ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE FORMACIÓN DE TECNÓLOGOS

IMPLEMENTACIÓN DE UNA HERRAMIENTA DE MONITOREO DE CÓDIGO ABIERTO DE INFRAESTRUCTURA TI

TRABAJO DE INTEGRACIÓN CURRICULAR PRESENTADO COMO REQUISITO PARA LA OBTENCIÓN DEL TÍTULO DE TECNÓLOGO SUPERIOR EN REDES Y TELECOMUNICACIONES

BYRON HERNANDO BENALCAZAR SALAZAR

DIRECTOR: ANDRÉS FERNANDO REYES CASTRO

DMQ, agosto 2024

CERTIFICACIONES

Yo, BYRON HERNANDO BENALCAZAR SALAZAR declaro que el trabajo de integración curricular aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

BYRON HERNANDO BENALCAZAR SALAZAR

byron.benalcazar@epn.edu.ec

byron.benalcazar@outlook.com

Certifico que el presente trabajo de integración curricular fue desarrollado por BYRON HERNANDO BENALCAZAR SALAZAR, bajo mi supervisión.

ANDRÉS FERNANDO REYES CASTRO
DIRECTOR

andres.reyes@epn.edu.ec

DECLARACIÓN DE AUTORÍA

A través de la presente declaración, afirmamos que el trabajo de integración curricular aquí descrito, así como el (los) producto(s) resultante(s) del mismo, son públicos y estarán a disposición de la comunidad a través del repositorio institucional de la Escuela Politécnica Nacional; sin embargo, la titularidad de los derechos patrimoniales nos corresponde a los autores que hemos contribuido en el desarrollo del presente trabajo; observando para el efecto las disposiciones establecidas por el órgano competente en propiedad intelectual, la normativa interna y demás normas.

_____

BYRON HERNANDO BENALCAZAR SALAZAR

DEDICATORIA

Este trabajo va dedicado a mi madre, ya que sin la ayuda que ella me brindo nada de esto hubiera sido posible. Su fe, su sacrificio y su amor que ella puso en mi fueron los pilares que me mantuvieron firme para alcanzar esta meta en mi vida. Por ello este trabajo y los futuros logros obtenidos a partir de este punto también serán suyos.

El agradecimiento desde lo más profundo de mi corazón a mi abuelita Luz, ya que gracias a ella he conocido grandes sentimientos, como el amor incondicional, la dedicación y sacrificio hacia los seres que se ama, que existen diferentes formas de enfrentar a la vida y que siempre hay porque seguir luchando.

A mi abuelito Plutarco que con su sabio concejo supo guiarme siempre por el camino correcto, donde las enseñanzas y experiencias que el supo compartir conmigo han llegado a forjar a la persona que soy ahora.

Con todo mi aprecio para mi Mama.

AGRADECIMIENTO

Mi agradecimiento a mi Padre que supo ser parte de este proceso por muchos años, por su apoyo y su preocupación. También desearía agradecer todos mis familiares que de alguna u otra manera me han apoyado para alcanzar esta meta.

Mi agradecimiento más sincero a la institución que por medio de cada maestro ha permitido que me convirtiera en profesional, a cada uno de mis profesores que hicieron parte de mi proceso de formación, y espero que en mi vida profesional poder retribuir de la mejor manera, a toda la dedicación y el sacrificio que ellos pusieron para que sus conocimientos ahora sean parte de los míos.

También quiero expresar mi agradecimiento al Ing. Andrés Reyes por haberme guiado en este trabajo, por su paciencia, por el tiempo que me brindo y por la vocación de docente que él realiza. Además, quisiera aprovechar esta ocasión para desearle éxitos en su carrera profesional.

ÍNDICE DE CONTENIDOS

RESUMEN

Este trabajo se definió en varias partes las cuales se debían cumplir para alcanzar todas las metas definidas.

En la primera sección se encuentran los objetivos que se deben cumplir, además de los alcances del proyecto y toda la información necesaria para desarrollar el componente y cumplir con todos los puntos establecidos en este trabajo.

La sección siguiente narra toda la metodología que se empleó para alcanzar objetivos generales y específicos, de esta forma alcanzar todos los requerimientos requeridos sin inconveniente.

En la tercera sección se detalla el funcionamiento de la herramienta como se realiza la monitorización y gestión de la red virtualizada la cual contiene diferentes servidores como correo y un web, además de dispositivos de conectividad entre redes, finalmente se simulo dispositivos de usuarios finales. Para cumplir con los objetivos establecidos se utilizó GNS3 como programa de simulación y se usara equipos de la marca Cisco y se utilizó OSPF como protocolo de enrutamiento para la comunicación de toda la red, para realizar la monitorización y gestión de toda la red se utilizó la herramienta *open source* Zabbix, el cual fue instalado en una máquina desde la cual se hará la gestión de toda la red.

Las ultimas dos secciones sirven para mostrar las conclusiones y recomendaciones que se obtuvieron al utilizar la herramienta de monitoreo, con el fin de brindar una idea más amplia del uso de Zabbix.

PALABRAS CLAVE: *Herramienta, red, Zabbix, dispositivos, servidor, monitorización, gestión.*

ABSTRACT

This work was defined in several parts which had to be completed to achieve all the defined goals.

In the first section are the objectives that must be met, in addition to the scope of the project and all the information necessary to develop the component and comply with all the points established in this work.

The following section narrates the entire methodology that was used to achieve general and specific objectives, in this way achieving all the required requirements without inconvenience.

The third section details the operation of the tool, how the monitoring and management of the virtualized network is carried out, which contains different servers such as email and a web, as well as connectivity devices between networks, finally end-user devices are simulated. To meet the established objectives, GNS3 was used as a simulation program and Cisco brand equipment was used and OSPF was used as a routing protocol for communication of the entire network. To monitor and manage the entire network, the Open Source Zabbix server, which was installed on a machine from which the entire network will be managed.

The last two sections serve to show the conclusions and recommendations that were obtained when using the monitoring tool, in order to provide a broader idea of the use of Zabbix.

KEYWORDS: *Tool, network, Zabbix, devices, server, monitoring, management.*

1 DESCRIPCIÓN DEL COMPONENTE DESARROLLADO

En la actualidad el avance tecnológico ha sufrido cambios inimaginables, y la convergencia que están teniendo todas las áreas tecnológicas en los últimos años es muy importante, por esta razón las brechas técnicas que existían en recolectar datos, transportar, almacenar y procesar la información tienden a perderse. Grandes organismos, sean públicos o privados, que manejan grandes cantidades de información y que se encuentran separados geográficamente a kilómetros sienten la necesidad de tener la capacidad de examinar en tiempo real el estado de cada uno de los datos que generan y los dispositivos que trabajan para ello, en una época donde la información y la transmisión de datos es la base fundamental del funcionamiento de las organizaciones.

Por estas razones se vuelve necesario tener la capacidad de gestionar y monitorear la red donde se encuentran montados todos los servicios y dispositivos. La instalación de una herramienta como prevención o solución en entidades donde su uso sea vital es importante, y así se pueda brindar información del estado actual de cada equipo para poder tomar decisiones y realizar labores de corrección y prevención de forma temprana o anticipada. La instalación de la plataforma libre Zabbix, permite observar de forma intuitiva todos los datos que esta aplicación genera y la manera de presentar la información pueda ser modificada dependiendo de las necesidades de cada usuario y que pueda advertir de manera automática de posibles eventualidades que la red y sus elementos genere.

Para la implementación de la plataforma Zabbix, se virtualizaron servidores y máquinas de usuario con sistemas operativos Linux y Windows, se utilizó GNS3 donde se simuló la red (compuesta por un servidor de correo y un servidor web). Adicionalmente, las redes que componen la LAN están separas por routers de la marca Cisco, se realizaron las configuraciones necesarias tanto de protocolos y de direccionamiento IP para que la red pueda tener comunicación total, en la herramienta y en los dispositivos se hizo las configuraciones necesarias para poder realizar el monitoreo de todos los dispositivos de red. Por último, se hizo uso del servidor de correo para enviar las alertas generadas desde la plataforma Zabbix.

1.1 Objetivo general

Implementar una herramienta de monitoreo de código abierto de infraestructura TI.

1.2 Objetivos específicos

- Establecer los requerimientos de la herramienta de monitoreo de código abierto.
- Definir los hosts y servicios a monitorear dentro la infraestructura.
- Configurar la herramienta de monitoreo y los hosts.
- Configurar alertas automáticas para notificar a los administradores sobre problemas o fallos en los equipos y/o servicios.
- Realizar pruebas de funcionamiento de la herramienta de monitoreo.

1.3 Alcance

Por medio del presente proyecto se busca realizar la implementación de una herramienta, la plataforma Zabbix de código abierto, para el monitoreo de redes y servicios en la infraestructura de TI mediante una topología virtualizada. El proyecto implica la implementación inicial y la configuración básica para realizar el monitoreo de hosts y servicios, en base a métricas y alertas.

Adicionalmente, se llevará a cabo la integración de la herramienta con el servicio de correo electrónico para la generación de alertas automáticas y se elaborarán manuales técnicos que sirvan como referencia para futuras implementaciones de la herramienta.

1.4 Marco Teórico

Sistema de gestión y monitoreo de Red.

Los sistemas usados para gestionar y monitorear redes consisten en tener un seguimiento permanente de eventos en tiempo real de lo que está pasando dentro de un entorno controlado de red, en el que se encarga de observar, vigilar, tomar datos y analizar todos los resultados obtenidos; para así tener información que pueda ayudar a los administradores de red solucionar problemas de formas más eficientes y de cierta forma anticiparse a eventualidades que puedan afectar el normal funcionamiento de la red. La monitorización de la red provee información específica de cada dispositivo como el consumo de los recursos asignado en el caso de haber usado una virtualización, el estado de la memoria, el estado del dispositivo, el funcionamiento del sistema operativo o del servicio, etc. [1].

Tipos de monitoreo

- **Local:** a este tipo de monitoreo se lo denomina así porque se está realizando un seguimiento a una red de tipo local, es decir no se debe acceder al servicio de Internet para poder realizar este tipo de monitoreo [1].
- **Remoto:** la monitorización remota se la realiza cuando el sistema que se quiere gestionar se encuentra a varios kilómetros de donde se encuentra instalado el servidor de monitorización y es necesario el servicio de Internet para tener acceso a la información [1].

SNMP

Simple Network Manangement Protocol (SNMP) es un protocolo que surgió como medida para la administración y gestión de redes TCP/IP, trabaja sobre la capa de aplicación y tiene la capacidad de informar sobre fallas de dispositivos, el rendimiento y acciones que estos están realizando lo hacen en tiempo real, trata de organizar en un esquema, que se lo utiliza para reunir, organizar y comunicar toda la información recopilada.

Existe una gran cantidad de dispositivos que soportan este protocolo, tales como enrutadores, *switches*, *acces point* e inclusive dispositivos de usuarios finales se pueden gestionar mediante este protocolo.

Este basa en el protocolo UDP por lo que no garantiza la entrega de paquetes ya que pretende ser más eficiente en el tiempo con sus notificaciones. Los dispositivos de red que utilizan SNMP utilizan el puerto 161 para su comunicación.

La estandarización de este protocolo se definió en el RFC 1157 y presenta los siguientes elementos [2]:

- **Estación de gestión**: Es una maquina o host donde se instalará la herramienta con el cual se va a realizar la gestión e la red.
- **Agente de gestión:** La implementación del protocolo SNMP en los diferentes equipos como *switches*, *routers*, computadoras, necesitan tener implementado un componente llamado agente que es el necesario para la gestión.
- **Base de información de gestión (MIB):** En términos generales se la considera como una base de datos necesaria que se rige por un orden jerárquico, que se encuentra guardada en forma de un árbol. El formato que se encuentra en MIB está definido como parte del protocolo SNMP. El concepto de árbol MIB detalla los niveles o jerarquías que se han fijado por las organizaciones.
- **Protocolo de gestión de red:** Es un concepto para identificar los elementos que se utilizan para realizar la comunicación necesaria para la gestión. Existen un

conjunto de comandos que se vuelven muy importantes y por lo tanto son los más usados dentro de las redes como, por ejemplo: *get* que sirve para obtener la información de cierto *host* ya sea a nivel de hardware o software, *set* que es muy importante para establecer un valor a un recurso y *notify* que es para las notificaciones necesarias [3].

Versiones de protocolos SNMP

En la actualidad existen 3 versiones de este protocolo que son las siguientes:

SNMPv1

La primera versión del protocolo utiliza los modelos básicos *MIB, Set/Get.* El mecanismo de seguridad que utiliza se lo conoce con el nombre de comunidad SNMP, pero este nombre de comunidad es muy rudimentario para la actualidad ya que esta contraseña está en texto plano, por lo que puede ser interceda fácilmente. Esta versión de SNMP desde que se estandarizo y se estableció fue la predominante en la industria [4].

SNMPv1 tiene un formato de mensajes que se parece mucho a la de la versión 2, ya que dichos mensajes tienen un formato con 3 indicadores que usan para la comunicación entre el administrador y el agente, estos indicadores son:

- **Versión:** Este indicador proporcionará la versión del protocolo que se está utilizando.
- **Nombre de comunidad:** Este nombre autentifica a todos los dispositivos y agrupa a un conjunto de estaciones de red o dispositivos que se administraran.
- **PDU:** Donde se encuentran diferentes características y los formatos como lo muestra la Figura 1.1.

Figura 1.1 Formato de las PDU [5]

SNMPv2

SNMP versión 2 comparada con la versión anterior tuvo una mejora en la parte de la seguridad, además de tener una mejora considerable en el mecanismo, se encarga de recuperar información que por algún motivo se podría haber perdido, además de haber mejorado toda la parte de gestión de mensaje encargados de alertar de errores e incluye una amplia variedad de códigos que se encargan de distinguir diferentes condiciones de

errores dentro de la red, además de que estos códigos pueden informar el tipo de error que está teniendo cierto dispositivo.

En esta versión trata de mejorar el protocolo integrando nuevos comandos, estos son:

- ***GetBulk*:** Esta operación recupera una gran cantidad de bloques de datos como pueden ser columnas de tablas, esto se lo realiza desde el gestor.
- ***Inform*:** Esta nueva opción trabaja enviando toda la información recopilada por el agente al gestor, de esta forma se obtendrá una confirmación.
- ***Report:*** Es una acción que el agente deberá enviará cuando exista información que sea considerada como un error que lo haya generado el protocolo

En el año 1995 se publicó una nueva versión considerada una mejora a la versión 2 que se la denomino SNMPv2c, esta nueva versión aparece con mejoras en la configuración haciendo de esta más sencilla, pero se mantuvo la autentificación de versiones anteriores que tenían como nombre 'comunidad'.

Estas nuevas mejoras que se le hicieron a la versión 2 se traducirían en una mejor eficiencia en el intercambio de información. Las operaciones que se realizaban con la versión 1 siguen siendo casi las mismas en esta nueva versión, el único cambio que se realizo fue que las 3 primeras operaciones ya no se caerán de manera simultánea si alguna falla, lo que quiere decir que las operaciones seguirán trabajando su alguna de estas tiene algún problema con un objeto [2].

SNMPv3

Esta es la tercera versión del protocolo SNMP que se aprobó por el organismo *Internet Engineering Task Force* (IETF) en 2022. Por lo que es la última versión conocida de este protocolo. Esta versión se caracteriza por que se reforzó la seguridad, con cierto énfasis en la autenticación, privacidad, el control de acceso y de administración de esta forma tener la posibilidad de realizar una configuración remota. SNMPv3 no pretende ser una versión que remplace las versiona anteriores, sino será el encargado de tener una mayor capacidad de administración y sobre todo de seguridad. Esta versión está orientada a evitar tener ataques cibernéticos protegiéndola usando encriptación y una autentificación más robusta y así evitar las siguientes amenazas [6]:

- **Modificación de información:** Este tipo de amenaza podría modificar el mensaje que genero el protocolo, por lo que es necesario tener control de usuarios que ingresan al archivo principal.
- **Enmascaramiento:** Usuarios que no estén autorizado a obtener información, podrían obtener entidades de algún administrador usando operación de

ciberataques, obteniendo autorizaciones que les permitirá realizar cualquier tipo de operación.

- **Reenvío de mensajes:** El protocolo SNMP trabajo sobre UDP lo que quiere decir que es de transporte sin ninguna conexión existe el riego de que los mensajes que genere puedan ser guardados en sitios fuera de los autorizados para posteriormente ser duplicados o reenviados.
- **Poca privacidad:** Cualquier tipo de Identidad podría observar la transmisión de los mensajes que existen entre el servidor y los agentes de equipos y recopilar información que podría ser una amenaza para red.

Protocolo de administración de red

La capa de administración también trabaja sobre la capa de aplicación, lo que significa que puede inspeccionar o modificar cualquier archivo o elemento de la MIB que desee del agente. Al realizar la comunicación entre el administrador y el agente se utiliza el protocolo SNMP, a través del cual se intercambian mensajes de protocolo. Otra función que realiza el protocolo de gestión de red es conectar la estación de gestión al agente.

El objetivo principal del uso del protocolo SNMP es monitorear exitosamente la red en cualquier nivel, especialmente interpretar la información proporcionada por el monitoreo. Los mensajes no solicitados, llamados trampas, son requeridos porque ahorran tiempo y atención en el sondeo que se realiza entre dispositivos. Se imponen límites de mensajes no solicitados, lo que mejora los objetivos de simplicidad y aumenta la eficiencia del tráfico pico generado por las funciones de gestión correspondientes. La Figura 1.2 muestra de manera gráfica la forma de comunicación que tiene el agente y la estación de administración [6].

Figura 1.2 Forma de trabajo del agente SNMP [5]

Estructura de PDU

Para entender a que se refieren las operaciones PDU se debe tener claro todos los datos que se van a incluir en los paquetes que serán enviados desde la PDU, estos datos son:

- **RequestID:** Este tipo de dato permite especificar el orden en el que se envían los datagramas. Otra característica importante es que permite que servicios de datos por paquetes poco confiables no envíen paquetes de datos duplicados [2].
- **ErrorStatus:** Tiene la capacidad de alerta si ha existido algún tipo de error o no. Por lo que debería ser normal que tome cualquier valor [6].
    - noError
    - tooBig
    - noSuchName
    - badValue
    - readOnly
    - genErr
- **ErrorIndex:** Este tipo de variable muestra los errores que se vayan presentando, siendo importante porque es el encargado de indicar la variable que genero el problema.
- **VarBindList:** Esta opción provee una lista de nombres de variables y sus valores correspondientes. Algunas PDU se definen únicamente por el nombre que se les asigna. Se recomienda definir valores con NULL ante este tipo de situaciones.

Una unidad de datos de protocolo (PDU) es el vocabulario básico de los administradores SNMP y los agentes de comunicación. Las PDU de información son asíncronas. Esto significa que la comunicación entre el gestor y el agente se divide en dos mensajes, una solicitud y una respuesta. De la versión 1 a la versión 3 del protocolo SNMP siempre harán las mismas cosas, aunque irán aumentando con cada versión y cada mejora que se haga. Las operaciones son las siguientes:

- getRequest: Es el encargado de enviar el aviso al agente SNMP para poder obtener un identificador con su valor de objeto (OID).
- getNextRequest: El trabajo de esta operación es informar al agente SNMP para que de esta forma se pueda obtener el valor de la próxima OID raíz de la petición OID.
- getResponse: Esta acción se produce en respuesta a una acción GetRequest, GetNextrequest o setRequest. Esta acción está incluida en la información requerida por el dispositivo objetivo o cualquier indicación de error
- setRequest: Tiene comunicación con el agente SNMP para de esta forma poder modificar el valor de un OID a cierto valor especifico.
- Trap: La acción de captura nos indicará si hay algún problema. Una aplicación SNMP genera solicitudes de entidades de protocolo. Cuando se recibe una

Software Libre

El software respeta la libertad del usuario y de la comunidad, es decir, los usuarios son libres de copiar, modificar, investigar, distribuir y mejorar el software. Con estas libertades, los programadores controlan el comportamiento del programa en lugar de dar a los usuarios un software que no se ajuste a las necesidades de cada uno [7].

Para que un programa se pueda considerar libre debe cumplir ciertos criterios:

- Tener la libertad de ejecutar el programa para realizar cualquier tipo de propósito.
- Que el programa esté disponible para poder estudiarlo y si fuera el caso poder modificarlo para que se comporte de una u otra manera.
- Tener la autorización de redistribuir el programa para las personas que lo necesitan.
- Redistribuir copias que estén modificadas sin tener ningún tipo inconveniente con los desarrolladores.

GNS3

Es una aplicación desarrollada en *Python* y que utiliza la biblioteca *Dynagen* para crear una interfaz gráfica de usuario (GUI). Su propósito general es el de editar archivos de texto.net además de realizar operaciones en un formato CLI que fueron creadas por *Dynagen* y *Dynamips*. Además, tiene la capacidad de emular una computadora [8].

Como se muestra en la Figura 1.3, la combinación de Dynamips-Dynagen-GNS3 crea una plataforma que facilita el diseño de topologías de red complejas, cuando se implementa simplemente arrastrando componentes y dibujando líneas entre enrutadores. Por tanto, GNS3 es muy adecuado para la formación de estudiantes que quieran familiarizarse con los equipos de red [8].

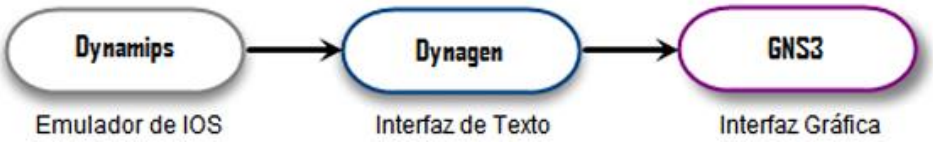

Figura 1.3 Plataforma GNS3 [8]

Las características más importantes que GNS3 posee y que lo convierte en uno de los softwares más utilizando son:

- Su disponibilidad es gratuita y se lo encuentra de manera muy sencilla en el internet.
- No tiene mucha dificultad para su instalación ya que en la descarga del archivo se encuentran todos los programas necesarios.
- Los desarrolladores de esta aplicación están en constante trabajo para brindar a la aplicación actualizaciones y mejoras.
- Permite que exista la comunicación entre una máquina virtual que este corriendo sobre la máquina y de forma sencilla.
- Permite tener una conexión entre los equipos virtuales y el internet.

Ubuntu

Está basado y desarrollado en Debían GNU/Linux y sus objetivos se centran en la facilidad de uso y la libertad de uso. El concepto fundamental de Linux es que todo su código fuente se puede utilizar, modificar y distribuir libremente siempre y cuando se cumplan los términos de la GPL.

Canonical Ltd. es una corporación de carácter privado fundada y financiada por el empresario sudafricano Mark Shuttleworth que promueve la creación de proyectos de software libre. Por tal motivo uno de los proyectos más importantes que se han financiado hasta la fecha es la distribución Debían GNU/Linux donde se basa el sistema operativo Ubuntu. Debían es una distribución de software de Linux basada en el kernel de Linux, que contiene muchos paquetes de software que cumplen las necesidades de los usuarios que utilizan esta distribución, dando como resultado versiones más fáciles de usar como: versión local, versión comercial y la versión más potente para servidores [9].

Zabbix

Zabbix es una herramienta de software libre, que tiene la capacidad de hacer un monitoreo de redes, su diseño cumple funciones tales como consultar y hacer el registro de los estados de servicios de red y cualquier dispositivo que se encuentre conectado a la red.

Para esto usa diferentes tipos de base de datos que se puede usar indistintamente, estas pueden ser: MySQL y PostgreSQL [9].

Para tener una reseña completa de cómo se comporta esta herramienta se tiene las siguientes características:

- La capacidad para monitorear distintos dispositivos es muy alta, y así también rendimiento.
- La monitorización completa de la red se la realiza desde un dispositivo centralizado.
- Su capacidad de analizar los servicios que ofrece es muy alta.
- Tiene la facilidad de que sus agentes, necesarios para la monitorización se pueden instalar en cualquier sistema operativo.
- Usa el protocolo SNMP para realizar los trabajos de monitorización, este protocolo puede ser usado en cualquiera de sus tres versiones.
- El muestreo de los datos se lo realiza con gráficos que puede llegar hacer muy intuitivos.
- Utiliza diferentes tipos de alertas para notificar eventos dentro de la red.
- Se puede realizar configuraciones variadas, que incluyen la creación de plantillas.
- Usa scripts externos.

Principios de funcionamiento de Zabbix

La herramienta está diseñada para ser instalada en diferentes tipos de software, una vez alojada en el sistema operativo que se haya elegido comienza a realizar el trabajo de la recolección de la información. De esta forma se podrá observar toda la información que se esté recolectando en una interfaz web que puede ser modificada de diferentes formas [10].

Zabbix tiene la capacidad de almacenar la información que recibe desde los agentes SNMP de todos los dispositivos de la red, para que por medio de las interfaces graficas con las que cuenta pueda ser analizada por los administradores de red.

Cuando se realiza la instalación de los agentes, estos se vuelven dependientes del servidor, a la espera de ordenes o pedidos que este necesite, por lo que los agentes únicamente envían información que el servidor Zabbix necesita.

2 METODOLOGÍA

Para iniciar con la instalación de Zabbix, se realizó un análisis de las necesidades que necesita la estación o maquina donde se instalara la herramienta, y de esta manera para establecer los requerimientos necesarios que la implementación tanto de Zabbix, como los servicios y máquinas de usuarios puedan funcionar sin inconvenientes y alcanzar todos los objetivos establecidos.

Una vez que se han determinado todos los requerimientos y definir los componentes necesarios que el hardware necesita para realizar la instalación de las máquinas virtuales y del programa de simulación, se determinó los sistemas operativos que correrán en las máquinas virtuales tanto para los servidores como para las máquinas de usuario.

Para la red simulada se utilizó GNS3 que es un software que permite el trabajo en conjunto de máquinas virtuales y equipos de conexión de red. Para el montaje del servidor web se utilizó Apache, se reemplazó el archivo de configuración PHP para tener una página prediseñada, se usó Ubuntu desktop 22.04 como sistema operativo para su instalación. Por otro lado, para el servidor de correo se utilizó Postfix que es el agente necesario para realizar la trasferencia de correo, sirve para enviar y recibir los correos, además de esto se debe instalar Devecot, este servicio permite a los usuarios acceder a correos nuevos con la ayuda de protocolos POP o IMAP. La configuración de dos máquinas cliente, de las cuales en una se instaló Windows 11, y en la otra se usó el sistema operativo Ubuntu 22.04. Finalmente, para la interconexión entre redes se utilizaron 3 routers de la marca Cisco en los cuales se realizó las configuraciones necesarias, tanto en todas sus interfaces como en el protocolo de enrutamiento, OSPF fue el protocolo que se configuro en los dispositivos.

Una vez que se completó la instalación de todos los recursos necesarios para el correcto funcionamiento del sistema y su fin, se llevaron a cabo pruebas donde se puso a prueba tanto servidores, como usuarios y la plataforma Zabbix. Se provocó un error en la red, en donde se apagó el equipo para realizar la simulación de la caída del servidor web, una vez hecho esto se pudo comprobar que la máquina del servicio era inaccesible, la herramienta hizo saltar la alerta en su interfaz principal y la notificación de la alerta se envió por medio de correo a la cuenta configurada.

3 RESULTADOS

3.1 Requerimientos de la herramienta de monitoreo de código abierto

Para establecer los requerimientos que son necesarios para que la herramienta Zabbix pueda funcionar de la mejor manera se tuvo presente la Tabla 3.1, creada a partir de las especificaciones de la página oficial. Por lo tanto, se establece que los requerimientos mínimo necesarios para este trabajo se necesita un procesador que al menos cuente con 2 núcleos y una memoria de 8 (GB).

Tabla 3.1 Características de hardware y software necesarias para el funcionamiento de la herramienta Zabbix dependiente de dispositivos a monitorear [11]

Tamaño de Instalación	Métricas Monitoreadas	Núcleos CPU/vCPU	Memorias (GB)	Base de datos
Pequeño	1.000	2	8	Servidor MySQL, Servidor Percona, Servidor MariaDB, PostgreSQL
Mediano	10.000	4	16	Servidor MySQL, Servidor Percona, Servidor MariaDB, PostgreSQL
Grande	10.0000	16	64	Servidor MySQL, Servidor Percona, Servidor MariaDB, PostgreSQL
Muy grande	1.000.000	32	96	Servidor MySQL, Servidor Percona, Servidor MariaDB, PostgreSQL, Oracle.

La computadora utilizada para hacer la virtualización de la red tiene las siguientes características.

- Intel Core I5 11400f.
- 6 núcleos.
- 32 (GB) de RAM.
- 1 (TB) de espacio en disco duro.
- Sistema Operativo Windows 11 Pro.

Las máquinas virtualizadas son para: servidor web, servidor de correo, cliente Ubuntu, cliente Windows y Zabbix. Todas las virtualizaciones tienen las mismas características, las cuales son:

- 4 (GB) de Ram.
- Hipervisor: *VirtualBox.*

- 25 (GB) de espacio en disco duro.
- 4 núcleos de procesamiento asignados.
- Conexión de red: controlador genérico.

3.2 Definición de los hosts y servicios a monitorear

Para definir todos los servicios y los hosts necesarios en la red, se debe citar la Figura 3.1 que muestra la virtualización de la red en donde se puede observar un servidor de correo, un servidor web, la herramienta Zabbix, un cliente con sistema operativo Ubuntu y un cliente con sistema operativo Windows finalmente 3 routers de la marca Cisco. El enrutamiento utilizado para la red virtualizada fue OSPF.

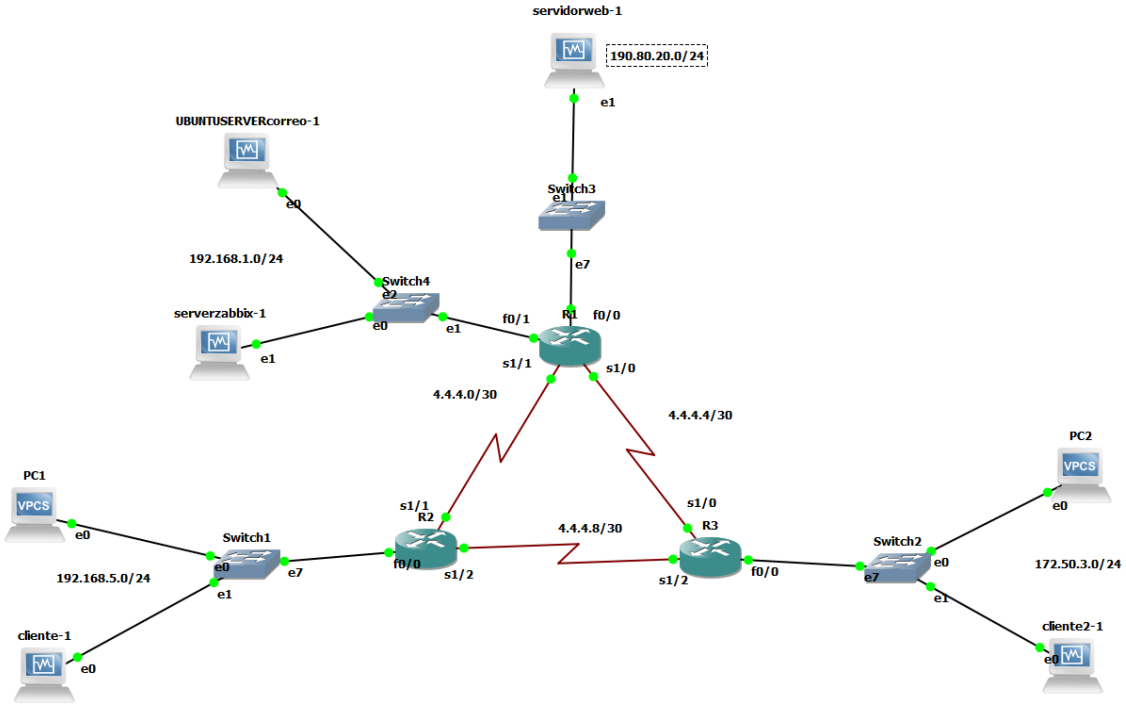

Figura 3.1 Red virtualizada

La **Figura 3.2** representa la porción de red donde se encuentran alojado el usuario, al cual se le instaló el sistema operativo Ubuntu 22.04 y se le asignó la dirección IP 192.168.5.10/24, dentro la red 192.168.5.0/24. Desde este dispositivo se puede ingresar al servidor de correo y web, y lleva instalado un agente Zabbix diseñado para Linux.

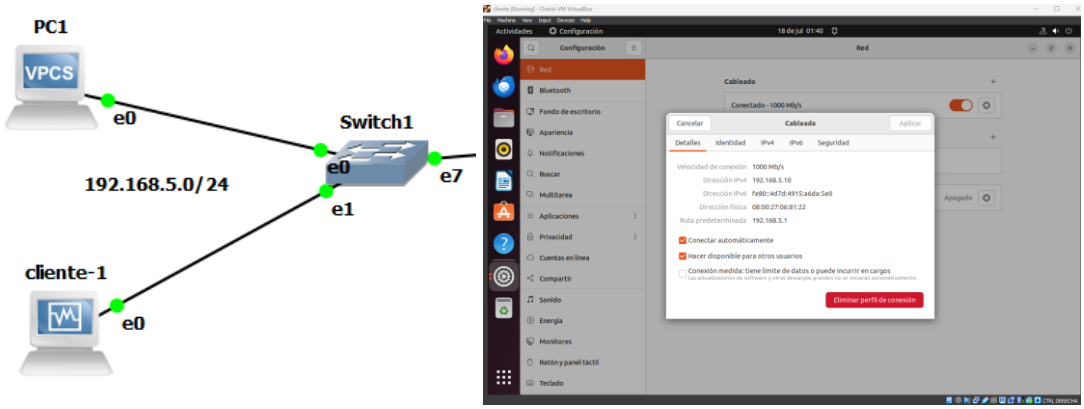

Figura 3.2 Usuario Ubuntu

A la parte de la red que se observa en la **Figura 3.3**, se le instaló el sistema operativo Windows 11, la máquina tiene configurada la dirección IP 172.50.3.10/24. Este host tiene instalado un agente diseñado para Windows que ayuda a Zabbix en su monitoreo.

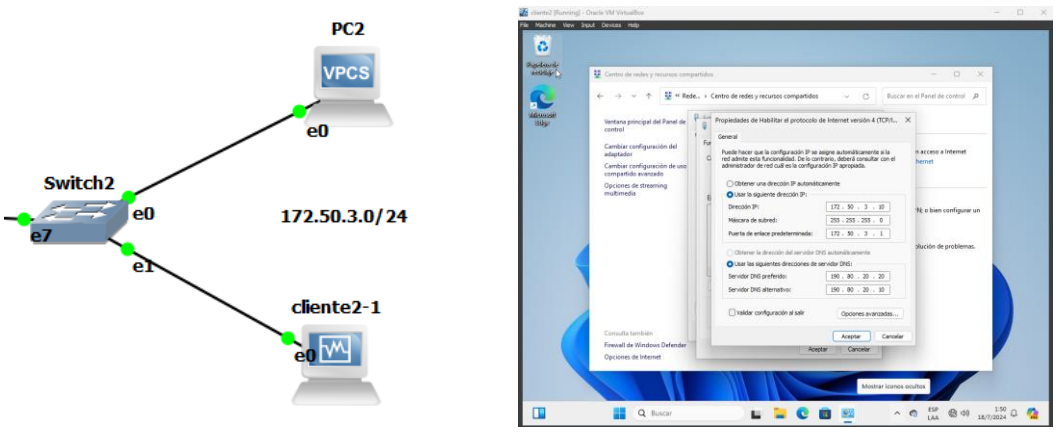

Figura 3.3 Usuario windows

En la Figura 3.4 se muestra una captura de pantalla del servidor Apache implmentado, dicho servidor tiene la dirección IP 192.168.20.10/24, a la cual los usuarios de la red se deben conectar para poder acceder a este servicio.

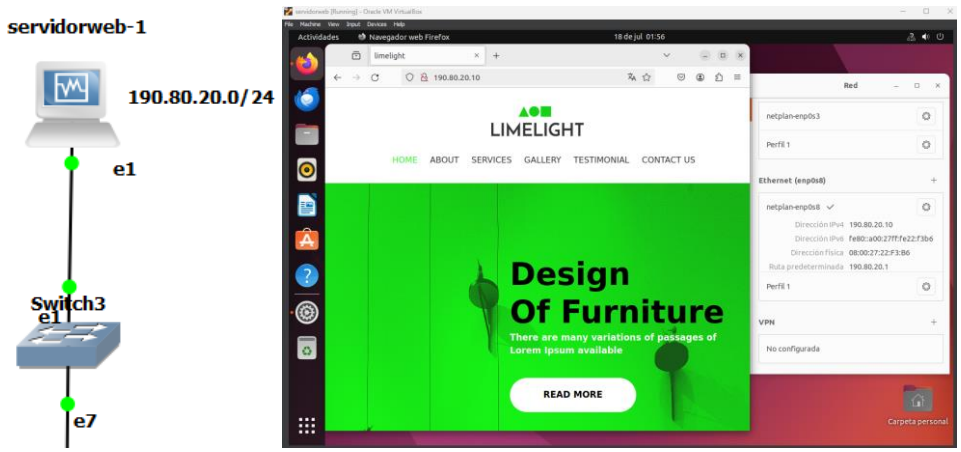

Figura 3.4 Red del servidor web

El servidor de correo y la herramienta Zabbix que se muestra en la Figura 3.5 y la Figura 3.6 se encuentran instalados en la red 192.168.1.0/24. Se designó la dirección 192.168.1.14/24 para el servidor Zabbix y para el servidor el correo se utiliza la dirección 192.168.1.8/24, asignadas estas direcciones los dos dispositivos están listos para que puedan tener interacción con toda la red.

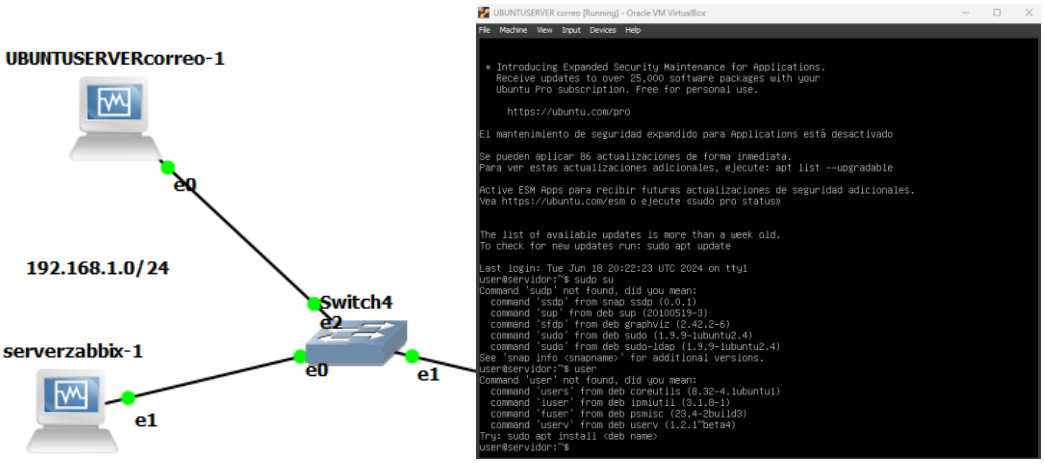

Figura 3.5 Red con el servidor de correo

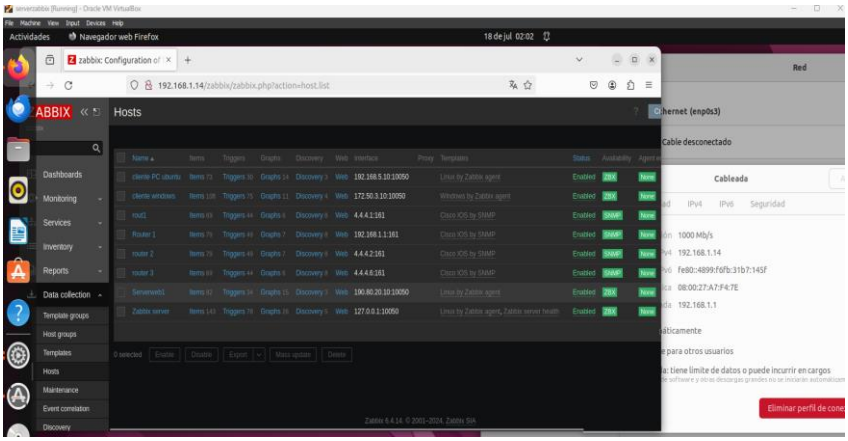

Figura 3.6 Host que contiene Zabbix

Para que todos los dispositivos creados tengan comunicación entre si se realizó la configuración de routers de la Figura 3.7, los routers tienen una configuración OSPF como protocolo de enrutamiento.

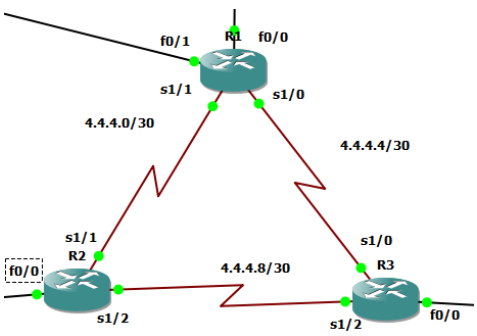

Figura 3.7 Routers de la red virtualizada

3.3 Configuración la herramienta de monitoreo y los *hosts*.

Para este trabajo se realizará la instalación de los hosts en la versión de UBUNTU 22.04 DESKTOP.

Paso 1. Instalación de la máquina virtual

Lo primero que se debe hacer, para realizar la instalación del servidor, es tener una máquina virtual activa y corriendo en la maquina física, para lo cual se hizo uso de programas de virtualización, en este caso se utilizó VirtualBox y las características que tendrá esta máquina virtual y como muestra la Figura 3.8, serán los siguientes: 4 (GB) de RAM y se usarán 4 procesadores recursos que serán utilizados desde la maquina física.

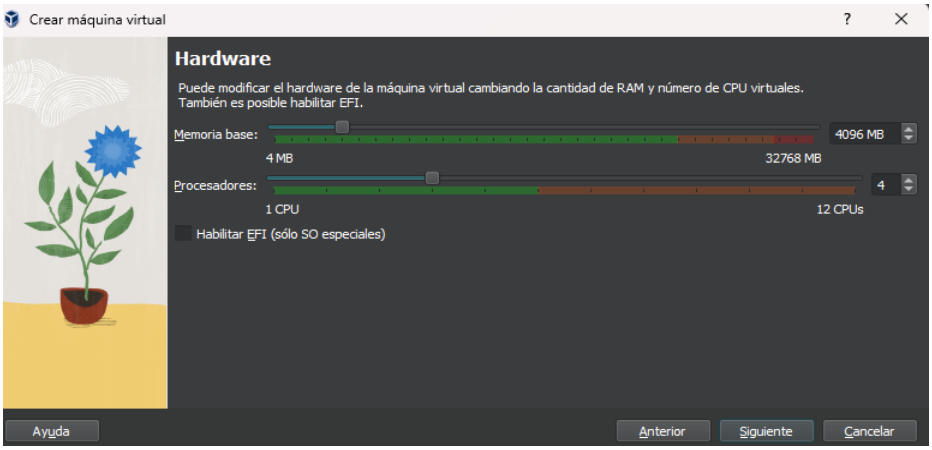

Figura 3.8 Asignación de memoria RAM y procesadores

El tamaño necesario del disco duro que se utilizará para alojar Zabbix será de 25 (GB), este espacio se usó tomando como referencia el espacio libre que se tiene en el disco duro principal, además de las maquinas necesarias para todas las maquinas. Este espacio se tendrá instalado en la computadora donde está instalado el servidor, por lo que se debe tomar en cuenta el espacio libre que se tenga disponible, la Figura 3.9 muestra el paso donde se le asigna el espacio de disco a la máquina virtual.

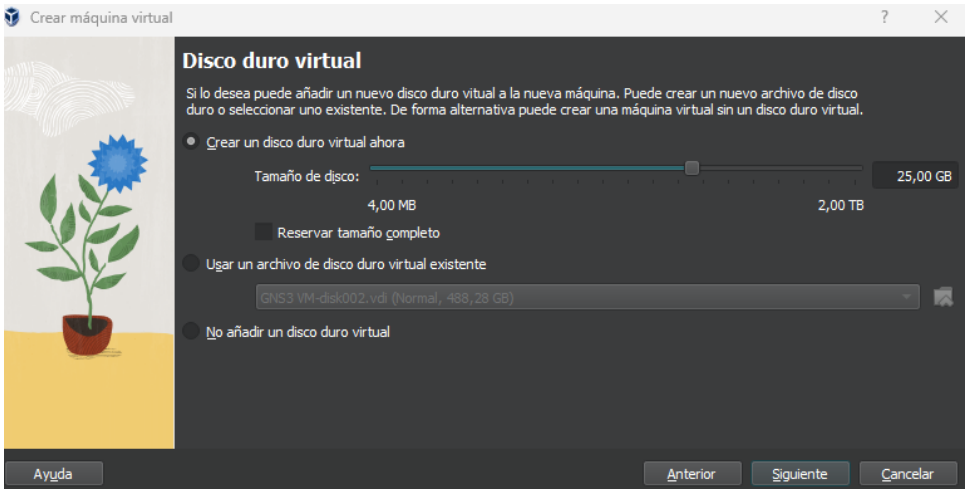

Figura 3.9 Asignación de espacio en disco duro

Finalmente, la Figura 3.10 indica una pantalla en donde muestra una última vez las características que tendrá la máquina virtual que se ha creado y en la que se alojara el servidor Zabbix.

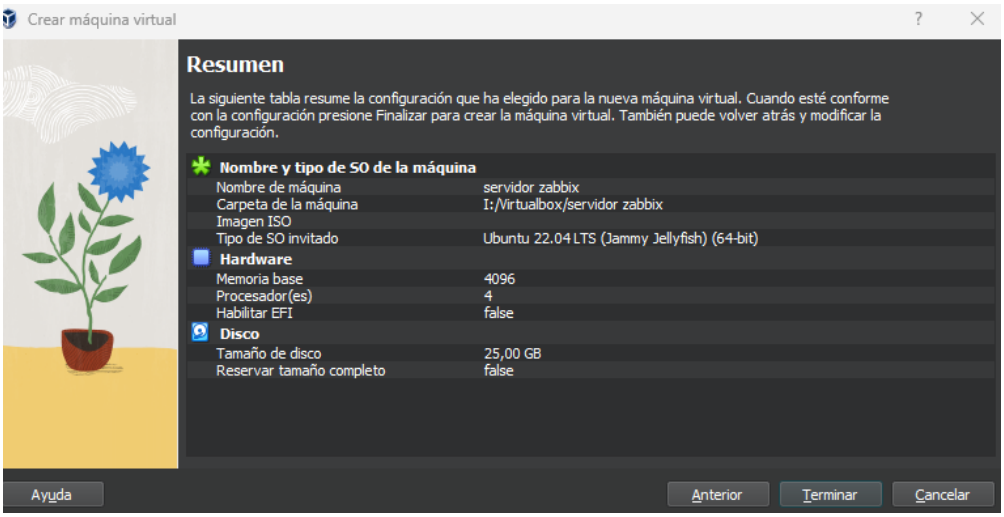

Figura 3.10 Características finales de la máquina virtual

Paso 2. Instalación del servidor Zabbix

Instalación del repositorio de Zabbix

Para comenzar con la instalación del servidor es necesario visitar la página oficial que se ilustra en la Figura 3.11, en donde se seleccionó la versión de Zabbix que se desea instalar, el sistema operativo en el cual se va a realizar la instalación y las diferentes características necesarias para el funcionamiento correcto del servidor. Para este caso se utilizó una base de datos basada en MySQL y el servidor web utilizando Apache.

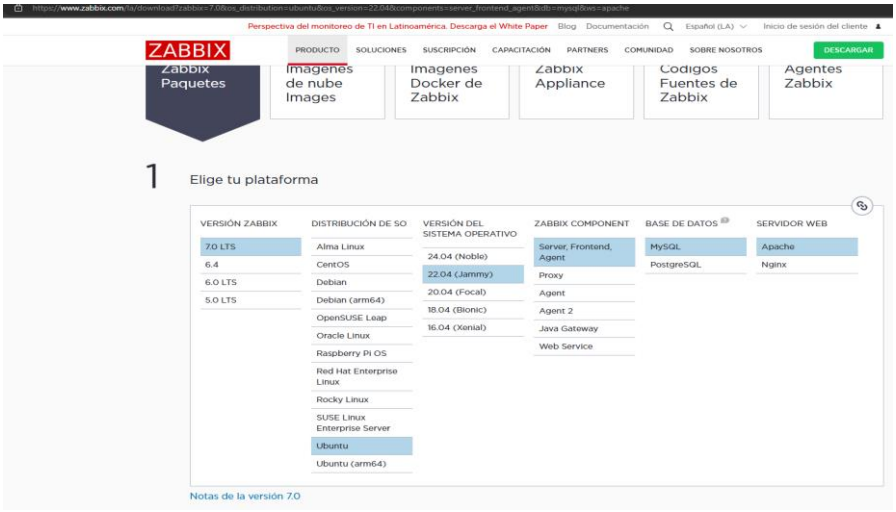

Figura 3.11 Elección de la plataforma y características a instalar [11]

En las siguientes 3 Figuras se indica cómo se instaló el repositorio de Zabbix siguiendo los pasos que la página principal indica.

Las instrucciones que se encuentran en la Figura 3.12 son las necesarias para realizar la instalación del repositorio de Zabbix.

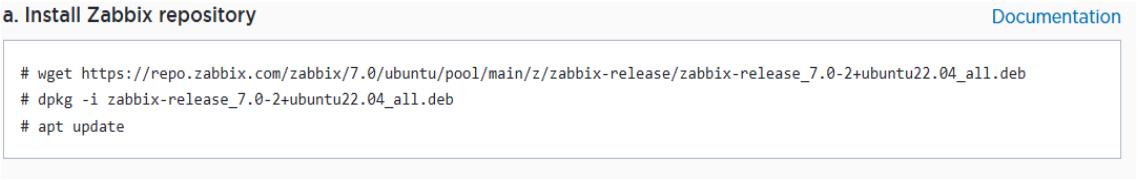

Figura 3.12 Instrucciones para instalar paquetes [11]

Al momento de ingresar cada instrucción en el terminal de Ubuntu, se puede observar en las Figura 3.13 y Figura 3.14 el procedimiento que realizar el sistema operativo para realizar la instalación de los paquetes.

Figura 3.13 Proceso de instalación de paquetes

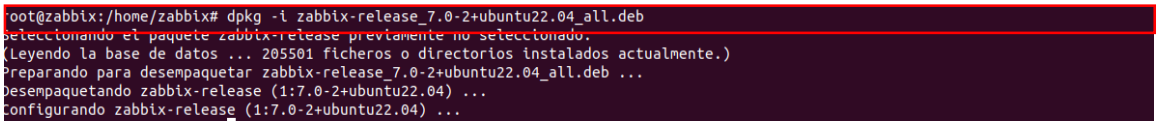

Figura 3.14 Instalación del zabbix-release

Instalación del servidor y sus dependencias

En el siguiente paso lo que se realiza es la instalación del servidor, la interfaz web y el agente de Zabbix que ayudara a la recolección de datos del servidor. Para ellos se debio hacer uso de la instrucción que indica la Figura 3.15.

b. Install Zabbix server, frontend, agent

```
# apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent
```

Figura 3.15 Instrucciones para la instalación de Zabbix *server*, *agent* y *scripts* [11]

Una vez ingresada la línea de código se deberá aceptar las condiciones de instalación requeridas, como lo muestra la Figura 3.16, para comenzar la instalación de todas las características que Zabbix necesita.

```
root@zabbix:/home/zabbix# apt install zabbix-server-mysql zabbix-frontend-php zabbix-agent
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
  libwpe-1.0-1 libwpebackend-fdo-1.0-1
Utilice «sudo apt autoremove» para eliminarlos.
Se instalarán los siguientes paquetes adicionales:
  apache2 apache2-bin apache2-data apache2-utils default-mysql-server fping libaio1 libapache2-mod-php8.1 libapr1 libaprutil1
  libaprutil1-dbd-sqlite3 libaprutil1-ldap libblas3 libcgi-fast-perl libcgi-pm-perl libevent-core-2.1-7 libevent-pthreads-2.1-7
  libfcgi-bin libfcgi-perl libfcgi0ldbl libhtml-template-perl liblinear4 libmecab2 libmysqlclient21 libodbc1 libodbc2 libodbccr2
  libonig5 libopenipmi0 libpq5 libprotobuf-lite23 libssh2-1 lua-lpeg mecab-ipadic mecab-ipadic-utf8 mecab-utils mysql-client-8.0
  mysql-client-core-8.0 mysql-common mysql-server-8.0 mysql-server-core-8.0 nmap nmap-common php php-bcmath php-common php-gd
  php-ldap php-mbstring php-pgsql php-xml php8.1 php8.1-bcmath php8.1-cli php8.1-common php8.1-gd php8.1-ldap php8.1-mbstring
  php8.1-opcache php8.1-pgsql php8.1-readline php8.1-xml snmpd traceroute
Paquetes sugeridos:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom php-pear libipc-sharedcache-perl liblinear-tools liblinear-dev
  odbc-postgresql tdsodbc mailx tinyca ncat ndiff zenmap snmptrapd snmp-mibs-downloader
Se instalarán los siguientes paquetes NUEVOS:
  apache2 apache2-bin apache2-data apache2-utils default-mysql-server fping libaio1 libapache2-mod-php8.1 libapr1 libaprutil1
  libaprutil1-dbd-sqlite3 libaprutil1-ldap libblas3 libcgi-fast-perl libcgi-pm-perl libevent-core-2.1-7 libevent-pthreads-2.1-7
  libfcgi-bin libfcgi-perl libfcgi0ldbl libhtml-template-perl liblinear4 libmecab2 libmysqlclient21 libodbc1 libodbc2 libodbccr2
  libonig5 libopenipmi0 libpq5 libprotobuf-lite23 libssh2-1 lua-lpeg mecab-ipadic mecab-ipadic-utf8 mecab-utils mysql-client-8.0
  mysql-client-core-8.0 mysql-common mysql-server-8.0 mysql-server-core-8.0 nmap nmap-common php php-bcmath php-common php-gd
  php-ldap php-mbstring php-pgsql php-xml php8.1 php8.1-bcmath php8.1-cli php8.1-common php8.1-gd php8.1-ldap php8.1-mbstring
  php8.1-opcache php8.1-pgsql php8.1-readline php8.1-xml snmpd traceroute zabbix-agent zabbix-frontend-php zabbix-server-mysql
0 actualizados, 67 nuevos se instalarán, 0 para eliminar y 5 no actualizados.
Se necesita descargar 61,0 MB de archivos.
Se utilizarán 364 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n]
```

Figura 3.16 Indica que la ejecución de las instrucciones

Cuando la instalación haya terminado se deberá revisar el estado del servidor, para asegurarse que este este activo. La Figura 3.17 muestra que el servicio de Zabbix no está activo.

```
root@zabbix: /home/zabbix
root@zabbix:/home/zabbix# systemctl status zabbix-server.service
○ zabbix-server.service - Zabbix Server (MySQL/MariaDB)
     Loaded: loaded (/lib/systemd/system/zabbix-server.service; enabled; vendor preset: enabled)
     Active: inactive (dead)
       Docs: man:zabbix_server
```

Figura 3.17 Muestra el estado de la herramienta que esta inactiva

Para activar el servicio de Zabbix se deberá ingresar la instrucción que se encuentra en la Figura 3.18, además se muestra que se realizó otra vez la consulta, y se comprobó que después de haber ingresado la instrucción de activación, este está corriendo sin ningún inconveniente.

Figura 3.18 Activación de los servicios

Instalación de la base de datos basada en MySQL

En este paso se debe realizar la instalación de la base de datos basada en MySQL, para lo cual se debió ingresar la instrucción que se encuentra en la Figura 3.19 para instalar el servicio. Una vez ingresada la instrucción comenzara el proceso de instalación como lo muestra, esta base de datos sirve para proporcionar a la herramienta la información necesaria para su funcionamiento.

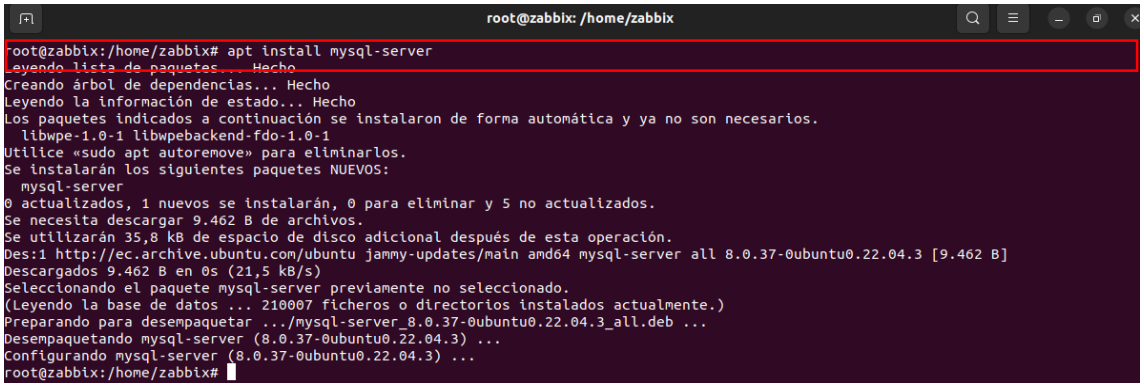

Figura 3.19 Proceso de la instalación de server MySQL

Una vez que el proceso de instalación haya terminado, se debió seguir los pasos que se muestran en la Figura 3.20, estas instrucciones se encuentran en la página, y sirven para realizar una configuración correcta de la base de datos que estará orientada a Zabbix.

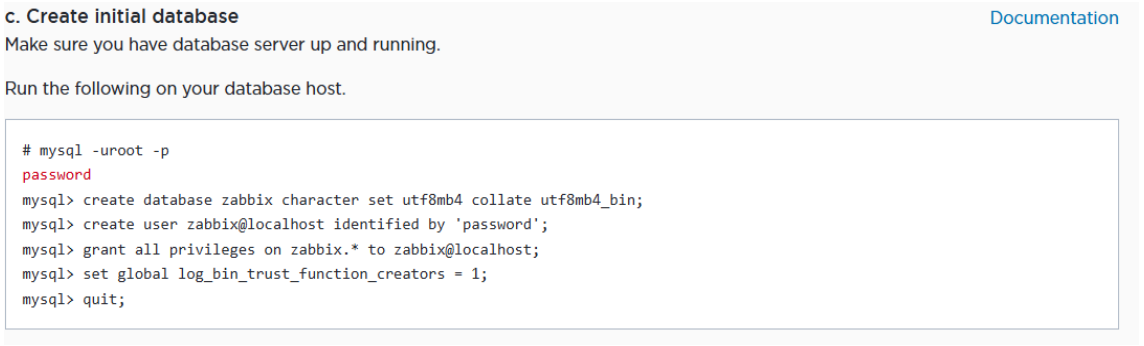

Figura 3.20 Secuencia de instrucciones para la configuración de MySQL [11]

Como casi en todo el procedimiento solo se debe copiar y pegar la mayoría de instrucciones que la página indica, pero en este punto lo más relevante es el segundo paso, donde se tuvo que seleccionar una contraseña; para este trabajo la contraseña elegida es “tesis2024”. La Figura 3.21 ilustra el paso a paso de las instrucciones ingresadas.

```
root@zabbix:/home/zabbix# mysql
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 41
Server version: 8.0.37-0ubuntu0.22.04.3 (Ubuntu)

Copyright (c) 2000, 2024, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> create database zabbix character set utf8mb4 collate utf8mb4_bin;
Query OK, 1 row affected (0,02 sec)

mysql> create user zabbix@localhost identified by 'tesis2024';
Query OK, 0 rows affected (0,04 sec)

mysql> grant all privileges on zabbix.* to zabbix@localhost;
Query OK, 0 rows affected (0,01 sec)

mysql> grant all privileges on zabbix.* to zabbix@localhost;
Query OK, 0 rows affected (0,01 sec)
```

Figura 3.21 Cambio de contraseña

Usando el comando *show databases* apareció una tabla que representa las bases de datos que se instalaron, esta tabla se observa en la Figura 3.22, donde se puede notar el nombre de todas las bases de datos creadas, sin embargo, la de Zabbix es la importante en este documento.

```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| sys                |
| zabbix             |
+--------------------+
5 rows in set (0,01 sec)

mysql>
```

Figura 3.22 Bases de datos

Para que se importe el esquema de la base de datos de Zabbix se debe ingresar la instrucción que se detalla en la Figura 3.23.

On Zabbix server host import initial schema and data. You will be prompted to enter your newly created password.

```
# zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz | mysql --default-character-set=utf8mb4 -uzabbix -p zabbix
```

Figura 3.23 Instrucciones para la importación de esquemas [11]

Una vez se ingresó la instrucción que se detalla en el paso anterior se debió esperar unos segundos, pasado este tiempo se solicitó el ingreso de la clave que se ingresó en

la configuración de la base de datos. Cuando la contraseña se haya registrado de forma correcta el programa continuara sin ningún problema como se observa en la Figura 3.24.

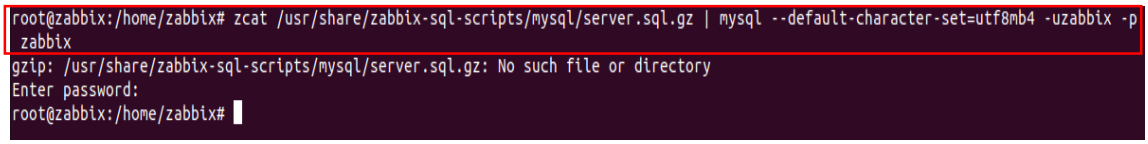

Figura 3.24 Sincronización de Zabbix con la base de datos

Finalmente, se deberá ingresar una instrucción más, que es necesaria para la comparación de funciones creadas, estas instrucciones se las puede observar en la Figura 3.25.

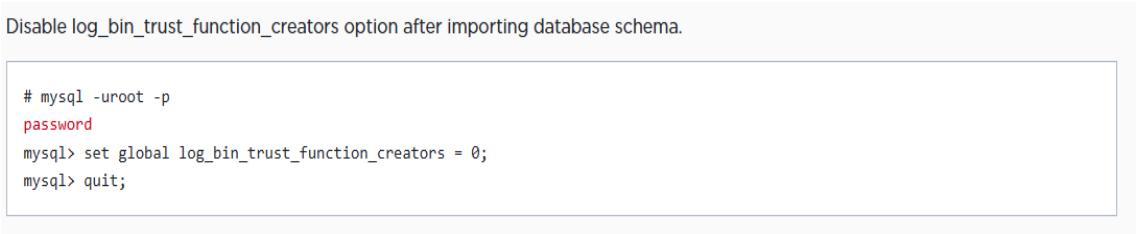

Figura 3.25 Deshabilita la función después de importar la base de datos [11]

La Figura 3.26 representa los últimos pasos que se realizan para terminar con la instalación de la base de datos.

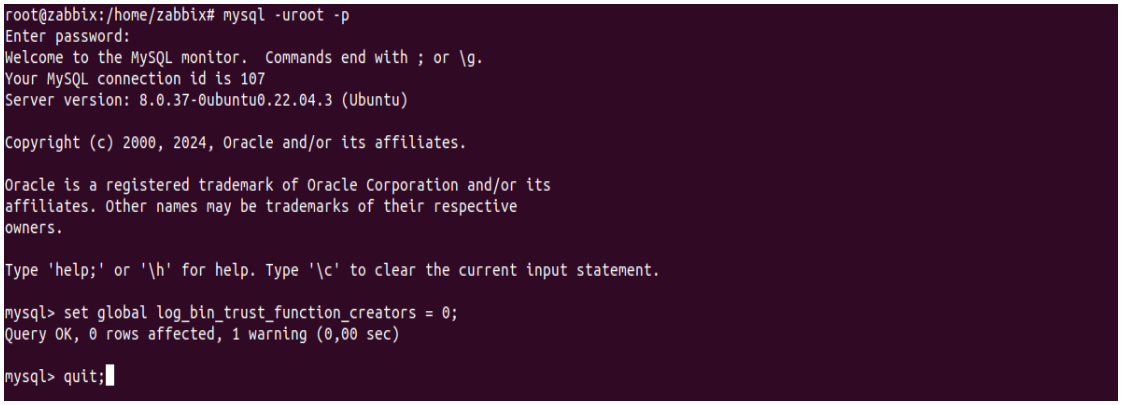

Figura 3.26 Procedimiento final de la instalación de la base de datos

Habilitación para el uso de datos

Para que la base datos quede activa y pueda tener comunicación con todos los archivos de Zabbix, se deberá seguir una serie de pasos en los que se tiene que ingresar la clave que anteriormente se configuró la base de datos MySQL en el archivo nano /etc/zabbix/zabbix_server.conf y modificando la línea de código que muestra la Figura 3.27.

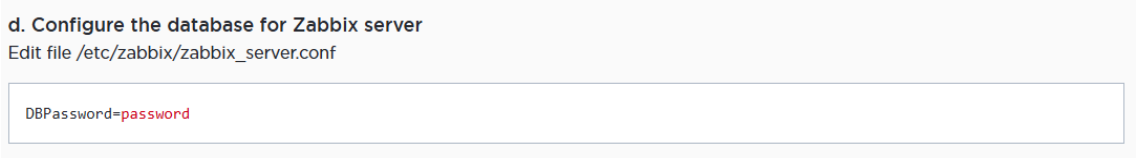

Figura 3.27 Modificación de la clave de la base de datos [11]

En la Figura 3.28 se puede ver como se ingresó al archivo para poder editar la línea de código que se indica anteriormente.

Figura 3.28 Dirección del archivo donde se va a modificar la línea de código

Para que todos los archivos instalados y modificados se pongan en marcha, se debió resetear el servidor, el agente y Apache2, para ello se debió ingresar las secuencias de código que se muestran en la Figura 3.29.

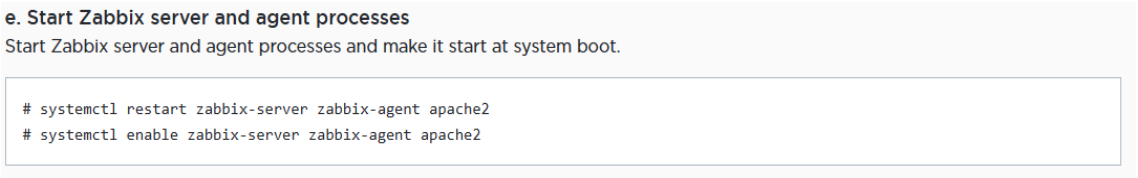

Figura 3.29 Código para reiniciar servicios [11]

Finalmente, la Figura 30 indica como el software realiza las acciones de reiniciar los servicios y activar el agente y servidor.

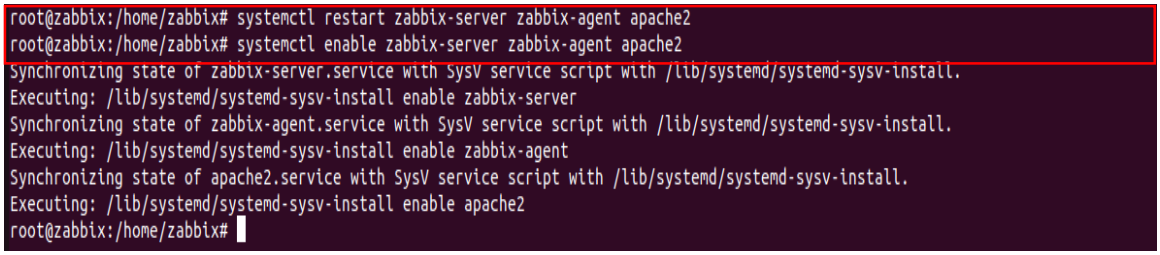

Figura 30 Habilitación del agente y del servidor

Configuración de la interfaz web gráfica del servidor

Para ingresar a esta sección fue necesario utilizar el siguiente enlace http://host/zabbix, es importante conocer la dirección IP de la maquina donde se encuentra alojada la herramienta. Para este trabajo la dirección IP de la máquina virtual es la 192.168.1.14, por lo tanto, el enlace de ingreso a la interfaz es http://192.168.1.14/zabbix. La ventana se muestra en la Figura 3.31.

Figura 3.31 Muestra la interfaz de bienvenida a el servidor

La Figura 3.32 muestra la verificación de requisitos previos, si todo esta correcto se podrá continuar con la instalación.

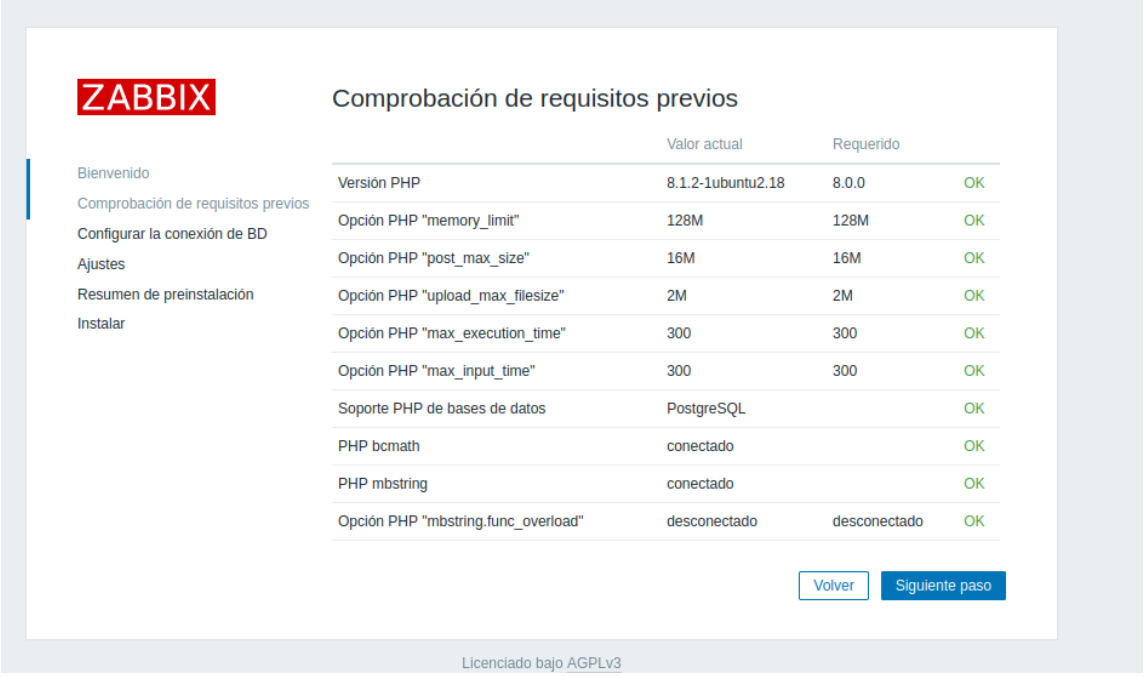

Figura 3.32 Verificación de requisitos

En el siguiente paso, que se encuentra en la Figura 3.33, fue la configuración del servidor con la base de datos que se creó, donde se verificó todas las configuraciones realizadas donde los parámetros más importantes es el nombre de la base de datos, el nombre del usuario y la contraseña creada.

Figura 3.33 Verificación de la configuración de la base de datos

Para obtener una sincronización correcta entre las alertas, los dispositivos y Zabbix, es importante tener la misma zona horaria en todo el sistema por lo tanto asegurar que esta opción este correcta es fundamental, también se puede configurar el tema que la aplicación llevara, se seleccionó la opción de oscuro. Esta configuración se encuentra en la Figura 3.34.

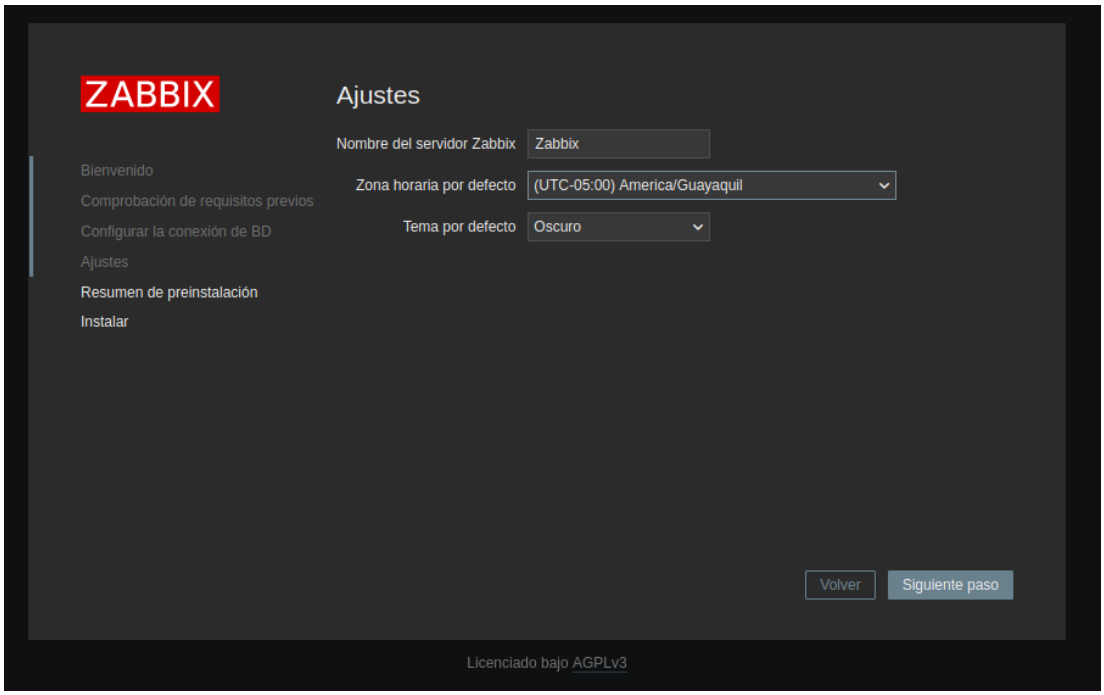

Figura 3.34 Zona horaria para la sincronización

La información que se hace presente en la Figura 3.35 presenta toda la información que la cual se proporcionó en pasos anteriores para realizar la instalación de la herramienta,

esta ventana es importante ya que confirmará por última vez que los datos que se muestran son los correctos.

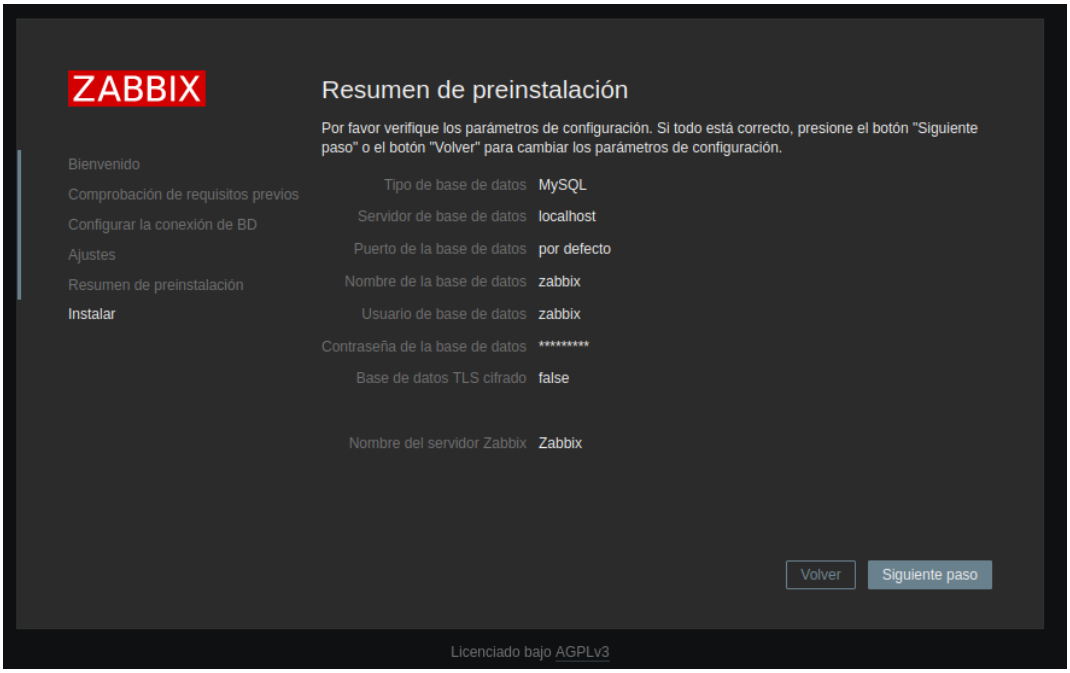

Figura 3.35 Resumen de toda la configuración

Al realizar todos estos pasos de manera correcta se llegó a la ventana que se puede observar en la Figura 3.36, indicando que se ha tenido éxito en la instalación y que Zabbix está listo para ser configurado y usado.

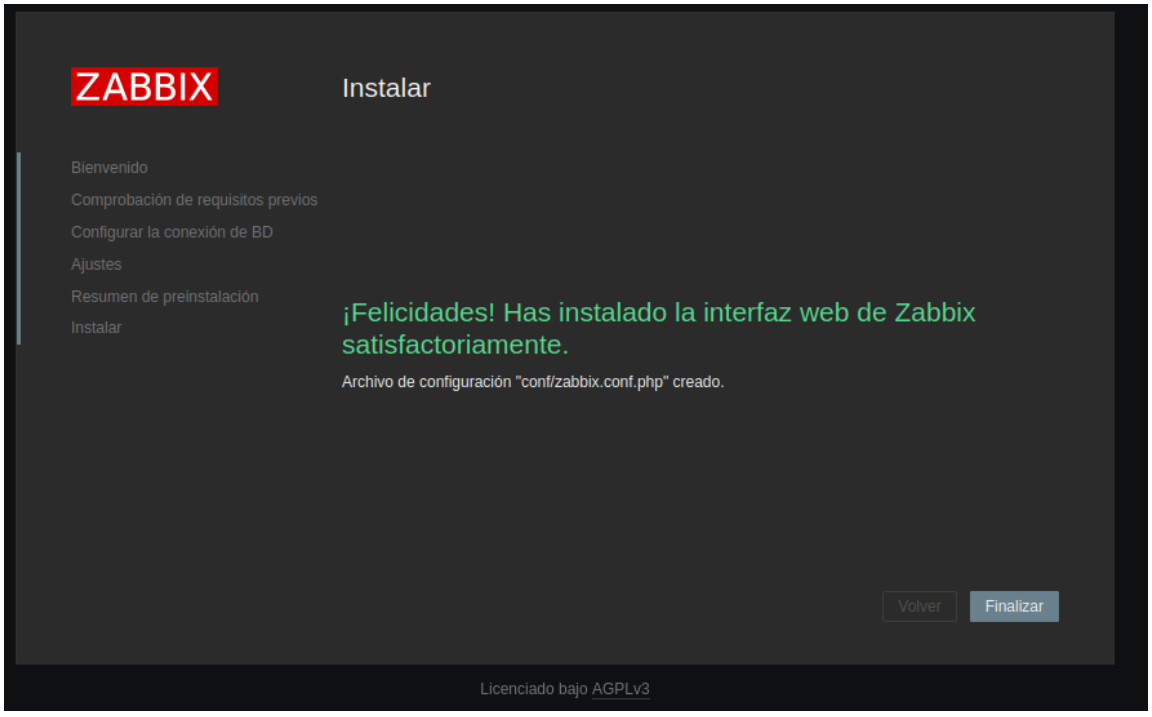

Figura 3.36 Confirmación de instalación exitosa

Una vez que la instalación se haya terminado, saltó una ventana se representa en la Figura 3.37 de inicio de sesión automáticamente y en ella se debió ingresar un usuario y una contraseña. Por default el usuario será Admin y la contraseña Zabbix.

Figura 3.37 Interfaz de inicio de sesión

Finalmente se pudo observar la interfaz web de la herramienta como lo muestra la Figura 3.38, donde se encuentra el panel de control principal, de esta forma el servidor quedo listo para hacer uso de los componentes para el monitoreo de red.

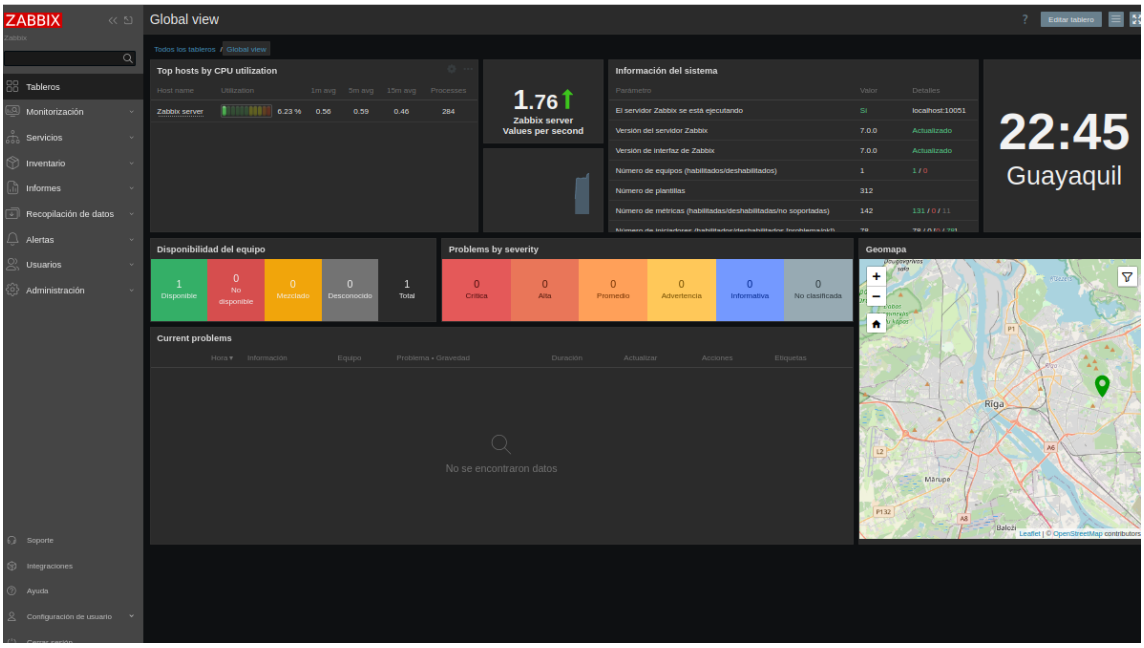

Figura 3.38 Interfaz web de la herramienta Zabbix

Paso 3. Configuración de los dispositivos

La Figura 3.39 presenta la pantalla de la herramienta donde se puede observar todos los dispositivos agregados y donde se puede ingresar más. Cuando se va a agregar uno de estos se debe dirigir a la parte derecha de la pantalla y en la opción *Monitoring* se debe elegir la opción *de Host. Create Host* que se encuentra en la parte superior

derecha, es la opción para ingresar toda la información para agregar un nuevo dispositivo.

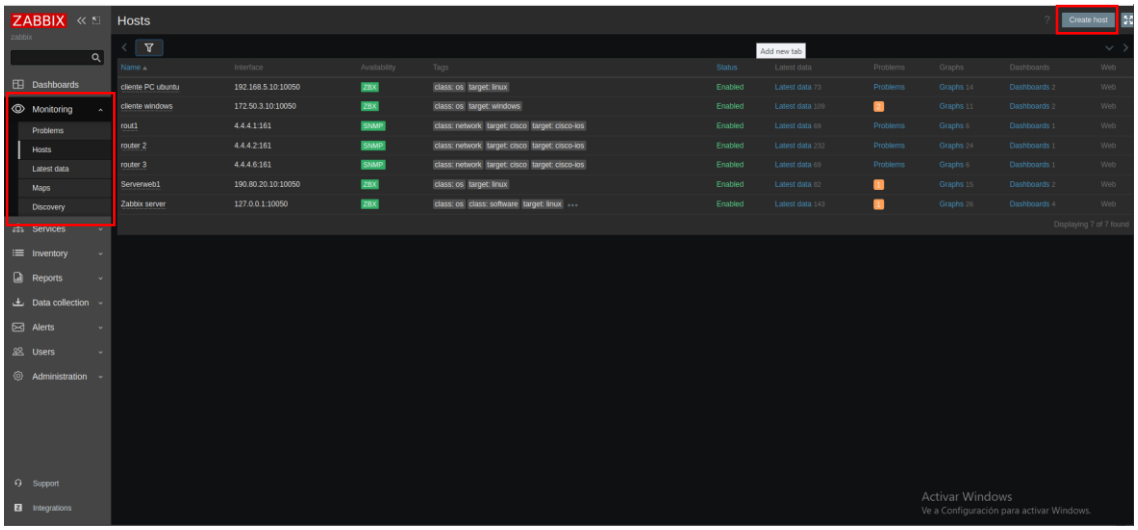

Figura 3.39 Pantalla de administración de host

La Figura 3.40 muestra la pantalla en donde se debe ingresar la información necesaria para agregar dispositivos, las dos primeras opciones que se encuentran en esta pantalla sirven para darle un nombre al dispositivo, para distinguirlo de entre todos los que se vaya agregar.

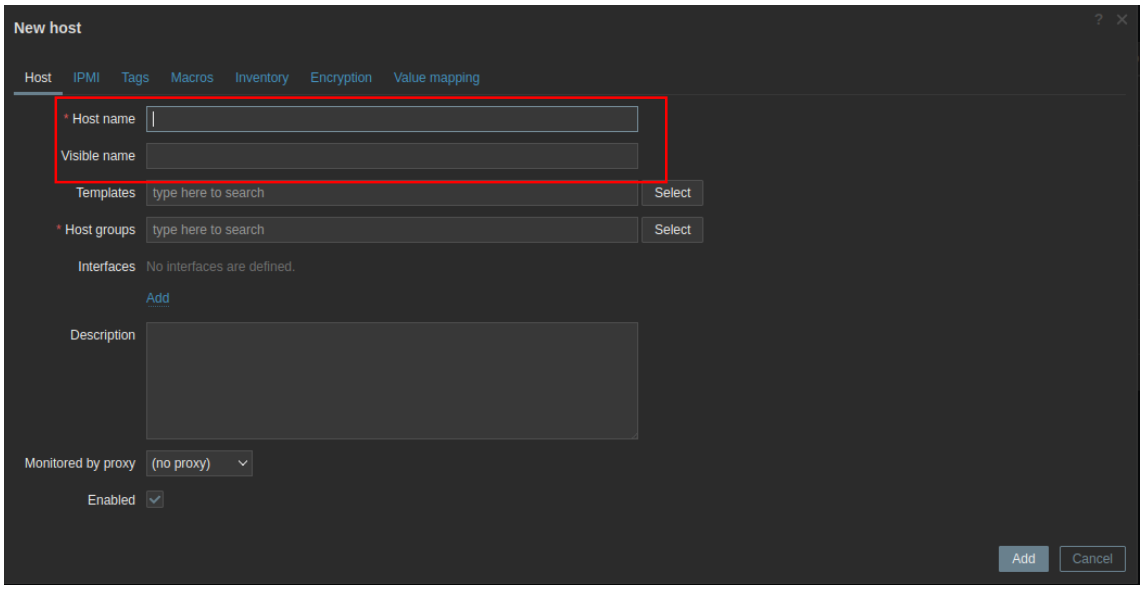

Figura 3.40 Ventana para ingresar dispositivos

La siguiente opción que se debe modificar es *Template*, esta sección es donde se debe elegir que dispositivo se va a ingresar, el criterio para elegirlo se basa en cómo trabaja y para qué sirve, todas las opciones llevan un nombre asociado Figura 3.41.

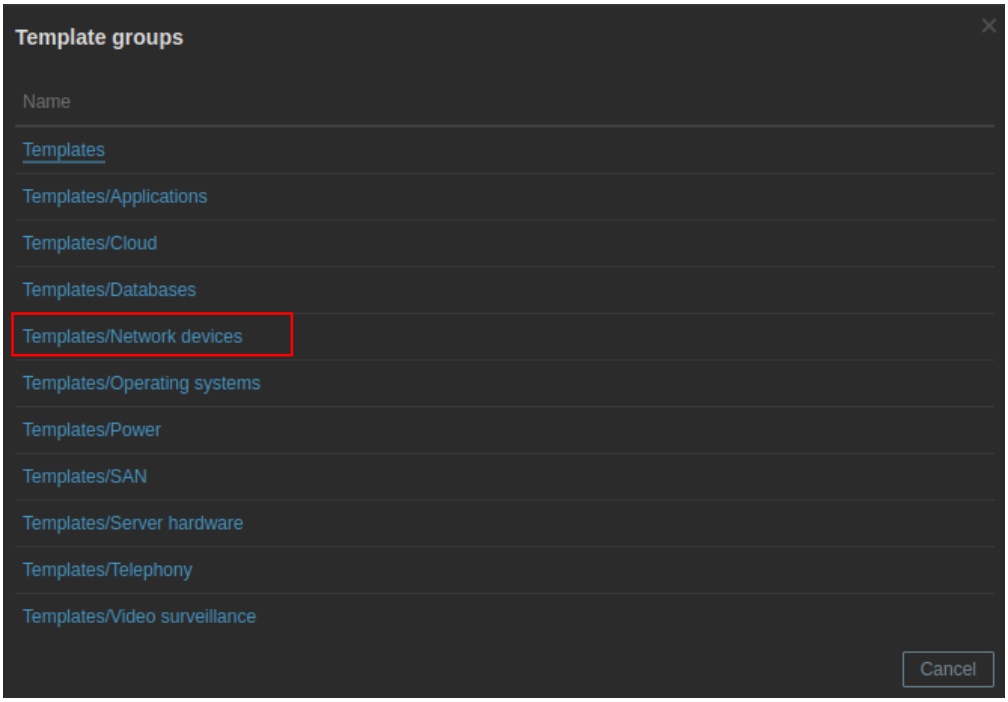

Figura 3.41 Selección de Template

El *Template* es importante elegirlo de manera correcta, ya que de esta selección depende el funcionamiento del dispositivo que se va a ingresar, para esta sección se va a ingresar un router de la marca Cisco y que trabaja con el protocolo SNMP, por ello se selecciona la opción *CISCO IOS by SNMP,* esto se aprecia en la Figura 3.42.

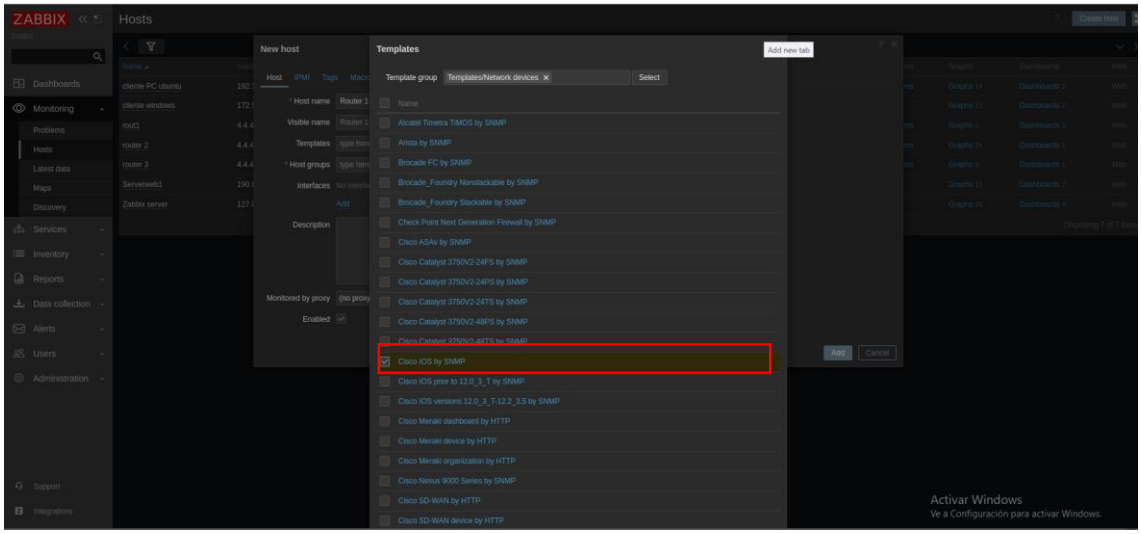

Figura 3.42 Selección de *Template* del dispositivo

La opción de *Host Groups* es donde se puede hacer una segmentación de los dispositivos, es decir que da la opción de realizar grupos de equipos usando cualquier criterio, ya sea por marca o por forma de trabajo. Como se puede hacer esta selección se indica en la Figura 3.43.

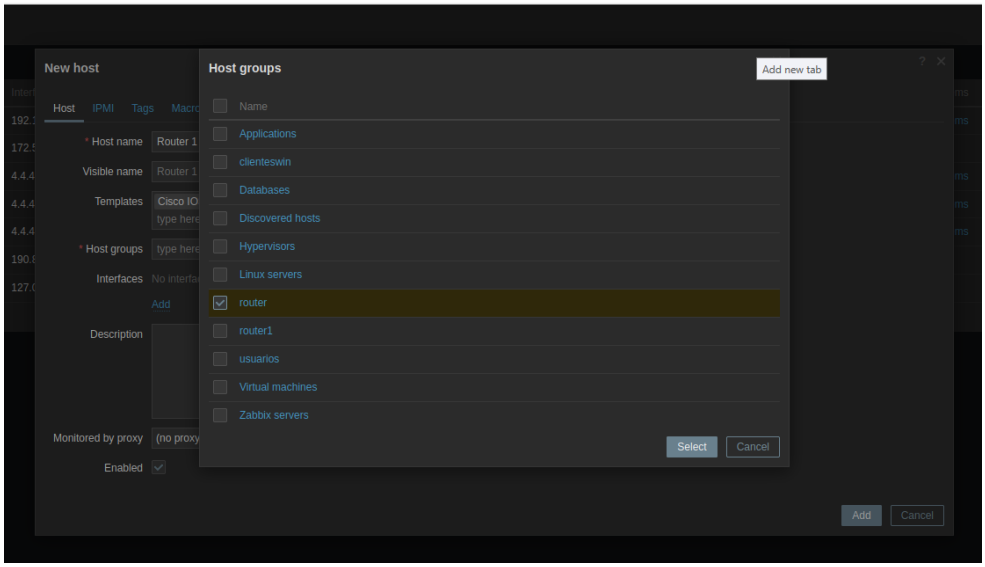

Figura 3.43 Grupos de dispositivos segmentados

Una vez realizadas las configuraciones anteriores se debe pasar a un último paso en esta ventana, la sección que se encuentra resaltada en la Figura 3.44, es donde se debe elegir como el dispositivo va a realizar el intercambio de información con Zabbix, las opciones más comunes a ser elegidas don: un agente o el protocolo SNMP; para este paso se eligió el protocolo SNMP.

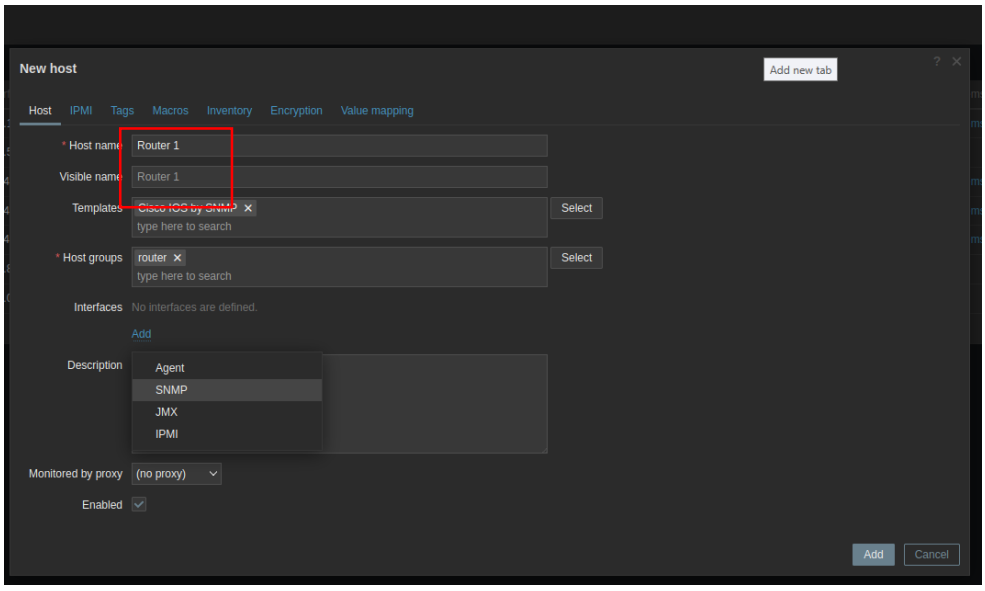

Figura 3.44 Opciones del tipo de monitoreo

Cuando en la herramienta se elige el protocolo SNMP se debió configurar algunas opciones extras, tales como: comunidad, versión del protocolo, dirección IP vinculada al dispositivo. En la Figura 3.45 se puede observar que la IP es la 192.168.1.1 para una de las interfaces *Fast Ethernet* configuradas al router.

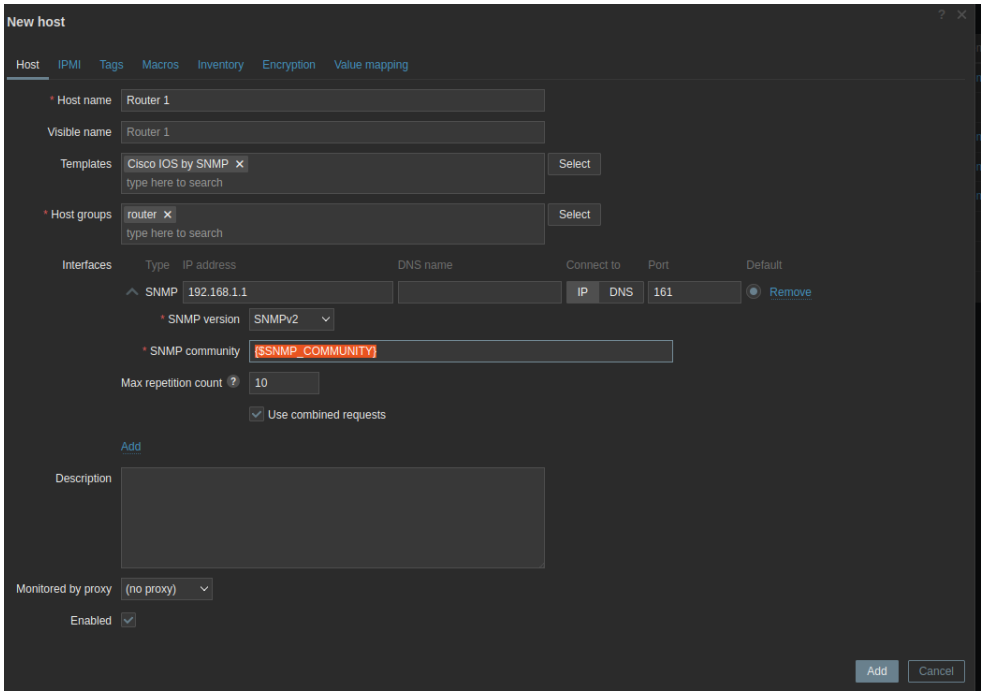

Figura 3.45 Configuración final del host

Los parámetros que se configuraron en el router son los que se muestran en la Figura 3.46, donde los parámetros que se ingresaron son el nombre de la comunidad que es *tesis2024,* la versión *2 y* la dirección IP de la maquina donde se encuentra instalado Zabbix.

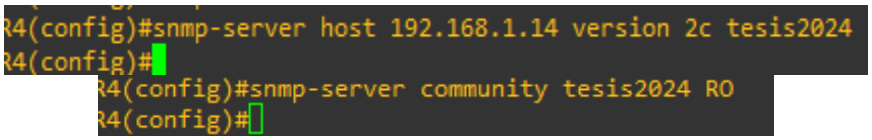

Figura 3.46 Configuración SNMP en el router

De la ventana anterior se debe realizar una copia de la opción *SNMP Community* y pegarlo en la versión *MACRO*, como se puede observar en la Figura 3.47. En la sección de *VALUE* se debe especificar el nombre de la comunidad que se eligió y se configuro en el router.

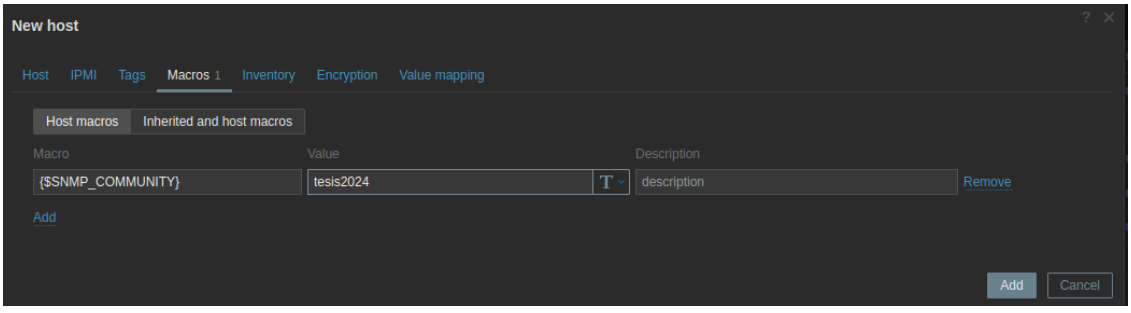

Figura 3.47 Configuración de la comunidad

Inmediatamente después de terminar con la instalación del dispositivo, la ventana donde se encuentran todos los hosts se puede observar que se agregó al router Figura 3.48, pero aún este no se encuentra activo observar la columna *AVAILABILITY* en la que se muestra que el dispositivo no se encuentra activo, ya que el icono que indica que el protocolo SNMP aún no está activado.

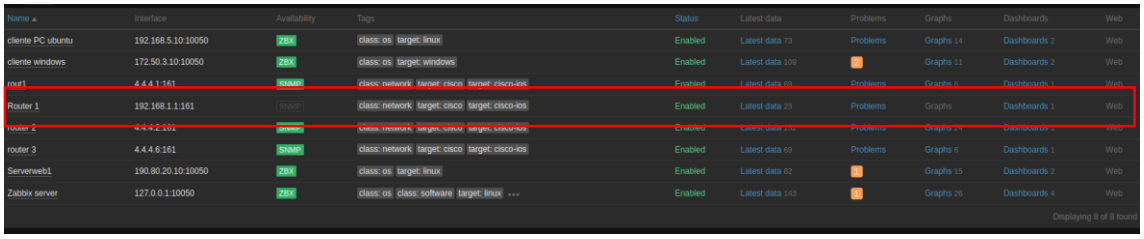

Figura 3.48 Equipo agregado

Después de unos minutos se puede observar que ya se activó el protocolo como lo indica la **Figura 3.49**, la muestra de esto es que el icono cambio su color a verde.

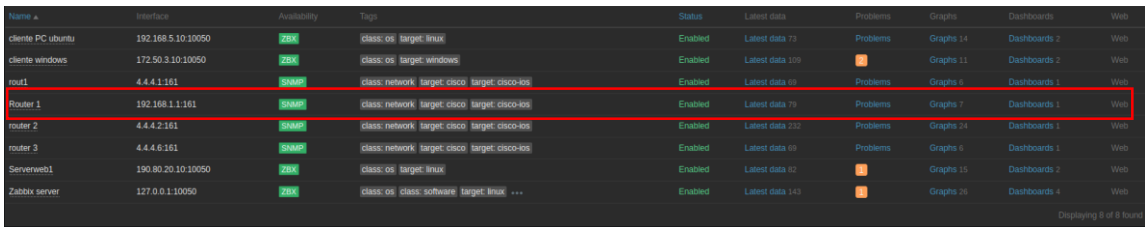

Figura 3.49 Router activado

Para realizar el monitoreo en una maquina donde se encuentra un sistema operativo más convencional se puede usar el agente de Zabbix para este caso se usó el diseñado para Windows, para obtenerlo se debe dirigirse a la página web principal de agentes Zabbix, como se muestra en la Figura 3.50, aquí se debió elegir el sistema operativo, y los parámetros que corresponden para su correcto funcionamiento, la versión recomendada es *Zabbix agent 2 v7.0.0.*

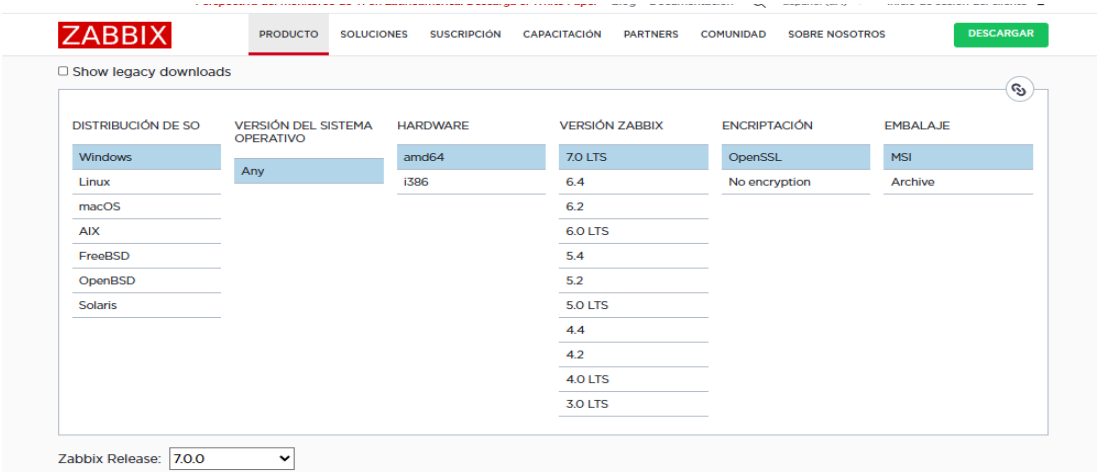

Figura 3.50 Página oficial para descargar el agente de Windows

Cuando se ejecuta el archivo descargado saltó la ventana de la Figura 3.51, que indica el comienzo de la instalación el agente, para los siguientes pasos solo se debe saltar hasta llegar a la ventana final ya que no conllevan ninguna configuración extra.

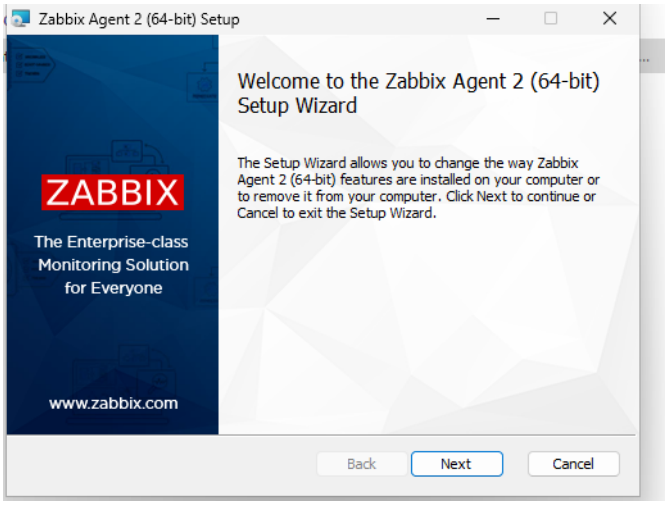

Figura 3.51 Instalación del Agente

Al finalizar la instalación del agente se deberá comprobar que este este activo y ejecutándose, la Figura 3.52 muestra la pantalla de todos los servicios que corren sobre Windows y al final de todas estas opciones se puede observar que el agente está ejecutándose, si esto no sucede se deberá dirigirse a la ventana de servicios y ejecutarlo, ya que suele parar su funcionamiento.

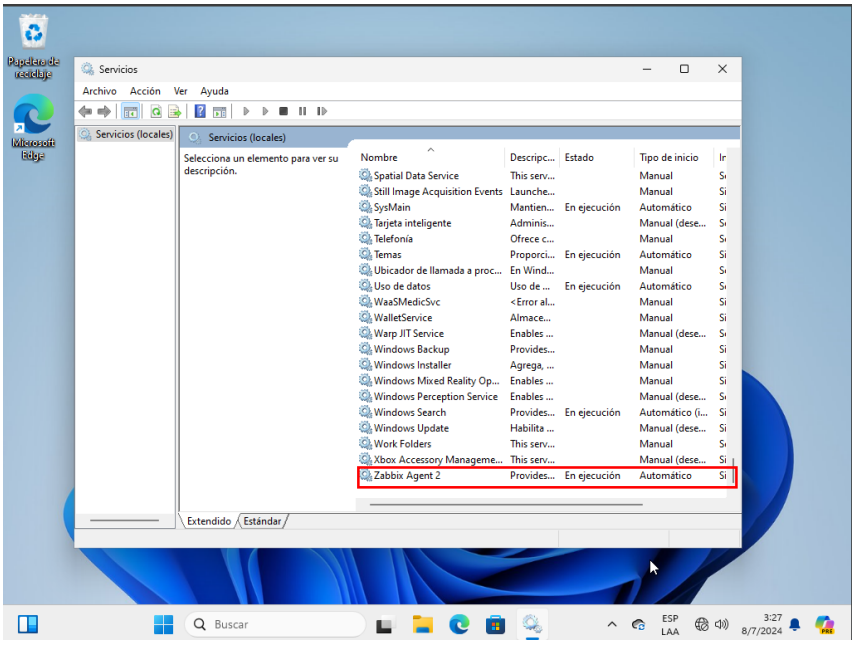

Figura 3.52 Comprobación del agente

3.4 Configuración de alertas automáticas

A continuación, se procederá a la configuración necesaria para activar las alertas por correo cuando se haya producido un error, para entender la función de la herramienta se debe conocer que todos los eventos que se producen dentro de la red se muestran en la pantalla principal de Zabbix, como se observa en la Figura 3.53, y estas alertas son las que se enviaron por correo.

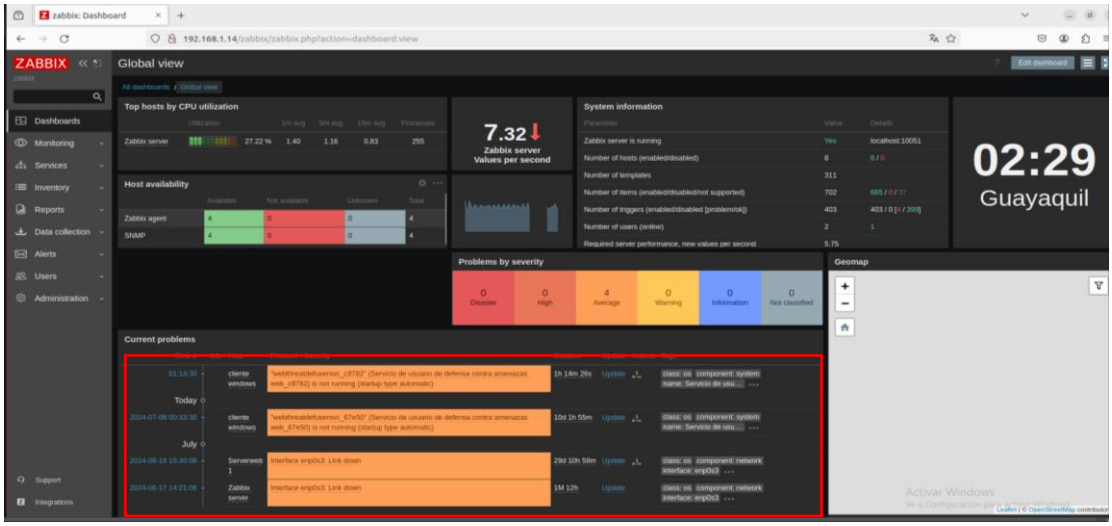

Figura 3.53 Alertas de Zabbix

Para comenzar la configuración de las alertas se debió dirigir a la ventana de opciones que se encuentra en la parte izquierda de la herramienta, una vez en esta parte hay que buscar la opción de *Alerts,* se puede observar la Figura 3.54 para que muestra la opción.

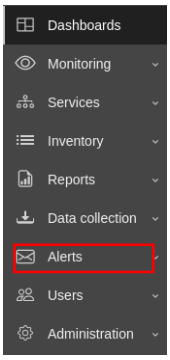

Figura 3.54 Opciones de configuración de Zabbix

Las opciones que se despliegan al elegir *Alerts* se observan en la Figura 3.55, de todas las alternativas desplegadas se tuvo que elegir *Media Types*.

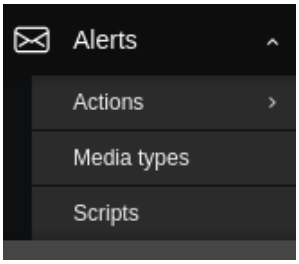

Figura 3.55 Opciones de la ventana *Alerts*

Cuando se selecciona *Media Types* se despliegan todas las opciones que la herramienta ofrece para notificar con alertas los problemas que detecta, en esta ocacion se realizará la configuracion de correo como medio de notificaciones. El recuadro que resalta la Figura 3.56, es la opcion elegida para el envio de las notificaciones, el estado de *Email* se encuentra desabilitado por lo que el primer paso es habilitarlo. Esto se logra simplemente dando un click en la opcion de *Disable* y el estado cambiara automaticamente, finalmente se tuvo que dar un clic en la opcion de *Email* para ingresar cierta infromacion para terminar con la configuracion.

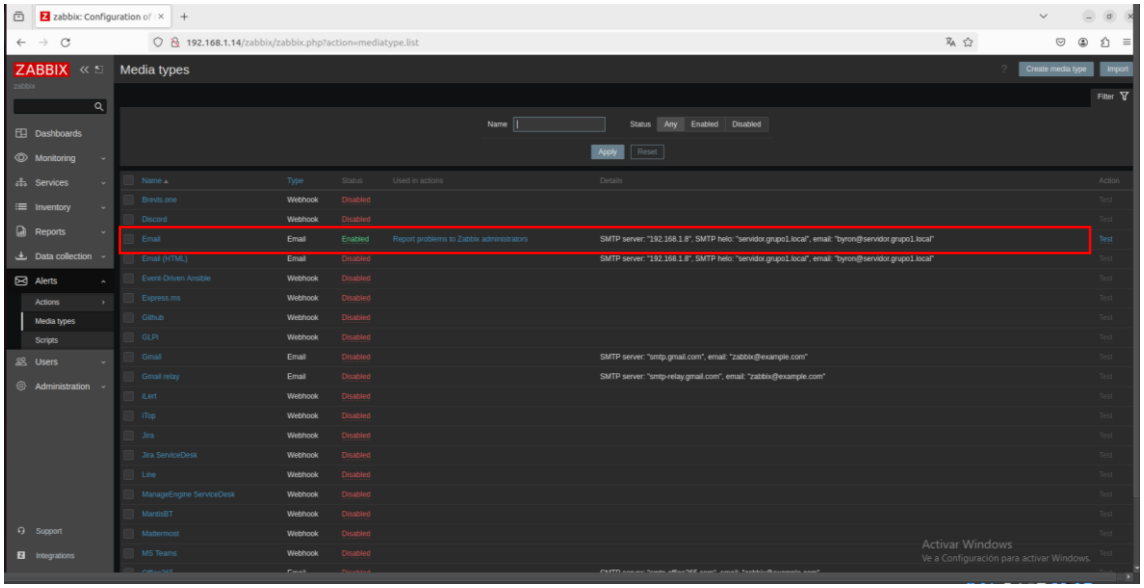

Figura 3.56 Alternativas para notificaciones

La Figura 3.57 muestra todas las opciones que se tuvieron que completar para que las notificaciones vía correo queden activas, para completar todos los recuadros necesarios se hizo uso del servidor de correo que se instaló en la red, siendo la opción de *SNMP server* la dirección IP de la maquina donde está instalado el servidor.

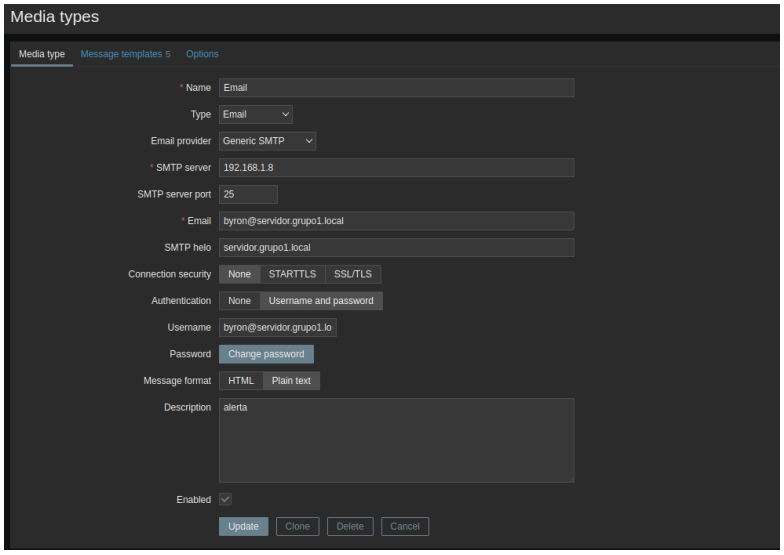

Figura 3.57 Configuración notificaciones de correo

3.5 Pruebas de funcionamiento de la herramienta de monitoreo

Es necesario debe comprobar que la red y el sistema esté funcionando correctamente, para ello se apagó el servidor web como lo muestra la Figura 3.58, simulando que este tuvo un problema y que dejo de funcionar.

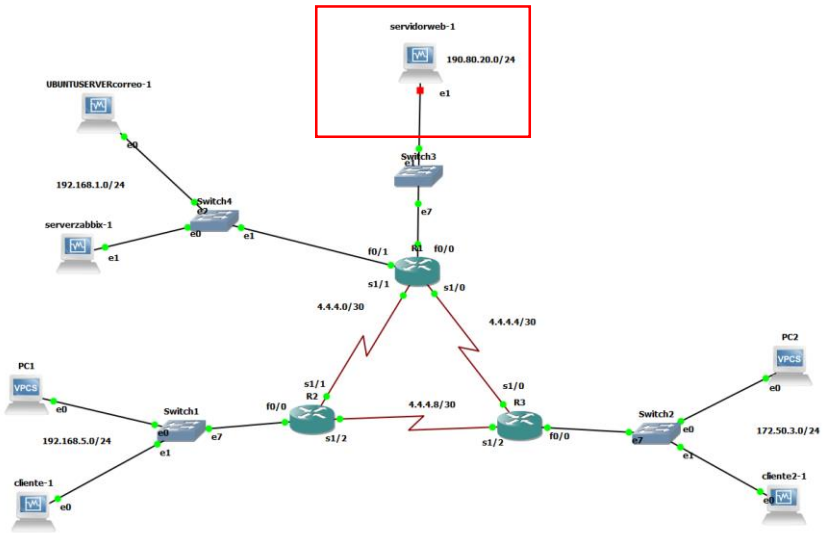

Figura 3.58 Red con inconvenientes

La imagen de la Figura 3.59, muestra el interfaz inicial de Zabbix la parte resaltada muestra la zona donde se muestran todas las notificaciones, las que se encuentran activas en la imagen indican que el firewall de Windows se apagó y que es necesario iniciarlo, este inconveniente se lo provoco para poder ingresar una dirección estática en el usuario de Windows, con el fin de que tenga comunicación con la red.

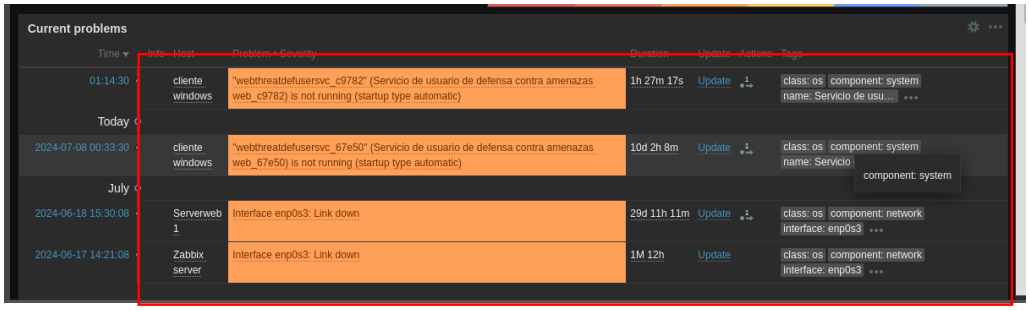

Figura 3.59 Ventana principal de Zabbix

Los cuadros resaltados que se muestran en la Figura 3.60, indican que se ha provocado un error y que se ha emitido la alerta vía correo. El recuadro naranja indica el error especifico que ha sucedido, el otro cuadro indica que se ha emitido un correo indicando cual es el problema que ha detectado la herramienta.

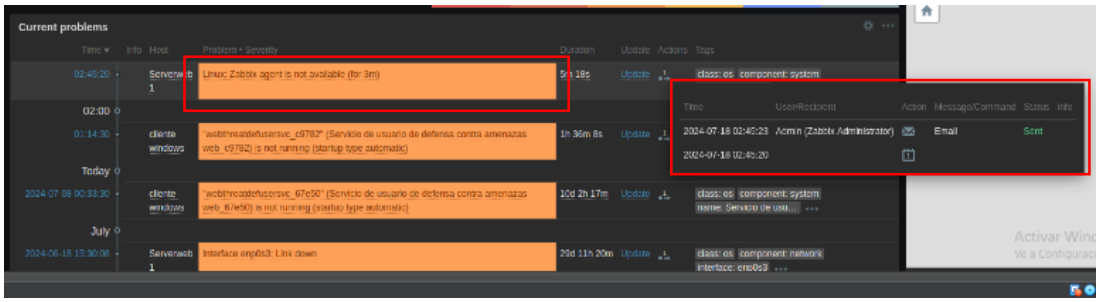

Figura 3.60 Salto de alertas en la ventana principal

La interfaz del servidor de correo se muestra en la Figura 3.61, se creó un usuario dentro del servidor, el cual fue ingresado en la configuración de notificaciones de alertas, a este usuario se le hace llegar la información, cuando el servidor web fue desactivado se emitió el error al correo y su descripción.

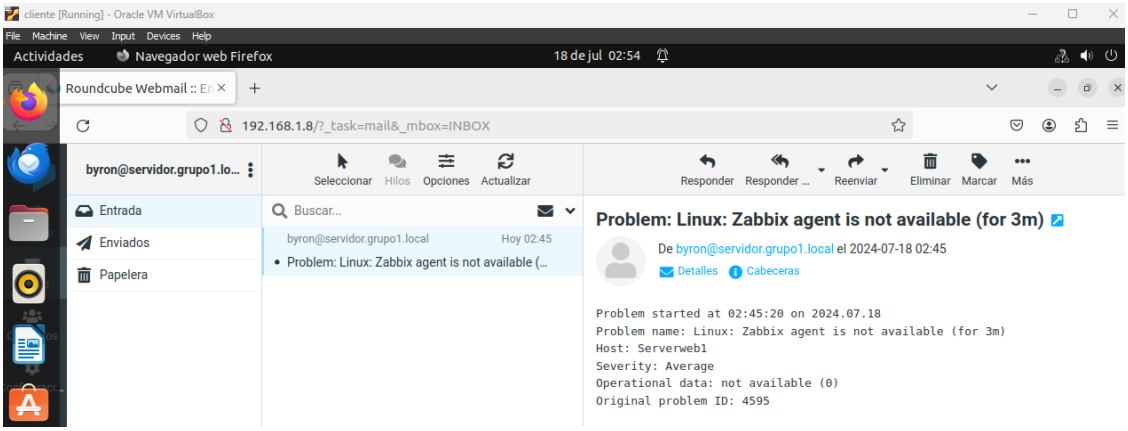

Figura 3.61 Interfaz del servidor correo

A continuación, se volvió a encender el servidor web simulando que el problema que existió se solucionó y se volvió a levantar el servicio. La Figura 3.62 muestra la red activa y todos sus dispositivos funcionando.

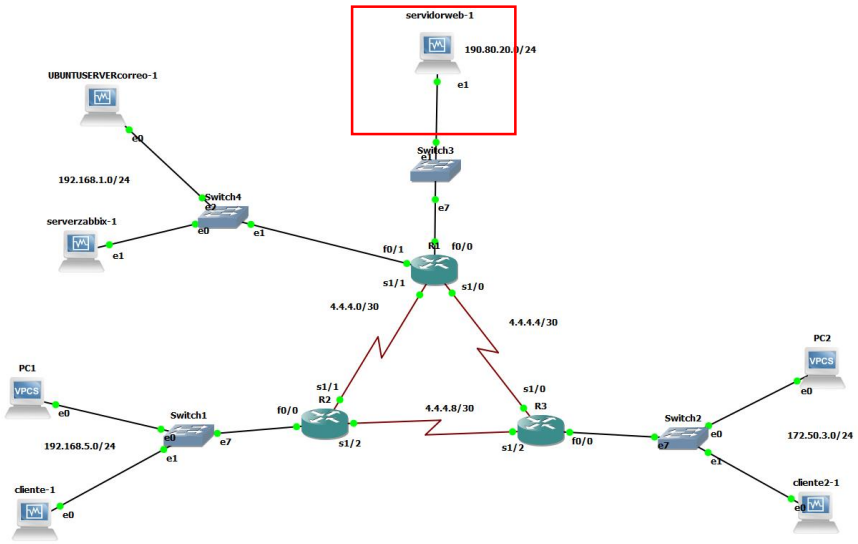

Figura 3.62 Red activa y funcionando

Tras la activación del servidor web saltaron nuevas notificaciones en la pantalla principal de Zabbix, indicando que el problema se ha solucionado, y que la notificación por correo indicando este evento se ha enviado. Los recuadros resaltados en la Figura 3.63 muestran estas dos actividades.

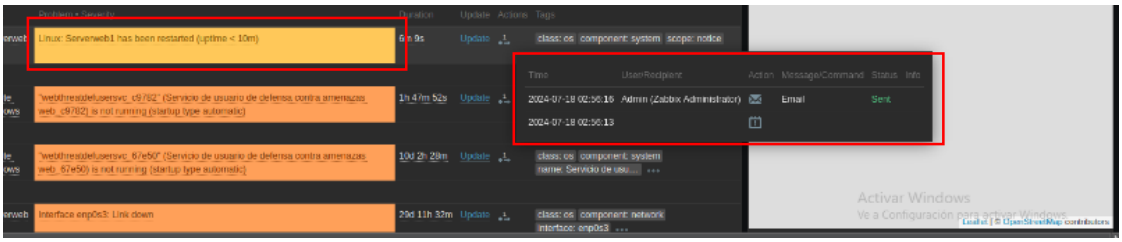

Figura 3.63 Notificaciones de eventos solucionados

De la misma forma como los correos son enviados automáticamente cuando se ha producido un error, los correos notificando que se el problema es solucionado también serán enviados de la misma forma. La Figura 3.64 muestra la interfaz del servidor de correo y los mensajes de solución del problema y que la maquina está funcionando correctamente.

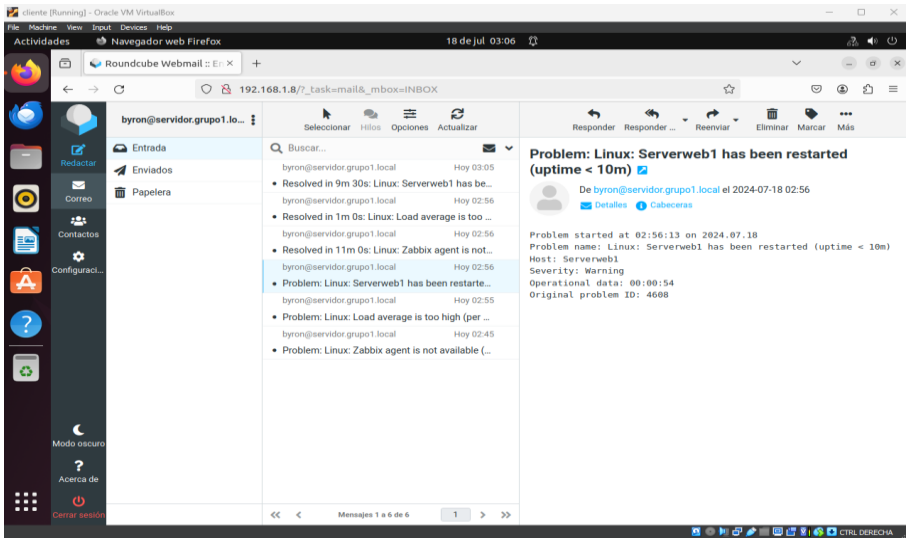

Figura 3.64 Mensajes de problemas solucionados

Para la siguiente prueba se instaló una máquina virtual con el sistema de Kali Linux, y se la posiciono en la red 192.168.5.0/24 como se muestra en la Figura 3.65, desde esta parte de la configuración se simulo un ataque DDoS, y así se obtuvo datos de la herramienta y las alertas correspondientes.

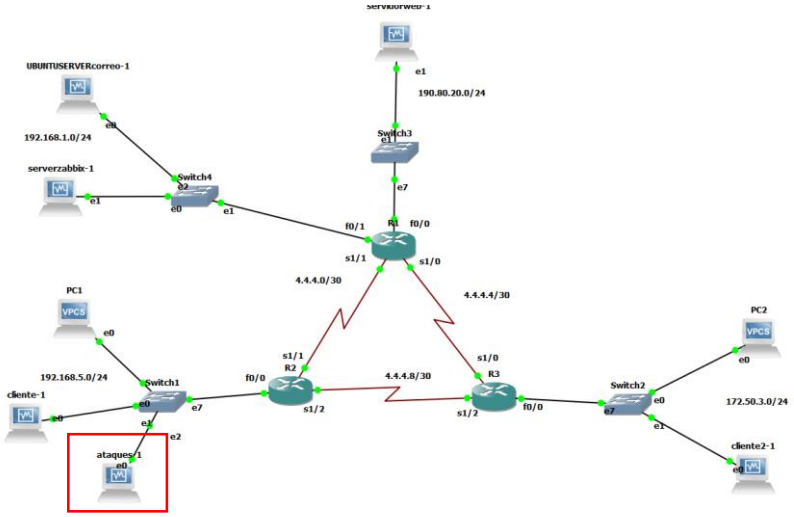

Figura 3.65 Red modificada

Dentro del software de Kali, se utilizó la herramienta de Metasploit, la Figura 3.66 muestra la herramienta que se utilizó, para la simulación del ataque, desde aquí se apuntó al servidor web para realizar la denegación de servicio

Figura 3.66 Herramienta de ataque

Una vez que se inició el ataque, Zabbix comenzó a emitir errores dentro de la red que se los puede observar en la Figura 3.67, este ataque afectó a más de una máquina, por lo que el comportamiento que se puede observar es inusual dando la alerta que algo no está funcionando de manera correcta.

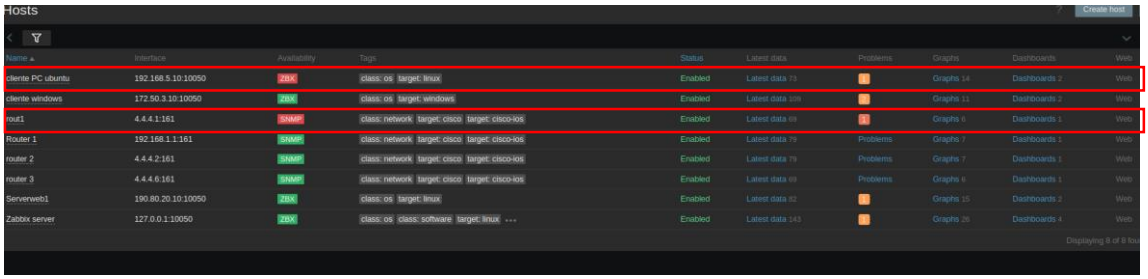

Figura 3.67 Protocolos sin funcionar

La Figura 3.68 se indica la ventana que señala el error especifico que tuvieron los dispositivos al realizar el ataque de prueba además de la confirmación de envió del correo de notificación.

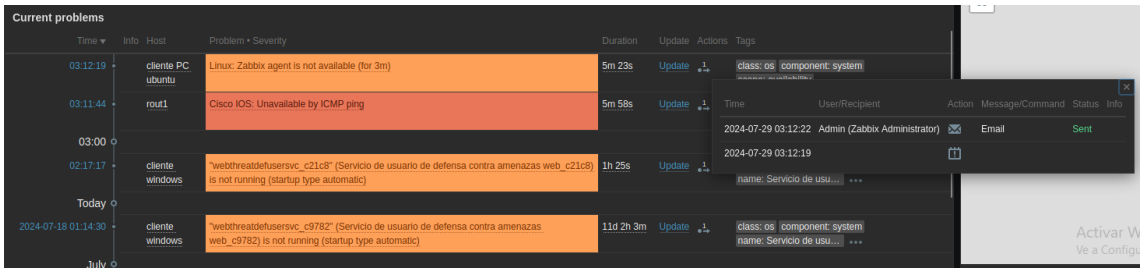

Figura 3.68 Ventana de errores

En el servidor de correo se encuentran las notificaciones que fueron enviadas por la herramienta como se observa en la Figura 3.69, para esta prueba se utilizó el sistema operativo de Windows para ingresar al correo.

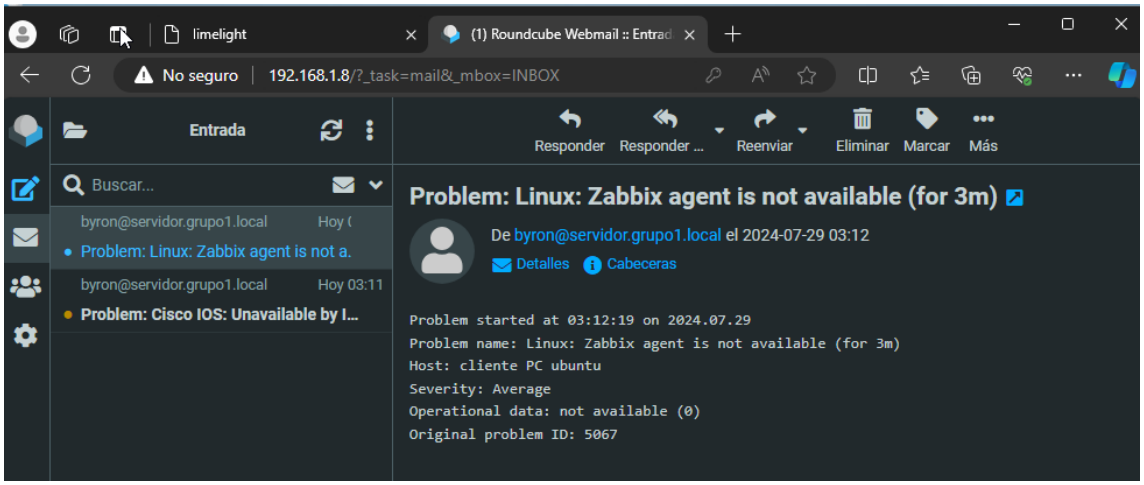

Figura 3.69 Notificaciones de problemas

La Figura 3.70 muestra que los protocolos están funcionando nuevamente cuando se apagó la maquina con la que se estaba realizando el ataque.

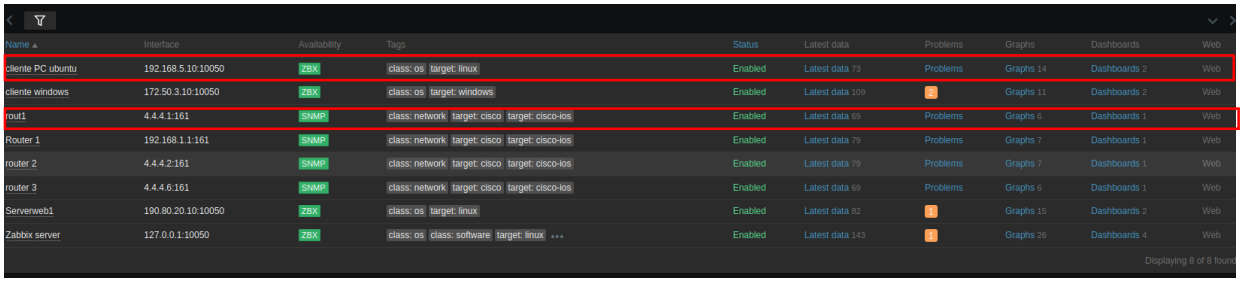

Figura 3.70 Protocolos funcionando

Los correos indicando que los errores fueron corregidos se enviaron nuevamente al servidor de correo, estos correos se los puede observar en la Figura 3.71.

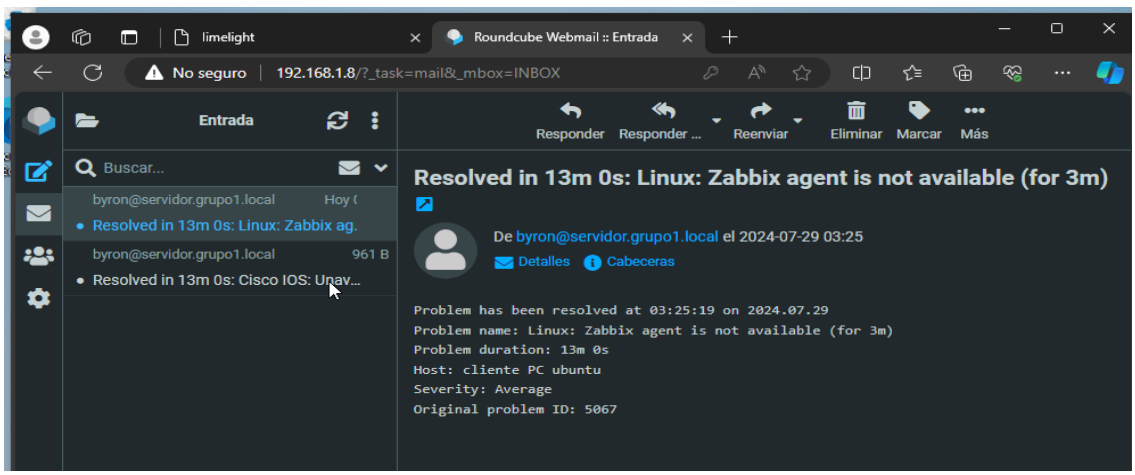

Figura 3.71 Correos de solución de errores

Para la siguiente simulación de errores se optó por eliminar una línea de conexión entre routers como lo muestra la Figura 3.72.

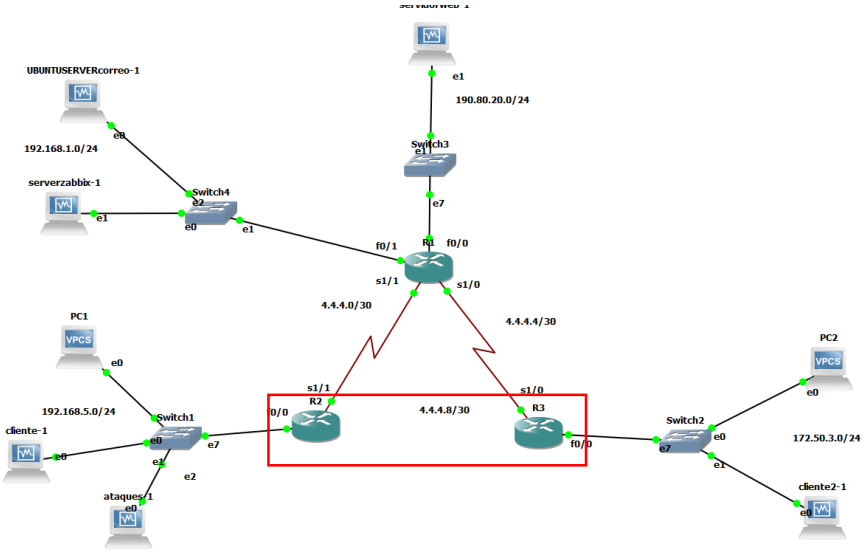

Figura 3.72 Red modificada

El error se observó en la ventana principal de Zabbix se indica en la Figura 3.73, el error que la herramienta reflejó es interfaces caídas.

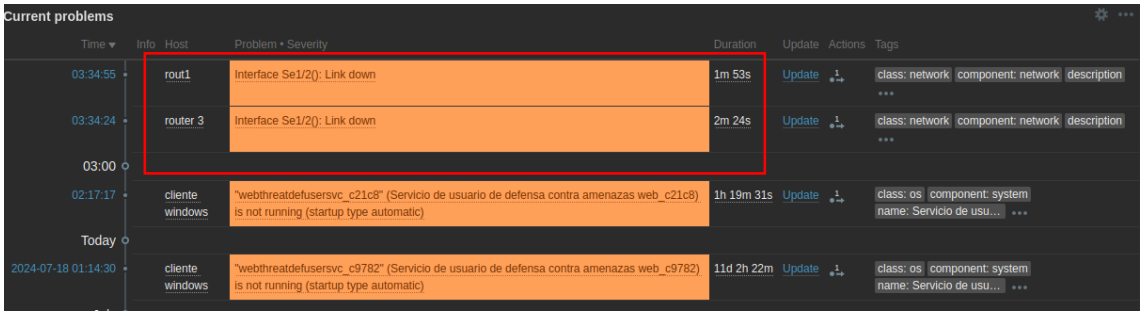

Figura 3.73 Ventana de errores de Zabbix

Cuando se volvió a levantar las interfaces y el error se solucionó los mensajes de notificación se enviaron al correo configurado como lo muestra la Figura 3.74.

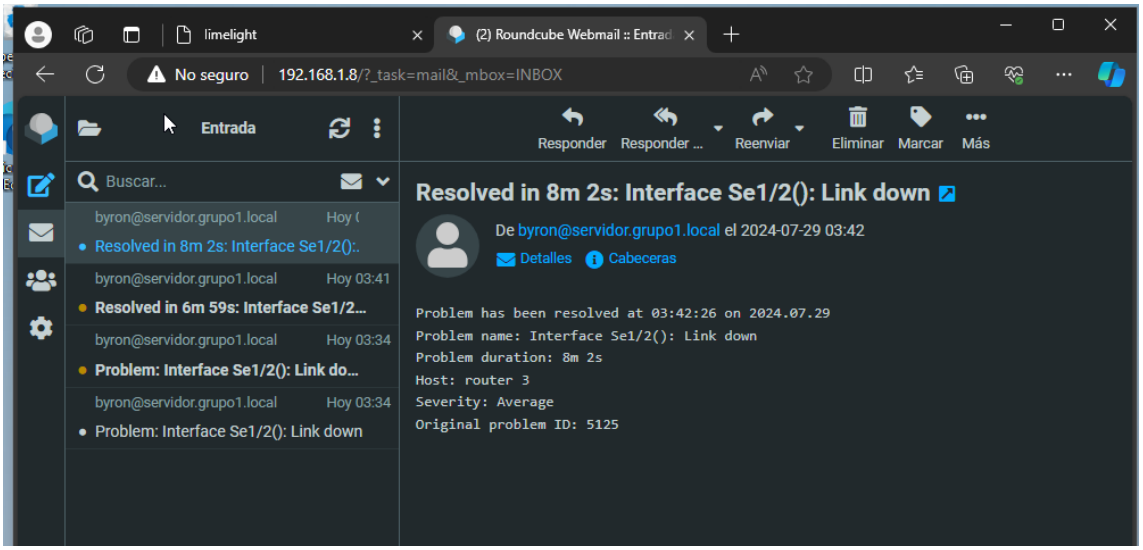

Figura 3.74 Servidor de correo

Los dispositivos de usuario que se encuentran en la red están generando métricas en todo momento y se pueden monitorear desde la plataforma, entre las métricas que se pueden verificar son: la cantidad de CPU que se está utilizando, el espacio de disco que está en uso, la memoria RAM utilizada y el ancho de banda usado por la interfaz de red. La Figura 3.75 muestra los *widgets* de todas estas características.

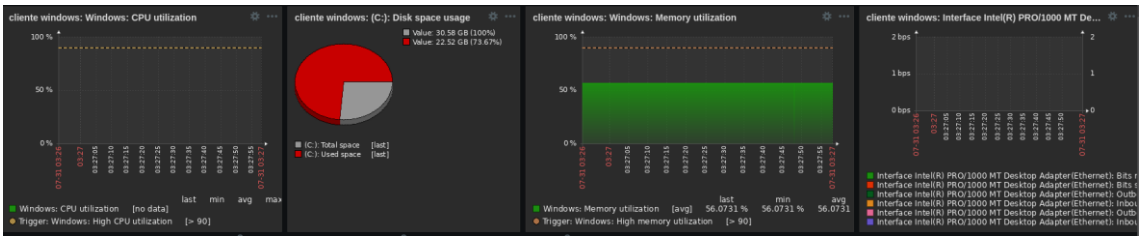

Figura 3.75 Widgets de dispositivos de usuario

Los dispositivos de red, que en este caso son routers Cisco también generan sus propias métricas, la Figura 3.76 presenta algunos ejemplos, la información que se proporciona de estos equipos es: el uso de la memoria, la cantidad de CPU utilizada y la velocidad de cada interfaz.

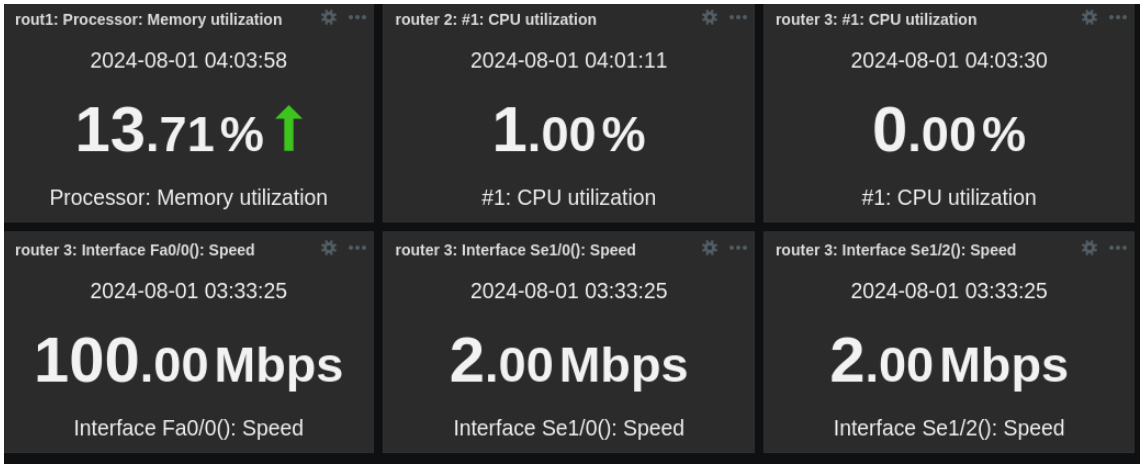

Figura 3.76 Información de recursos de equipos de red

4 CONCLUSIONES

- Zabbix es una herramienta *Open Source* que permite tener una gran cantidad de dispositivos monitoreados, ya que utiliza el protocolo estandarizado SNMP, esto hace posible que cualquier dispositivo que contenga este protocolo pueda ser monitoreado. De todas maneras, existe el agente Zabbix para los dispositivos que no pueda hacer uso de SNMP. Por estas razones, la herramienta puede monitorear al mismo tiempo dispositivos con diferente software y hardware.
- Las variables y características de los dispositivos que la herramienta monitoriza, son a nivel de hardware por lo que las notificaciones que se puedan generar pueden llevar estas características, haciendo que Zabbix sea una plataforma de monitoreo completa y confiable.
- Para el correcto funcionamiento de la plataforma se debe evaluar la cantidad de dispositivos y servicios que se van a monitorizar y consultar la tabla de características que se encuentra en la página principal de Zabbix y así determinar que hardware requerido para la implementación de la herramienta.
- Para este trabajo se utilizó Ubuntu en la versión 22.04, que es el sistema operativo donde se instalara Zabbix, la razón por la que se usó esta distribución es porque existen instrucciones específicas de instalación en la página principal de Zabbix para esta versión de Ubuntu. Además de que es un sistema operativo muy estable, seguro y robusto.
- La herramienta puede trabajar las 24 horas del día los 7 días de la semana, monitoreando de forma constante toda la red, de forma que la recolección de datos sea continua, lo que asegura que las alertas serán enviadas sin importar el horario en el que se produjeron.

- La implementación de Zabbix, tiene como fin ser una herramienta que permita mejorar la administración de todos los recursos que integran una red, además de la detección y la prevención de errores de forma temprana. La eficiencia y eficacia para procesar eventos dañinos aumentaría, de la misma forma sucedería con la optimización de los recursos de los dispositivos.

5 RECOMENDACIONES

- El criterio para la instalación de la herramienta no solo deberá ser su funcionalidad, sino el tamaño de la red, ya que en un ambiente pequeño donde la cantidad de dispositivos es muy pequeña su implementación llevara un gasto innecesario y los beneficios serán casi nulos.
- El sistema de alertas con las que cuenta el software es muy completo, ya que además de correo electrónico se puede usar las alertas vía SMS, Telegram, Ms Teams, etc.
- Zabbix es un software que permite la monitorización de un sin sinfín de dispositivos de red, pero existe un grupo muy pequeño de estos que no soporta el trabajo con el protocolo SNMP, por lo que al adquirir un nuevo equipo se debe estar completamente seguro de que puedan soportar esta característica.
- La dirección IP que se usa para la monitorización de los routers donde se usa el protocolo SNMP, debe estar que alguna de las interfaces las cuales esta utilizando el router, de la misma forma el nombre de la comunidad que se utilizara para la comunicación debe ser el mismo para seguir agregando nuevos dispositivos.
- Se deberá prever que la red que se monitoriza escalará con el tiempo, por lo que la escalabilidad de la herramienta se deberá tener en cuenta al momento de seleccionar los recursos de la maquina donde se alojará la herramienta donde se vaya hacer la instalación.

6 REFERENCIAS BIBLIOGRAFICAS

[1] M. L. I. CEDEÑO, «COMPARATIVA ENTRE HERRAMIENTAS DE MONITOREO DE RED DE COMPUTADORAS APLICADAS A LA EMPRESA PUERTO ATÚN,» de *Informe de titulacion. Obtencion del titulo de Magister en tecnologia de la Informacion*, Calceta, 2019.

[2] D. X. Viñan Carrillo, «ANÁLISIS Y PROBLEMAS DE LAS DIFERENTES VERSIONES DEL PROTOCOLO SNMP,» de *Tesis, Previa la obtención del Título Ingeniero Telecomunicacion*, Guayaquil, Ecuador, 2015.

[3] J. I. B. Villagómez, «SERVIDOR DE CONTROL DE DISPOSITIVOS Y SERVICIOS MEDIANTE EL PROTOCOLO SNMP PARA LA RED DE DATOS EN CELEC .E.P. UNIDAD DE NEGOCIO HIDROAGOYAN,» de *Proyecto de investigación, presentado previo la obtención del título de Ingeniero en Electrónica y Comunicaciones*, Ambato, 2015.

[4] Xerox, «Simple Network Management Protocol (SNMP) Primer,» Julio 2003. [En línea]. Available: https://www.office.xerox.com/support/dctips/dc00cc0118.pdf.

[5] A. G. M. R. Soraya Lorena Serna Guerrero, «Proyecto previo a la obtencion del titulo de ingeniero en Electronica y Redes de la Informacion,» de *Diseño e implementacion de un prototipo de software para la administracion de red usando SNMPv3*, Quito, 2013.

[6] A. &. D. M. Lago, «Implementación virtual de redes LAN, enfocadas en el análisis comparativo de las ventajas y desvetajas del uso y aplicación de las diferentes versiones del protocolo SNMP,» Guayaquil, 2013.

[7] A. A. A. Cevallos, «Diseño e implementacion de una heraamienta de monitoreo y control de data center basado en herramientas open source.,» de *Tesis de grado previo a la obtencion del titulo en ineniero en sistemas*.

[8] L. D. Cervantes, «Evaluación de la herramienta GNS3 con conectividad a enrutadores reales,» de *Proyecto final de carreara. Previo a la obtencion del titulo Ingeniera en Telecounicaciones*, Barcelona.

[9] M. A. U. SOLIS, «IMPLEMENTACIÓN DE PLATAFORMA DE MONITOREO ZABBIX PARA SISTEMAS DE TELECOMUNICACIONES TELSUR,» de *Tesis. Previo para la obtencion del titulo Ingeniero Civil Electronico* , Valdivia, Chile, 2014.

[10] Zabbix, «Documentacion, Manual de Zabbix,» 2024. [En línea]. Available: https://www.zabbix.com/documentation/current/es/manual.

[11] Z. L. All, «Zabbix,» [En línea]. Available: https://www.zabbix.com/.

[12] M. Fuszner, «Graphical Network Simulator, Academia,» [En línea]. Available: https://www.academia.edu/33073375/GNS3_Graphical_Network_Simulator.

[13] D. A. y. W. T. A. J. Salcedo Sambachi, «Implementación, administración y monitoreo de una red corporativa simulada en el laboratorio de Redes Virtual de la Universidad de las Fuerzas Armadas ESPE sede Latacunga,» de *Monografía, previo a la obtención de título de Tecnólogo Superior en Redes y Telecomunicaciones*, Quito, 2021.

[14] A. S. T. David J. Wetherall, «Redes de computadoras,» Mexico, https://gc.scalahed.com/recursos/files/r161r/w25733w/redes_de_computadoras-freelibros-org.pdf, 2012.

[15] 4. J. P. A Telesca, «System performance monitoring of the ALICE Data Acquisition System with Zabbix,» Journal of Physics: Conference Series, [En línea]. Available: https://iopscience.iop.org/article/10.1088/1742-6596/513/6/062046/pdf.

7 ANEXOS

ANEXO I. Certificado de originalidad

ANEXO II. Enlaces

ANEXO I: Certificado de Originalidad

CERTIFICADO DE ORIGINALIDAD

Quito, D.M. 1 de agosto de 2024

De mi consideración:

Yo, ANDRÉS FERNANDO REYES CASTRO, en calidad de Director del Trabajo de Integración Curricular titulado IMPLEMENTACIÓN DE UNA HERRAMIENTA DE MONITOREO DE CÓDIGO ABIERTO DE INFRAESTRUCTURA TI elaborado por el estudiante BYRON HERNANDO BENALCAZAR SALAZAR de la carrera en Tecnología Superior en Redes y Telecomunicaciones, certifico que he empleado la herramienta Turnitin para la revisión de originalidad del documento escrito completo, producto del Trabajo de Integración Curricular indicado.

El documento escrito tiene un índice de similitud del 12%.

Es todo cuanto puedo certificar en honor a la verdad, pudiendo el interesado hacer uso del presente documento para los trámites de titulación.

NOTA: Se adjunta el link del informe generado por la herramienta Turnitin.

LINK

Atentamente,

ANDRÉS FERNANDO REYES CASTRO

Docente

Escuela de Formación de Tecnólogos

ANEXO II: Enlaces

https://drive.google.com/file/d/1nhir3jWHvhmX2nEIpnrZEraZCf4IgAiO/view?usp=sharing

Anexo II.I Código QR de la implementación y pruebas de funcionamiento

https://drive.google.com/file/d/1W5uYO9QxSu16FzC2a_oZlphBC6hwABcz/view?usp=sharing

Anexo III.II Manual de Zabbix