



Implementación de un servidor de administración de redes mediante software libre para el monitoreo y administración de la red de datos de la Escuela de Formación de Soldados Vencedores del Cenepa (ESFORSE).

Sangucho Sangucho, Nelson Patricio

Departamento de Eléctrica y Electrónica

Carrera de Tecnología Superior en Redes y Telecomunicaciones

Monografía, previo a la obtención del título de Tecnólogo Superior en Redes y Telecomunicaciones

Ing. Casa Guayta, Carlos Wellington

Latacunga

24 febrero del 2022



DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA
CARRERA DE TECNOLOGÍA SUPERIOR REDES Y TELECOMUNICACIONES

Certificación

Certifico que la monografía, "Implementación de un servidor de administración de redes mediante software libre para el monitoreo y administración de la red de datos de la Escuela de formación de Soldados Vencedores del Cenepa (ESFORSE)." fue realizado por el señor Sangucho Sangucho, Nelson Patricio la cual ha sido revisada y analizada en su totalidad por la herramienta de verificación de similitud de contenido; por lo tanto, cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, razón por la cual me permito acreditar y autorizar para que lo sustente públicamente.

Latacunga, 25 de febrero del 2022

Ing. Casa Guayta, Carlos Wellington

C. C: 0502352180

Reporte de verificación de contenido



Overall Similarity Score



Results Found



Total Words in Text

Identical Words	409
Words with Minor Changes	81
Paraphrased Words	332
Omitted Words	0

Ing. Casa Guayta, Carlos Wellington

C. C: 0502352180



DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE TECNOLOGÍA SUPERIOR REDES Y TELECOMUNICACIONES

Responsabilidad de autoría

Yo, Sangucho Sangucho, Nelson Patricio, con cédula de ciudadanía N° 0504268442, declaro que el contenido, ideas y criterios de la monografía: **Implementación de un servidor de administración de redes mediante software libre para el monitoreo y administración de la red de datos de la Escuela de formación de Soldados Vencedores del Cenepa (ESFORSE)**, es de mi autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos, y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Latacunga, 25 de febrero del 2022

Sangucho Sangucho, Nelson Patricio

C.C.: 0504268442



DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE TECNOLOGÍA SUPERIOR REDES Y TELECOMUNICACIONES

Autorización de publicación

Yo Sangucho Sangucho, Nelson Patricio Autorizo a la Universidad de las Fuerzas Armadas ESPE publicar la monografía: Implementación de un servidor de administración de redes mediante software libre para el monitoreo y administración de la red de datos de la Escuela de formación de Soldados Vencedores del Cenepa (ESFORSE). en el repositorio institucional, cuyo contenido, ideas y criterios son de mi responsabilidad.

Latacunga, 25 de febrero del 2022

Sangucho Sangucho, Nelson Patricio

C.C.: 0504268442

Dedicatoria

Agradezco a Dios y a mi madre por su amor, enseñanza y disciplina; valores que me ayudaron a cumplir cada una de mis metas trazadas, y me forjaron como una persona de bien y de valores, los cuales siempre están presente en cada día de mi vida.

Agradezco a mi familia por sus palabras de aliento y motivación para seguir adelante en mis estudios.

Agradezco a mi tutor por el constante apoyo brindado e interés en mi proyecto.

SANGUCHO SANGUCHO, NELSON PATRICIO

Agradecimiento

Agradezco a mi familia y al Ejército Ecuatoriano por darme la oportunidad de continuar mi preparación intelectual, y a la Universidad de las Fuerzas Armadas ESPE por brindarme los conocimientos necesarios, los cuales se verán reflejados en las actividades del Ejército para lograr su misión.

Gracias a mi mentor, utilizó su experiencia y apoyo para guiarme por el camino correcto en el desarrollo del trabajo de grado.

Y todo aquel que contribuya a la formación de mi carrera profesional y como persona en la sociedad.

SANGUCHO SANGUCHO, NELSON PATRICIO

Tabla de contenidos

Carátula.....	1
Certificación	2
Reporte de verificación de contenido	3
Responsabilidad de autoría.....	4
Autorización de publicación.....	5
Dedicatoria.....	6
Agradecimiento.....	7
Tabla de contenidos	8
Índice de figuras	13
Índice de tablas	17
Resumen	18
Abstract.....	19
Generalidades	20
Introducción.....	20
Antecedentes.....	22
Justificación e importancia.....	23
Objetivos	24
<i>Objetivo General</i>	24
<i>Objetivos Específicos</i>	24
Alcance.....	25
Marco teórico	26
Historia de redes de computadora.....	26
Definición de administración de redes.....	27
Arquitectura de un sistema de administración de redes	27

Funciones de administración de redes	30
<i>Monitoreo</i>	<i>30</i>
<i>Rendimiento.....</i>	<i>31</i>
<i>Fallas.....</i>	<i>32</i>
<i>Configuración</i>	<i>32</i>
<i>Seguridad</i>	<i>33</i>
Protocolo de administración de red	33
<i>SNMP (Simple Network Management Protocol)</i>	<i>34</i>
<i>CMIP (Common Management Information Protocol)</i>	<i>35</i>
<i>CORBA (Common Object Request Broker Architecture)</i>	<i>35</i>
Historia de los servidores de red	35
<i>Tipos de servidores de red.....</i>	<i>36</i>
Open Source y Software libre.....	38
<i>Sistema operativo Linux.....</i>	<i>39</i>
<i>Componentes de Linux.....</i>	<i>40</i>
<i>SNMP en Linux.....</i>	<i>41</i>
Versiones de SNMP	42
<i>SNMPv1.....</i>	<i>42</i>
<i>SNMPv2.....</i>	<i>42</i>
<i>SNMPv3.....</i>	<i>43</i>
Herramientas para el monitoreo de redes.....	43
<i>Nagios.....</i>	<i>43</i>
<i>Pandora FMS.....</i>	<i>44</i>
<i>Cacti</i>	<i>45</i>
<i>Zabbix</i>	<i>46</i>
Zabbix con otros agentes de monitorización	48

<i>Agente Zabbix</i>	49
<i>Interfaz Web</i>	49
¿Cómo funcionan los agentes en los servidores?	50
<i>Funcionamiento de monitoreo en Zabbix</i>	50
Zabbix con otros agentes de monitorización	51
Qué es Gns3	52
<i>Característica de Gns3</i>	52
Qué es Vmware WORKSTATION PRO.....	52
Desarrollo del proyecto	54
Introducción.....	54
Planificación	54
<i>Propósito</i>	54
<i>Alcance</i>	55
<i>Personales involucrados</i>	55
<i>Perspectiva del producto</i>	55
Requisitos funcionales.....	55
Servidor Zabbix	56
<i>Descarga del sistema operativo Ubuntu server</i>	57
<i>Descarga del programa Rufus portable</i>	58
<i>Ejecución del programa Rufus</i>	59
<i>Selección de la ISO de Ubuntu y booteo en Rufus</i>	60
<i>Inicio de la instalación de Ubuntu Server</i>	60
<i>Selección de idioma de instalación de Ubuntu Server</i>	61
<i>Disposición del teclado</i>	62
<i>Actualización y otro softwares</i>	62
<i>Tipo de instalación</i>	63

<i>Localización</i>	64
<i>Creación de usuario y asignación del nombre del servidor</i>	64
<i>Visualización del proceso de instalación</i>	65
Instalación de Zabbix en el servidor Ubuntu Server	66
<i>Requerimientos para la instalación del servidor Zabbix</i>	67
<i>Selección de la versión de Zabbix</i>	67
<i>Instalación del repositorio de Zabbix en Ubuntu</i>	68
<i>Instalación del servidor, con su respectivo agente Zabbix</i>	70
<i>Instalación de la base de datos de Zabbix</i>	70
<i>Importación del esquema y los datos iniciales</i>	71
<i>Configuración de la base de datos del servidor Zabbix</i>	72
<i>Configuración de la zona horaria para Frontend de Zabbix</i>	72
<i>Iniciación del agente y del servidor Zabbix</i>	73
<i>Asignación de la Ip del servidor en el Zabbix Agentd</i>	74
<i>Comprobación de la ejecución Zabbix Agentd y Zabbix Server</i> ..	74
<i>Inicio de instalación de la interfaz web del servidor Zabbix</i>	75
<i>Requisitos previos para la instalación de la interfaz Web</i>	76
<i>Configuración de la base de datos de Zabbix</i>	76
<i>Aspectos importantes del servidor Zabbix</i>	77
<i>Resumen de la Instalación</i>	78
<i>Inicio de sesión del servidor</i>	78
<i>Panel de control de Zabbix</i>	79
Monitoreo de los equipos de la red de datos de la “ESFORSE”	80
<i>Host groups para Zabbix</i>	80
<i>Creación de host groups del departamento de TICs.</i>	81
<i>Habilitación del protocolo SNMP</i>	82

<i>Registro de la computadora en el servidor Zabbix.....</i>	84
<i>Verificación del host creado</i>	85
Descarga del Agente Zabbix para la monitorización	86
<i>Instalación de agente Zabbix.....</i>	87
<i>Asignación de Ip del servidor Sabir.....</i>	88
<i>Configuración de Firewall de Windows</i>	88
<i>Asignación del host en el servidor Zabbix.....</i>	93
Monitoreo de los equipos de red del departamento Financiero	95
<i>Instalación del Agente Zabbix</i>	95
Configuración del protocolo SNMP en impresora de compras públicas..	99
Monitoreo de los equipos de red del departamento Académico	102
<i>Descarga y configuración de Zabbix Agent.....</i>	102
<i>Monitoreo de host del departamento Académico.</i>	107
Monitoreo de los equipos Ubiquiti Ac Lite.....	109
<i>Configuración del protocolo SNMP</i>	109
<i>Asignación de los dispositivos en Zabbix</i>	110
Verificación de los equipos agregados en el servidor Zabbix	113
Notificación de errores en el servidor Zabbix a través del Telegrama.....	113
Conclusiones y recomendaciones	116
Conclusiones.....	116
Recomendaciones	117
Bibliografía	118
Anexos	123

Índice de figuras

Figura 1 <i>Diagrama simple de una red de datos</i>	26
Figura 2 <i>Arquitectura de un sistema de administración de red</i>	28
Figura 3 <i>Protocolo de administración de red</i>	34
Figura 4 <i>Arquitectura de sistema operativo Linux</i>	40
Figura 5 <i>Características del protocolo SNMP</i>	41
Figura 6 <i>Interface Principal de Nagios</i>	44
Figura 7 <i>Interfaz de los diagramas de monitorización de Pandora FMS</i>	45
Figura 8 <i>Interfaz principal de Cacti</i>	46
Figura 9 <i>Arquitectura de un sistema de administración de red</i>	47
Figura 10 <i>Proceso de monitoreo en Zabbix</i>	50
Figura 11 <i>Funcionamiento de Zabbix</i>	56
Figura 12 <i>Descarga de la ISO de Ubuntu Server</i>	58
Figura 13 <i>Descarga de software Rufus</i>	59
Figura 14 <i>Interfaz principal de Rufus</i>	59
Figura 15 <i>Booteo de Ubuntu Server</i>	60
Figura 16 <i>Interfaz de inicialización de instalación</i>	61
Figura 17 <i>Interfaz de selección de idioma</i>	61
Figura 18 <i>Interfaz de selección de teclado</i>	62
Figura 19 <i>Interfaz de actualizaciones y otros softwares</i>	63
Figura 20 <i>Interfaz principal de tipos de instalación</i>	63
Figura 21 <i>Interfaz gráfica de la zona horaria</i>	64
Figura 22 <i>Creación de usuario</i>	65
Figura 23 <i>Interfaz de instalación de Ubuntu</i>	66
Figura 24 <i>Interfaz principal para la descarga de Zabbix</i>	68

Figura 25 <i>Instalación del servidor Zabbix</i>	69
Figura 26 <i>Actualización de los repositorios</i>	69
Figura 27 <i>Instalación de Zabbix server, MySQL y Zabbix-apache</i>	70
Figura 28 <i>Interfaz de la creación de la base de datos MySQL</i>	71
Figura 29 <i>Habilitación del host del servidor Zabbix</i>	71
Figura 30 <i>Configuración de la base de datos</i>	72
Figura 31 <i>Cambio de la zona horaria para Fronted de Zabbix</i>	73
Figura 32 <i>Inicialización del sistema</i>	73
Figura 33 <i>Asignación de Ip en Zabbix Agentd</i>	74
Figura 34 <i>Interfaz de comprobación</i>	75
Figura 35 <i>Inicio de bienvenida de Zabbix</i>	75
Figura 36 <i>Comprobación de requisitos</i>	76
Figura 37 <i>Conexión de la base de datos</i>	77
Figura 38 <i>Interfaz de detalle de Zabbix</i>	77
Figura 39 <i>Verificación de la instalación</i>	78
Figura 40 <i>Inicio de sesión</i>	79
Figura 41 <i>Interfaz principal de Zabbix</i>	80
Figura 42 <i>Interfaz principal de Host Groups</i>	81
Figura 43 <i>Creación de host groups de las TICs</i>	82
Figura 44 <i>Habilitación del protocolo SNMP</i>	83
Figura 45 <i>Asignación de la Ip del servidor Zabbix</i>	83
Figura 46 <i>Asignación del host en el servidor Zabbix</i>	84
Figura 47 <i>Configuración de Templates</i>	85
Figura 48 <i>Interfaz de datos monitorizados</i>	85
Figura 49 <i>Interfaz gráfica del tráfico de red</i>	86
Figura 50 <i>Interfaz principal de Agentes Zabbix</i>	86

Figura 51 <i>Descarga de la Agente Zabbix</i>	87
Figura 52 <i>Inicio de instalación del agente Zabbix</i>	87
Figura 53 <i>Asignación de Ip en el host</i>	88
Figura 54 <i>Interfaz de Firewall de Windows</i>	89
Figura 55 <i>Interfaz de la nueva regla de entrada</i>	89
Figura 56 <i>Asignación de protocolos y puertos</i>	90
Figura 57 <i>Perfiles de regla de entrada</i>	90
Figura 58 <i>Dirección de regla de entrada TCP</i>	91
Figura 59 <i>Puerto de entrada UDP</i>	91
Figura 60 <i>Dirección de regla de entrada UDP</i>	92
Figura 61 <i>Comprobación de las reglas de entrada</i>	92
Figura 62 <i>Asignación del host en el servidor Zabbix</i>	93
Figura 63 <i>Asignación del templete</i>	94
Figura 64 <i>Verificación de datos del PCU</i>	94
Figura 65 <i>Descarga del agente Zabbix</i>	95
Figura 66 <i>Asignación de Ip del servidor</i>	96
Figura 67 <i>Configuración de Firewall</i>	96
Figura 68 <i>Comprobación de reglas de entrada</i>	97
Figura 69 <i>Asignación del host en Zabbix</i>	97
Figura 70 <i>Asignación de Template</i>	98
Figura 71 <i>Interfaz de monitoreo del hosts</i>	98
Figura 72 <i>Interfaz gráfica de la memoria</i>	99
Figura 73 <i>Configuración protocolo SNMP</i>	100
Figura 74 <i>Verificación de la dirección Ip</i>	100
Figura 75 <i>Asignación del servidor Zabbix</i>	101
Figura 76 <i>Interfaz gráfica de monitoreo</i>	101

Figura 77 <i>Configuración de Zabbix</i>	102
Figura 78 <i>Agregación de reglas de entradas</i>	103
Figura 79 <i>Interfaz de agregación TCP</i>	103
Figura 80 <i>Interfaz de agregación UDP</i>	104
Figura 81 <i>Verificación de las reglas de entradas</i>	104
Figura 82 <i>Interfaz del host de planificación curricular</i>	105
Figura 83 <i>Asignación de plantillas Zabbix</i>	105
Figura 84 <i>Interfaz de Monitoreo del CPU</i>	106
Figura 85 <i>Interfaz de Monitoreo de Memoria</i>	106
Figura 86 <i>Descarga del agente Zabbix</i>	107
Figura 87 <i>Asignación de Ip del servidor Zabbix</i>	107
Figura 88 <i>Asignación del host en Zabbix</i>	108
Figura 89 <i>Interfaz de monitoreo</i>	108
Figura 90 <i>Interfaz de inicio en UniFi</i>	109
Figura 91 <i>Interfaz de configuración de UniFi</i>	110
Figura 92 <i>Asignación de Ap Ubiquiti Ac Lite</i>	111
Figura 93 <i>Asignación del template</i>	111
Figura 94 <i>Interfaz de tráfico de red</i>	112
Figura 95 <i>Interfaz de red en eth0</i>	112
Figura 96 <i>Dispositivos monitoreados en Zabbix</i>	113
Figura 97 <i>Dashboard de Zabbix</i>	114
Figura 98 <i>Verificación de errores por Telegram</i>	115

Índice de tablas

Tabla 1 <i>Tipos de servidores</i>	37
Tabla 2 <i>Comparación entre Zabbix y otros agentes de monitorización</i>	51
Tabla 3 <i>Personal Involucrado 1</i>	55
Tabla 4 <i>Comparación de las herramientas de monitoreo</i>	66

Resumen

En la actualidad, el servidor de administración y monitoreo de la red de datos es un componente básico, proactivo, y buscará evitar problemas a los administradores y gerentes, ya que mejorará la escalabilidad actual de la red de datos de la Escuela de Formación de Soldados Vencedores del Cenepa "ESFORSE". En la Escuela de Formación de Soldados Vencedores del Cenepa "ESFORSE" se desconoce el estado actual del servidor, el consumo de ancho de banda y el estado del enlace de comunicación entre las diferentes dependencias de la Escuela. Lo cual ha generado la presencia del virus debido al uso de dispositivos de almacenamiento, que forman parte de la Escuela de Formación de Soldados Vencedores del Cenepa "ESFORSE", lo que ha provocado problemas con la configuración de las máquinas entregadas a los usuarios. En donde la necesidad del uso de software le da más confiabilidad y viabilidad, de manera que se puede monitorear y controlar los recursos de la red en los equipos de comunicación. Se implementará un servidor para administrar y monitorear los equipos y servicios de la red de datos y controlar el estado de todos los enlaces de conexión y detectar si hay congestión, de tal forma que el servidor envíe una alarma cuando los recursos estén saturados.

Palabras clave:

- **SERVIDOR DE ADMINISTRACIÓN**
- **MONITORIZACIÓN DE LA RED**
- **SOFTWARE LIBRE**
- **CONTROL DE RED**

Abstract

Currently, the administration and monitoring server of the data network is a basic, proactive component, and will seek to avoid problems for administrators and managers, since it will improve the current scalability of the data network of the Escuela de Formación de Soldados Vencedores del Cenepa "ESFORSE". The current status of the server, the bandwidth consumption and the status of the communication link between the different units of the School is unknown at the Escuela de Formación de Soldados Vencedores del Cenepa "ESFORSE". This has generated the presence of the virus due to the use of storage devices, which are part of the Training School of Soldiers Victors of the Cenepa "ESFORSE", which has caused problems with the configuration of the machines delivered to users. Where the need for the use of software gives more confidentiality and viability, so that you can monitor and control the network resources in the communication equipment. A server will be implemented to manage and monitor the equipment and services of the data network and control the status of all the connection links and detect if there is congestion, so that the server will send an alarm when the resources are saturated, and make the server load of the high bandwidth and services.

Key words:

- **ADMINISTRATION SERVER**
- **NETWORK MONITORING**
- **FREE SOFTWARE**
- **NETWORK CONTROL**

Capítulo I

1 Generalidades

1.1 Introducción

El presente proyecto técnico se desarrolla en la Escuela de Formación de Soldados Vencedores del Cenepa, con el objetivo de implementar un servidor de administración de redes con software libre, para el monitoreo y administración de la red de datos de la institución, de esta manera se podrá obtener información acerca del sistema, recursos, servicios, rendimiento, estadísticas entre otros datos que ayuden a la organización, planeación y control de actividades que se involucran en el funcionamiento de la red de datos dentro de la ESFORSE.

La implementación de administración de redes asegura el uso eficiente de la misma, en la actualidad se lo implementa para adaptarse a las nuevas necesidades que presenta los usuarios de la red, como la detección y aislamiento de fallas, evaluación de tráfico de datos, mantener un histórico de los problemas encontrados, además se puede tener un mejor control de acceso a la red.

Siguiendo el desarrollo, en el avance de la administración de la redes de datos se debe determinar un software open source, conocido como software de código abierto adaptando a las necesidades de la red de datos de la ESFORSE, al implementar un sistema basado en código abierto, se lo hace en el sistema operativo Ubuntu para poder integrar todo el sistema a la red, además al tener software abierto permite que varios programadores de la internet puedan leer, modificar, mejorar y reescribir el código fuente por lo que esto ayuda a que el programa elegido para la administración evolucione constantemente, cumplido con el desafío de esta proyecto que es monitorear

y administrar los datos de la red, lo único que se tiene en cuenta que al ser un software de código abierto pueden existir algunos que son pagados por lo que al escoger se debe considerar esto.

El fin de utilizar software libre en la administración de datos de la red de la ESFORSE es debido a que ofrece cualidades como estabilidad, es seguro, confiable, no ocupa mucho espacio en la memoria (liviano) y muchos de ellos son multiplataforma por lo que al aprovechar todas estas cualidades se decide realizar el proyecto con el software Zabbix, el cual tiene como principal trabajo es la monitorización y registro del estado de varios servicios de red, de los servidores de la misma y adicionalmente el estado de hardware de la red.

1.2 Antecedentes

La administración de redes de datos empezó en la década de los 60 y a partir de ahí se lo aplicado en la mayoría de instituciones privadas y públicas con el fin de mejorar la gestión de la red, seguridad, acceso a la red entre otros aspectos, en consecuencia a todo esto se plantea que en la Escuela de Formación de Soldados Vencedores del Cenepa “ESFORSE”, se implemente la administración de su red ya que hasta ahora la institución no cuenta con una herramienta que permita monitorear los datos de la misma, por lo que no se tiene información o históricos de la red sobre funcionamiento y problemas que haya presentado durante su tiempo de operación.

Dado que la tecnología informática se ha desarrollado de una manera tan asombrosa que la información procesada en ellas y en las redes institucionales no ha sido manejada de la mejor manera posible durante estos años de funcionamiento, esta iniciativa nace a partir de la propuesta y ejecución del proyecto de implementación de una red sistema de gestión para mejorar su rendimiento, disponibilidad y servicios de red convergentes.

1.3 Justificación e importancia

Es indiscutible la importancia que tiene la red que opera actualmente en la Escuela de Formación de Soldados Vencedores del Cenepa ESFORSE, desde que entró en funcionamiento no presenta problemas graves, pero tiene una pequeña deficiencia siendo la falta de un sistema que monitoreo de la red, debido a esto se desea implementar la administración de la red, la cual aprovechará al máximo los recursos tanto físicos como internos de la misma, de esta manera se la mantendrá operativa y segura para cada usuario ya que incluirá un monitoreo constante, debido a todo lo expuesto anteriormente se evidencia y se justifica la importancia por la cual la institución de la ESFORSE debe contar con un sistema de administración en redes, además que a futuro se desarrolle más proyectos e investigaciones en esta área dentro de la institución.

1.4 Objetivos

1.4.1 Objetivo General

- Implementar un servidor de administración de redes mediante software libre para el monitoreo y administración de la red de datos de la Escuela de Formación de Soldados Vencedores del Cenepa (ESFORSE).

1.4.2 Objetivos Específicos

- Determinar un servidor Open Source de administración de red de datos que sea más factible para ser aplicado en la ESFORSE.
- Establecer los requerimientos de administración y monitoreo en el departamento de TICS de la ESFORSE.
- Instalar el servidor de administración de redes y configurar los diferentes dispositivos de red para establecer comunicación con el servidor mediante el protocolo SNMP.
- Realizar pruebas de funcionamiento del servidor de administración de redes implementado.

1.5 Alcance

La mayoría de servidores no cuentan con un software de monitoreo que ayude a optimizar la seguridad, monitoreo de tráfico de datos para el control de datos en el Data Center, por lo que se ha convertido en un problema en la vulnerabilidad en el departamento de TICs.

El presente proyecto tiene como finalidad la implementación de un servidor de administración de redes mediante software libre, para el monitoreo y administración de la red de datos de la Escuela de Formación de Soldados Vencedores del Cenepa ESFORSE.

El desarrollo e implementación del monitoreo nos ayudará a controlar las redes del departamento de TICs para el beneficio de la ESFORSE y sus demás departamentos en la cual aplicará el control de monitoreo y verificación del ancho de banda de los dispositivos que se encuentren monitorizados por el servidor Zabbix.

En conclusión, se elaboró la propuesta en base a los fundamentos obtenidos en la observación de la vulnerabilidad de datos en el departamento de TICs, para que sirvan para la verificación de todos los controles de la usabilidad y facilidad del monitoreo y verificación del ancho de banda en el departamento de TICs de la ESFORSE.

Cápítulo II

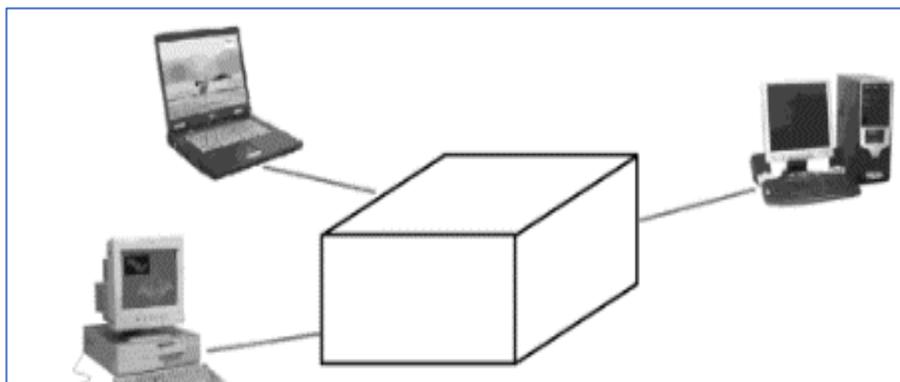
2 Marco teórico

2.1 Historia de redes de computadora

Desde el inicio de la era informática de las computadoras o computadores, se ha hecho una distinción entre dos partes básicas: el software (intangibile) y el hardware (físico), aunque también se les llama dispositivos y programas, la combinación de estos dos permite, crea, Implementación, control y gestión del funcionamiento de la red **Figura 1**, las primeras redes informáticas se diseñaron pensando únicamente en los equipos, y los programas que hoy son los elementos más importantes de la red quedan en un segundo plano, ya que actualmente permiten a los usuarios realizar diversos software, por lo que se cree que ha evolucionado en los últimos años con la aparición de nuevas formas de transferir datos, servicios informáticos y cómo se presenta la web en comunidades, empresas e instituciones en cualquier parte del mundo. (Robles, 2018)

Figura 1

Diagrama simple de una red de datos



Nota. En la figura se observa el diagrama de bloques de una comunicación entre ordenadores. Tomando de (SANTIAGO, 2016).

En las etapas iniciales de comunicación y gestión de la red, la transferencia de datos entre dispositivos es muy lenta y las interrupciones de comunicación tienden a ocurrir con frecuencia, es decir, inestable. En la década de 1970, la Universidad de Stanford propuso el desarrollo de varios protocolos de comunicación que permitirían transferir información a velocidades más altas entre diferentes tipos de redes y dispositivos informáticos, propuesto por Vinton G. Cerf, Robert E. Kahn y un equipo de estudiantes. Los protocolos TCP/IP utilizados hasta hoy, porque en la década de 1980 se limitaron al estándar para computadoras, lo que dio inicio a Internet, que creo que fue el comienzo de todas las redes que conocemos hoy en día, redes globales y locales.

2.2 Definición de administración de redes

Para definir qué es la gestión de datos o red informática, se puede deducir un conjunto de diversas tareas realizadas por los profesionales de la tecnología de la información de TI en una red informática con el fin de proporcionar de manera eficiente numerosos servicios dentro de la red. usuarios, garantizando su calidad y disponibilidad para cada institución. La administración de la red involucra no solo los dispositivos asociados con ella, sino también los usuarios, el hardware y el software. Los directamente involucrados son los profesionales de TI, quienes son quienes garantizan el servicio continuo a los usuarios de la red.

El conjunto de herramientas que componen la gestión de red es principalmente software porque es el programa que realiza las tareas de gestión de red. El hardware también es una parte fundamental, y tiene que ver con los equipos de red que se utilizan para gestionar la red. la red y todos los dispositivos se unen a ella. (Valdés, 2021)

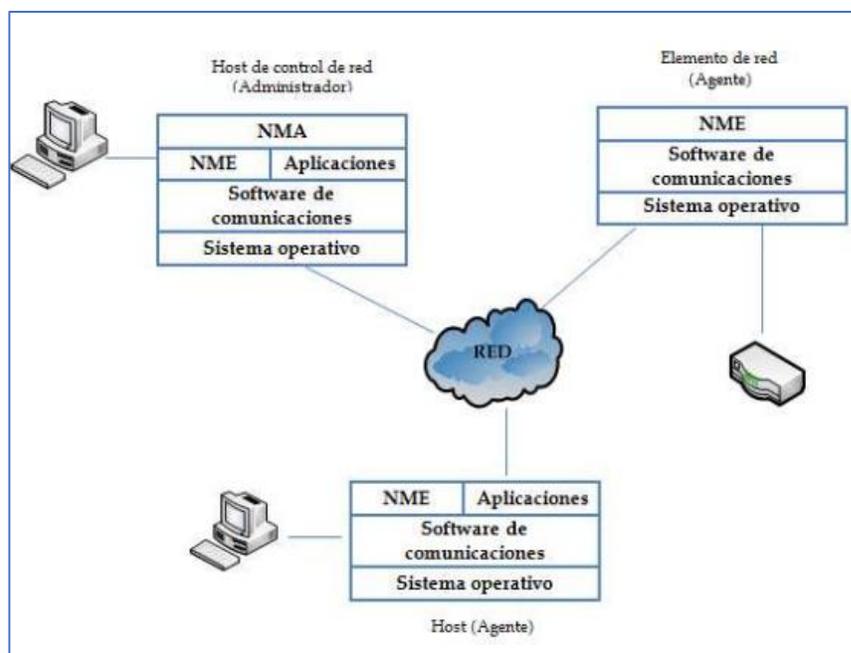
2.3 Arquitectura de un sistema de administración de redes

Cuando hablamos de la arquitectura de un sistema de administración de red, nos referimos a la organización de servicios, la capacidad de monitorear, sondear, probar,

configurar y controlar todos los dispositivos de hardware y software en la red de una organización. Debido a que los dispositivos de red se distribuyen en diferentes ubicaciones, los administradores deben tener la capacidad de recopilar información, monitorear entidades remotas y realizar cambios en ellas para poder controlarlas. Todo lo mencionado anteriormente se puede utilizar como arquitectura para un sistema de gestión de red, se debe confiar en los siguientes elementos sin antes mencionar que existen diversas arquitecturas de gestión, por lo que las detallaremos y la razón de ser de cada una de ellas. (SALAS, 2020)

Figura 2

Arquitectura de un sistema de administración de red



Nota. En la figura se observa el diagrama simplificado de un sistema de administración de redes. Tomando de (Moreno, 2015)

- **Entidad administradora** es un control humano que se ejecuta en una estación de gestión de red centralizada, que en algunos casos puede ser un

centro de operaciones de red (Noc), que es donde se realiza la gestión de la red y se recopilan, procesan, analizan y visualizan los datos con fines de gestión.

- **Dispositivo administrado** es un dispositivo de red, incluido el software, anclado en una red administrada. Los dispositivos administrados pueden ser hosts, enrutadores, conmutadores, módems o impresoras
- **Base de información de administración** es el lugar para almacenar los datos y la información de todos los objetos de gestión involucrados en la red.
- **Agente de administración de red** este es un proceso residente que se ejecuta en todos los dispositivos de la red y se comunica con el dispositivo de administración, realizando operaciones locales bajo control de comando según sea necesario.
- **Protocolo de administración de red** se ejecuta entre el ordenador del administrador y el dispositivo, permitiendo consultar el estado del dispositivo y, en caso de ser necesario, realizar acciones indirectamente sobre dicho dispositivo a través de un proxy.

En otros casos, las arquitecturas de gestión se categorizan según servicios de gestión o áreas funcionales denominadas redes, las cuales se enfocan en la supervisión, control y mantenimiento de redes de datos y se estructuran de la siguiente manera: Valarezo Saldarriaga & Simisterra Huila (2018)

- **Administración de prestaciones** mide el rendimiento del software y el hardware en función de las necesidades del usuario.
- **Administración de fallas** usar sondas para detectar, solucionar, aislar e informar problemas de red.

- **Administración de contabilidad** para manejar la facturación de la red por dispositivo y por dispositivo conectado.
- **Administración de configuraciones** preparar dispositivos para inicialización ordenada, conexión y desconexión de redes y mantenimiento y edición de nuevos dispositivos.
- **Administración de seguridad** controlar el acceso a los recursos de la red y protegerlos contra daños y contra daños intencionales o no intencionales.
(Valarezo Saldarriaga & Simisterra Huila, 2018)

2.4 Funciones de administración de redes

Los administradores de red atienden a los usuarios: crean un espacio de comunicación, enfócate en el asesoramiento; mantén las herramientas y el espacio que cada usuario necesita, sé puntual y en buena forma (piensa en quién quieres que sea un administrador si fueras usuario); mantén sus equipos y redes Responsables cuentan con hardware y software en buen estado, mantienen documentación que describe las redes, hardware y software que administran, respetan la privacidad de los usuarios y promueven el uso adecuado de los recursos. A cambio de tanta responsabilidad, la recompensa es el normal funcionamiento de la red, como medio de conexión de las personas, con los ordenadores y programas como herramientas para agilizar algunas tareas, dando tiempo y hora para realizar otras tareas. (Manuel, 2016)

2.4.1 Monitoreo

El monitoreo de red le permite mostrar información sobre la conexión entre su computadora y la red, que puede ser local o externa, o de área amplia. Asimismo, pueden indicar desde qué PC se conectan, identificar su dirección IP y la cantidad de información que pasa por la red, y las conexiones que se establecen en determinadas redes. Toda esta información se utiliza para la inspección general del funcionamiento de

la red desde una perspectiva global. Un buen monitoreo de red suele ser fácil de instalar y amigable para los usuarios no expertos, por lo que hay poco o ningún consejo o capacitación externa. (SALAS, 2020)

2.4.2 Rendimiento

Su objetivo es medir y proporcionar todos los aspectos del rendimiento de la red para que las interconexiones se puedan realizar a niveles aceptables. Las variables de rendimiento típicas son: rendimiento de la red, tiempo de respuesta del usuario, utilización de la línea, etc.

Generalmente incluye los siguientes pasos:

- Recoger datos sobre variables.
- Analizar datos para determinar valores normales (línea de base).
- Determinar los umbrales operativos apropiados para cada variable, por lo que exceder estos umbrales significa que hay un problema en la red que debe abordarse.
- Simulación de redes.

Se realiza a través de métodos reactivos o proactivos. En el tipo pasivo, el sistema reacciona enviando mensajes al sistema de gestión de la red cuando los usuarios superan los umbrales, lo que hace que la funcionalidad se vuelva inaceptable, y en el tipo activo, se utilizan simulaciones para evaluar el impacto del crecimiento de la red en los usuarios. (SALAS, 2020)

2.4.3 Fallas

Para tener éxito en el trabajo, los administradores de red deben detectar y resolver los problemas que surgen en la red. Es importante desarrollar acciones preventivas y correctivas con anticipación, por lo que debe contar con planes de contingencia adecuados. (Machado, 2016)

Está diseñado para detectar, registrar, notificar a los usuarios y, cuando sea posible, solucionar automáticamente los problemas de la red para mantener la red funcionando de manera eficiente.

- Implica los siguientes pasos:
- Identificar los síntomas del problema.
- Aislar el problema.
- Resuelve este problema.
- Verificar el mantenimiento de todos los subsistemas críticos.
- Detección y resolución de problemas de documentos.

2.4.4 Configuración

El monitoreo de red le permite mostrar información sobre la conexión entre su computadora y la red, que puede ser local o externa, o de área amplia. Asimismo, pueden indicar desde qué PC se conectan, identificar su dirección IP y la cantidad de información que pasa por la red, y las conexiones que se establecen en determinadas redes. Toda esta información se utiliza para la inspección general del funcionamiento de la red desde una perspectiva global. Un buen monitoreo de red suele ser fácil de instalar y amigable para los usuarios no expertos, por lo que rara vez o incluso es necesario el asesoramiento o la capacitación externos. (Machado, 2016)

2.4.5 Seguridad

Su propósito es controlar el acceso a los recursos de la red, de acuerdo a lo que se construya localmente para que la red no se interrumpa y no genere acceso a información importante sin la debida autorización. Estos sistemas funcionan al subdividir los recursos de la red en áreas autorizadas y no autorizadas, no debe confundirse con la seguridad que involucra al sistema operativo. Instala archivos, directorios protectores, también sin seguridad actividad física relacionada con la prevención del acceso no autorizado a las áreas del equipo, instale tarjetas de acceso al sistema, protectores de teclado, etc.

Implica los siguientes pasos:

- Identificar recursos de red confidenciales.
- Determinar la correspondencia entre recursos de red confidenciales y un conjunto de recursos de red
- Usuario.
- Supervise los puntos de acceso en busca de recursos de red confidenciales.
- Registrar el acceso no autorizado a recursos de red confidenciales. (Ing.Aldo N.Bianchi, 2015)

2.5 Protocolo de administración de red

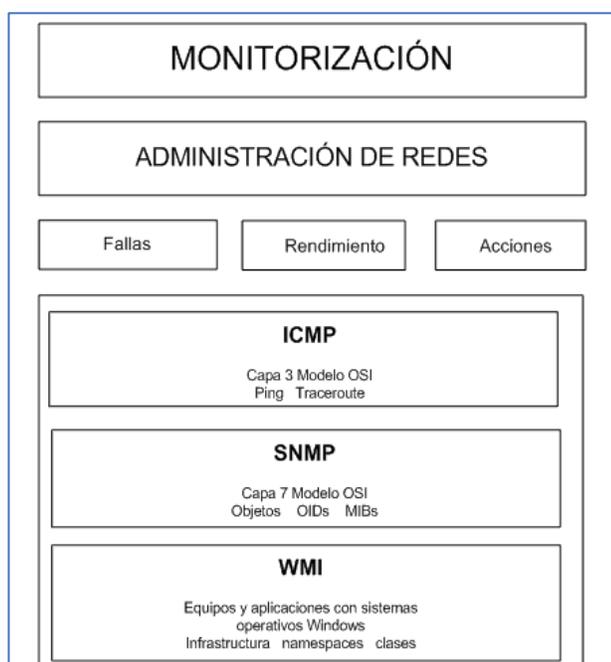
Se ejecuta entre la entidad NOC administradora y el dispositivo administrado (hardware o software); el protocolo le permite verificar el estado del dispositivo y realizar las acciones deseadas a través de los dos agentes mencionados. (UNAN, 2017). Un protocolo de red o comunicación es un conjunto de convenciones y estándares que especifican cómo realizar el intercambio de datos y comandos para enviar y recibir información entre los elementos de la red. La especificación especifica el contenido, el

formato de datos, la velocidad (emisor-receptor) y el manejo de errores en la red. Los protocolos más comunes e importantes en la gestión de redes son:

Todos los protocolos de gestión proponen una arquitectura y procedimientos para extraer, recopilar, transmitir, almacenar y reportar información de gestión de elementos gestionados.

Figura 3

Protocolo de administración de red



Nota. En la figura se observa el diagrama simplificado de un sistema de administración de redes. Tomado de (Rosa, 2021)

2.5.1 SNMP (Simple Network Management Protocol)

Protocolo Simple de Administración de Red. Es un protocolo de capa de aplicación de la suite TCP/IP que ha mejorado con el tiempo en SNMPv2, SNMPv2c y la versión actual de SNMPv3. SNMP se utiliza para enviar información entre elementos, estaciones de gestión y agentes en elementos de red.

2.5.2 CMIP (Common Management Information Protocol)

Protocolo común de administración de información, diseñado para tener en cuenta los errores y fallas de SNMP y convertirse en un administrador de red más poderoso y detallado. CMIP consta de seis protocolos: CMISE ISO 9595/9596, ACSE ISO 8649/8650, ROSE ISO 9072 -1/2, Presentación ISO, Sesión ISO, TRANSPORT ISO.

2.5.3 CORBA (Common Object Request Broker Architecture)

Patrón genérico de proxy en solicitudes de objetos. Fue introducido en 1991 y estandarizado por OMG (Grupo de gestión de objetos), el Grupo de gestión de objetos. CORBA es una arquitectura de programación distribuida diseñada para admitir objetos independientemente de su ubicación en una red o computadora.

2.6 Historia de los servidores de red

Castillo (2016) establece que:

En los primeros tiempos de la computación cliente-servidor, cada aplicación tenía su propio programa cliente y su interfaz de usuario, estos tenían que ser instalados separadamente en cada estación de trabajo de los usuarios. Una mejora al servidor, como parte de la aplicación, requería típicamente una mejora de los clientes instalados en cada una de las estaciones de trabajo, añadiendo un costo de soporte técnico y disminuyendo la eficiencia del personal. (p.28)

Un servidor de red actúa como una base de almacenamiento y contiene partes de software y hardware. Como tal, su historia más corta se remonta a la llegada de las computadoras e Internet, que primero dieron paso a las páginas web. Por su parte, los servidores web actualmente mantenidos se utilizan como almacenes de información cuando se navega por Internet.

De acuerdo con IONOS (2019) el desarrollo del servidor web estuvo estrechamente relacionado con el físico e informático británico Tim Berners-Lee, quien en 1989 sugirió que el intercambio de información del CERN (Organización Europea para la Investigación Nuclear) debería realizarse a través de un sistema de hipertexto más simple y rápido. "En 1990, junto con Robert Cailliau, propuso un proyecto que, con el tiempo, junto con el primer servidor web llamado "CERN httpd", el primer navegador web y otros elementos fundamentales de Internet, como HTML y HTTP. Este es hoy Berners-Lee es considerado el fundador de Internet.

2.6.1 Tipos de servidores de red

Los servidores no difieren mucho en arquitectura de las PC normales, ya sean servidores o PC, tienen los mismos componentes básicos, CPU, RAM, almacenamiento, etc. La diferencia entre ellos es que generalmente tienen un hardware más potente y permiten aprovechar al máximo. Aprovecha los recursos de un servidor web dependen de sus capacidades, por ejemplo, los servidores de aplicaciones generalmente tienen mucha capacidad de RAM y CPU para manejar solicitudes, ya que generalmente implican muchas demandas computacionales. (León, 2021)

Según DocuSign (2020) "Los tipos de servidores han servido como procesadores de miles de datos como correos electrónicos, documentos de texto, audios, videos, imágenes, programas, servicios empresariales, bases de datos, y muchas". (p.1) Se observa a continuación los tipos de servidores resumidos en una tabla.

Tabla 1*Tipos de servidores*

Tipo de servidor	Descripción
Servidor email	<ul style="list-style-type: none"> • Uno de los más antiguos • Funciona como una especie de oficina de correo para almacenar, recibir, enviar y permitir múltiples operaciones. • Posee subtipos: <ul style="list-style-type: none"> ○ PO3: retiene emails hasta que el usuario lo abre. ○ IMAP: permite interactuar con la información recibida. Sin descargarla en el equipo. ○ SWTP: Administra todos los emails salientes.
Servidores web	<ul style="list-style-type: none"> • Tras casi 28 años de Internet, según El Tiempo, existen más de 1.7 mil millones de páginas web, y cada una de ellas debe estar almacenada dentro de un servidor. • Guardados en formato HTML • Los servidores web también puede ser: <ul style="list-style-type: none"> ○ Apache: multiplataforma que brinda estabilidad y seguridad. ○ Microsoft IIS: solo funciona para sistemas Windows. ○ Sun Java System Web Server: servidor de código abierto. ○ Lighttpd: muy ligero y rápido. ○ Servidores virtuales: te brindan la posibilidad de optimizar costos en hardware.
Servidores con base datos	<p>Son dispositivos diseñados para almacenar grandes cantidades de información y poder gestionar los datos uno a uno.</p>
Servidores cloud	<p>Se utilizan para almacenar grandes cantidades de datos, protegiendo así la información de organizaciones o personas físicas.</p>

Tipo de servidor	Descripción
Servidor DNS	Son los encargados de gestionar los nombres de los dominios web. Su trabajo es crear un vínculo entre el dominio del sitio y su IP.
Servidor Telnet	Se utiliza principalmente en telecomunicaciones. Un protocolo que permite resolver problemas de red relacionados con la telefonía.
Servidor SIP	Su trabajo es establecer una conexión para telefonía por Internet. No transmite audio ni video, solo almacena direcciones IP.
Servidor FTP	Permite transferir archivos y datos entre otras computadoras y servidores.
Servidor del acceso remoto (RAS)	Controla la línea de módem del computadora u otros medios de comunicación por Internet.
Servidor compartido	Proporcionan espacio para almacenar información mientras comparten recursos con RAM, CPU, sistema operativo, conexión a Internet y dirección IP.

Nota. La tabla representa los tipos de servidores. Tomado de (DocuSign, 2020)

2.7 Open Source y Software libre

La idea detrás del código abierto es simple, evoluciona, se desarrolla y mejora cuando los programadores en Internet pueden leer, modificar y redistribuir el código fuente de un programa. Los usuarios pueden adaptarse a sus necesidades, corregir sus errores y más. Y esto puede suceder tan rápido que es inimaginable para aquellos que están acostumbrados a la velocidad de los procesos comerciales. A diferencia del código cerrado, el código abierto permite que varios programadores lean, modifiquen y redistribuyan el código fuente de un programa, lo que permite que el programa

evolucione con el tiempo. Las personas lo mejoran, modifican y corrigen errores a un ritmo mucho más rápido que el desarrollo de software tradicional o cerrado, lo que da como resultado un mejor software.

Todo el mundo sabe que Internet es una de las herramientas más poderosas e importantes en la actualidad, pero pocas personas se dan cuenta de que la mayoría de los sitios web que existen y los correos electrónicos que se intercambian todos los días en Internet son atendidos por programas de código abierto, incluso muy importante El sistema de dominio, que nos permite referirnos a los servidores de Internet usando palabras en lugar de números, se basa completamente en código abierto. Entonces, no hay duda de que Internet y su impacto económico y social actual en el mundo existen debido al código abierto. El código abierto está cambiando los viejos planes y las reglas rígidas de manera pragmática y lógica, a menudo amenazando a las empresas establecidas (como Microsoft) que, paradójicamente, afirman su superioridad en calidad y soporte, mientras prefieren emprender acciones legales como base para la defensa, a través patentes y patrañas, en parte de hacerlo en el plano de la excelencia técnica.

(Altavoz.net, 2021)

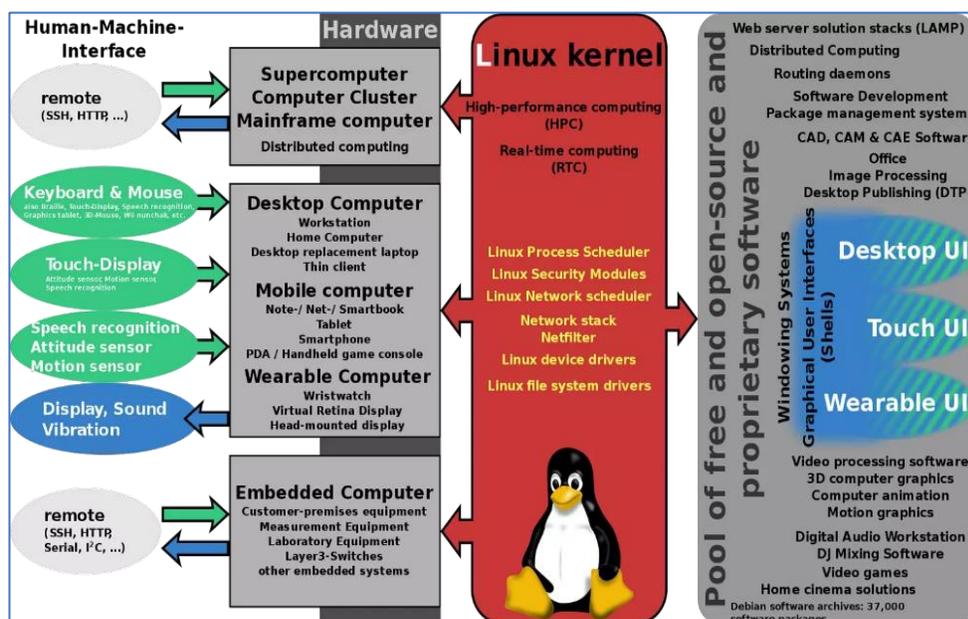
2.7.1 Sistema operativo Linux

Linux es un sistema operativo completamente libre y por lo tanto gratuito. A diferencia de Windows o macOS, el producto no es propiedad de una empresa y, por lo tanto, tiene un carácter gratuito, sino que es propiedad de un gran número de empresas o personas que contribuyen a su desarrollo y crean sus propias distribuciones de Linux. En definitiva, Linux es un sistema formado por varios proyectos, entre los que destacan GNU y la Free Software Foundation, y el propio kernel de Linux, liderado por Linus Torvalds. Su desarrollo es uno de los mejores ejemplos de software libre, y cualquiera

puede usar, modificar y distribuir libremente todo su código fuente bajo los términos de GPL o GNU General Public License y otras licencias. (Adeva, 2021)

Figura 4

Arquitectura de sistema operativo Linux



Nota. En la figura se observa la estructura de Linux. Tomada de (Adeva, 2021)

2.7.2 Componentes de Linux

El sistema operativo Linux sigue un diseño modular, que es clave para sus múltiples variantes y distribuciones. El cargador de arranque es responsable de iniciar el kernel de Linux. El kernel es el corazón del sistema Linux, gestiona el acceso a la red, programa los procesos o las aplicaciones, gestiona los periféricos básicos y supervisa los servicios del sistema de archivos.

Pero en realidad son muchos desarrolladores de terceros y proyectos GNU los que proporcionan al kernel de Linux características avanzadas para proporcionar un sistema operativo completamente implementado. Por ejemplo, hay módulos para proporcionar una interfaz de línea de comandos, implementar una interfaz gráfica de

usuario, administrar la seguridad, proporcionar servicios de entrada de video o audio y muchos otros, cada uno de los cuales puede modificarse y optimizarse para formar una distribución única para una tarea específica.

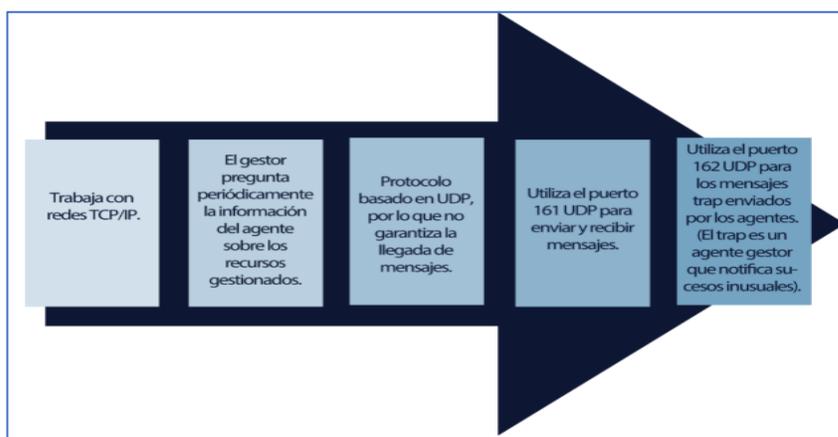
El software del gestor de paquetes suele agregar, actualizar o eliminar componentes de software bajo el sistema operativo Linux. Ejemplos de gestores de paquetes incluyen dpkg, OpenPKG, RPM Package Manager y Zero Install. (Bigelow, 2021)

2.7.3 SNMP en Linux

En una red configurada con SNMP, consistirá principalmente en dispositivos que contienen agentes SNMP. Un agente es un programa que recopila información sobre el hardware, la organiza en entradas predefinidas y responde a las consultas mediante el protocolo SNMP. El núcleo de un sistema de gestión SNMP es leer y escribir parámetros operativos de dispositivos remotos. Estos parámetros se denominan OID (Object Identifiers). (COMPILAR, 2021)

Figura 5

Características del protocolo SNMP



Nota. En la figura se detallan las principales características del protocolo. Tomado de (UNAN, 2017)

Al usar SNMP para acceder a los datos de administración de la red (como paquetes por segundo, índices de error de la red, etc.), los administradores de la red pueden administrar el rendimiento de la red y solucionar los problemas de la red. Hay dos versiones de SNMP, la versión 1 es el SNMP original, desarrollado por Case, McGlorie, Rose y Waldbuser, la versión 2 contiene: mejoras de seguridad y mejoras en la arquitectura de administración y operación del protocolo. (Ing.Aldo N.Bianchi, 2015)

2.8 Versiones de SNMP

Las versiones del protocolo SNMP más utilizadas son SNMPv1 y SNMPv2. La última versión de SNMPv3 tiene cambios importantes en comparación con su antecesor, especialmente en lo que respecta a temas de seguridad, sin embargo, no es muy utilizado por la comunidad internacional.

2.8.1 SNMPv1

Fue la versión inicial del protocolo y sigue siendo muy utilizado, principalmente por la sencillez del esquema de autenticación que emplea, aunque no es especialmente seguro. La primera versión se diseñó en un momento en que se prioriza la regulación de equipos de red en rápido crecimiento y no se le prestaba la atención que merecía al aspecto de seguridad. En este sentido, por ejemplo, la autenticación del dispositivo se realiza únicamente mediante una cadena de octetos transmitida en texto plano. (Ing.Aldo N.Bianchi, 2015)

2.8.2 SNMPv2

Incluye mejoras en rendimiento, seguridad, confidencialidad y comunicación entre estaciones de gestión. Se ha introducido un nuevo tipo de mensaje para la gestión de dispositivos. Debido a varias clases (tipos), la segunda versión de SNMP no fue aceptada inicialmente debido a su complejidad y poca compatibilidad con la versión

anterior del protocolo; sin embargo, su última actualización logró la compatibilidad, y simplificó su uso y mejorando la seguridad de la anterior versión, por lo que es la más utilizada en la actualidad. (Ing.Aldo N.Bianchi, 2015)

2.8.3 SNMPv3

Proporciona importantes funciones de seguridad y configuración remota y constituye la mejor variante en cuanto a las medidas de seguridad que contiene y su rendimiento. También incorpora comprobaciones de integridad y criptográficas a la hora de autenticarse. Desafortunadamente, aún no está ampliamente implementado en la mayoría de las organizaciones, aunque se recomienda esta versión.

2.9 Herramientas para el monitoreo de redes

2.9.1 Nagios

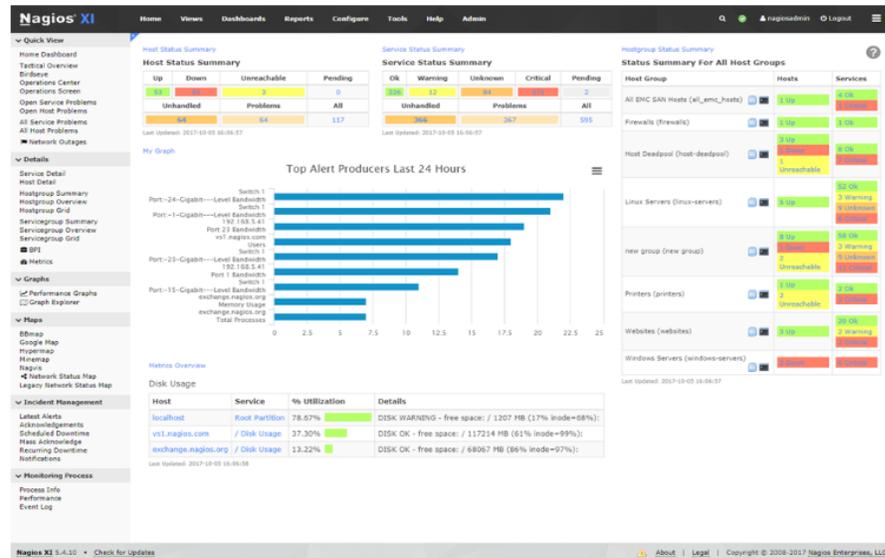
Nagios es una herramienta de monitoreo de red de código abierto que controla dispositivos y servicios (software) e informa su estado. Su función principal es el monitoreo de servicios de red (SMTP, POP3, HTTP, SNMP), que se puede ver en el monitoreo de recursos (carga del procesador, disco uso), memoria, estado del puerto. (Robledo, 2021)

Características

- Programación de capacidad
- Control del rendimiento
- Gestión del cambio
- Almacenamiento en la nube
- Virtualización de host
- Alta disponibilidad para equipos
- Mejora remota

Figura 6

Interface Principal de Nagios



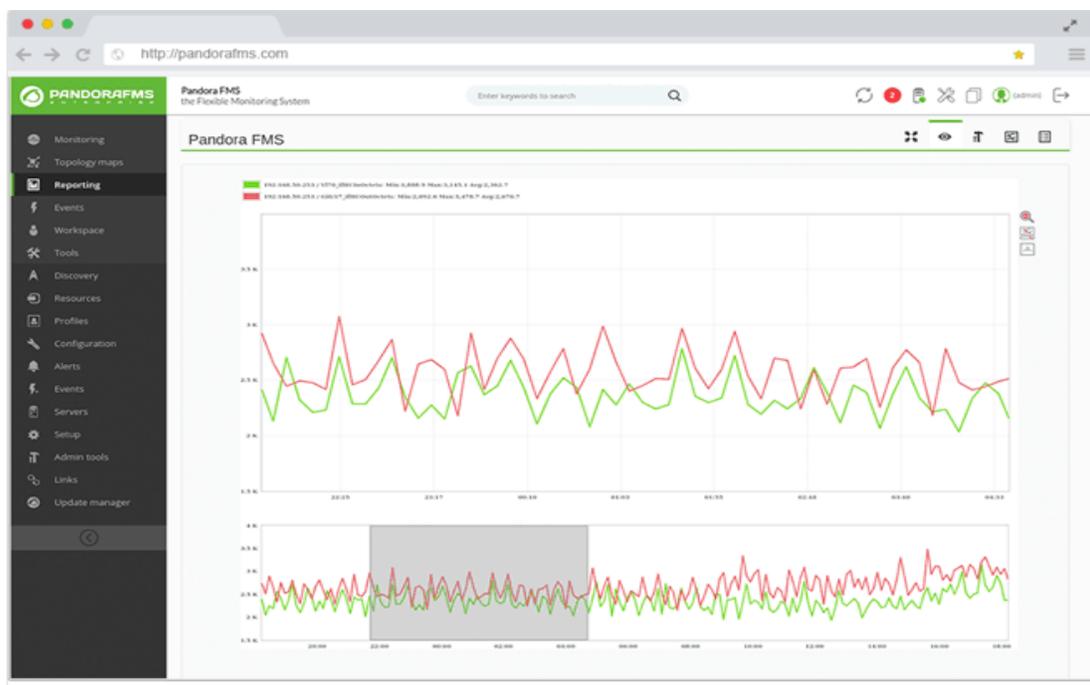
Nota. El gráfico representa la monitorización principal en Nagios. Tomado de (Open IT Networks, 2021)

2.9.2 Pandora FMS

Existen diferentes tipos de herramientas de monitorización de red, como Pandora FMS para empresas de distintos tamaños. Por ejemplo, las herramientas de monitoreo de red tradicionales son adecuadas para redes pequeñas y medianas, tanto cableadas como inalámbricas. Sin embargo, es posible que se requiera un conjunto más amplio de herramientas para entornos de redes distribuidas y redes empresariales que requieran servicios de monitoreo y visibilidad de varias cosas, como redes definidas por software, redes basadas en la nube y enlaces WAN. Y monitoreo de red de dispositivos móviles. (PANDORAFMS, 2021)

Figura 7

Interfaz de los diagramas de monitorización de Pandora FMS



Nota. El gráfico representa los valores obtenidos en la monitorización por Pandora FMS tomado de (PANDORAFMS, 2021)

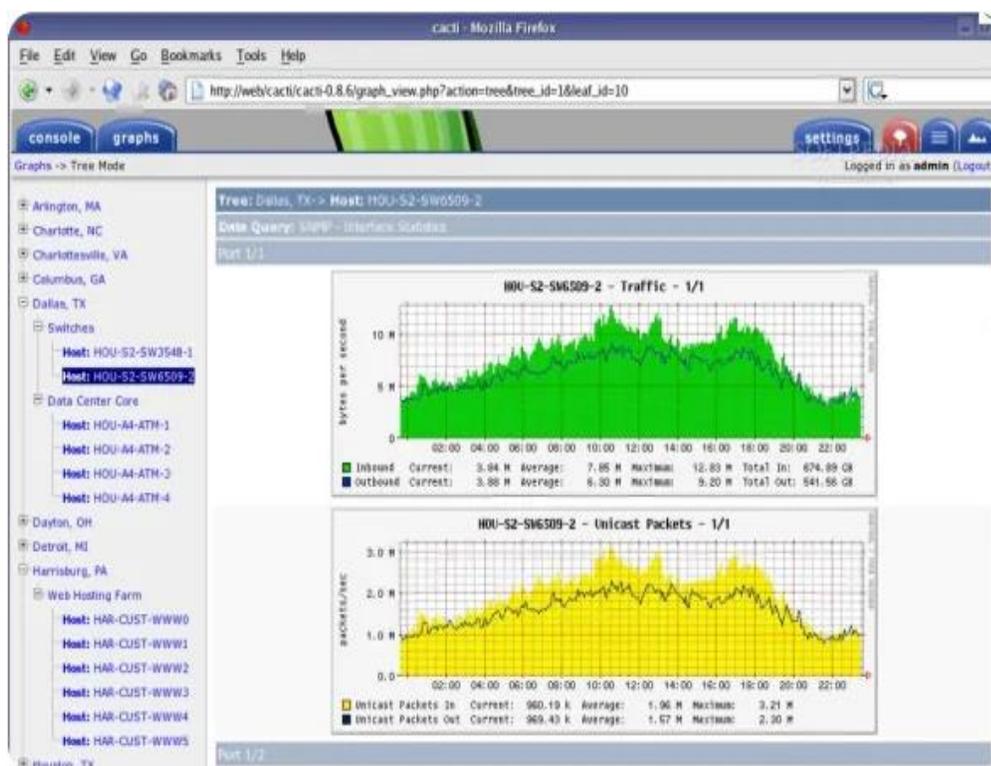
2.9.3 Cacti

Cacti es una interfaz gráfica conocida como RRDTOOL (Round Robin Date Tool), que es una herramienta para obtener gráficos de datos de series temporales y probar dispositivos de red para que respondan a algunas variables. equipo.

Existen diferentes tipos de herramientas de monitoreo. Una vez que se monitorea el dispositivo, cacti identificará la fuente de datos y su frecuencia de recopilación de datos. También puede generar diferentes tipos de gráficos. Para una mejor comprensión, cacti utiliza un diagrama de estructura de árbol. (Ramírez , 2017)

Figura 8

Interfaz principal de Cacti



Nota. El gráfico representa los diagramas de monitorización que se visualizan en Cacti.

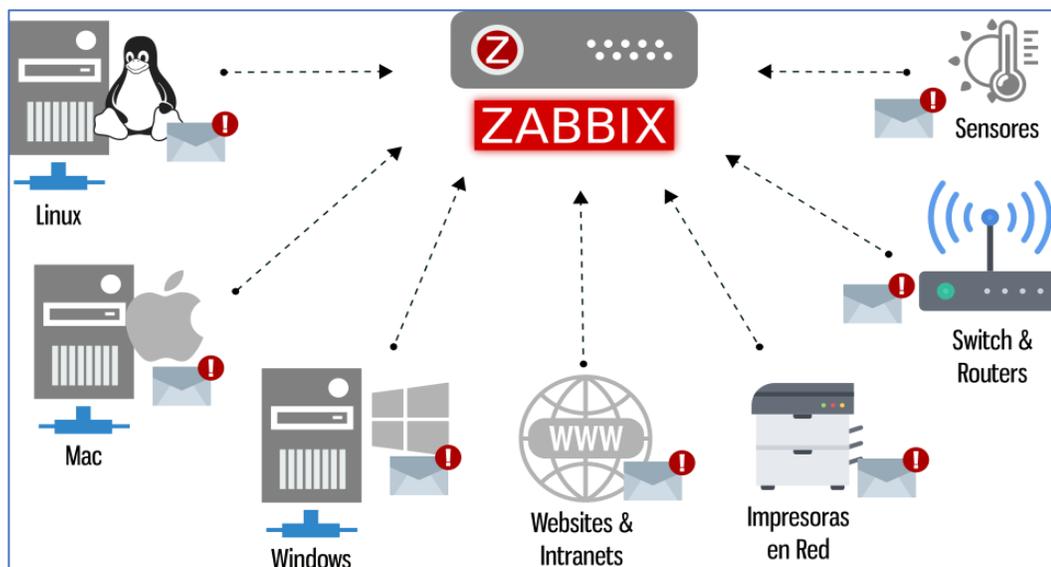
Tomado de (Ramírez , 2017)

2.9.4 Zabbix

Zabbix es una plataforma profesional de nivel empresarial sin concesiones creada para el monitoreo en tiempo real de miles de métricas recopiladas de decenas de miles de computadoras/servidores, dispositivos de red y máquinas virtuales, todos los cuales se pueden escalar fácilmente a entornos más grandes. mayor. La plataforma recopila y analiza con precisión estadísticas, métricas de rendimiento de la computadora, visualiza, recibe notificaciones sobre problemas actuales de la red y los habilita de inmediato, además utiliza soporte y desarrollo profesional. (Sri, 2018)

Figura 9

Arquitectura de un sistema de administración de red



Nota. En la figura se observa cómo interactúa Zabbix con dispositivos y ordenadores en la red. Tomado de (Sri, 2018)

Se puede identificar además características principales:

- Alto rendimiento y capacidad de monitoreo de dispositivos (Servidores, Hardware como Impresoras, Routers, entre otros)
- Monitoreo centralizado a través del administrador Web (FrontEnd)
- Agentes que puede instalarse en diferentes sistemas operativos ejemplo: Linux, Solaris, HP-UX, AIX, FreeBSD, OpenBSD, OS X, Tru64/OSF1, Windows 2000, Windows Server 2003, Windows XP, Windows Vista, Windows Server 2008, Windows 7, Windows 8 y recientemente Windows 2012.
- SLA que le permite analizar la calidad de los servicios prestados de su IT a su organización.

Zabbix ofrece monitoreo para "LAN, Redes locales" y "WAN, redes de área amplia". La aplicación se instala en un servidor (Linux) y luego es dedicada a "Recolectar información".

También se pueden determinar las principales características:

- Alto rendimiento y capacidades de monitoreo de dispositivos (hardware como servidores, impresoras, enrutadores, etc.)
- Monitoreo central a través del administrador web (front end)
- Agentes que se pueden instalar en diferentes sistemas operativos, por ejemplo: Linux, Solaris, HP-UX, AIX, FreeBSD, OpenBSD, OS X, Tru64/OSF1, Windows 2000, Windows Server 2003, Windows XP, Windows Vista, Windows Server 2008 , Windows 7, Windows 8 y, más recientemente, Windows 2012.
- SLAs que le permiten analizar la calidad del servicio que su TI brinda a su organización.

Zabbix proporciona monitoreo de "LAN, red local" y "WAN, red de área amplia". La aplicación se instala en el servidor (Linux) y luego se dedica a "recolectar información".

Proporciona una interfaz WEB en la que se muestra gráficamente toda la información que recopila. Tiene instalados agentes Linux, Mac y Windows en el "servidor" o "estación de trabajo" que le interesa monitorear. Además, esta solución le permite ver el estado de las impresoras, enrutadores, interruptores, sensores de temperatura y humedad, y más. (Hernández, 2020)-

2.10 Zabbix con otros agentes de monitorización

El servidor es el componente principal de Zabbix porque el servidor puede Inspección remota de servicios de red (como servidores web y servidores de servidor)

correo) a través de una simple verificación de servicio, además el agente informará Toda la información y estadísticas sobre la disponibilidad e integridad del servidor Esto convierte al servidor en un componente central ya que almacena todos los datos. Configuración, Estadísticas y Operadores.

Es una entidad del software Zabbix que Alerte proactivamente a los administradores cuando surjan problemas cualquier sistema monitoreado. Es decir, es el componente central. Responsable de recibir la información del reporte enviado por el agente, todos Se organizan la configuración, las estadísticas de datos y la manipulación de datos por el servidor. (Hernández, 2020)

2.10.1 Agente Zabbix

Los agentes de Zabbix son agentes que recopilan información operativa del sistema, donde se está ejecutando y reportando estos datos a los servidores para sus respectivos demandar. En caso de error (como un disco duro lleno el proceso de servicio está bloqueado), el agente Especialmente mal.

Los agentes de Zabbix son muy eficientes debido al uso de llamadas. El sistema recopila estadísticas de forma nativa. Es decir, se implementa en el host monitoreado (cliente), que es el encargado de recopilar los datos del host monitoreado, como CPU, memoria, base de datos y otros datos y luego envíarlos al servidor. (Hernández, 2020)

2.10.2 Interfaz Web

Para un fácil acceso a los datos de monitoreo y configuración Zabbix desde cualquier lugar y en cualquier plataforma, interfaces proporcionadas Basado en la web. La interfaz es parte del servidor, por lo general (pero no necesariamente) corriendo y corriendo servidor zabbix. (Hernández, 2020)

2.11 ¿Cómo funcionan los agentes en los servidores?

El agente es muy liviano y consume mínimos recursos en la computadora donde está instalado. Los agentes deben estar instalados de acuerdo a la versión del sistema operativo así como su base de datos y su respectivo Apache. (Hernandez, 2013)

2.11.1 Funcionamiento de monitoreo en Zabbix

Figura 10

Proceso de monitoreo en Zabbix



Nota. El gráfico representa el proceso del funcionamiento del monitoreo en zabbix.

Tomado de (Hernandez, 2013)

2.12 Zabbix con otros agentes de monitorización

Tabla 2

Comparación entre Zabbix y otros agentes de monitorización

Agentes de monitorización	Descripción	Contratación	Funcionamiento
Zabbix	Ayuda a definir una serie de sensores para diferentes usos	Es un software gratuito.	Usa MySQL, PostgreSQL, SQLite, Oracle o IBM DB2 como base de datos. Su backend está escrito en C y el frontend web está escrito en PHP.
NAGIOS	Esta herramienta ayuda monitoreando la disponibilidad de la red	Igual manera es de libre distribución	Se basa en el estado, generando alertas y alertas cuando el dispositivo monitoreado no se comporta como se esperaba.
SOLAR WINDS	es una herramienta de monitoreo de red de pago	Brinda un periodo de prueba gratis de 30 días.	Utiliza el módulo NPM (Network Performance Monitor) para realizar el monitoreo de la red.
Pandora FMS	Cuentan con las herramientas del cacti y nagios, permite un monitoreo en tiempo real de la red o conocido como Netflow	Es una herramienta de pago	Permite observar gráficas y el estado de la red mediante el monitoreo de equipos con ping, además realiza un mapa y revelación automática.
CACTI	Es una herramienta muy extendida para almacenar series de datos numéricas en escalas de tiempo	Es de libre distribución, la cual se basa en gráficas	Utiliza RRDTOol (Round Robin Database Tool Bases de datos circulares) para el manejo de gráficas siendo estas bastantes potentes y atractivas.

Nota. Información Tomado de (Vega, 2018)

2.13 Qué es Gns3

GNS3 es el software utilizado por cientos de miles de ingenieros de redes en todo el mundo para simular, configurar, probar y solucionar problemas de redes virtuales y reales. Le permite ejecutar pequeñas topologías que consisten en unos pocos dispositivos en una computadora portátil, así como alojar muchos dispositivos en múltiples servidores o incluso en la nube. (Telectronia, 2018)

2.13.1 Característica de Gns3

Para Carate & Pozo (2019) las características principales que se pueden destacar del simulador GNS3 son las:

- Funciona en cualquier plataforma de sistema operativo.
- Permite el diseño de redes complejas.
Permite simular una conexión de red real hacia Internet.
- Permite emular varias plataformas: Cisco IOS, IPS, Firewalls ASA y PIX, Junos.
- Tiene embebido los módulos: Dynamips, Dynagen, Qemu.
- Permite capturar paquetes mediante Wireshark. (p.20)

2.14 Qué es VMware WORKSTATION PRO

Según Carate & Pozo (2019) es un software de virtualización que permite ejecutar múltiples sistemas operativos en una sola computadora. Esto significa que le permite ejecutar múltiples entornos en su escritorio sin reiniciar. VMware reconoce la interoperabilidad entre los sistemas operativos y también permite el aislamiento y la protección de entornos operativos individuales, lo cual es útil al evaluar soluciones de TI, pruebas de aplicaciones o demostraciones de productos.

Las características que presenta son:

- Herramientas y funcionalidades para entornos empresariales.
- Permite compartir fácilmente archivos entre host y sistemas virtualizados.
- Es compatible con lectores de tarjetas inteligentes.
- Admite USB 3.0.
- Le permite crear instantáneas para restaurar fácilmente el estado de una máquina virtual
- Tiene una facilidad para compartir máquinas virtuales.
- Integración con vSphere7ESXi y vCloud Air.

Capítulo III

3 Desarrollo del proyecto

3.1 Introducción

La implementación de este servidor de administración de red es con fines de facilitar el control y administración de la red datos de la Escuela de Formación de Soldados Vencedores del Cenepa “ESFORSE” la cual será utilizada como una herramienta de trabajo, misma que ayudará a mejorar el tiempo de respuestas los equipos que se encuentren en la red monitoreada.

El objetivo principal para la implementación del servidor de administración de red es mejorar el tiempo de respuesta en el manejo del control y administración de la red de datos, la cual facilitara la resolución de los problemas de equipos que se encuentre monitorizados.

A continuación, se presenta el proceso de la implantación del servidor de administración de redes basado en software libre.

3.2 Planificación

3.2.1 *Propósito*

El presente documento tiene como finalidad definir y cumplir con los requerimientos funcionales y no funcionales para la implementación del servidor de administración de red de datos de la Escuela de Formación de Soldados Vencedores del Cenepa “ESFORSE”, permitiendo gestionar el control y administración al área de las TICs.

Una vez cumplido con todos los requerimientos funcionales y no funcionales de la implementación del servidor de administración, se realizan pruebas de monitoreo en los equipos conectados a la red.

3.2.2 Alcance

En el control de los dispositivos que se encuentran conectados a la red, el cual permite la administración de la red de datos para la Escuela de Formación de Soldados Vencedores del Cenepa “ESFORSE”.

3.2.3 Personales involucrados

Tabla 3

Personal Involucrado 1

Nombre	Sangucho Sangucho Nelson Patricio
Rol	Desarrollador
Categoría profesional	Tecnología en Redes y Telecomunicaciones
Información de contacto	Npsangucho1@espe.edu.ec / 0958856196
Aprobación	

Nota. Datos del personal involucrado en la implementación del servidor

3.2.4 Perspectiva del producto

La Escuela de Formación de Soldado Vencedores del Cenepa “ESFORSE” cuenta con una red interna de la Escuela, la cual engloba los dispositivos que se encuentran conectados a la red. El presente documento se encargará de la monitorización del hardware y software, lo que permite facilidad y eficacia al momento de hacer la monitorización de la red.

3.3 Requisitos funcionales

En esta sección se dará una descripción global de la implementación del servidor de monitorización Zabbix el cual se ha desarrollado, permitiendo dar una visualización de los dispositivos monitorizados.

3.4 Servidor Zabbix

En la investigación del servidor Zabbix se sabe que se utiliza para monitorear y administrar dispositivos o dispositivos de red, servidores, sistemas operativos, se puede agregar como host activando el protocolo SNMP, y a su vez también se puede instalar el agente Zabbix. como en el dispositivo en el servidor. Para llevar a cabo su implementación se verifican los componentes a instalar como agente Zabbix, server Zabbix, interfaz web y bases de datos requeridas para su funcionamiento.

Figura 11

Funcionamiento de Zabbix

The screenshot displays the Zabbix web interface with the following components and annotations:

- 1**: Global view summary showing system information and a status bar with colored indicators (green, red, orange).
- 2**: Configuration form for a host, including fields for DNS, Port, and Severity (Not classified, Warning, High, Information, Average, Disaster).
- 3**: Items configuration page showing details for a specific item, including Name, Type, and Host.
- 4**: Triggers configuration page showing details for a specific trigger, including Name, Severity, and Expression.
- 5**: Hosts table listing monitored hosts with columns for Name, Interface, and Availability.

Name	Interface	Availability
servidor-zabbix	10.21.227.44: 10050	ZBX OK

Nota. El gráfico representa las funciones principales para el monitoreo de un dispositivo de red.

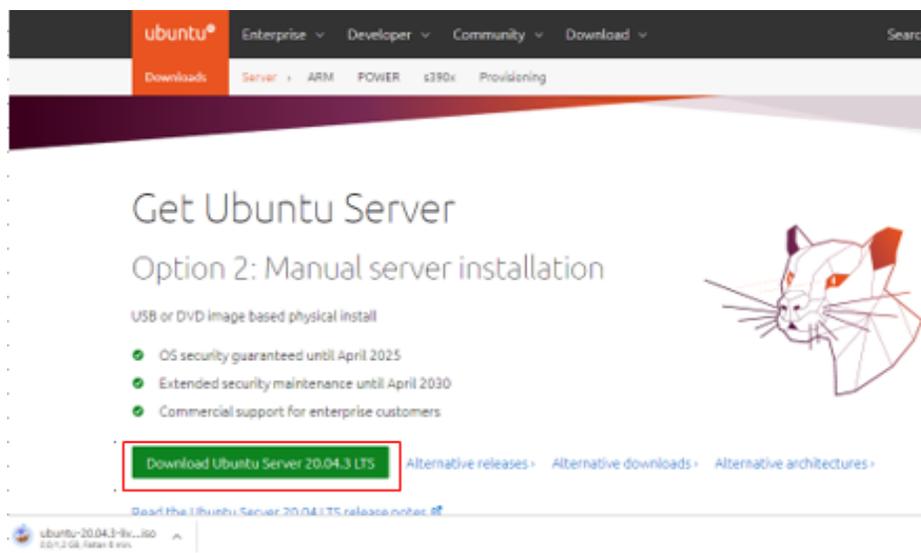
1. Una vez instalado el agente Zabbix y todos sus repositorios, representa el entorno gráfico del servidor.
2. El host es la opción donde colocamos el dispositivo que queremos monitorear. Los dispositivos monitoreados a través del protocolo snmp, a su vez, pueden tener instalados agentes Zabbix.
3. Estos elementos recopilan información sobre los dispositivos de red, como la memoria, el tamaño del disco y la carga de la CPU, utilizando claves como parámetros del servidor.
4. Los disparadores son datos recopilados de elementos que representan el estado del sistema, donde los parámetros creados en los elementos son condicionales.
5. Las notificaciones son problemas presentados por las condiciones establecidas en el disparador y se mostrarán en el tablero.

3.4.1 Descarga del sistema operativo Ubuntu server

En la página de inicio de Ubuntu accedemos a las opciones de descarga, aquí elegiremos el tipo de sistema operativo que puede ser Ubuntu Desktop, Ubuntu Server, en este caso se descarga la ISO de Ubuntu Server usando la opción de instalar manualmente el servidor.

Figura 12

Descarga del la ISO de Ubuntu Server



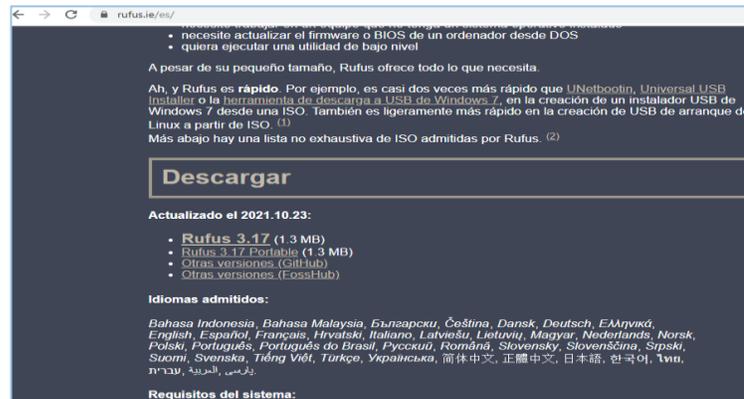
Nota. El gráfico representa la descarga de la ISO de Ubuntu Server. Tomada de (Ubuntu, 2022)

3.4.2 Descarga del programa Rufus portable

Accedemos en el navegador de Google a la página principal de Rufus, en donde en su interfaz principal encontraremos las opciones de descarga, en esta cuestión se instalará de forma portable y luego se procederá a ejecutar el programa.

Figura 13

Descarga de software Rufus



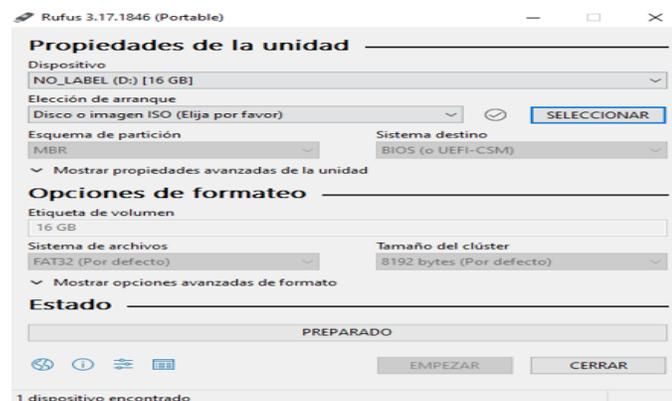
Nota. La figura representa la interfaz principal para la descarga de Rufus. Tomado de (Rufus, 2022)

3.4.3 Ejecución del programa Rufus

Una vez descargada la imagen ISO del sistema operativo Ubuntu Server 20.04 se procede a ejecutar el programa Rufus, el cual nos permitirá crear una USB de arranque la misma que será utilizada en la instalación del servidor.

Figura 14

Interfaz principal de Rufus



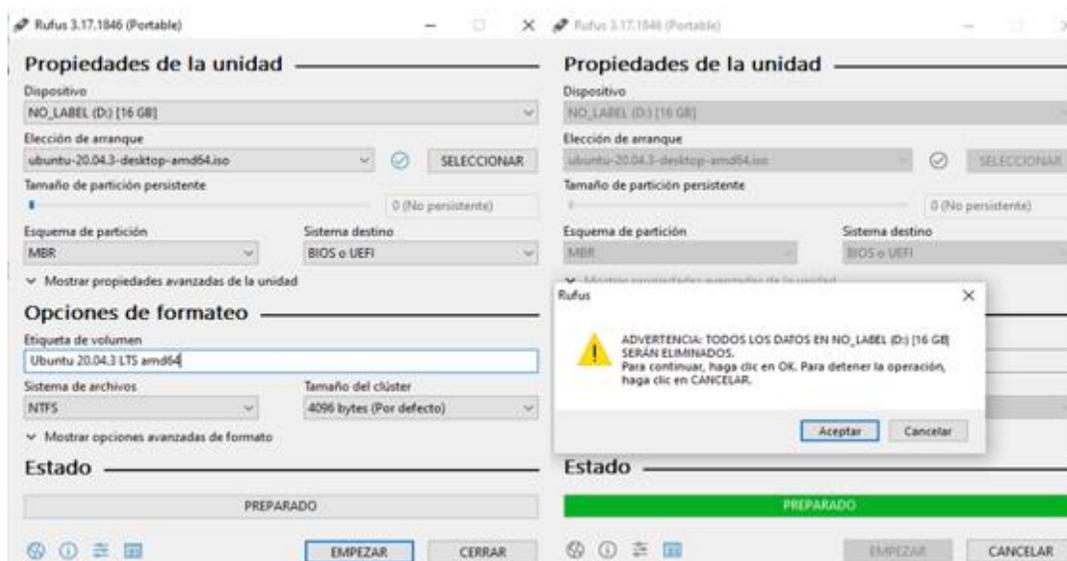
Nota. El gráfico representa la interfaz principal de Rufus para el inicio del booteo

3.4.4 Selección de la ISO de Ubuntu y booteo en Rufus

En la opción elección de arranque, seleccionamos la imagen ISO de Ubuntu Server 20.04, teniendo en cuenta el esquema de partición que se va utilizar para realizar el arranque. En la opción de formateo seleccionamos el sistema de archivo que se va utilizar “NTFS”, y seleccionamos la opción empezar para que inicie el Booteo.

Figura 15

Booteo de Ubuntu Server



Nota. El gráfico representa los pasos a seguir para empezar el booteo en la USB.

3.4.5 Inicio de la instalación de Ubuntu Server

Una vez finalizado el booteo de la USB se ejecuta el arranque del sistema operativo, donde automáticamente nos muestra la interfaz de instalación del sistema operativos en el monitor. En este paso el disco es verificado para una correcta instalación.

Figura 16

Interfaz de inicialización de instalación



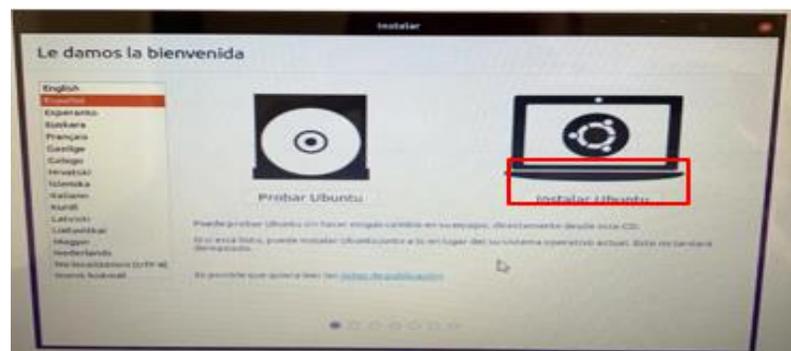
Nota. El gráfico representa la interfaz de instalación y el chequeo del disco.

3.4.6 Selección de idioma de instalación de Ubuntu Server

Una vez verificado los archivos del disco, el instalador del sistema operativo permite al usuario la elección del idioma en que se va a instalar Ubuntu Server, en este caso elegiremos el español. Ubuntu facilita dos opciones al momento de la instalación los cuales son probar el sistema operativo y otro instalarlo.

Figura 17

Interfaz de selección de idioma



Nota. El gráfico representa los idiomas opcionales para la instalación de Ubuntu.

3.4.7 Disposición del teclado

El siguiente paso consistirá en configurar el tipo de teclado, que debería estar fijado de manera automática de acuerdo al idioma elegido. Para esta instalación seleccionaremos el teclado Latino Americano.

Figura 18

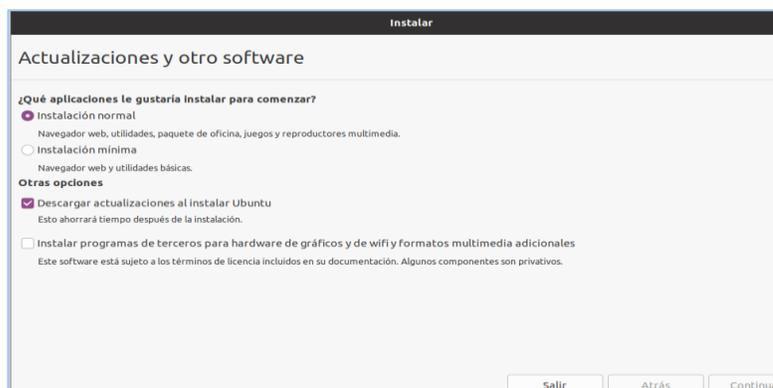
Interfaz de selección de teclado



Nota. El gráfico representa las opciones para selección del idioma del sistema operativo.

3.4.8 Actualización y otro softwares

En estas dos opciones se determina el tipo de instalación que se va a realizar, conjuntamente con las actualizaciones que se quieren descargar. La instalación de Ubuntu Server se realiza en una instalación normal, el cual permite la accesibilidad a todos sus servicios.

Figura 19*Interfaz de actualizaciones y otros softwares*

Nota. El gráfico representa la configuración de las actualizaciones en Ubuntu Server.

3.4.9 Tipo de instalación

En el tipo de instalación se muestran las dos opciones que nos permite Ubuntu realizar, en donde la opción elegida será borrar disco e instalar Ubuntu server. Asimismo se puede elegir más opciones en donde podremos instalar ya sea en una solo partición de disco o borrar todas las particiones que tenga.

Figura 20*Interfaz principal de tipos de instalación*

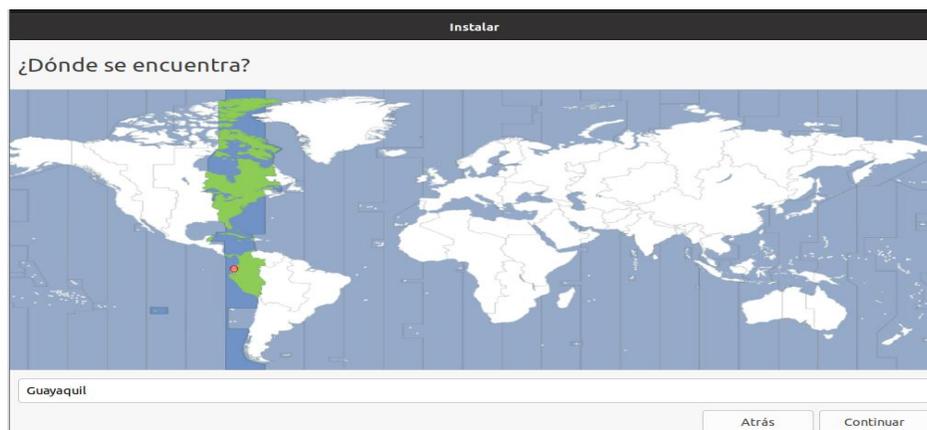
Nota. El gráfico representa las opciones de instalación del sistema operativo.

3.4.10 Localización

Para que nuestro Ubuntu server tenga un funcionamiento adecuado elegiremos la zona horaria en donde nos encontremos, ya que mediante esta acción el sistema operativo fija la hora en el sistema de acuerdo al zona horaria y lugar elegido.

Figura 21

Interfaz gráfica de la zona horaria



Nota. El gráfico representa el lugar y la zona horaria en donde nos encontramos.

3.4.11 Creación de usuario y asignación del nombre del servidor

En esta interfaz colocaremos el nombre de usuario y el nombre del servidor como se lo va asignar, es necesario asignar una contraseña que brinde la seguridad de nuestro servidor Ubuntu, y activar la opción solicitar mi contraseña para iniciar sesión.

Figura 22

Creación de usuario



Instalar

¿Quién es usted?

Su nombre: ✓

El nombre de su equipo: ✓
El nombre que utiliza al comunicarse con otros equipos.

Elija un nombre de usuario: ✓

Elija una contraseña: **Contraseña corta**

Confirme su contraseña: ✓

Iniciar sesión automáticamente

Solicitar mi contraseña para iniciar sesión

Use Active Directory

You'll enter domain and other details in the next step.

Atrás Continuar

Nota. El gráfico representa las opciones en donde se puede colocar el nombre del servidor y asignar su respectiva contraseña.

3.4.12 Visualización del proceso de instalación

La interfaz de bienvenida del proceso de instalación del Ubuntu Server, tiende a demorar por tal razón es necesario esperar unos minutos mientras se instala todos los paquetes necesarios para la funcionalidad de Ubuntu.

Figura 23

Interfaz de instalación de Ubuntu



Nota. El gráfico representa el inicio de la instalación de los paquetes de Ubuntu

3.5 Instalación de Zabbix en el servidor Ubuntu Server

Al momento de elegir el mejor software de monitoreo entre Nagios, Cacti, Zabbix y Pandora FMS se escogió Zabbix, ya que es una herramienta open source donde se puede administrar mediante una interfaz web, además posee una gran cantidad de pantallas y gráficos que se pueden crear de forma sencilla. Todas estas y más características se muestran en la Tabla 4 de forma detallada para dar una visión global de las 4 herramientas de monitorización.

Tabla 4

Comparación de las herramientas de monitoreo

Herramientas	Zabbix	Cacti	Nagios	Pandora FMS
Características y requerimientos				
Monitoreo de la red	X	X	X	X
Monitoreo en servidores	X	X	X	X
Monitoreo en aplicaciones	X	X	X	X

Herramientas	Zabbix	Cacti	Nagios	Pandora FMS
Características y requerimientos				
Monitoreo para máquinas virtuales	X	X	X	X
Monitoreo de los correos electrónicos	X	X	X	X
Monitoreo en la base de datos	X	X	X	X
Temperatura de seguridad	X		X	X
Monitoreo de rendimiento de PC	X	X	X	
Instalación en Linux	X	X	X	X
Dificultad de instalación			X	X
Verificación a través de correo electrónico.	X	X	X	X
Fáciles usos	X	X		X
Gráficas	X	X	X	X
Mapas	X	X	X	
SNMP Administración	X	X	X	X

Nota. La tabla representa la comparación de las características y requerimientos de las herramientas de monitorización.

3.5.1 Requerimientos para la instalación del servidor Zabbix

Para la utilización de Zabbix es necesario verificar el espacio de la memoria en el disco duro ya que Zabbix requiere una memoria física de 128 MB y 256 MB, igualmente requiere tener un sistema operativo Linux ya instalado para su ejecución. La cantidad de memoria que debe poseer el disco dependerá del número de dispositivos a monitorear.

3.5.2 Selección de la versión de Zabbix

Para instalar Zabbix en Ubuntu 20.04 acceder a la página oficial y en la sección de descargas seleccionar la versión de Zabbix 5.0 LTS en distribución de SO Ubuntu,

versión del sistema operativo 20.04 con una base de datos MySQL y un servidor web Apache.

Figura 24

Interfaz principal para la descarga de Zabbix



Nota. El gráfico representa la versión de Zabbix y componentes a instalar. Tomado de (ZABBIX, 2022)

3.5.3 Instalación del repositorio de Zabbix en Ubuntu

En el servidor Ubuntu 20.04 ingresamos al terminal colocamos el comando `sudo su` con la respectiva contraseña, para acceder al directorio raíz `root`. Instalar el repositorio de Zabbix desde la página principal, el cual hay que copiar y ejecutar los enlaces para descargar los paquetes que contiene la información del repositorio de Zabbix.

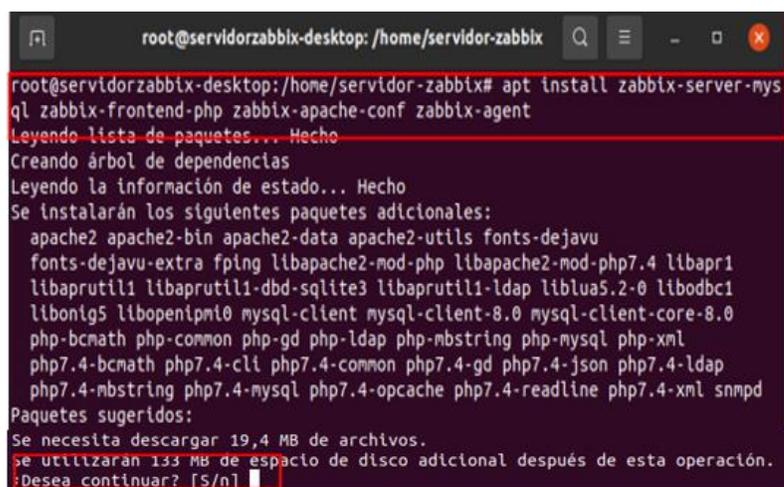
Instalado el primer código se procede a instalar el segundo código del enlace, el mismo que actualiza los paquetes que no se hayan instalado y los paquetes rotos que se encuentre en el repositorio de Zabbix, y por último copiamos el tercer código del enlace en la terminal de Ubuntu, para actualizar todos los repositorios locales que se encuentre en el sistema operativo.

3.5.4 Instalación del servidor, con su respectivo agente Zabbix

En la instalación del servidor, interfaz, agente Zabbix y conjuntamente con el soporte de la base de datos MySQL permite la recolección de los datos sobre el estado de nuestro servidor, donde posteriormente se podrá visualizar en la interfaz gráfica de monitorización. En la ejecución se preguntará si quiere continuar y presionar yes para continuar.

Figura 27

Instalación de Zabbix server, MySQL y Zabbix-apache



```

root@servidorzabbix-desktop: /home/servidor-zabbix
root@servidorzabbix-desktop:/home/servidor-zabbix# apt install zabbix-server-mys
ql zabbix-frontend-php zabbix-apache-conf zabbix-agent
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
apache2 apache2-bin apache2-data apache2-utils fonts-dejavu
fonts-dejavu-extra fping libapache2-mod-php libapache2-mod-php7.4 libapr1
libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap liblua5.2-0 libodbc1
libonig5 libopenipmi0 mysql-client mysql-client-8.0 mysql-client-core-8.0
php-bcmath php-common php-gd php-ldap php-mbstring php-mysql php-xml
php7.4-bcmath php7.4-cli php7.4-common php7.4-gd php7.4-json php7.4-ldap
php7.4-mbstring php7.4-mysql php7.4-opcache php7.4-readline php7.4-xml snmpd
Paquetes sugeridos:
Se necesita descargar 19,4 MB de archivos.
Se utilizarán 133 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n]

```

Nota. El gráfico representa la instalación del servidor Zabbix con su respectivo agente.

3.5.5 Instalación de la base de datos de Zabbix

Para el monitoreo con el servidor Zabbix es necesario tener un base de datos, el servidor recoge los datos de los agentes y los almacena para posteriormente utilizarlos, para el ingreso de la creación de la base de datos, primero ingresamos a la terminal de host con la contraseña password. Después se realiza la creación de la base de datos MySQL, completando la información requerida por Zabbix, también se crea un usuario para la base de datos y se establece una contraseña o se lo podría dejar por defecto.

Figura 28

Interfaz de la creación de la base de datos MySQL

```

root@servidorzabbix-desktop: /home/servidor-zabbix
root@servidorzabbix-desktop:/home/servidor-zabbix# mysql -uroot -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 8
Server version: 8.0.27-0ubuntu0.20.04.1 (Ubuntu)

Copyright (c) 2000, 2021, 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 utf8 collate utf8_bin;
Query OK, 1 row affected, 2 warnings (0,15 sec)

mysql> create user zabbix@localhost identified by 'password';
Query OK, 0 rows affected (0,09 sec)

mysql> grant all privileges on zabbix.* to zabbix@localhost;
Query OK, 0 rows affected (0,10 sec)

mysql> quit;

```

Nota. El gráfico representa la creación de la base de datos MySQL con su respectivo usuario.

3.5.6 Importación del esquema y los datos iniciales

En este paso configurar el esquema inicial e importar los datos de la base de datos de Zabbix e introducir la contraseña para el usuario MySQL Zabbix que se configuró en el paso anterior y utilizar zcat porque los datos en el archivo están comprimidos. Adicional al ejecutar el comando puede tardar 1 minuto.

Figura 29

Habilitación del host del servidor Zabbix

```

root@servidorzabbix-desktop: /home/servidor-zabbix
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 utf8 collate utf8_bin;
Query OK, 1 row affected, 2 warnings (0,15 sec)

mysql> create user zabbix@localhost identified by 'password';
Query OK, 0 rows affected (0,09 sec)

mysql> grant all privileges on zabbix.* to zabbix@localhost;
Query OK, 0 rows affected (0,10 sec)

mysql> quit;
Bye
root@servidorzabbix-desktop:/home/servidor-zabbix# zcat /usr/share/doc/zabbix-server-mysq
l*/create.sql.gz | mysql -uzabbix -p zabbix
Enter password:
root@servidorzabbix-desktop:/home/servidor-zabbix#
root@servidorzabbix-desktop:/home/servidor-zabbix#
root@servidorzabbix-desktop:/home/servidor-zabbix#

```

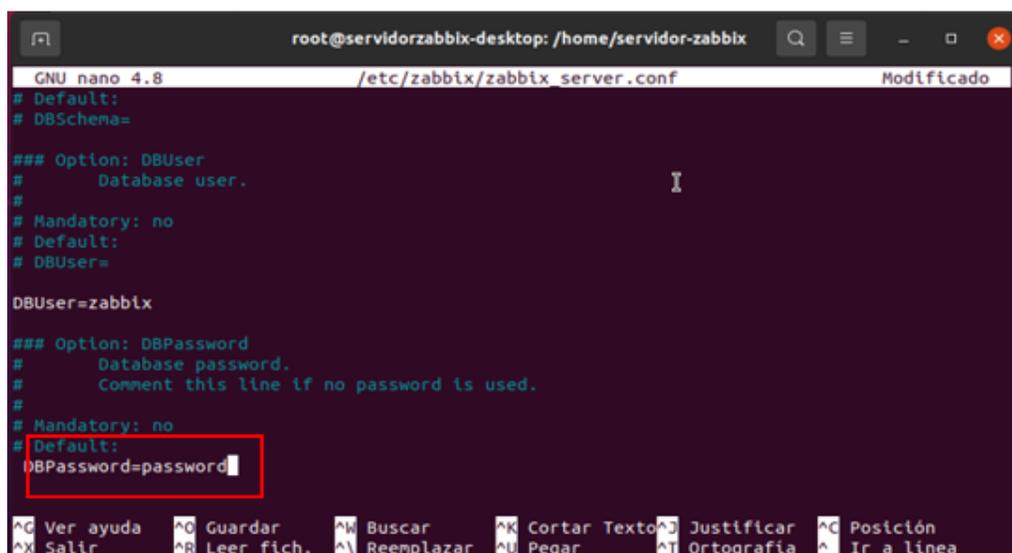
Nota. El gráfico representa la habilitación del host en el servidor Zabbix.

3.5.7 Configuración de la base de datos del servidor Zabbix

Para la utilización de la base de datos del servidor Zabbix, es necesario la configuración de la contraseña, para lo cual se debe establecer en la interfaz principal la línea de comando `sudo nano /etc/zabbix/zabbix_server.conf`. Al ejecutar el comando una vez iniciado buscamos el parámetro `DBpassword=password`, finalmente guardamos los cambios realizados.

Figura 30

Configuración de la base de datos



```
root@servidorzabbix-desktop: /home/servidor-zabbix
GNU nano 4.8 /etc/zabbix/zabbix_server.conf Modificado
# Default:
# DBSchema=

### Option: DBUser
# Database user.
# Mandatory: no
# Default:
# DBUser=
DBUser=zabbix

### Option: DBPassword
# Database password.
# Comment this line if no password is used.
# Mandatory: no
# Default:
DBPassword=password
```

Nota. El gráfico representa el cambio de la contraseña en la base de datos de Zabbix.

3.5.8 Configuración de la zona horaria para Frontend de Zabbix

En la configuración de la interfaz de Zabbix necesitas configuraciones especiales, ya que Zabbix está vinculado a php, posteriormente se accede al directorio que se encuentra ubicado en `sudo nano /etc/zabbix`, en donde nos permite cambiar la zona horaria del servidor Zabbix.

Figura 31

Cambio de la zona horaria para Frontend de Zabbix

```
GNU nano 4.8 /etc/apache2/conf-enabled/zabbix.conf
Allow from all

<IfModule mod_php5.c>
php_value max_execution_time 300
php_value memory_limit 128M
php_value post_max_size 16M
php_value upload_max_filesize 2M
php_value max_input_time 300
php_value max_input_vars 10000
php_value always_populate_raw_post_data -1
# php_value date.timezone Europe/Riga
</IfModule>
<IfModule mod_php7.c>
php_value max_execution_time 300
php_value memory_limit 128M
php_value post_max_size 16M
php_value upload_max_filesize 2M
php_value max_input_time 300
php_value max_input_vars 10000
php_value always_populate_raw_post_data -1
php_value date.timezone America/Guayaquil
</IfModule>
</Directory>
```

Nota. El gráfico representa el cambio de la zona horaria.

3.5.9 Iniciación del agente y del servidor Zabbix

Ejecutar los comandos para reiniciar el cual reiniciará el servidor de Zabbix y los procesos de agente para aplicar la nueva configuración realizada, digitamos el comando `enable` para habilitar el sistema para su inicialización.

Figura 32

Inicialización del sistema

```
root@servidorzabbix-desktop:/home/servidor-zabbix# systemctl restart zabbix-server zabbix-agent apache2
root@servidorzabbix-desktop:/home/servidor-zabbix#
Executing: /lib/systemd/systemd-sysv-install enable zabbix-server
Synchronizing state of zabbix-agent.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable zabbix-agent
Synchronizing state of apache2.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable apache2
Created symlink /etc/systemd/system/multi-user.target.wants/zabbix-server.service → /lib/systemd/system/zabbix-server.service.
Created symlink /etc/systemd/system/multi-user.target.wants/zabbix-agent.service → /lib/systemd/system/zabbix-agent.service.
root@servidorzabbix-desktop:/home/servidor-zabbix#
```

Nota. El gráfico representa la inicialización y habilitación de los servicios del servidor Zabbix.

3.5.10 Asignación de la Ip del servidor en el Zabbix Agentd

El servidor Zabbix necesita la configuración y asignación de la ip del servidor en sus parámetros que son Server, Server Active, en donde a través del comando `sudo nano /etc/zabbix/zabbix_agentd.conf`, buscamos los dos parámetros señalados, y se asigna la ip de nuestro servidor Zabbix, el cual se encarga de la recopilación de datos de los servicios monitorizados.

Figura 33

Asignación de Ip en Zabbix Agentd

```

servidor-zabbix@servidorzabbix-desktop: -
GNU nano 4.8 /etc/zabbix/zabbix_agentd.conf
# LogRemoteCommands=0

##### Passive checks related

### Option: Server
# List of comma delimited IP addresses, optionally in CIDR notation
# Incoming connections will be accepted only from the hosts
# If IPv6 support is enabled then '127.0.0.1', '::127.0.0.1'
# and '::/0' will allow any IPv4 or IPv6 address.
# '0.0.0.0/0' can be used to allow any IPv4 address.
# Example: Server=127.0.0.1,192.168.1.0/24,::1,2001:db8::/32
#
# Mandatory: yes, if StartAgents is not explicitly set to 0
# Default:
# Server=
Server=10.21.227.44

servidor-zabbix@servidorzabbix-desktop: -
GNU nano 4.8 /etc/zabbix/zabbix_agentd.conf
# Default:
# StartAgents=3

##### Active checks related

### Option: ServerActive
# List of comma delimited IP:port (or DNS name:port)
# If port is not specified, default port is used.
# IPv6 addresses must be enclosed in square brackets
# If port is not specified, square brackets for IPv6
# If this parameter is not specified, active checks
# Example: ServerActive=127.0.0.1:20051,zabbix.dona
#
# Mandatory: no
# Default:
# ServerActive=
ServerActive=10.21.227.44

```

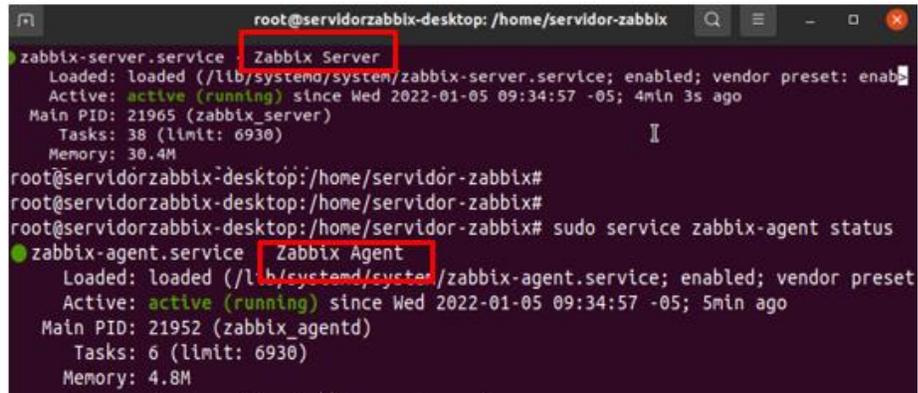
Nota. El gráfico representa la asignación de ip en las interfaces de Zabbix.

3.5.11 Comprobación de la ejecución Zabbix Agentd y Zabbix Server

Una vez finalizado la instalación del repositorio de Zabbix, se comprueba la ejecución de Zabbix Agentd y Zabbix Server, estos dos parámetros son factores importantes para la monitorización, y el acceso al interfaz web a través de un navegador.

Figura 34

Interfaz de comprobación



```

root@servidorzabbix-desktop: /home/servidor-zabbix
zabbix-server.service Zabbix Server
Loaded: loaded (/lib/systemd/system/zabbix-server.service; enabled; vendor preset: enable
Active: active (running) since Wed 2022-01-05 09:34:57 -05; 4min 3s ago
Main PID: 21965 (zabbix_server)
Tasks: 38 (limit: 6930)
Memory: 30.4M
root@servidorzabbix-desktop:/home/servidor-zabbix#
root@servidorzabbix-desktop:/home/servidor-zabbix#
root@servidorzabbix-desktop:/home/servidor-zabbix# sudo service zabbix-agent status
zabbix-agent.service Zabbix Agent
Loaded: loaded (/lib/systemd/system/zabbix-agent.service; enabled; vendor preset: enable
Active: active (running) since Wed 2022-01-05 09:34:57 -05; 5min ago
Main PID: 21952 (zabbix_agentd)
Tasks: 6 (limit: 6930)
Memory: 4.8M

```

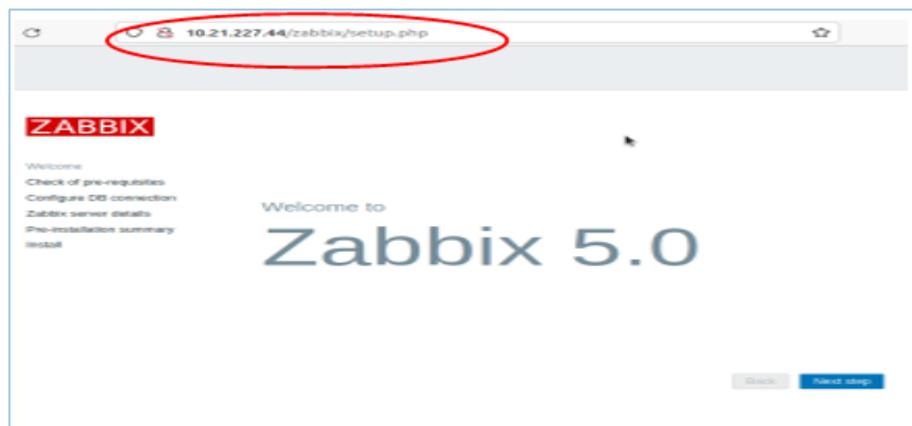
Nota. Se visualiza la ejecución de Zabbix Agentd y Zabbix Server en el servidor Zabbix.

3.5.12 Inicio de instalación de la interfaz web del servidor Zabbix

Una vez comprobados la ejecución de Zabbix Agentd y Zabbix Server, en el navegador de Firefox colocamos la dirección IP 10.21.227.44 y el nombre del servidor configurado.

Figura 35

Inicio de bienvenida de Zabbix



Nota. Visualización del ingreso a la interfaz web de Zabbix con la dirección IP y el nombre del servidor.

3.5.13 Requisitos previos para la instalación de la interfaz Web

En la interfaz de verificación de requisitos previos del servidor web Zabbix comprobar que todos los componentes estén en OK ya que es importante para continuar con el proceso de instalación y no tener errores al momento del funcionamiento del servidor.

Figura 36

Comprobación de requisitos

	Current value	Required	
PHP version	7.4.3	7.2.0	OK
PHP option "memory_limit"	128M	128M	OK
PHP option "post_max_size"	16M	16M	OK
PHP option "upload_max_filesize"	2M	2M	OK
PHP option "max_execution_time"	300	300	OK
PHP option "max_input_time"	300	300	OK
PHP option "date.timezone"	America/Guayaquil		OK
PHP databases support	MySQL		OK
PHP bcmath	on		OK
PHP mbstring	on		OK

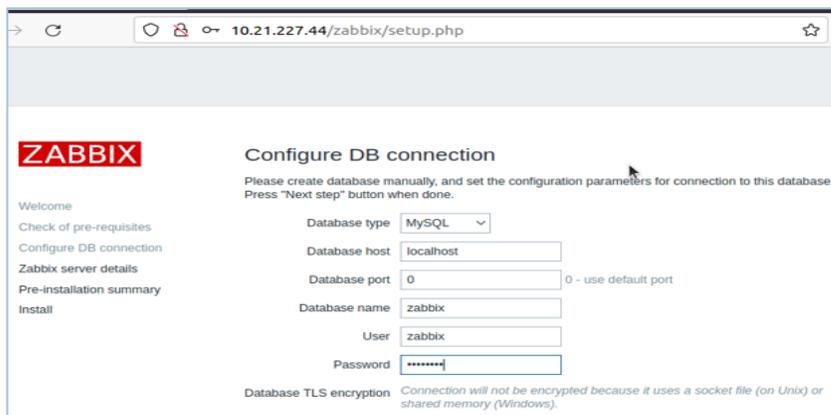
Nota. Se observa el chequeo de los requisitos en el servidor Zabbix.

3.5.14 Configuración de la base de datos de Zabbix

En Zabbix es necesario la configuración de la base de datos, en la interfaz principal se debe verificar que los pasos ya realizados con anterioridad, introducimos en nombre de la base de datos, usuario y su respectiva contraseña password.

Figura 37

Conexión de la base de datos



The screenshot shows a web browser window at the URL `10.21.227.44/zabbix/setup.php`. The page title is "Configure DB connection". On the left, there is a navigation menu with the following items: Welcome, Check of pre-requisites, Configure DB connection (highlighted), Zabbix server details, Pre-installation summary, and Install. The main content area contains the following fields and instructions:

- Database type:
- Database host:
- Database port: - use default port
- Database name:
- User:
- Password:

At the bottom, there is a note: "Database TLS encryption Connection will not be encrypted because it uses a socket file (on Unix) or shared memory (Windows)."

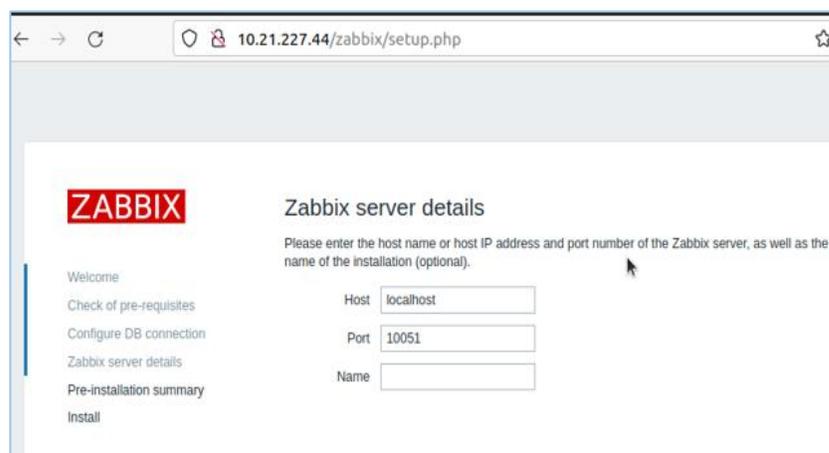
Nota. Se visualiza la conexión de la base de datos y asignación de su contraseña.

3.5.15 Aspectos importantes del servidor Zabbix

En esta interfaz se revisa el nombre y las opciones que nos brinda Zabbix, las conexiones y la monitorización se hará por el puerto 10051. Especificamos el nombre de la interfaz web, el cual distinguirá qué servidor se está monitorizando.

Figura 38

Interfaz de detalle de Zabbix



The screenshot shows a web browser window at the URL `10.21.227.44/zabbix/setup.php`. The page title is "Zabbix server details". On the left, there is a navigation menu with the following items: Welcome, Check of pre-requisites, Configure DB connection, Zabbix server details (highlighted), Pre-installation summary, and Install. The main content area contains the following fields and instructions:

- Host:
- Port:
- Name:

The instructions state: "Please enter the host name or host IP address and port number of the Zabbix server, as well as the name of the installation (optional)."

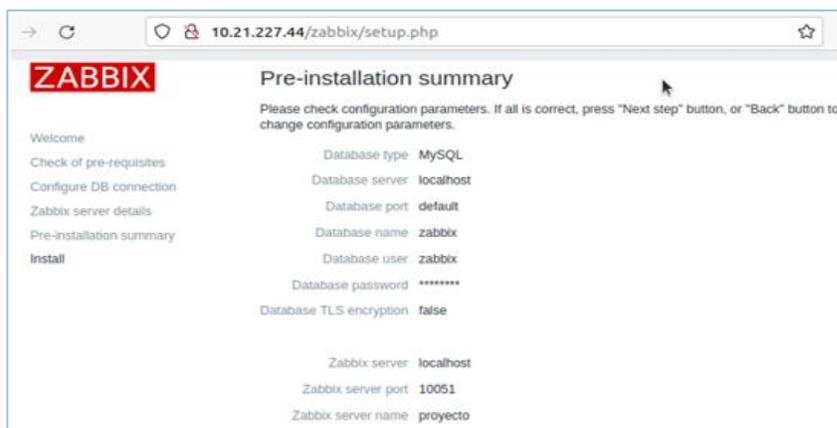
Nota. Se observa la configuración predeterminada del servidor Zabbix y la asignación del nombre.

3.5.16 Resumen de la Instalación

Después de la ejecución de la interfaz web en el servidor, Zabbix facilita la función de observar los parámetros que han sido asignados, verificar que las configuraciones estén acorde a su configuración realizada en los pasos anteriores.

Figura 39

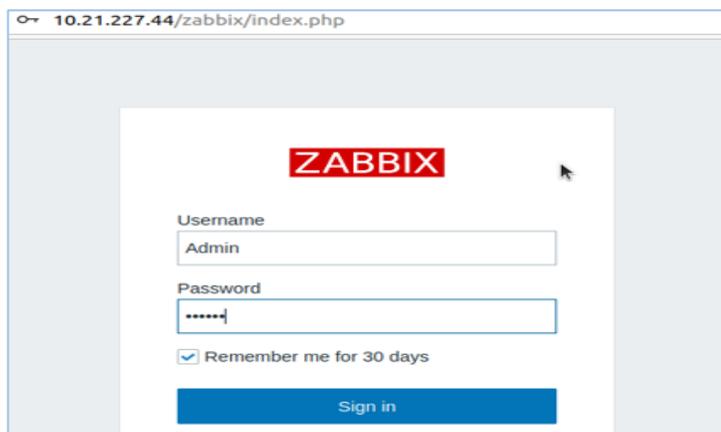
Verificación de la instalación



Nota. Se visualizan las configuraciones realizadas en la instalación del servidor Zabbix.

3.5.17 Inicio de sesión del servidor

Instalado y configurado todos los parámetros de Zabbix, se coloca en la interfaz de inicio de sesión el usuario Admin y la contraseña zabbix, luego presione en Sign in para acceder a la interfaz

Figura 40*Inicio de sesión*The image shows a web browser window with the address bar displaying "10.21.227.44/zabbix/index.php". The main content area features a white login form centered on a light gray background. At the top of the form is the "ZABBIX" logo in red. Below the logo are two input fields: "Username" with the text "Admin" and "Password" with masked characters "*****". A checkbox labeled "Remember me for 30 days" is checked. At the bottom of the form is a blue "Sign in" button.

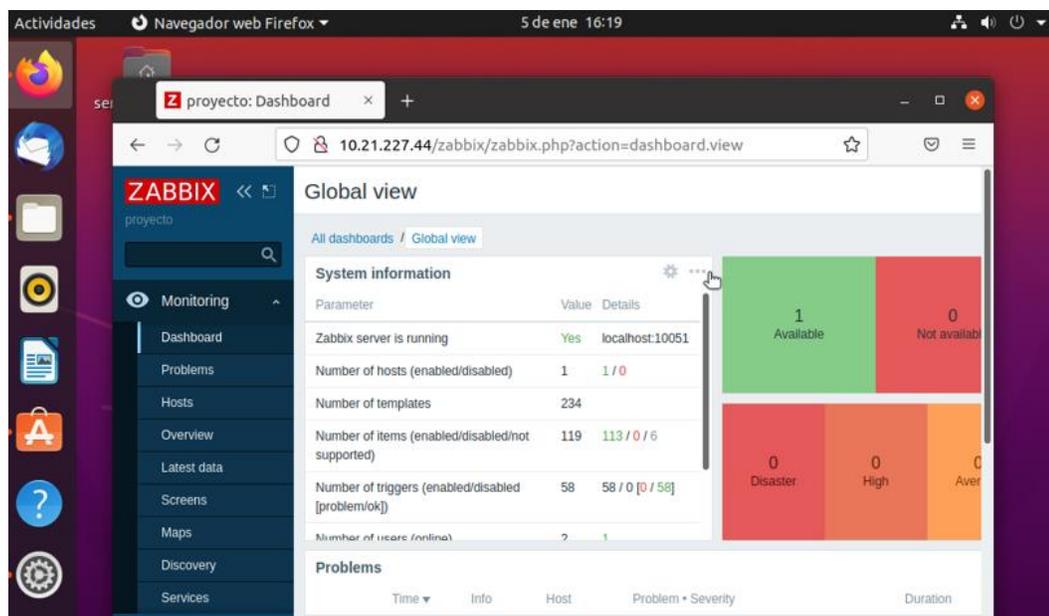
Nota. El gráfico representa la interfaz para la colocación del usuario y la contraseña.

3.5.18 Panel de control de Zabbix

Terminado el proceso de la instalación de Zabbix, configuración, asignación de usuario y contraseña, finalmente se podrá visualizar la interfaz gráfica de Zabbix, permitiendo realizar el monitoreo de red en su entorno principal. También se observa la habilitación del servidor conjuntamente con su puerto de salida.

Figura 41

Interfaz principal de Zabbix



Nota. Se visualiza la interfaz principal de Zabbix conjuntamente con el sistema de información y sus parámetros.

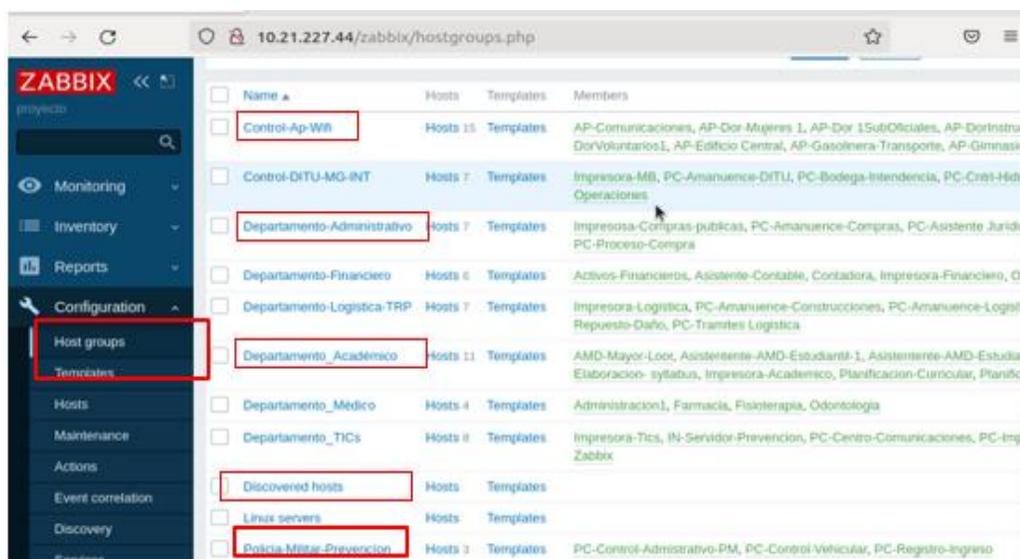
3.6 Monitoreo de los equipos de la red de datos de la “ESFORSE”

3.6.1 Host groups para Zabbix

Para el control de la red de la Escuela de Formación de Soldados Vencedores del Cenepa “ESFORSE”, se deben crear ciertos grupos de host para una administración más detallada de los equipos de cada departamento que se va a monitorear. Por tal razón el parámetro configuración, presionamos en la opción Host groups y se elige la opción crear new groups.

Figura 42

Interfaz principal de Host Groups



Nota. El gráfico representa la creación de los grupos de los departamentos monitoreados.

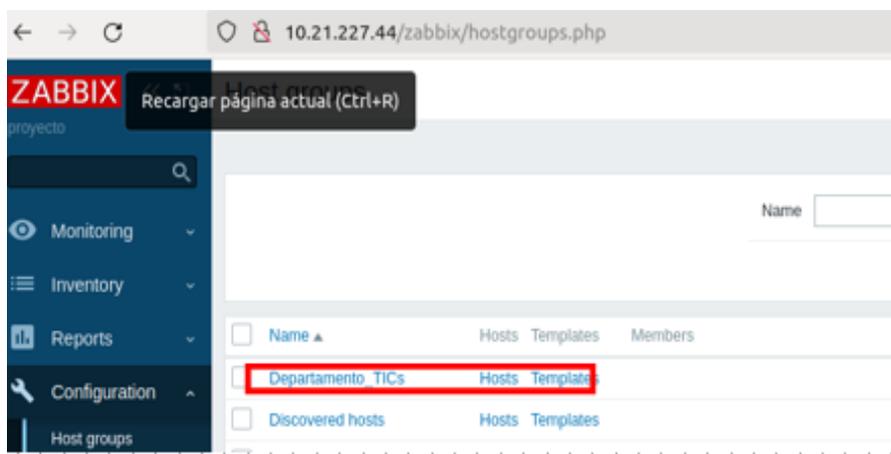
3.6.2 Creación de host groups del departamento de TICs.

El departamento de TICs consta de varios equipos conectados a la misma red, en donde a cada equipo se asigna a un grupo de monitorización, permitiendo un mejor control al momento de la verificación de errores. En el panel de navegación de Zabbix en la opción configuración se selecciona host groups y se crea un nuevo grupo.

Para la monitorización de este departamento se realiza mediante el protocolo SNMP, y la utilización de Zabbix agent, el mismo que se puede descargar desde su página principal.

Figura 43

Creación de host groups de las TICs



Nota. Se observa la creación del grupo del departamento de TICs de la ESFORSE.

3.6.3 Habilitación del protocolo SNMP

En la máquina principal del jefe administrativo del departamento de las Tics, se procede a descargar los paquetes SNMP en la computadora, ingresamos a configuración y seleccionamos aplicaciones, se escoge la opción características opcionales y se descarga los archivos del protocolo SNMP. Se abre el protocolo SNMP en la opción servicios, en el parámetro seguridad se agrega el nombre de la comunidad public. En la opción configuración de SNMP se agrega la dirección IP del servidor Zabbix.

Figura 44

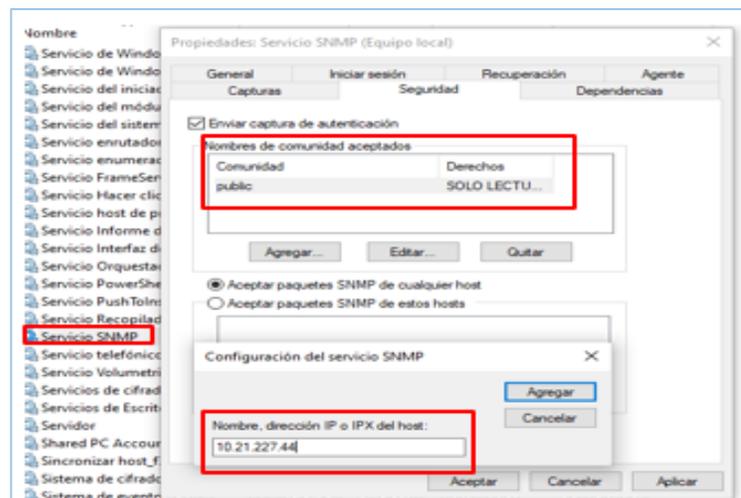
Habilitación del protocolo SNMP



Nota. Se observa la instalación del protocolo SNMP en la computadora.

Figura 45

Asignación de la Ip del servidor Zabbix



Nota. Asignación de la dirección Ip, en el servicio SNMP de la máquina del jefe administrativo de las TICs,

3.6.4 Registro de la computadora en el servidor Zabbix.

Con la asignación de la dirección Ip en servicio SNMP, se registra el host a ser monitorizado, en la opción de interfaces colocamos la dirección Ip del computador y asignamos su respectivo template y la versión de SNMP que se va utilizar. En el parámetro de templates se escoge la opción del template Net Network Device SNMP, para que envíe los datos del monitoreo al servidor, una vez que se configura los parámetros para el monitoreo se añade el equipo al presionar la opción Add.

Figura 46

Asignación del host en el servidor Zabbix

The screenshot shows the Zabbix web interface for adding a host. The browser address bar indicates the URL is `10.21.227.44/zabbix/hosts.php?form=create&groupids[0]=20`. The page title is "Hosts". The navigation menu includes "Templates", "IPMI", "Tags", "Macros", "Inventory", and "Encryption". The form fields are as follows:

- Host name:** IMC-Jefe-TICs
- Visible name:** (empty)
- Groups:** Departamento TICs, Templates/Operating systems
- Interface:**

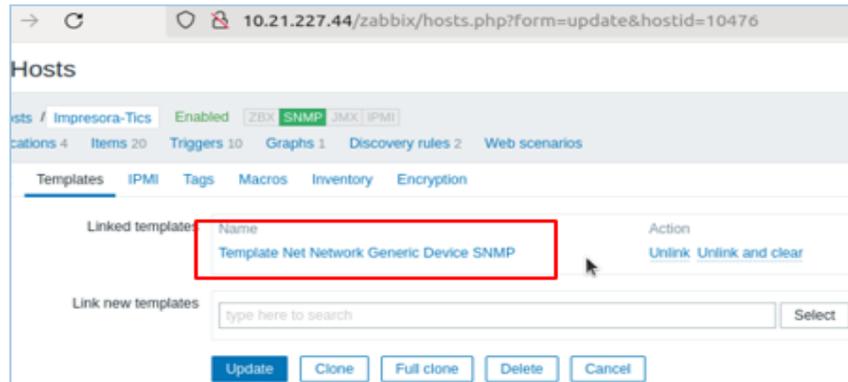
Type	IP address	DNS name	Connect to	Port
SNMP	10.21.227.129		IP	161
- SNMP version:** SNMPv2
- SNMP community:** {SNMP_COMMUNITY}
- Use bulk requests:**

At the bottom of the form, there is a "Description" text area, a "Monitored by proxy" dropdown set to "(no proxy)", an "Enabled" checkbox which is checked, and "Add" and "Cancel" buttons.

Nota. El gráfico representa el registro de la PC en el servidor Zabbix con su respectivo template.

Figura 47

Configuración de Plantillas



Nota. Se observa la asignación del template Net Network Device SNMP.

3.6.5 Verificación del host creado

Una vez registrado en el servidor Zabbix se verifica la carga de los datos en la opción latest data y se comprobará los gráficos de monitoreo.

Figura 48

Interfaz de datos monitorizados

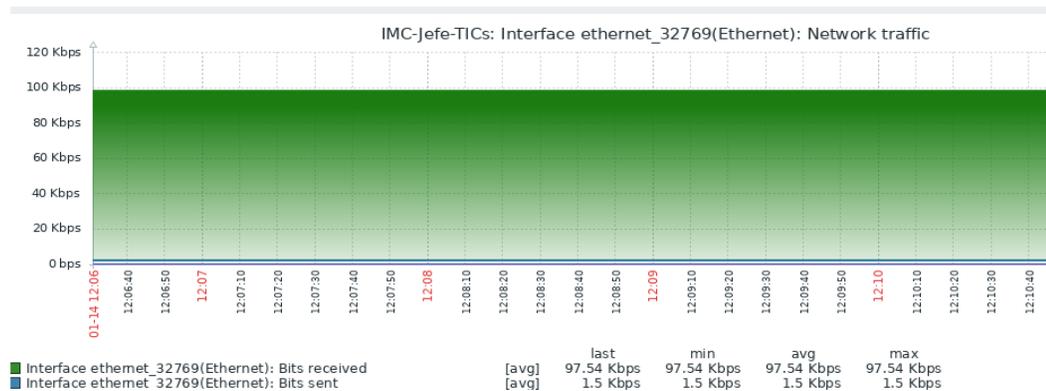
The screenshot shows the 'Latest data' view for the host 'IMC-Jefe-TICS' in the Zabbix web interface. The browser address bar shows the URL: 10.21.227.44/zabbix/zabbix.php?action=latest.view&filter_hostids[]=10457&fil... The page has search filters for 'Hosts' (set to 'IMC-Jefe-TICS') and 'Application'. There are 'Apply' and 'Reset' buttons. Below the filters is a table of monitored items. The table has columns for 'Host', 'Name', 'Last check', and 'Last value'. The data is as follows:

Host	Name	Last check	Last value
IMC-Jefe-TICS	CPU (1 Item)		
IMC-Jefe-TICS	CPU utilization	2022-01-14 12:05:26	0 %
IMC-Jefe-TICS	Filesystem C:\ Label: Serial Number ca03ed5f (3 Items)		
IMC-Jefe-TICS	C:\ Label: Serial Number ca03ed5f: Space utilization		
IMC-Jefe-TICS	C:\ Label: Serial Number ca03ed5f: Total space	2022-01-14 12:05:26	443.23 GB
IMC-Jefe-TICS	C:\ Label: Serial Number ca03ed5f: Used space	2022-01-14 12:05:26	37.7 GB
IMC-Jefe-TICS	Filesystem E:\ Label: Serial Number be62152f (3 Items)		
IMC-Jefe-TICS	E:\ Label: Serial Number be62152f: Space utilization		
IMC-Jefe-TICS	E:\ Label: Serial Number be62152f: Total space	2022-01-14 12:05:26	194.25 GB
IMC-Jefe-TICS	E:\ Label: Serial Number be62152f: Used space	2022-01-14 12:05:26	142.17 GB

Nota. Se observa las características del hardware de la computadora monitoreada.

Figura 49

Interfaz gráfica del tráfico de red



Nota. Visualización de los bits enviados y recibidos en la tarjeta Ethernet.

3.7 Descarga del Agente Zabbix para la monitorización

Para el monitoreo con el agente Zabbix en el servidor de la prevención, se elige el sistema operativo en el que se instalará el agente, se debe elegir la versión del servidor Zabbix. En el parámetro Zabbix reléase se selecciona la versión acorde al servidor Zabbix, y se descarga el agente desde su página oficial.

Figura 50

Interfaz principal de Agentes Zabbix



Nota. Se observa los parámetros para la descarga de Agentes Zabbix. Tomada de (ZABBIX, 2022)

Figura 51

Descarga de la Agente Zabbix



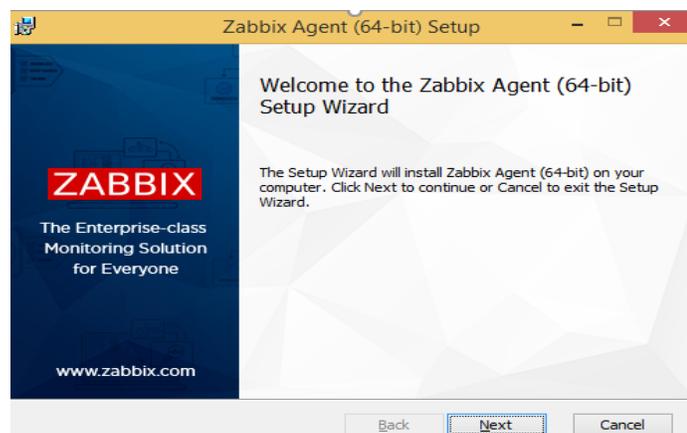
Nota. Se observa la descarga de la versión de Zabbix reléase. Tomado de (ZABBIX, 2022)

3.7.1 Instalación de agente Zabbix

Finalizado la descarga en el host servidor-prevención se ejecuta el instalador del agente, se mostrará una interfaz en donde se colocará la dirección IP del servidor Zabbix, se debe dar clic en todas las opciones de siguiente sin cambiar ningún parámetro.

Figura 52

Inicio de instalación del agente Zabbix



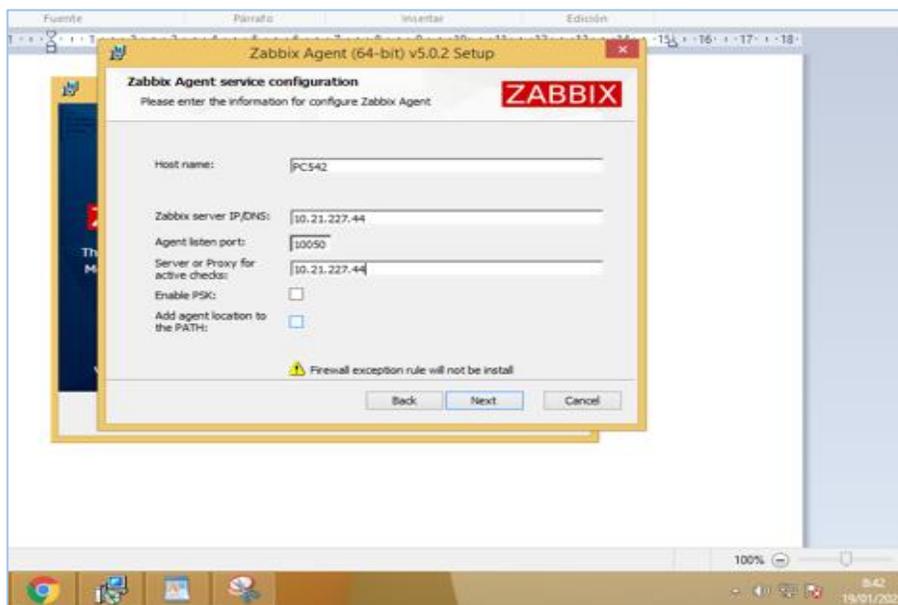
Nota. El gráfico representa la interfaz principal para la instalación de Zabbix.

3.7.2 Asignación de Ip del servidor Sabir

En interfaz Zabbix Agent se coloca la dirección IP del servidor Zabbix en los parámetros, Zabbix server, Zabbix Proxy y el listen puerto 10050 por defecto. Colado la dirección IP se presiona en Next y se carga el archivo, por último, se dará clic en finalizar.

Figura 53

Asignación de Ip en el host



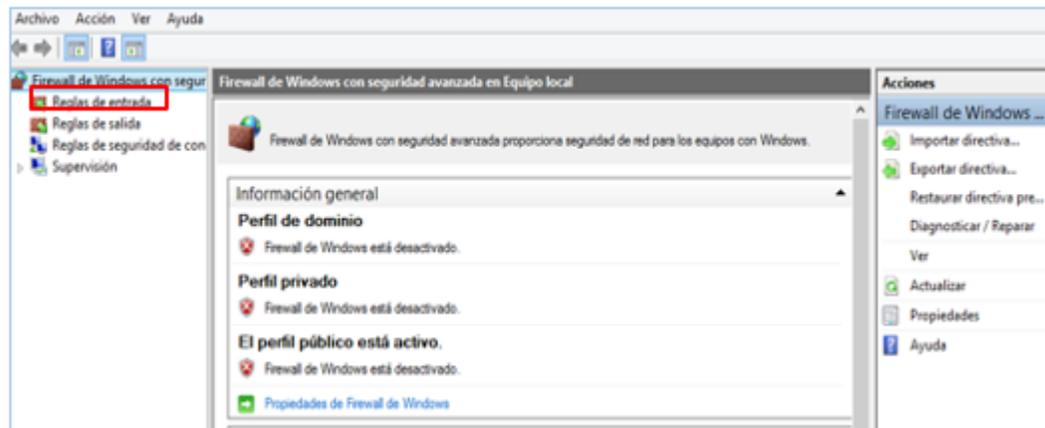
Nota. El gráfico representa la asignación de la Ip del servidor Zabbix en el host servidor de la prevención.

3.7.3 Configuración de Firewall de Windows

En esta opción se creará reglas de entradas para la habilitación de Zabbix, clic en el parámetro reglas de entradas seleccione nueva regla y en la lista de selección, habilite la opción puerto y configure los respectivos parámetros de entrada.

Figura 54

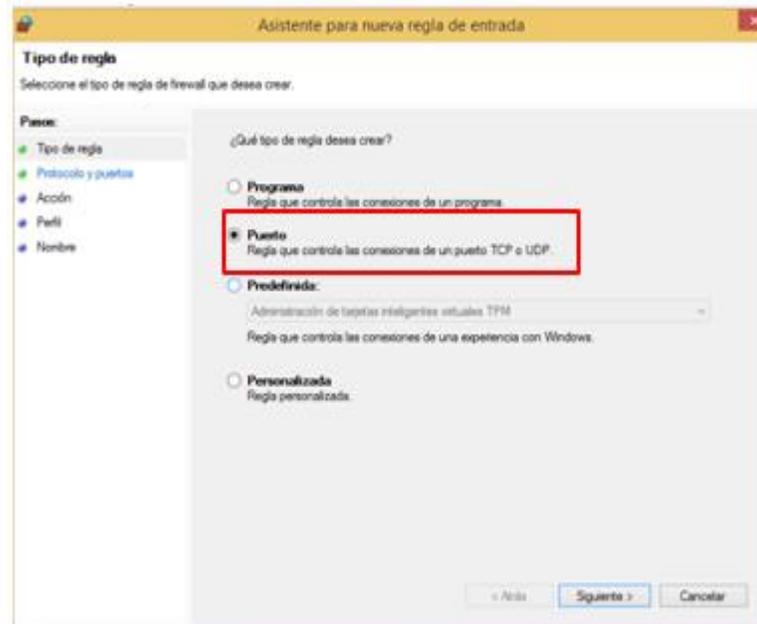
Interfaz de Firewall de Windows



Nota. Se observa la interfaz principal de Firewall de Windows y la selección de del parámetro reglas de entrada.

Figura 55

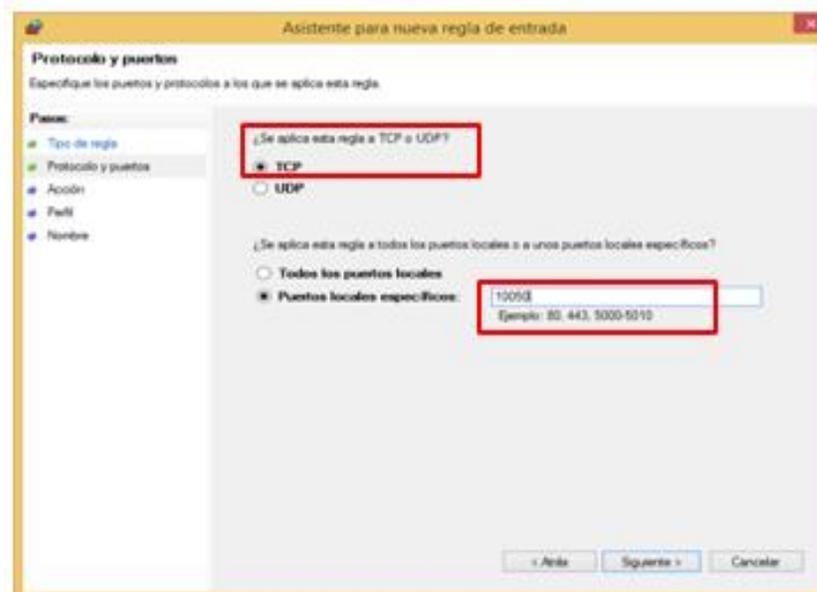
Interfaz de la nueva regla de entrada



Nota. El gráfico representa la selección de la regla puerto como tipo de entrada.

Figura 56

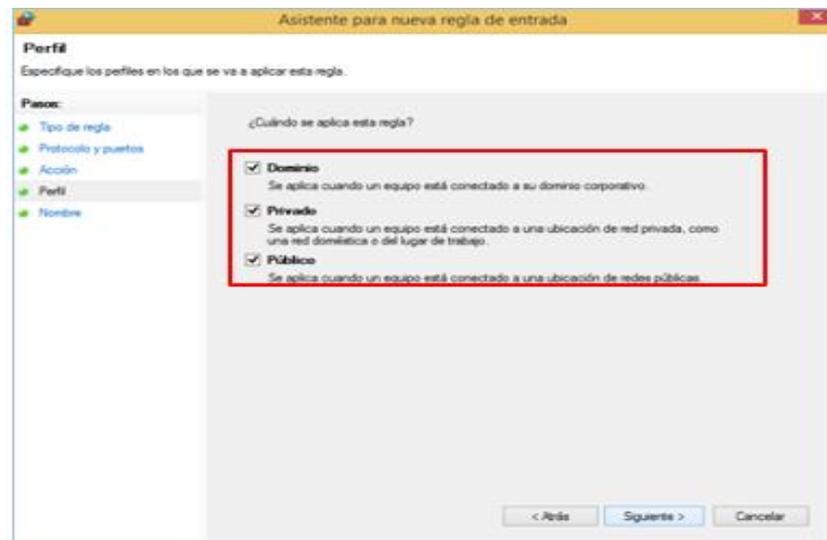
Asignación de protocolos y puertos



Nota. El gráfico representa la activación de la regla TCP y asignación del puerto 10050.

Figura 57

Perfiles de regla de entrada



Nota. El gráfico representa la activación de los perfiles de la regla de entrada.

Figura 58*Dirección de regla de entrada TCP*

Asistente para nueva regla de entrada

Nombre
Especifique el nombre y la descripción de esta regla.

Pasos:

- Tipo de regla
- Protocolo y puertos
- Acción
- Perfil
- Nombre

Nombre:
Zabbix_TCP

Descripción (opcional):

< Atrás Finalizar Cancelar

Nota. El gráfico representa la asignación de la dirección de entra Zabbix_TCP.

Figura 59*Puerto de entrada UDP*

Asistente para nueva regla de entrada

Protocolo y puertos
Especifique los puertos y protocolos a los que se aplica esta regla.

Pasos:

- Tipo de regla
- Protocolo y puertos
- Acción
- Perfil
- Nombre

¿Se aplica esta regla a TCP o UDP?

TCP

UDP

¿Se aplica esta regla a todos los puertos locales o a unos puertos locales específicos?

Todos los puertos locales

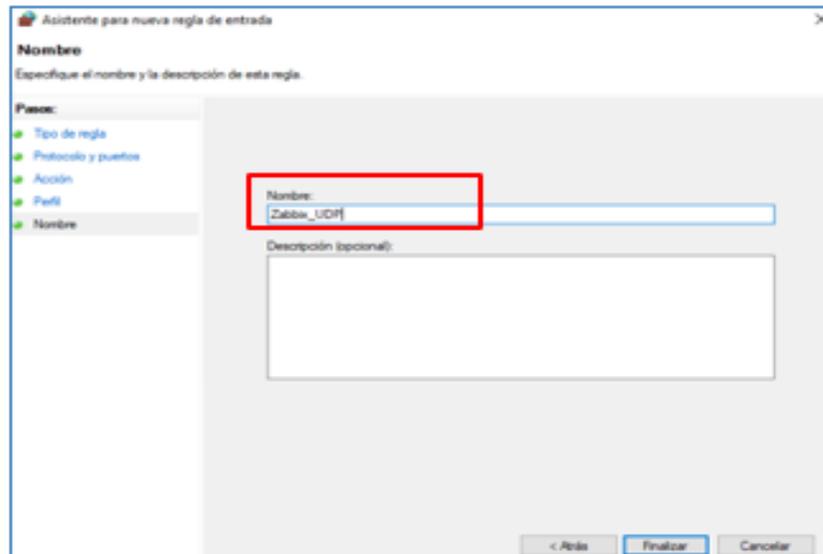
Puestos locales específicos: 10050
Ejemplo: 40-402-9888-010

< Atrás Siguiente > Cancelar

Nota. El gráfico representa la activación de la regla UDP y asignación del puerto 10050.

Figura 60

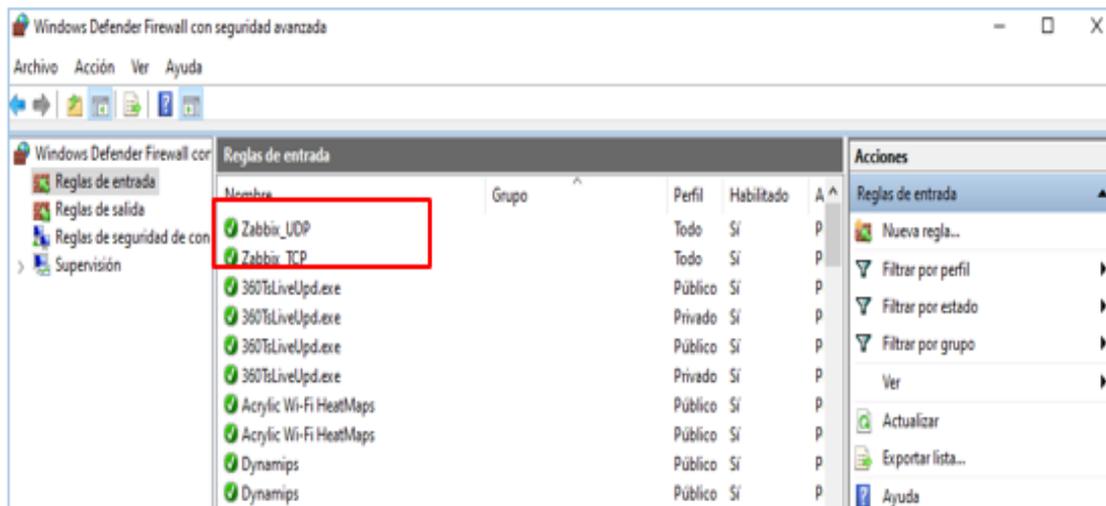
Dirección de regla de entrada UDP



Nota. El gráfico representa la asignación de la dirección de entra Zabbix_UDP.

Figura 61

Comprobación de las reglas de entrada



Nota. El gráfico representa la creación de las dos reglas de entrada en la interfaz principal de Windows Defender.

3.7.4 Asignación del host en el servidor Zabbix

Para la asignación del servidor de la prevención con el agente Zabbix, los pasos a seguir son iguales, la diferencia se realiza en el cambio de los templates y la habilitación del parámetro del agent Zabbix y se coloca la dirección IP del host a ser monitoreado.

Figura 62

Asignación del host en el servidor Zabbix

The screenshot shows the Zabbix web interface for configuring a host. The browser address bar indicates the URL is `10.21.227.44/zabbix/hosts.php?form=create&groupids[0]=20`. The page title is "Hosts". The form includes the following fields:

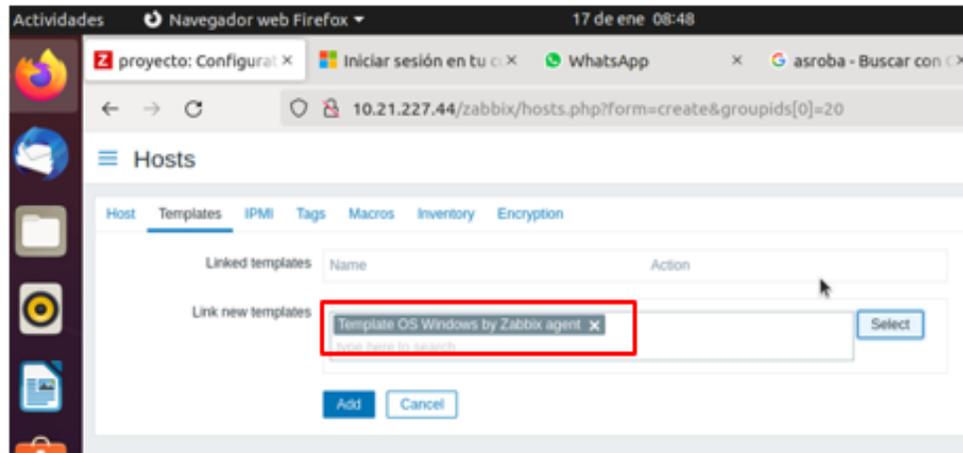
- Host name:** IMC-Servidor-Prevencion
- Visible name:** (empty)
- Groups:** Departamento_TICs, Templates/Operating systems
- Interfaces:**

Type	IP address	DNS name	Connect to	Port
Agent	10.21.227.18		IP	10050

Nota. El gráfico representa la asignación de host al servidor Zabbix mediante el Agent Zabbix.

Figura 63

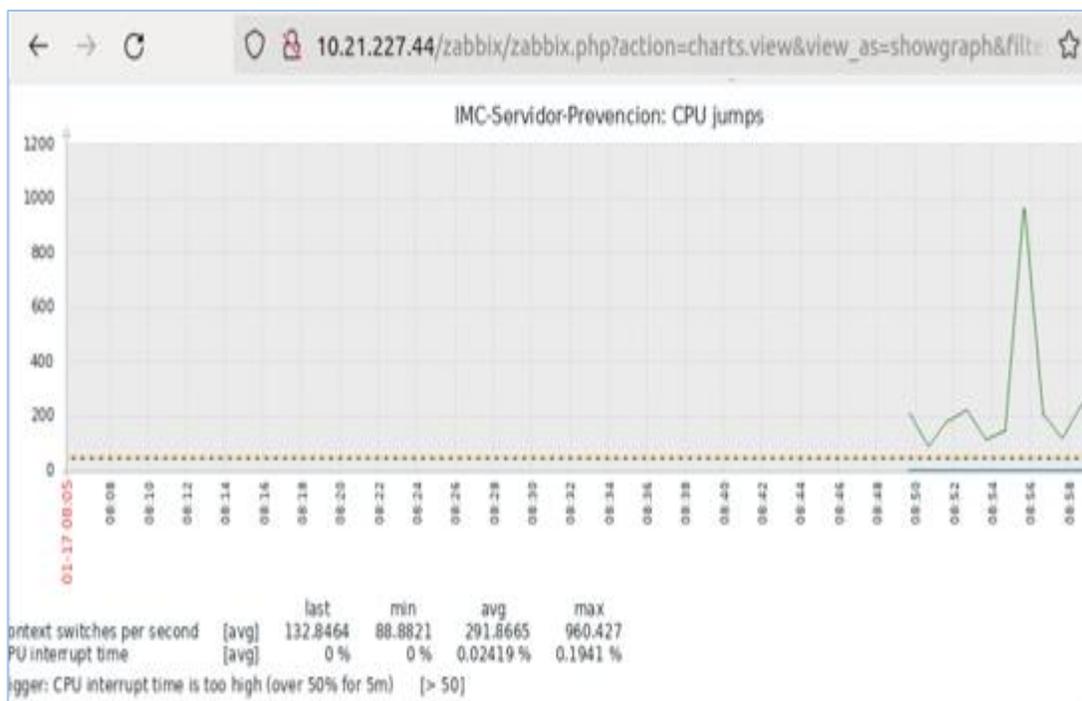
Asignación del template



Nota. El gráfico representa la asignación del template Zabbix Agent.

Figura 64

Verificación de datos del PCU



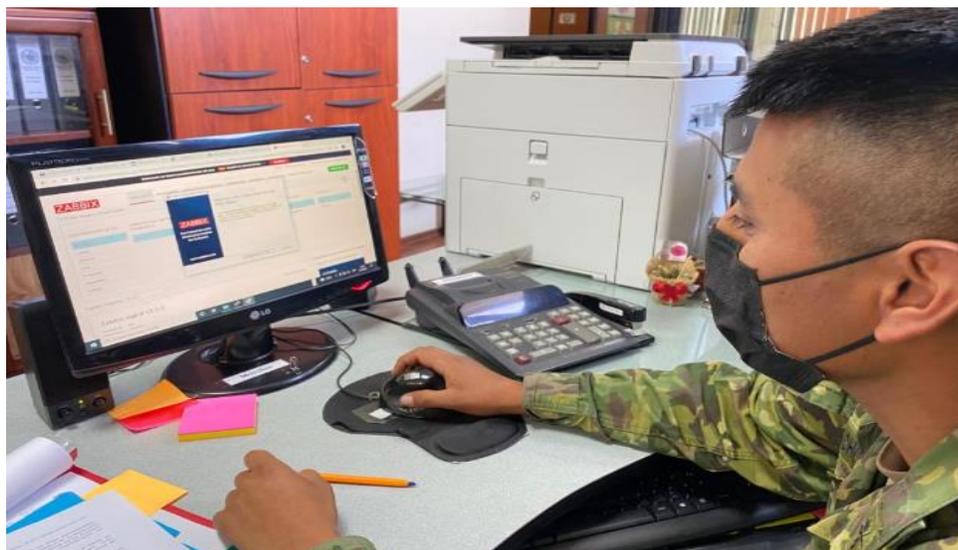
Nota. El gráfico representa el tiempo de interrupción del CPU en 0,1941%.

3.8 Monitoreo de los equipos de red del departamento Financiero

El departamento financiero de la Escuela de Formación de soldado Vencedores del Cenepa, cuenta con varios equipos de red como computadoras e impresoras, a los cuales se realiza el monitoreo de la red, como se detalla en las siguientes figuras.

Figura 65

Descarga del agente Zabbix



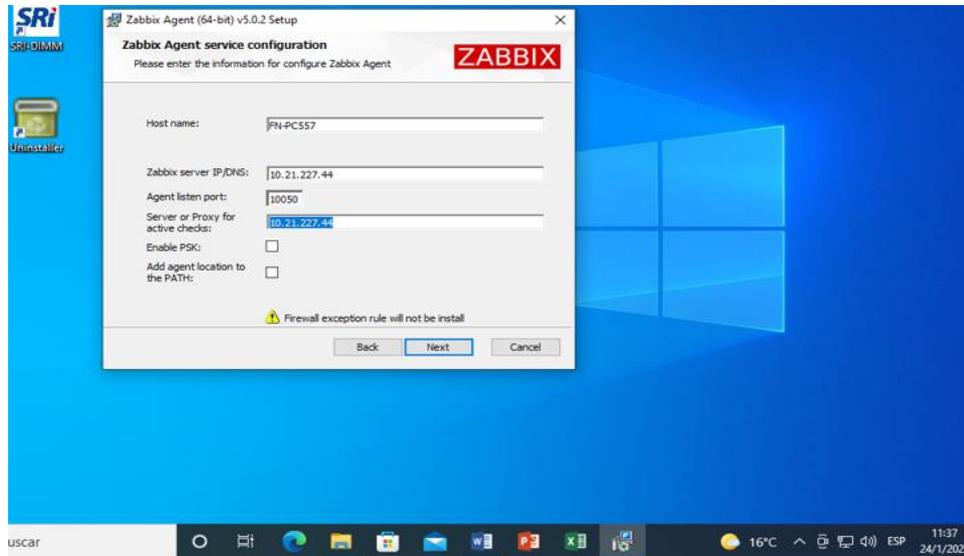
Nota. El gráfico representa la descarga del agente Zabbix en la computadora de contabilidad.

3.8.1 Instalación del Agente Zabbix

Finalizado la descarga del agente Zabbix en la interfaz de asignación de Ip, se asigna la dirección ip del servidor Zabbix, y se presiona siguiente en todas las opciones.

Figura 66

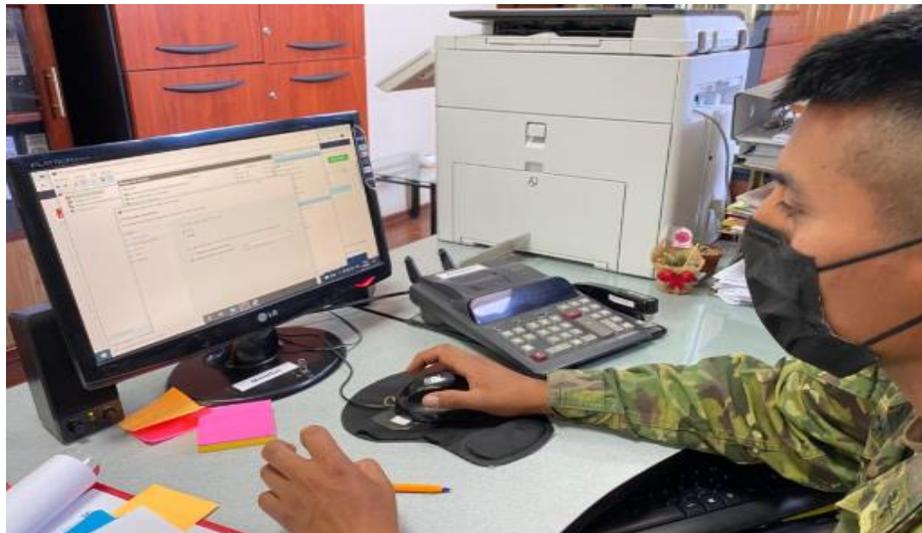
Asignación de Ip del servidor



Nota. Se puede observar la asignación de la Ip del servidor en el host de contabilidad.

Figura 67

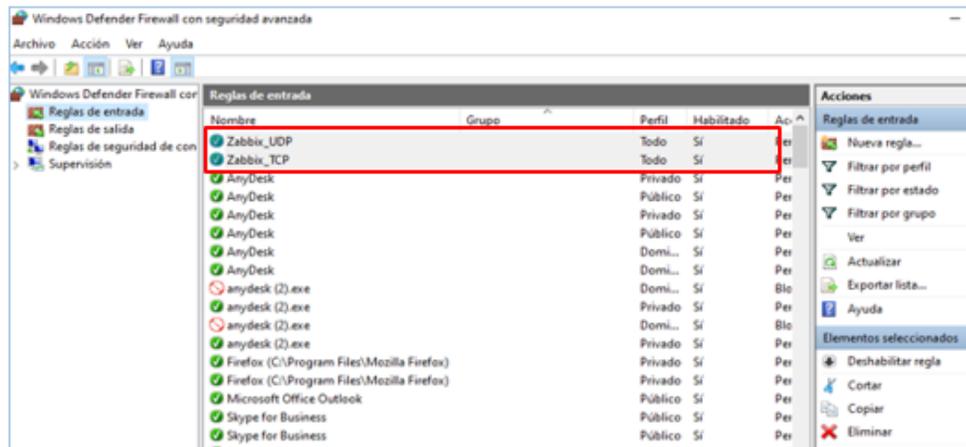
Configuración de Firewall



Nota. El gráfico representa la asignación de las reglas de entradas TCP- UDP en la seguridad de Windows

Figura 68

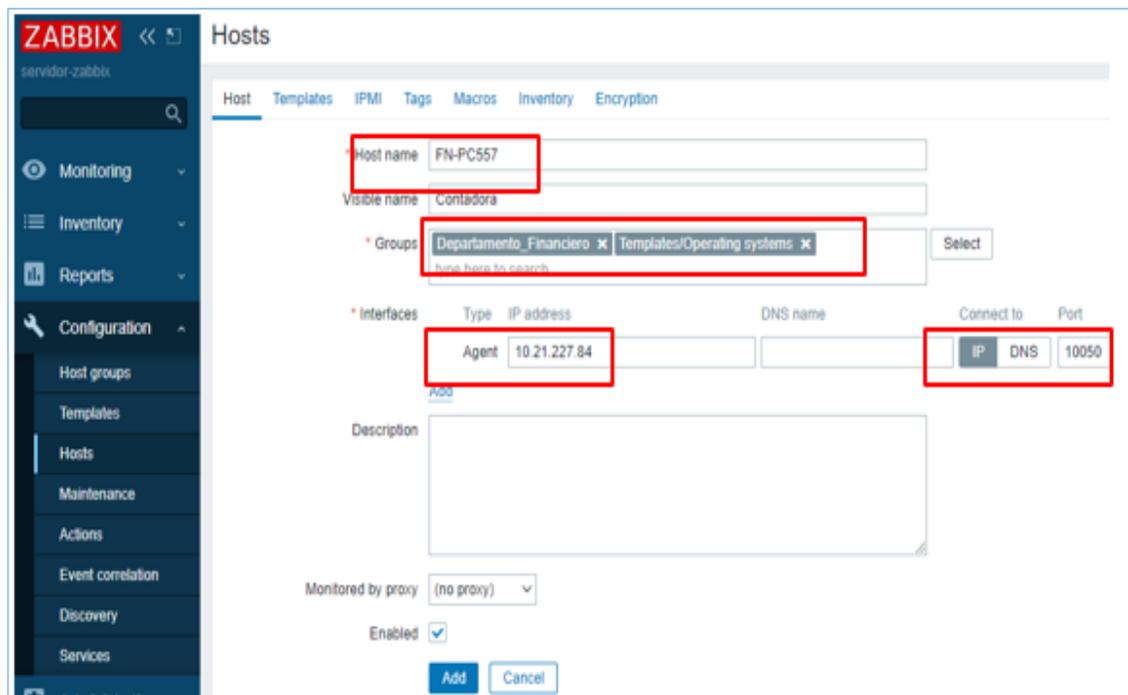
Comprobación de reglas de entrada



Nota. El gráfico representa la comprobación de las dos reglas de entradas.

Figura 69

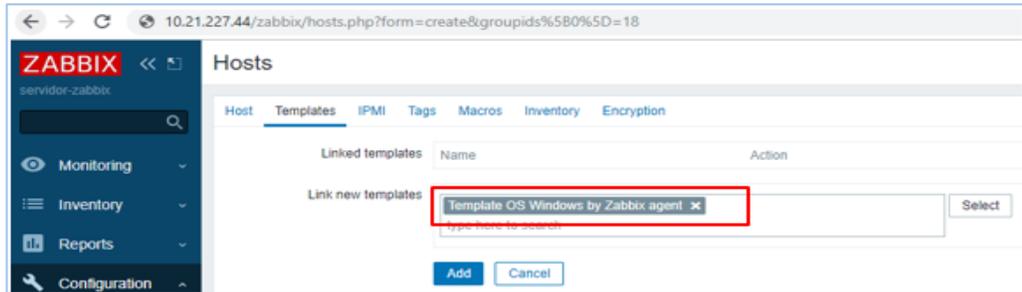
Asignación del host en Zabbix



Nota. Se visualiza los pasos a seguir para agregar el host en la interfaz web de Zabbix.

Figura 70

Asignación de Template



Nota. El gráfico representa la asignación del template para Zabbix agent.

Figura 71

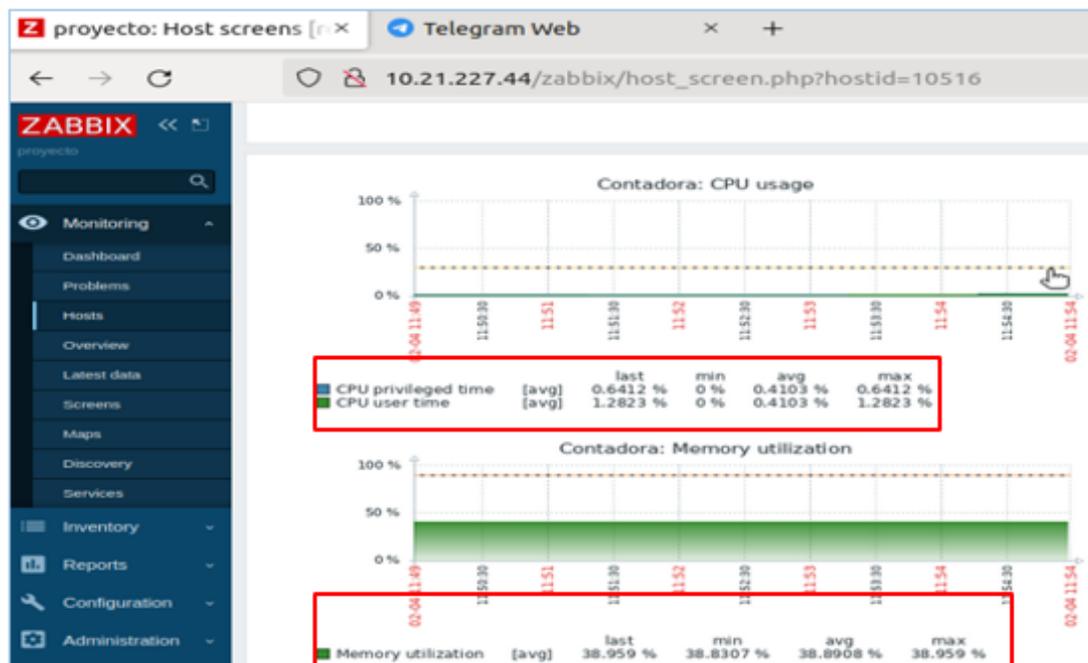
Interfaz de monitoreo del hosts



Nota. El gráfico representa la escritura y lectura de las unidades de disco del host.

Figura 72

Interfaz gráfica de la memoria



Nota. El gráfico representa la utilización del CPU y la memoria RAM.

3.9 Configuración del protocolo SNMP en impresora de compras públicas

En el panel de control de la impresora ir a la opción ajustes del sistema, clic en la opción ajustes de interfaces donde se verifica la dirección Ip 10.21.227.235. En la interfaz transferencia de archivos y en la opción servidor SNMP se coloca el nombre de servidor-zabbix, en el número del puerto se coloca 161, finalmente presionamos OK para guardar las configuraciones.

Figura 73*Configuración protocolo SNMP*

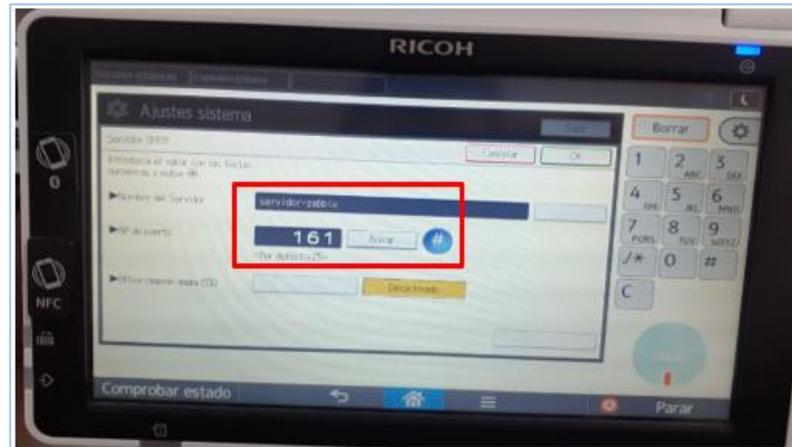
Nota. El gráfico representa la verificación de la dirección IP para la configuración del protocolo SNMP.

Figura 74*Verificación de la dirección Ip*

Nota. El gráfico representa la verificación de la dirección ip 10.21.227.235.

Figura 75

Asignación del servidor Zabbix



Nota. El gráfico representa la asignación del nombre del servidor-zabbix y la asignación del puerto de monitoreo 161.

Figura 76

Interfaz gráfica de monitoreo



Nota. El gráfico representa el tráfico de red en el envío y la recepción de bits en la impresora.

3.10 Monitoreo de los equipos de red del departamento Académico

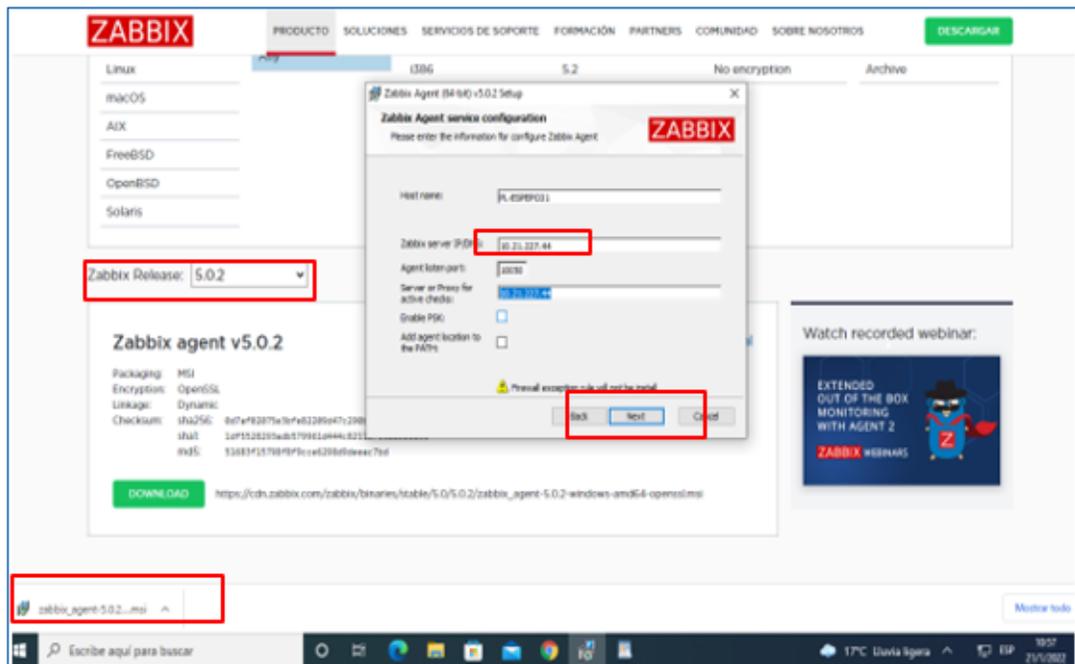
El departamento Académico de la Escuela de Formación de soldado Vencedores del Cenepa, cuenta con varios equipos de red como computadoras e impresoras, a los cuales se realiza el monitoreo de la red, como se detalla en las siguientes figuras.

3.10.1 Descarga y configuración de Zabbix Agent

Descargado el agente Zabbix desde su página principal, se abre el ejecutador del programa descargado, en los siguientes pasos damos clic en la opción Next. En la interfaz servicios de configuración se coloca la dirección Ip del servidor Zabbix 10.21.227.44 permitiendo la conexión entre el host y el servidor.

Figura 77

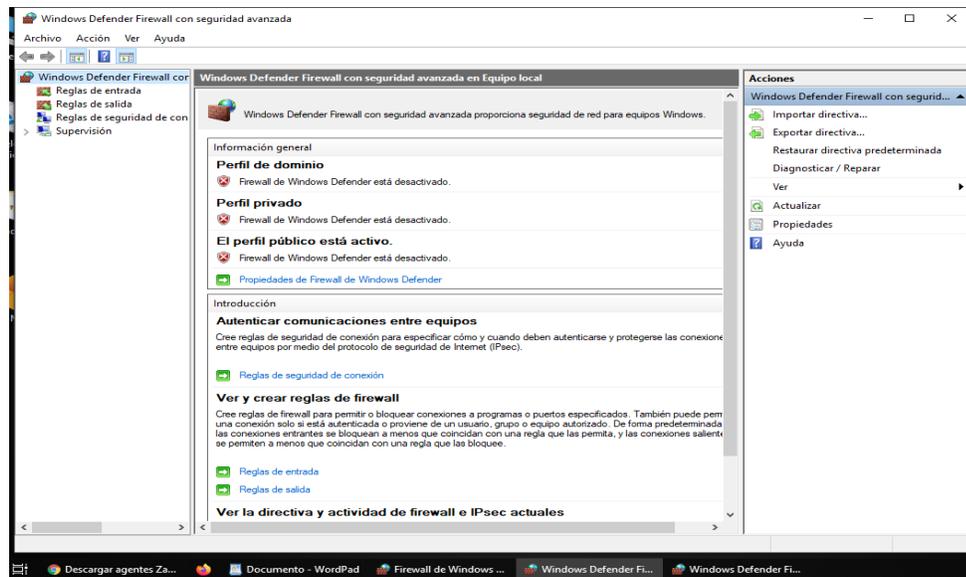
Configuración de Zabbix



Nota. El gráfico representa la descarga e instalación del agente Zabbix en el host de planificación curricular.

Figura 78

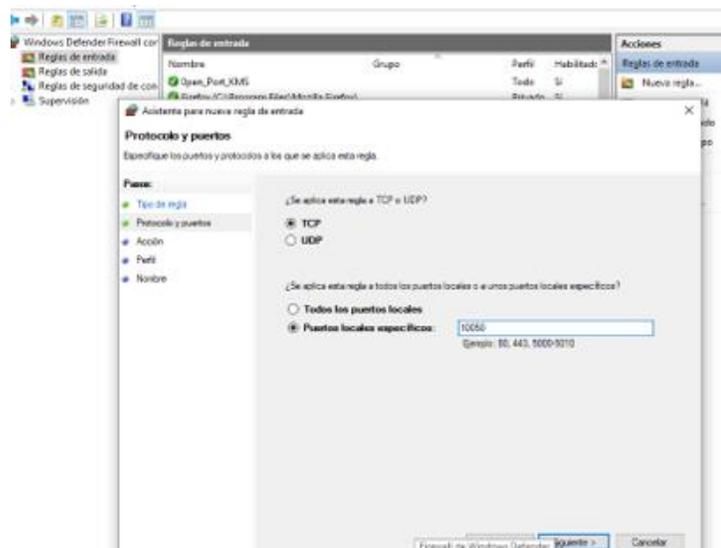
Agregación de reglas de entradas



Nota. Se observa la agregación de las reglas de entradas en el firewall de Windows.

Figura 79

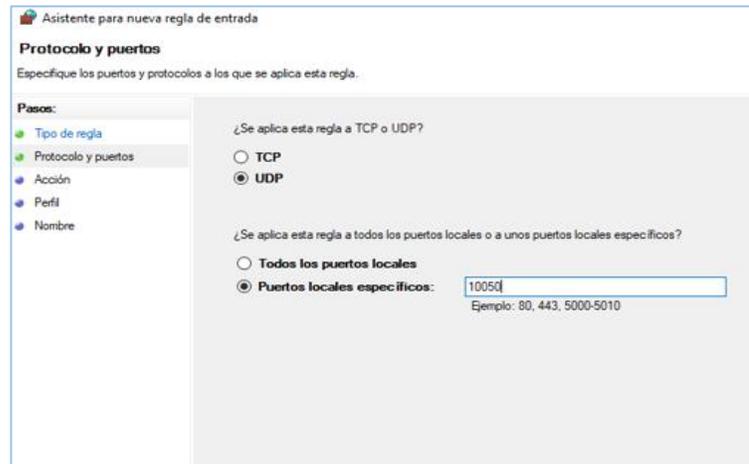
Interfaz de agregación TCP



Nota. El gráfico representa la asignación de la entrada TCP y el puerto 10050.

Figura 80

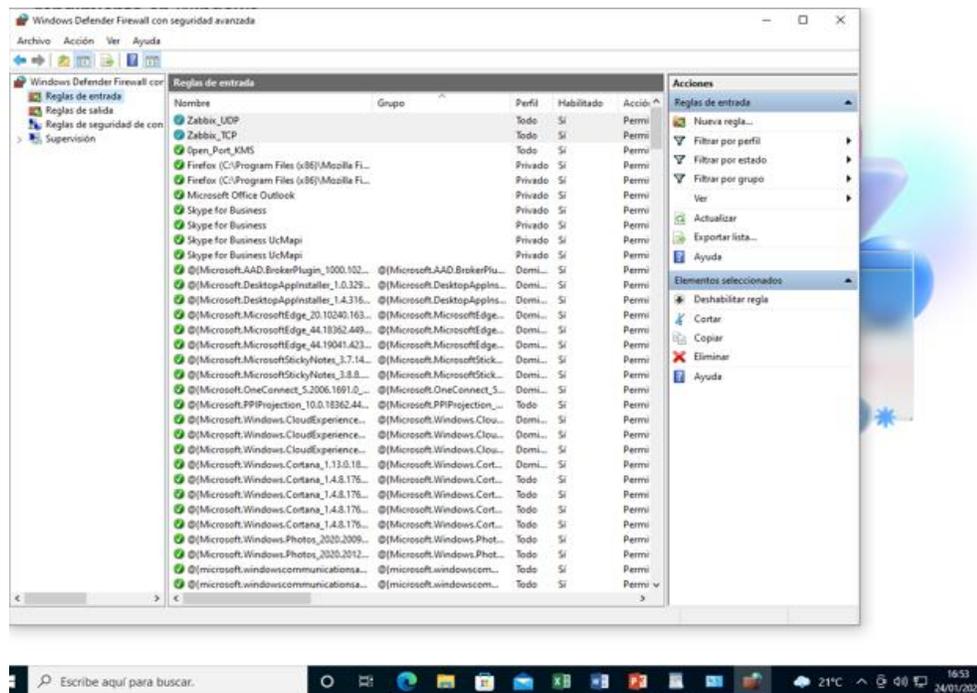
Interfaz de agregación UDP



Nota. El gráfico representa la asignación de la entrada UDP y el puerto 10050.

Figura 81

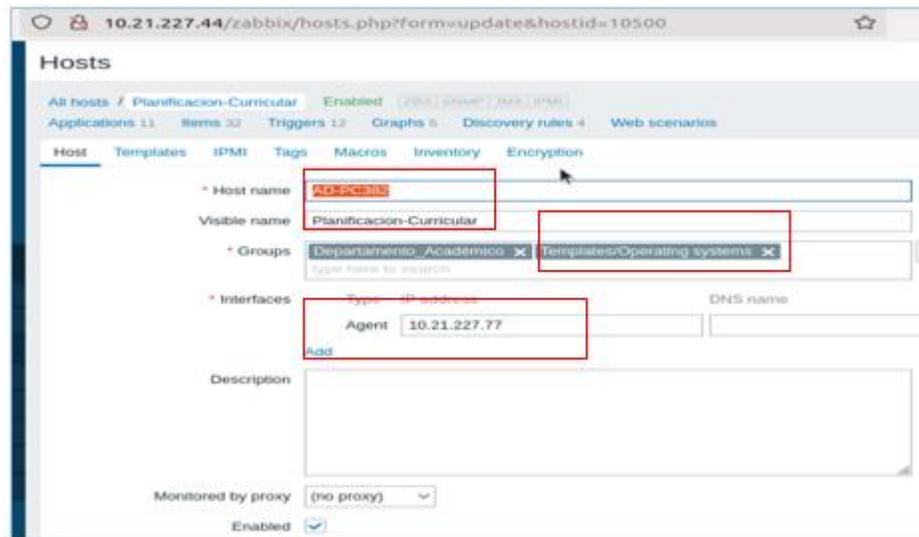
Verificación de las reglas de entradas



Nota. El gráfico representa la creación de las reglas de entrada en el computador.

Figura 82

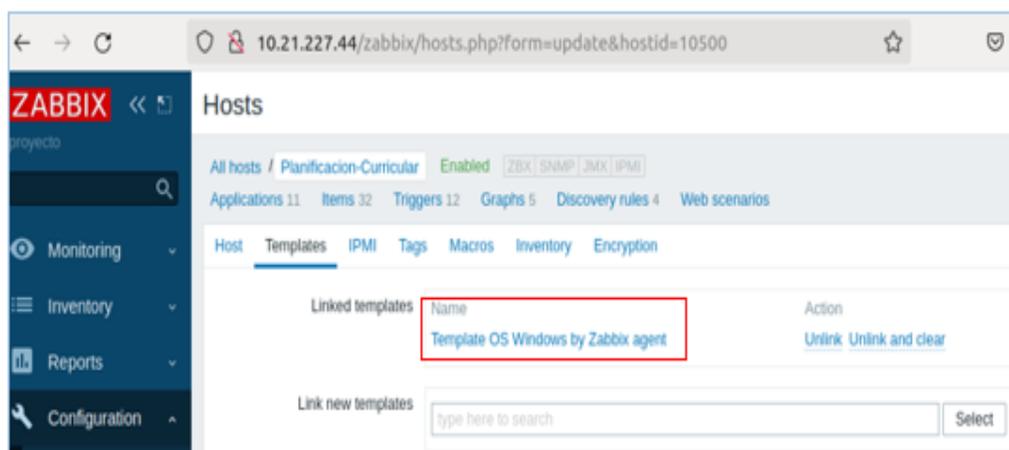
Interfaz del host de planificación curricular



Nota: El gráfico representa la asignación de la dirección ip y el template en la interfaz web de Zabbix al host de planificación curricular.

Figura 83

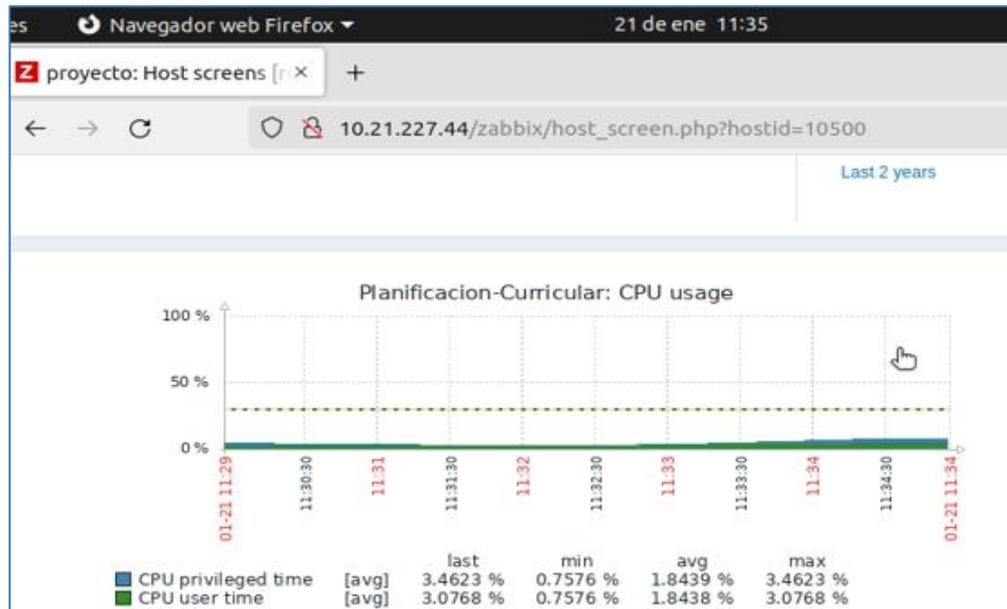
Asignación de templates Zabbix



Nota. El gráfico representa la asignación del template Zabbix agent en el host de planificación curricular.

Figura 84

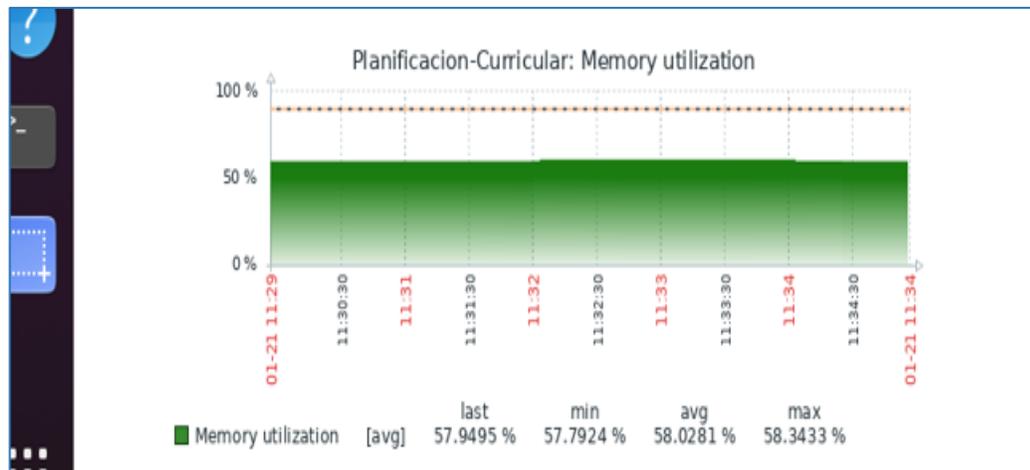
Interfaz de Monitoreo del CPU



Nota. El gráfico representa el tiempo de uso máximo del CPU en un 3,463%.

Figura 85

Interfaz de Monitoreo de Memoria



Nota. El gráfico representa la utilización máxima de 58,34 % de la memoria RAM.

3.10.2 Monitoreo de host del departamento Académico.

Para el monitoreo de este host se debe seguir los siguientes pasos, en la opción de servicio de configuración asignamos la dirección IP del servidor y presionamos Next.

Figura 86

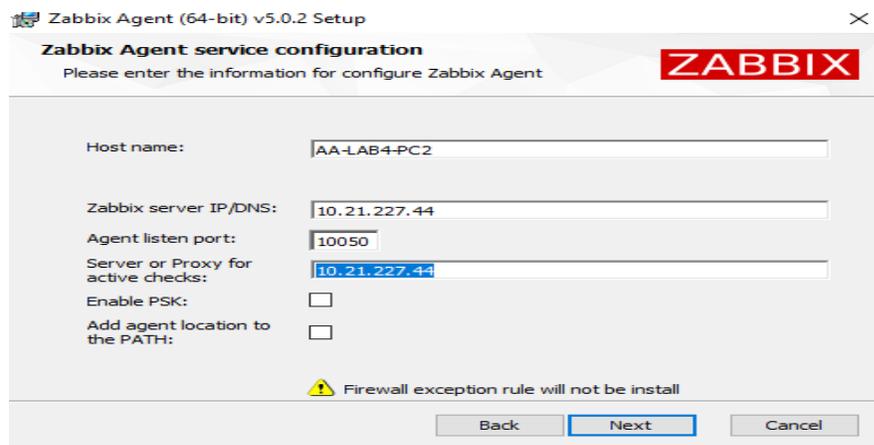
Descarga del agente Zabbix



Nota. El gráfico representa todos los parámetros a cumplirse para la descarga de Agentes Zabbix. Tomado de (ZABBIX, 2022)

Figura 87

Asignación de Ip del servidor Zabbix



Nota. El gráfico representa la asignación de la dirección IP del servidor Zabbix.

Figura 88

Asignación del host en Zabbix

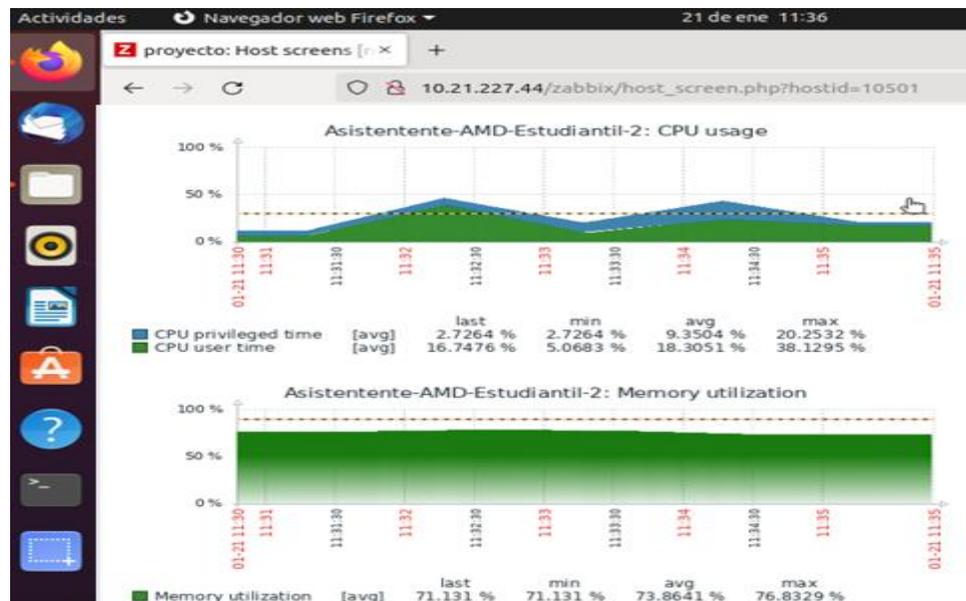
The screenshot shows the Zabbix 'Hosts' configuration page. The browser address bar displays '10.21.227.44/zabbix/hosts.php?form=create&groupids[0]=24'. The page title is 'Hosts'. There are tabs for 'Host', 'Templates', 'IPMI', 'Tags', 'Macros', 'Inventory', and 'Encryption'. The form contains the following fields:

- * Host name: AA-PC460
- Visible name: Asistente-AMD-Estudiantil-2
- * Groups: Departamento Académico
- * Interfaces: A table with columns 'Type', 'IP address', and 'DNS name'. One entry is 'Agent' with IP address '10.21.227.72', which is highlighted with a red box.
- Description: (empty text area)
- Monitored by proxy: (no proxy)
- Enabled: (checked)
- Buttons: 'Add' and 'Cancel'

Nota. El gráfico representa la asignación de los parámetros esenciales en el host.

Figura 89

Interfaz de monitoreo



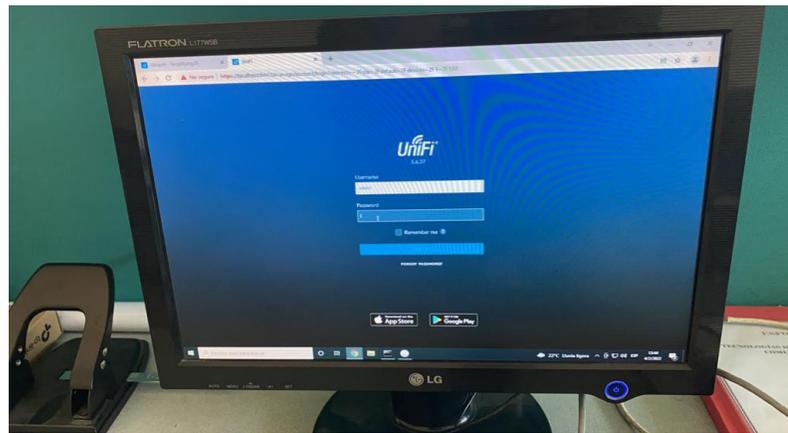
Nota. El gráfico representa la utilización del CPU y el uso de la memoria en el host.

3.11 Monitoreo de los equipos Ubiquiti Ac Lite

Para el monitoreo de los equipos Ubiquiti Ac Lite accederemos a su consola principal UniFi, en donde se colocará el usuario y la contraseña, lo que permite acceder al interfaz principal de los equipos.

Figura 90

Interfaz de inicio en UniFi



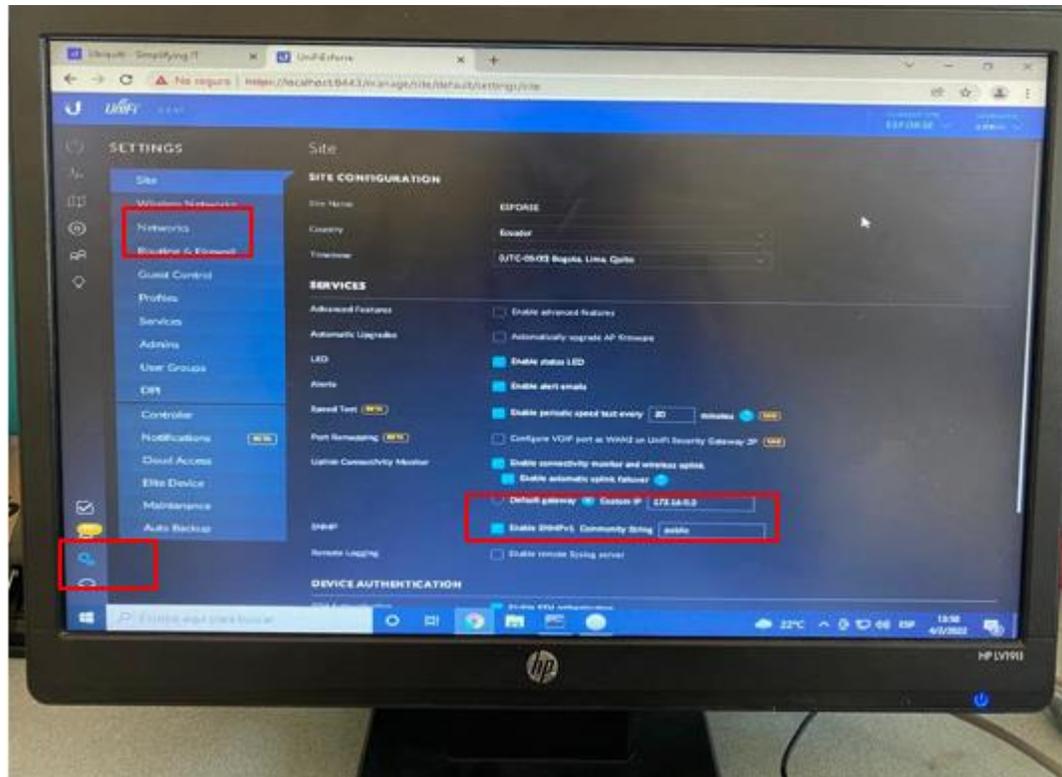
Nota: El gráfico representa la interfaz principal para la asignación de usuario y contraseña.

3.11.1 Configuración del protocolo SNMP

En la interfaz principal de UniFi damos clic en la opción de configuración, clic en el parámetro Networks y buscamos la opción enable SNMPv1 y se habilita la opción señalada. En el parámetro de Community String colocamos la palabra public, guardamos los cambios y salimos de la interfaz.

Figura 91

Interfaz de configuración de UniFi



Nota. El gráfico representa la habilitación del protocolo SNMPv1 y Community String public.

3.11.2 Asignación de los dispositivos en Zabbix

En la interfaz principal del servidor Zabbix en la opción de configuración dar clic en nuevo host, se edita el nombre del equipo y se elige el respectivo grupo de template al que pertenece. Se agrega la dirección de Ip del equipo 172.16.2.96 con su respectivo puerto, en el parámetro templates elegimos el Template Net Ubiquiti Airos SNMP, dar clic en Add para agregar el equipo al servidor.

Figura 92

Asignación de Ap Ubiquiti Ac Lite

The screenshot shows the Zabbix configuration interface for a host named 'UWH-AP-AC-11'. The browser address bar indicates the URL is '10.21.227.44/zabbix/hosts.php?form=update&hostid=10485'. The page title is 'Hosts'. The configuration is for a host in the 'Gasolinera-Transporte' group, which is enabled. The host name is 'UWH-AP-AC-11' and the visible name is 'Gasolinera-Transporte'. The host is assigned to the 'Control-AP-WiFi' and 'Templates/Network devices' groups. An interface is configured with type 'SNMP', IP address '172.16.2.96', and port '161'. The 'Enabled' checkbox is checked.

Nota. El gráfico representa la asignación de la dirección Ip y el template en la AP de gasolinera y transportes.

Figura 93

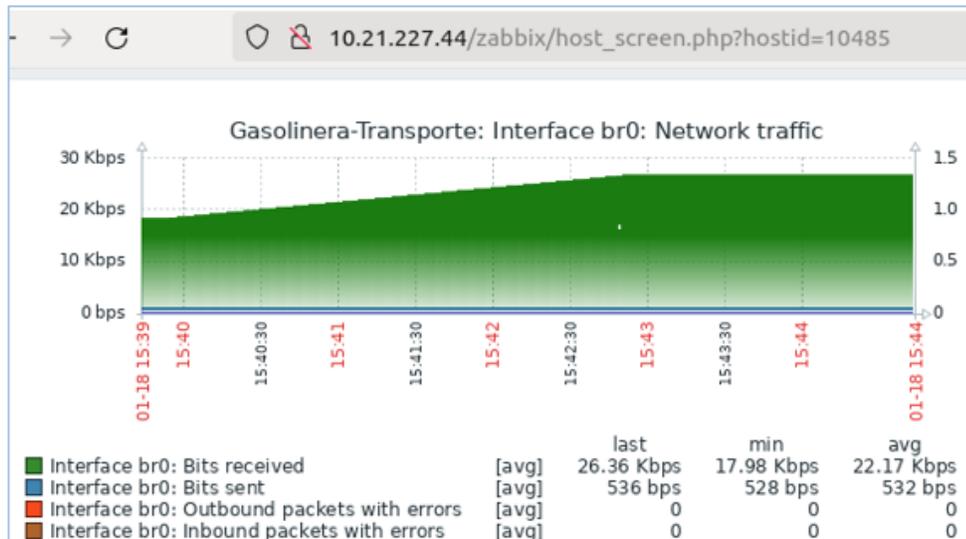
Asignación del template

The screenshot shows the 'Link new templates' section of the Zabbix configuration interface. The browser address bar indicates the URL is '10.21.227.44/zabbix/hosts.php?form=create&groupids[0]=22'. The page title is 'Hosts'. The 'Link new templates' dropdown menu is open, showing 'Template Net Ubiquiti AirOS SNMP' selected. The 'Add' button is highlighted.

Nota. Se observa la agregación del template de Ubiquiti en la AP de gasolinera y transportes.

Figura 94

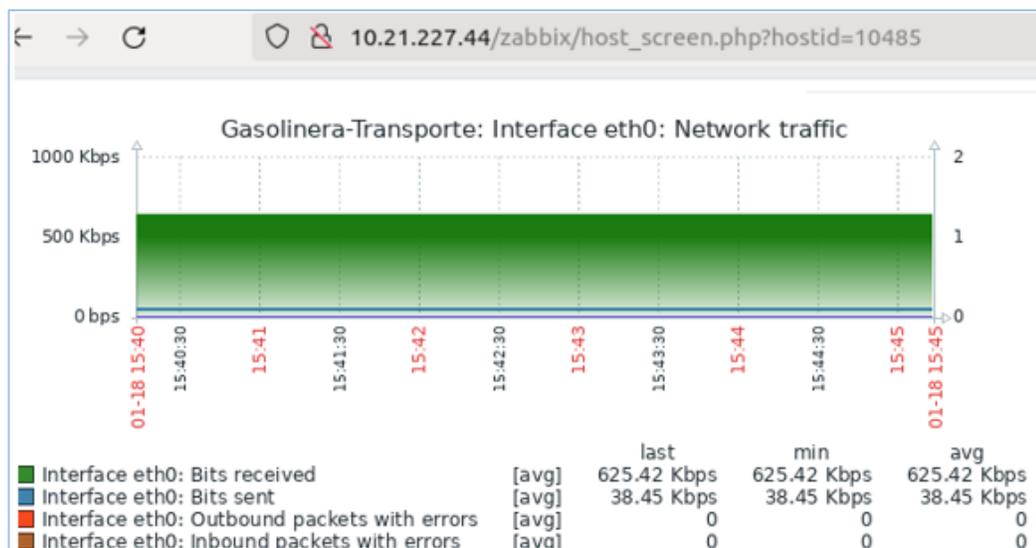
Interfaz de tráfico de red



Nota. El gráfico representa los valores monitorizados de la interface bridge en la Ap.

Figura 95

Interfaz de red en eth0



Nota. Se observa los valores de los bits enviados y recibidos en la interfaz eth0.

3.12 Verificación de los equipos agregados en el servidor Zabbix

Figura 96

Dispositivos monitoreados en Zabbix

Name	Interface	Availability	Tags	Problems	Status	Latest data	Problems	Graphs
Sub-Proceso-Planificacion	10.21.227.148: 10050	zbx SHAMP JMX IPMI		21	Enabled	Latest data	Problems 22	Graphs 1
Sistema-Finaciero-1	10.21.227.47: 10050	zbx SHAMP JMX IPMI		18	Enabled	Latest data	Problems 18	Graphs 1
Servidor-Zabbix	10.21.227.44: 10050	zbx SHAMP JMX IPMI		1	Enabled	Latest data	Problems 1	Graphs 1
Planificacion-Horario-Docente	10.21.227.223: 10050	zbx SHAMP JMX IPMI		5	Enabled	Latest data	Problems 8	Graphs 1
Planificacion-Curricular	10.21.227.77: 10050	zbx SHAMP JMX IPMI		7	Enabled	Latest data	Problems 8	Graphs 2
PC-Tramites Logistica	10.21.227.219: 10050	zbx SHAMP JMX IPMI		17	Enabled	Latest data	Problems 18	Graphs 1
PC-Seg-Informatica	10.21.227.48: 10050	zbx SHAMP JMX IPMI		15	Enabled	Latest data	Problems 15	Graphs 1
PC-Repuesto-Daño	10.21.227.135: 10050	zbx SHAMP JMX IPMI		1	Enabled	Latest data	Problems 14	Graphs 1
PC-Registro-Ingreso	10.21.227.144: 10050	zbx SHAMP JMX IPMI		14	Enabled	Latest data	Problems 14	Graphs 1
PC-Proyectos-Construcciones	10.21.227.171: 10050	zbx SHAMP JMX IPMI		6	Enabled	Latest data	Problems 7	Graphs 1
PC-Proceso-Compra	10.21.227.95: 10050	zbx SHAMP JMX IPMI		11	Enabled	Latest data	Problems 13	Graphs 1
PC-Partes- Operaciones	172.16.2.58: 10050	zbx SHAMP JMX IPMI		1	Enabled	Latest data	Problems 2	Graphs 5
PC-Oficial-Tics-Control	10.21.227.213: 10050	zbx SHAMP JMX IPMI		18	Enabled	Latest data	Problems 19	Graphs 1
PC-Oficial-Juridico	10.21.227.65: 10050	zbx SHAMP JMX IPMI		1	Enabled	Latest data	Problems 8	Graphs 2
PC-Oficial-COM-Social	10.21.227.87: 10050	zbx SHAMP JMX IPMI		5	Enabled	Latest data	Problems 6	Graphs 1
PC-Material-Bélico	10.21.227.136: 10050	zbx SHAMP JMX IPMI		25	Enabled	Latest data	Problems 26	Graphs 1
PC-Jefe-TICS	10.21.227.129: 161	zbx SHAMP JMX IPMI		1	Enabled	Latest data	Problems 1	Graphs 2
PC-Imprenta	10.21.227.70: 10050	zbx SHAMP JMX IPMI		19	Enabled	Latest data	Problems 20	Graphs 2
PC-Control-Vehicular	10.21.227.144: 10050	zbx SHAMP JMX IPMI		14	Enabled	Latest data	Problems 14	Graphs 1
PC-Control-Datos-DITU	172.16.2.9: 10050	zbx SHAMP JMX IPMI		9	Enabled	Latest data	Problems 9	Graphs 1
PC-Control-Administrativo-PM	10.21.227.102: 10050	zbx SHAMP JMX IPMI		26	Enabled	Latest data	Problems 27	Graphs 1

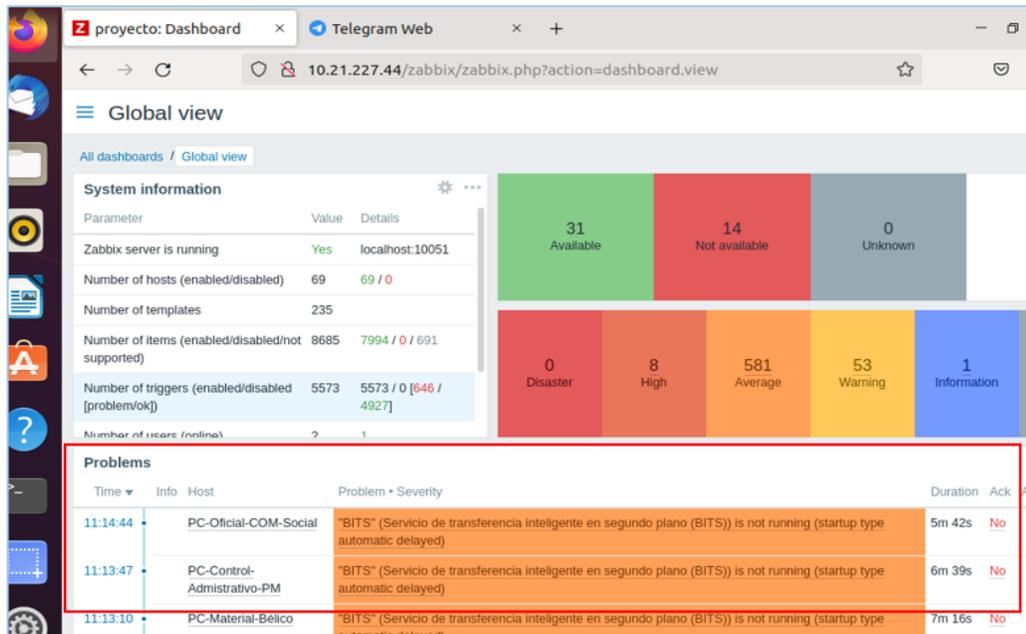
Nota. El gráfico representa los hosts añadidos en el servidor Zabbix con su respectiva IP.

3.13 Notificación de errores en el servidor Zabbix a través del Telegrama.

En el interfaz principal del servidor web de Zabbix y en la parte de problems es donde se mostrará los errores que se vayan presentando de la red o del mismo servidor Zabbix los mismos que serán notificados inmediatamente al grupo de telegram agregado.

Figura 97

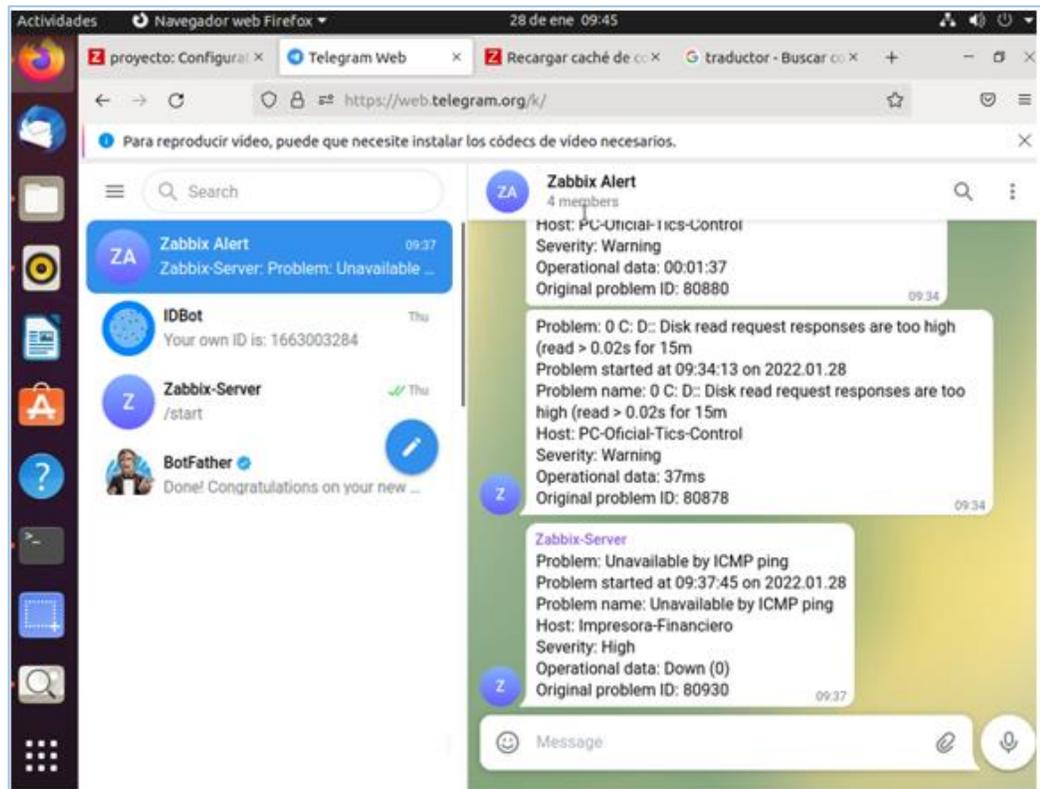
Dashboard de Zabbix



Nota. El gráfico representa la información principal de los equipos agregados y los problemas que tiene cada host.

Figura 98

Verificación de errores por Telegram



Nota. El gráfico representa la notificación de los errores de los equipos monitoreados

Capítulo IV

4 Conclusiones y recomendaciones

4.1 Conclusiones

- Se realizó una investigación acerca de los servidores Open Source de administración de red y se concluyó que, para la monitorización y administración de los diferentes equipos de red como servidores, hardware de red y aplicaciones, es más factible utilizar el servidor Zabbix, donde ayuda a facilitar la administración de la red mediante la habilitar el agente SNMP y el agente Zabbix.
- Se determinó los requerimientos de administración y monitoreo en el departamento de TICS de la ESFORSE, donde unos de los principales requerimientos es obtener las estimaciones sobre los servicios, tráfico de la red, y la capacidad de funcionamiento tanto del hardware como software de los equipos monitoreados.
- Se instaló el servidor de administración de red Zabbix en el sistema operativo Ubuntu Server 20.04, conjuntamente con la configuración y habilitación del protocolo SNMP he instalación del agente Zabbix en los equipos de red a ser monitoreados.
- Se realizó pruebas de funcionamiento del servidor Zabbix instalado, obteniendo datos como el tráfico de red, tiempo de utilización de memoria, procesamiento del CPU, los mismos que son representados en gráficos de monitorización.

4.2 Recomendaciones

- Se recomienda investigar de forma exhaustiva acerca de la implementación del servidor Zabbix, ya que al momento de la instalación de la versión del servidor Zabbix en el Ubuntu Server 20.04, el repositorio del servidor no es compatible o viene con errores internos.
- Se recomienda al momento de instalar y habilitar el protocolo SNMP en los dispositivos de red a ser monitoreados, revisar que esté asignado el puerto de comunicación 161, ya que a través de este puerto se establecerá la conexión con servidor Zabbix.
- Se recomienda verificar el valor de la asignación de la memoria caché ya que por defecto se instala con 8M, el cual al momento de realizar la asignación de los hosts tiende a ocasionar errores por la baja capacidad de memoria caché lo que origina la deshabilitación del servidor Zabbix.
- Se recomienda verificar los requerimientos técnicos del servidor Zabbix, como la memoria de almacenamiento y la memoria RAM, ya que el uso de la memoria dependerá de los hosts y los parámetros que se vayan monitorear en el servidor.

Bibliografía

Adeva, R. (4 de Junio de 2021). *adslzone*. Recuperado el 26 de Diciembre de 2021, de

<https://www.adslzone.net/reportajes/software/que-es-linux/>

Altavoz.net. (2021). *Tecnológico Nacional de México*. Recuperado el 26 de Diciembre de

2021, de <http://www.dgest.gob.mx/telecomunicaciones/open-source>

Bigelow, S. J. (Abril de 2021). *Computer Weekly*. Recuperado el 27 de Noviembre de

2021, de <https://www.computerweekly.com/es/definición/Sistema-operativo-Linux>

Carate, B. &. (2019). *DISEÑO DE UN SISTEMA DE DETECCIÓN DE INTRUSOS*

(NIDS) PARA UNA RED SIMULADA PYMES EN GNS3, IMPLEMENTADA EN

UN MÓDULO RASPBERRY PI PORTÁTIL. UNIVERSIDAD POLITÉCNICA

SALESIANA. Obtenido de

[https://dspace.ups.edu.ec/bitstream/123456789/17546/1/UPS%20-](https://dspace.ups.edu.ec/bitstream/123456789/17546/1/UPS%20-%20ST004141.pdf)

[%20ST004141.pdf](https://dspace.ups.edu.ec/bitstream/123456789/17546/1/UPS%20-%20ST004141.pdf)

Carate, B., & Pozo, D. (2019). *DISEÑO DE UN SISTEMA DE DETECCIÓN DE*

INTRUSOS (NIDS) PARA UNA RED SIMULADA PYMES EN GNS3,

IMPLEMENTADA EN UN MÓDULO RASPBERRY PI PORTÁTIL.

UNIVERSIDAD POLITÉCNICA SALESIANA. Obtenido de

[https://dspace.ups.edu.ec/bitstream/123456789/17546/1/UPS%20-](https://dspace.ups.edu.ec/bitstream/123456789/17546/1/UPS%20-%20ST004141.pdf)

[%20ST004141.pdf](https://dspace.ups.edu.ec/bitstream/123456789/17546/1/UPS%20-%20ST004141.pdf)

Castillo, J. (2016). *“ESTUDIO COMPARATIVO DEL RENDIMIENTO DE SERVIDORES*

WEB DE VIRTUALIZACIÓN SOBRE LA PLATAFORMA WINDOWS SERVER

2008”. ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO. Obtenido de

<http://dspace.esPOCH.edu.ec/bitstream/123456789/1946/1/98T00016.pdf>

- CONPILAR. (16 de Marzo de 2021). Recuperado el 2022 de Febrero de 14, de <https://compilar.es/que-es-snmp-instalar-y-configurar-snmp-en-linux/>
- DocuSign. (2020). *10 tipos de servidores que debes conocer*. Recuperado el 26 de Noviembre de 2021, de <https://www.docuSign.mx/blog/tipos-de-servidores>
- Hernández, J. E. (08 de Agosto de 2013). Recuperado el 30 de Diciembre de 2021, de Configura Ubuntu: http://911-ubuntu.weebly.com/zabbix_como_funciona/conoce-la-estructura-de-zabbix-y-como-usarlo#comments
- Hernández, J. E. (03 de Agosto de 2020). *Ubuntu*. Recuperado el 30 de Diciembre de 2021, de <http://911-ubuntu.weebly.com>
- Ing.Aldo N.Bianchi, M. (2015). *Geocities*. Recuperado el 11 de Diciembre de 2021, de <http://www.geocities.ws/abianchi04/textoredes/snmp.pdf>
- IONOS, D. G. (2019). Recuperado el 26 de Noviembre de 2021, de ¿Qué es un servidor web y qué soluciones de software existen?: <https://www.ionos.es/digitalguide/servidores/know-how/servidor-web-definición-historia-y-programas/>
- León, D. (2021). *Servidores de Red: Características, Ventajas y Desventajas*. Recuperado el 26 de Noviembre de 2021, de <https://blog.infranetworking.com/servidores-de-red/>
- Machado, A. (8 de Febrero de 2016). *Naps Tecnología y educación*. Recuperado el 10 de Diciembre de 2021, de <https://naps.com.mx/blog/funciones-de-un-administrador-de-redes/>
- Manuel, S. O. (16 de Septiembre de 2016). *ITD*. Recuperado el 12 de Noviembre de 2021, de

<https://sites.google.com/a/itdurango.edu.mx/10040372/system/app/pages/sistema-p/hierarchy>

Moreno, A. G. (2015). *Diseño e implementación de un prototipo de software para la administración de red usando snmp v3 sobre el sistema operativo android*. Quito: EPN (Escuela Politécnica Nacional).

Open IT Networks. (2021). Recuperado el 29 de Diciembre de 2021, de <https://www.openitnet.com/index.php/software/nagios/nagios-xi>

PANDORAFMS. (08 de Julio de 2021). Recuperado el 29 de Diciembre de 2021, de <https://pandorafms.com/blog/es/monitorización-de-red/>

Ramírez , F. N. (09 de Septiembre de 2017). *Software Construimos Ideas*. Recuperado el 29 de Diciembre de 2021, de <https://itsoftware.com.co/content/cacti-sistema-recolección-datos-gráficas/>

Robledo, J. C. (26 de Febrero de 2021). *NORTH NETWORKS*. Recuperado el 29 de Diciembre de 2021, de <https://www.north-networks.com/que-es-nagios/>

Robles, F. J. (2018). *Planificación y Administración de Redes (GRADO SUP.)*. España: RA-MA.

Rosa, I. L. (22 de Octubre de 2021). *pandorafms*. Recuperado el 26 de Diciembre de 2021, de <https://pandorafms.com/blog/es/protocolos-de-administración-de-redes/>

Rufus. (2022). Recuperado el 26 de Enero de 2022, de <https://rufus.ie/es/>

SALAS, J. S. (2020). *DISEÑO DE UNA HERRAMIENTA DE MONITOREO Y CONTROL DE SERVIDORES UTILIZANDO COMO EJE PRINCIPAL CACTI. APLICADO A UNA PYME MEDIANA*. Bogotá: UNIVERSIDAD COOPERATIVA DE COLOMBIA.

SANTIAGO, A. C. (2016). *DESARROLLO DE UN SISTEMA INALÁMBRICO BASADO EEG PARA EL MONITOREO DEL SUEÑO EN UN CONDUCTOR*. CUENCA.

Sri, Y. (2018). *capterra*. Recuperado el 29 de Diciembre de 2021, de <https://www.capterra.ec/software/135902/zabbix-monitoring-solution>

Telectronia. (2018). *GNS3 Guía Introductoria: Características y Requerimientos Mínimos*. Recuperado el 26 de Diciembre de 2021, de <https://www.telectronika.com/articulos/ti/que-es-gns3/>

Ubuntu. (2022). *ubuntu*. Recuperado el 26 de Enero de 2021, de <https://ubuntu.com/download/server>

UNAN. (2017). *UNAN*. Recuperado el 11 de Diciembre de 2021, de https://programas.cuaed.unam.mx/repositorio/moodle/pluginfile.php/931/mod_resource/content/4/contenido/index.html

Valarezo Saldarriaga, G. G., & Simisterra Huila, J. C. (2018). *Implementación de un sistema de gestión y administración de redes basados en el protocolo simple de monitoreo de redes SNMP en la red ESPOL-FIEC*. Guayaquil: ESPOL.

Valdés, B. (Enero de 2021). *Administración de redes*. Recuperado el 14 de Noviembre de 2021, de <https://www.administracionderedes.com>

Vega, G. (2018). *IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO PARA EL ANÁLISIS DE LA DISPONIBILIDAD, CAPACIDAD, CALIDAD Y LATENCIA DE ENLACES CORPORATIVOS DE ÚLTIMA MILLA*. Obtenido de <http://repositorio.ucsg.edu.ec/bitstream/3317/11890/1/T-UCSG-POS-MTEL-118.pdf>

ZABBIX. (2022). *ZABBIX*. Recuperado el 27 de Enero de 2022, de
https://www.zabbix.com/la/download_agents

Anexos