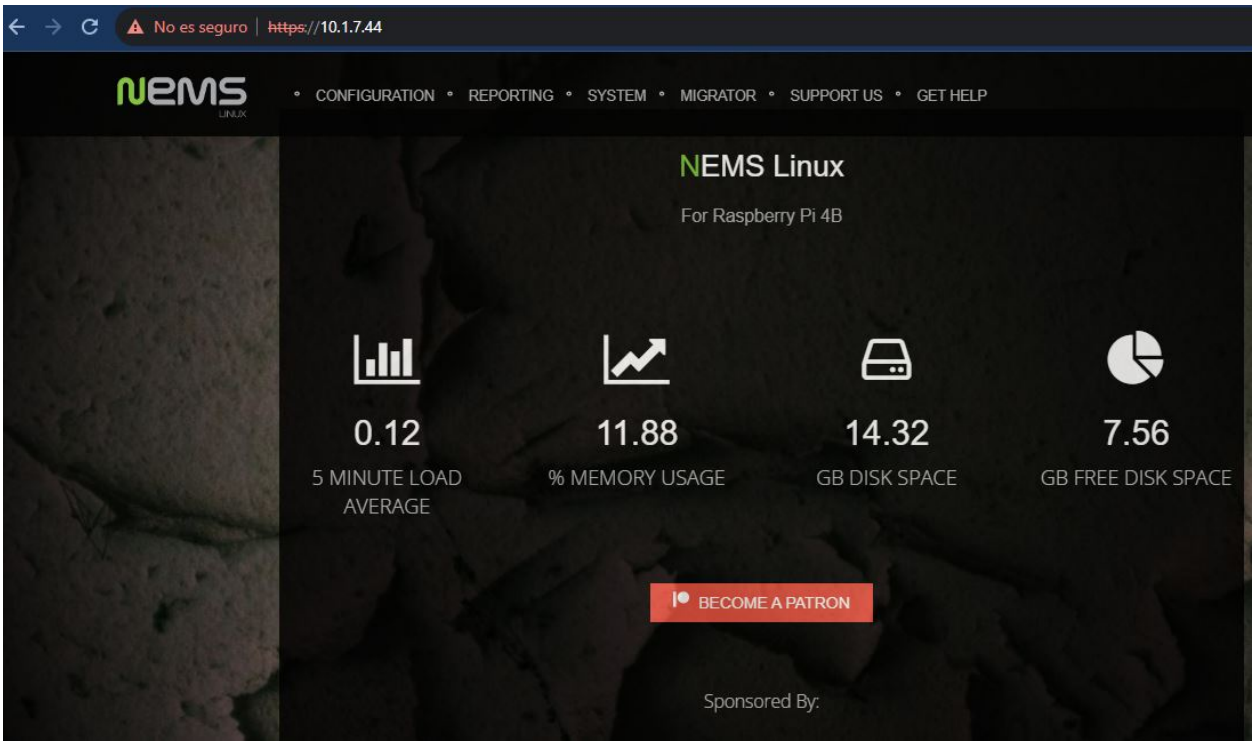

Figura B.2 Pantalla inicial de NEMS: opciones de configuración y reportes.

B.2. Documentación NEMS

En la siguiente dirección url encontrará la documentación oficial referente a NEMS Linux.

`https://docs.nemslinux.com/en/latest/gettingstarted/introduction.html`