



**Implementación, administración y monitoreo de una red corporativa simulada en el Laboratorio de Redes Virtual de la Universidad de las Fuerzas Armadas ESPE sede Latacunga mediante un servidor Zabbix**

Salcedo Sambachi, Daniela Aracely y Wamputsrik Tanguila, Alex Jamil

Departamento de Eléctrica y Electrónica

Carrera de Tecnología Superior en Redes y Telecomunicaciones

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

Ing. Caicedo Altamirano, Fernando Sebastián

6 de Septiembre del 2021



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

**CERTIFICACIÓN**

Certifico que la monografía, "Implementación, administración y monitoreo de una red corporativa simulada en el laboratorio de redes virtual de la Universidad de las Fuerzas Armadas ESPE Sede Latacunga mediante un servidor Zabbix." fue realizado por los señores Salcedo Sambachi, Daniela Aracely y Wamputsrik Tanguila, Alex Jamil, 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, 6 de septiembre del 2021



FERNANDO SEBASTIÁN  
CAICEDO ALTAMIRANO

Caicedo Altamirano Fernando Sebastián

C. C.1803935020

## Reporte de verificación (urkund)



### Document Information

Analyzed document	Monografia_Daniela_Salcedo_y_Alex_Wamputrik_Monitores_Red_GNS3_con_Zabbix.pdf (D112146593)
Submitted	9/6/2021 10:45:00 PM
Submitted by	
Submitter email	biblioteca@espe.edu.ec
Similarity	4%
Analysis address	ibiblioteca.GDC@analysis.orkund.com

### Sources included in the report

<b>W</b>	URL: <a href="https://repositorio.unican.es/xmlui/bitstream/handle/10902/14184/409473.pdf">https://repositorio.unican.es/xmlui/bitstream/handle/10902/14184/409473.pdf</a> sequence=1&isAllowed=y Fetched: 11/29/2019 7:41:40 AM		2
<b>W</b>	URL: <a href="https://docplayer.es/8790740-Universidad-tecnica-de-ambato.html">https://docplayer.es/8790740-Universidad-tecnica-de-ambato.html</a> Fetched: 2/7/2020 7:03:10 AM		3
<b>W</b>	URL: <a href="http://911-ubuntu.weebly.com/zabbix_como_funciona/conoce-la-estructura-de-zabbix-y-como-usarlo">http://911-ubuntu.weebly.com/zabbix_como_funciona/conoce-la-estructura-de-zabbix-y-como-usarlo</a> Fetched: 9/6/2021 10:47:00 PM		3
<b>W</b>	URL: <a href="https://docplayer.es/107931226-Trabajo-fin-de-grado.html">https://docplayer.es/107931226-Trabajo-fin-de-grado.html</a> Fetched: 6/5/2021 3:12:02 AM		4
<b>W</b>	URL: <a href="http://911-ubuntu.weebly.com/zabbix_advanced_configuration/cmo-utilizar-simple-check-para-revisar-equipos-de-forma-sencillo">http://911-ubuntu.weebly.com/zabbix_advanced_configuration/cmo-utilizar-simple-check-para-revisar-equipos-de-forma-sencillo</a> Fetched: 9/6/2021 10:47:00 PM		1
<b>W</b>	URL: <a href="https://www.digitalocean.com/community/tutorials/how-to-install-and-configure-zabbix-to-securely-monitor-remote-servers-on-ubuntu-20-04-es">https://www.digitalocean.com/community/tutorials/how-to-install-and-configure-zabbix-to-securely-monitor-remote-servers-on-ubuntu-20-04-es</a> Fetched: 9/6/2021 10:47:00 PM		4



Firmado electrónicamente por:  
**FERNANDO SEBASTIAN  
CAICEDO ALTAMIRANO**

.....  
**Caicedo Altamirano Fernando Sebastián**

C. C.1803935020



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

**RESPONSABILIDAD DE AUTORÍA**

Nosotros, **Salcedo Sambachi, Daniela Aracely** con cedula de ciudadanía n°1725922247 y **Wamputsrik Tanguila, Alex Jamil** con cedula de ciudadanía n°1727555243, declaramos que el contenido, ideas y criterios de la monografía: **Implementación, administración y monitoreo de una red corporativa simulada en el laboratorio de redes virtual de la Universidad de las Fuerzas Armadas ESPE Sede Latacunga mediante un servidor Zabbix** es de nuestra 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, 6 de septiembre del 2021

**Wamputsrik Tanguila Alex Jamil**

C.C:1727555243

**Salcedo Sambachi Daniela Aracely**

C.C:1725922247



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

**AUTORIZACIÓN DE PUBLICACIÓN**

Nosotros **Salcedo Sambachi Daniela Aracely** y **Wamputsrik Tanguila Alex Jamil** autorizamos a la Universidad de las Fuerzas Armadas ESPE publicar la monografía: **Implementación, administración y monitoreo de una red corporativa simulada en el laboratorio de redes virtual de la Universidad de las Fuerzas Armadas ESPE Sede Latacunga mediante un servidor Zabbix.** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de nuestra responsabilidad.

Latacunga, 6 de septiembre del 2021

**Wamputsrik Tanguila Alex Jamil**

C.C:1727555243

**Salcedo Sambachi Daniela Aracely**

C.C:17259247

## **Dedicatoria**

Quiero dedicar de manera muy especial este proyecto principalmente a Dios, quien me dio las fuerzas de voluntad para culminar exitosamente mi carrera. A mi Abuelo que siempre estuvo motivándome y apoyándome incondicionalmente cada día que lo visitaba. A mi Madre quien siempre estuvo a mi lado en las buenas y en las malas brindándome su cariño y amor de Madre, estuvo siempre regañándome, corrigiéndome que tengo que seguir a pesar de las dificultades. A mis tías y hermanos quienes siempre estuvieron para escuchar mis problemas y saber animarme en los días pésimos.

Alex Wamputsrik

### **Dedicatoria**

El presente trabajo lo dedico principalmente a Dios, por ser el inspirador y darme fuerzas para continuar en este proceso de obtener mis anhelos más deseados. A mi madre, por su amor, trabajo y sacrificio en todos estos años, gracias a ella he logrado llegar a la etapa en la que estoy. Ha sido mi orgullo y privilegio. A mis hermanos por estar siempre estar presentes, acompañándome y por el apoyo moral e incondicional, que me brindaron a lo largo de esta etapa de mi vida.

Daniela Salcedo

## **Agradecimiento**

Primero agradezco a Dios, por haberme guiado e iluminado durante todo este camino y así poder culminar esta importante etapa de mi vida. A mis Abuelos y a mi Madre, que fueron mis mayores promotores para realizar este proyecto. Agradecer a esta prestigiosa Universidad de la ESPE, que me acogió y me permitió formarme en ella para poder ser alguien en la vida. Agradecer también a mi compañera de proyecto por haberme elegido como su dúo, y también gracias a sus habilidades de investigación se pudo completar con el desarrollo de nuestro proyecto.

Alex Wamputsrik

## **Agradecimiento**

Agradezco a Dios por bendecirme, por guiarme a lo largo de mi existencia, ser el apoyo y fortaleza en aquellos momentos de dificultad y de debilidad. Gracias a mi madre por el principal motor de mis sueños, por confiar y creer en mis expectativas, por los consejos, valores y principios que me ha inculcado. Gracias a mi hermano por los consejos que me brindado durante este proceso de mi vida y haberme guiado de la mejor manera.

Agradezco a los docentes de la carrera de Redes y Telecomunicaciones de la Universidad de las Fuerzas Armadas ESPE, en especial al Ing. Fernando Caicedo por guiar esta investigación y formar parte de un objetivo alcanzado. Agradezco también a mi compañero por ser un buen equipo para culminar juntos unos de nuestros sueños tan anhelados.

Daniela Salcedo

**Tabla de contenido**

<b>Carátula</b> .....	<b>1</b>
<b>Certificación</b> .....	<b>2</b>
<b>Reporte de verificación (urkund)</b> .....	<b>3</b>
<b>Responsabilidad de auditoría</b> .....	<b>4</b>
<b>Autorización de publicación</b> .....	<b>5</b>
<b>Dedicatoria</b> .....	<b>6</b>
<b>Agradecimiento</b> .....	<b>8</b>
<b>Índice de contenido</b> .....	<b>10</b>
<b>Índice de tablas</b> .....	<b>19</b>
<b>Índice de figuras</b> .....	<b>20</b>
<b>Resumen</b> .....	<b>25</b>
<b>Abstract</b> .....	<b>26</b>
<b>Introducción</b> .....	<b>27</b>
<b>Antecedentes</b> .....	<b>27</b>
<b>Planteamiento del problema</b> .....	<b>28</b>
<b>Justificación e importancia</b> .....	<b>29</b>
<b>Objetivos</b> .....	<b>30</b>
<b>Objetivo general</b> .....	<b>30</b>
<b>Objetivos específicos</b> .....	<b>30</b>
<b>Alcance</b> .....	<b>31</b>

<b>Marco Teórico .....</b>	<b>32</b>
<b>Redes .....</b>	<b>32</b>
<i>Dispositivos .....</i>	<i>32</i>
<i>Tipos de redes .....</i>	<i>32</i>
Red de área local (LAN) .....	33
Red de área metropolitana (MAN).....	33
Red de área amplia (WAN).....	33
<i>Topologías de redes.....</i>	<i>34</i>
Tipos de topologías de red.....	34
Topología de Anillo.....	35
Topología de árbol.....	35
Topología de bus.....	36
Topología Estrella .....	36
Topología Malla .....	36
<b>Implementación de red.....</b>	<b>37</b>
<i>Elegir los recursos materiales .....</i>	<i>37</i>
<i>Conocer las redes .....</i>	<i>37</i>
<i>Conocer los dispositivos.....</i>	<i>38</i>
<i>Pensar siempre en el cliente.....</i>	<i>38</i>
<i>Revisar y evaluar la red .....</i>	<i>38</i>

Administración de red .....	39
<i>Protocolos de administración de red.....</i>	39
ICMP .....	39
SNMP .....	40
<i>Arquitectura SNMP .....</i>	41
WMI.....	42
<i>Arquitectura de WMI .....</i>	42
Monitoreo de red .....	44
<i>Los tipos de monitoreo son:.....</i>	44
Red corporativa.....	45
<i>Protocolo OSPF.....</i>	45
Características básicas de OSPF .....	45
Ventajas de OSPF .....	46
<i>Tunnel VPN.....</i>	46
Funcionamiento de túnel de VPN con IPsec con dispositivos Mikrotik .....	47
Mikrotik.....	47
Herramienta Romon .....	48
Winbox.....	49
Simulador de red.....	50
GNS3.....	50
Funciones de GNS3.....	50

Máquinas virtuales.....	51
VMware.....	52
Herramientas de monitoreo de una red.....	53
<i>Nagios</i> .....	53
<i>Pandora FMS</i> .....	54
<i>Zabbix</i> .....	55
Servidor Zabbix.....	56
Funcionamiento de Zabbix.....	56
Componentes de Zabbix.....	57
Servidor Zabbix.....	57
Agente Zabbix.....	58
Interfaz web.....	58
Funcionamiento de monitoreo en Zabbix.....	59
Interfaz web de Zabbix.....	61
<i>Panel de control</i> .....	61
<i>Problems</i> .....	62
<i>Host</i> .....	62
<i>Screens</i> .....	62
<i>Maps</i> .....	62
<i>Latest data</i> .....	63
<i>Graphs</i> .....	63

<i>Ítems</i> .....	63
<i>Triggers</i> .....	63
<i>Media types</i> .....	63
Desarrollo .....	64
Servidor Zabbix .....	64
Implementación de la red corporativa.....	66
<i>Requisitos de instalación de VMware Workstation 15.5.1 Pro</i> .....	66
Visualización de la interfaz VMware instalado .....	68
Instalación GNS3/VMware en VMware Workstation .....	68
<b>GNS3</b> .....	70
Requisitos mínimos GNS3.....	70
Instalación GNS3 .....	70
Aceptación de licencia .....	71
Selección de componentes .....	72
Selección del destino de instalación.....	73
Proceso de instalación de aplicaciones .....	74
Finalización de instalación .....	75
Asistente de configuración .....	76
Visualización de la interfaz GNS3.....	77
Configuración general de GNS3/VM.....	78

Verificación de conexión de GNS3/VM.....	79
<i>Creación de la red corporativa .....</i>	<i>80</i>
Configuración de la herramienta Romon.....	83
Configuración IP .....	84
Configuración del protocolo OSPF .....	86
Configuración de IPsec.....	87
Agregación de peers .....	89
<i>Instalación de la máquina virtual Ubuntu en VMware.....</i>	<i>91</i>
<i>Asistente de instalación .....</i>	<i>91</i>
<i>Selección de imagen ISO.....</i>	<i>92</i>
<i>Configuración de usuario.....</i>	<i>93</i>
<i>Ubicación de instalación de la máquina virtual.....</i>	<i>94</i>
<i>Configuración tamaño de disco .....</i>	<i>95</i>
<i>Resumen de las configuraciones de la máquina virtual .....</i>	<i>96</i>
<i>Inicio de instalación de la máquina virtual Ubuntu.....</i>	<i>97</i>
Visualización del proceso de instalación .....	98
Iniciar sesión en Ubuntu .....	99
Instalación del servidor Zabbix en la máquina virtual Ubuntu.....	101
<i>Requisitos de instalación del servidor web Zabbix .....</i>	<i>102</i>
Selección de la versión de Zabbix.....	102

Instalación del repositorio de Zabbix.....	102
Instalación del servidor, la interfaz y el agente de Zabbix .....	103
Instalación de la Base de Datos.....	104
Importación del esquema y los datos iniciales.....	105
Configuración de la Base de Datos para el servidor Zabbix .....	106
Configuración PHP para Zabbix Fronted .....	107
Iniciación y restauración del agente y el servidor .....	107
Instalación de la herramienta de red y verificación IP .....	108
Inicio de instalación de la interfaz web del servidor .....	109
Verificación de pre-requisitos .....	110
Configuración de conexión de la base de datos .....	111
Detalles del servidor Zabbix.....	112
Resumen de la preinstalación.....	113
Inicio de sesión .....	114
Panel de control de la interfaz web de Zabbix .....	115
Monitoreo de la red corporativa simulada .....	116
<i>Habilitación protocolo SNMP.....</i>	<i>116</i>
Creación del host.....	118
Verificación de host creados.....	120
Latest data del Router .....	121

<b>Verificación de gráficas .....</b>	<b>122</b>
<b>Creación de Maps .....</b>	<b>124</b>
<b>Creación de elementos .....</b>	<b>124</b>
<b>Configuración de equipos en maps .....</b>	<b>125</b>
<b>Creación de topología .....</b>	<b>126</b>
<b>Creación screen .....</b>	<b>128</b>
<b>Configuración Screens Red .....</b>	<b>128</b>
<b>Creación de notificaciones por Gmail.....</b>	<b>130</b>
<b>Habilitación trigger actions .....</b>	<b>130</b>
<b>Configuración de trafico de red .....</b>	<b>132</b>
<b>Comprobación de notificaciones por Gmail.....</b>	<b>134</b>
<b>Implementación del servidor Zabbix en las computadoras del laboratorio de comunicaciones de la ESPEL.....</b>	<b>136</b>
<b><i>Características de la computadora .....</i></b>	<b><i>136</i></b>
<b>    <b>Instalación de los simuladores GNS3, VMware .....</b></b>	<b>137</b>
<b>Implementacion del manual del servidor Zabbix y guía de laboratorio de la administracion de red.....</b>	<b>140</b>
<b>Conclusiones y recomendaciones .....</b>	<b>143</b>
<b>    <b>Conclusiones.....</b></b>	<b>143</b>
<b>    <b>Recomendaciones .....</b></b>	<b>144</b>

<b>Bibliografía .....</b>	<b>145</b>
<b>Anexos .....</b>	<b>148</b>

**Índice de tablas**

**Tabla 1** Direccionamiento IP ..... 82

**Tabla 2** Comparación de las herramientas de monitoreo ..... 101

## Índice de figuras

<b>Figura 1</b> <i>Tipos de redes</i> .....	34
<b>Figura 2</b> <i>Tipos de topologías de red</i> .....	35
<b>Figura 3</b> <i>Funcionamiento ICMP</i> .....	40
<b>Figura 4</b> <i>Arquitectura SNMP</i> .....	42
<b>Figura 5</b> <i>Arquitectura de WMI</i> .....	43
<b>Figura 6</b> <i>RouterOS Mikrotik</i> .....	48
<b>Figura 7</b> <i>Romon</i> .....	49
<b>Figura 8</b> <i>Winbox</i> .....	50
<b>Figura 9</b> <i>Interfaz de GNS3</i> .....	51
<b>Figura 10</b> <i>VMWare Workstation</i> .....	53
<b>Figura 11</b> <i>Interfaz principal de Nagios</i> .....	54
<b>Figura 12</b> <i>Interfaz principal de Pandora FMS</i> .....	55
<b>Figura 13</b> <i>Funcionamiento de Zabbix</i> .....	57
<b>Figura 14</b> <i>Monitoreo en Zabbix</i> .....	59
<b>Figura 15</b> <i>Panel de control del servidor web Zabbix</i> .....	61
<b>Figura 16</b> <i>Funcionamiento de Zabbix</i> .....	65
<b>Figura 17</b> <i>Características de instalación VMware Workstation 15.5.1 Pro</i> .....	67
<b>Figura 18</b> <i>Interfaz principal VMware</i> .....	68
<b>Figura 19</b> <i>Instalación GNS3/VM</i> .....	69
<b>Figura 20</b> <i>Selección de GNS3VM del escritorio</i> .....	69
<b>Figura 21</b> <i>Interfaz de bienvenida GNS3</i> .....	71
<b>Figura 22</b> <i>Contrato de licencia</i> .....	72

<b>Figura 23</b> <i>Elegir componentes</i> .....	73
<b>Figura 24</b> <i>Ubicación de instalación</i> .....	74
<b>Figura 25</b> <i>Final de Instalación</i> .....	75
<b>Figura 26</b> <i>Instalación completada</i> .....	76
<b>Figura 27</b> <i>Setup Wizard</i> .....	77
<b>Figura 28</b> <i>Interfaz de GNS3</i> .....	78
<b>Figura 29</b> <i>Preferencias de GNS3/VM</i> .....	79
<b>Figura 30</b> <i>Interfaces de conexión entre GNS3 y VMware</i> .....	80
<b>Figura 31</b> <i>Topología de red</i> .....	81
<b>Figura 32</b> <i>IP del RouterOS Mikrotik</i> .....	81
<b>Figura 33</b> <i>Configuración de Romon y nombre de los Routers</i> .....	83
<b>Figura 34</b> <i>Conexión a la herramienta Romon</i> .....	84
<b>Figura 35</b> <i>Lista de direcciones de IP Matriz</i> .....	85
<b>Figura 36</b> <i>Configuración de ip y Gateway</i> .....	85
<b>Figura 37</b> <i>Configuración protocolo OSPF</i> .....	86
<b>Figura 38</b> <i>Comprobación de conectividad</i> .....	87
<b>Figura 39</b> <i>Configuración Ipsec en los routers</i> .....	88
<b>Figura 40</b> <i>Configuración peers de IPsec</i> .....	88
<b>Figura 41</b> <i>Creación de IPsec Identity</i> .....	89
<b>Figura 42</b> <i>Creación de propuesta IPsec</i> .....	90
<b>Figura 43</b> <i>Creación de política de IPsec</i> .....	90
<b>Figura 44</b> <i>Interfaz principal de VMware</i> .....	91
<b>Figura 45</b> <i>Ventana de asistente de creación</i> .....	92
<b>Figura 46</b> <i>Ventana de selección imagen ISO</i> .....	93

<b>Figura 47</b> <i>Creación de usuario y contraseña</i> .....	94
<b>Figura 48</b> <i>Ventana de ubicación de instalación</i> .....	95
<b>Figura 49</b> <i>Configuración de tamaño del disco virtual</i> .....	96
<b>Figura 50</b> <i>Configuración general de la máquina virtual</i> .....	97
<b>Figura 51</b> <i>Ventana de inicialización de instalación</i> .....	98
<b>Figura 52</b> <i>Interfaz de bienvenida Ubuntu</i> .....	99
<b>Figura 53</b> <i>Interfaz de inicio de sesión</i> .....	100
<b>Figura 54</b> <i>Interfaz menú principal de Ubuntu</i> .....	100
<b>Figura 55</b> <i>Página oficial de Zabbix</i> .....	102
<b>Figura 56</b> <i>Instalación del repositorio de Zabbix</i> .....	103
<b>Figura 57</b> <i>Instalación de Zabbix server, frontend y agent</i> .....	104
<b>Figura 58</b> <i>Instalación y creación de la base de datos</i> .....	105
<b>Figura 59</b> <i>Configuración del host del servidor Zabbix</i> .....	106
<b>Figura 60</b> <i>Interfaz de configuración de la base de datos</i> .....	106
<b>Figura 61</b> <i>Configuración PHP para frontend de Zabbix</i> .....	107
<b>Figura 62</b> <i>Inicialización del sistema</i> .....	108
<b>Figura 63</b> <i>Instalación de herramientas de red</i> .....	109
<b>Figura 64</b> <i>Interfaz de bienvenida Zabbix</i> .....	110
<b>Figura 65</b> <i>Interfaz de verificación</i> .....	111
<b>Figura 66</b> <i>Configuración de conexión de la base de datos</i> .....	112
<b>Figura 67</b> <i>Interfaz Zabbix server details</i> .....	113
<b>Figura 68</b> <i>Resumen de preinstalación</i> .....	114
<b>Figura 69</b> <i>Interfaz de inicio de sesión</i> .....	115
<b>Figura 70</b> <i>Panel de control principal</i> .....	116

<b>Figura 71</b> Configuración protocolo SNMP .....	117
<b>Figura 72</b> Configuración SNMP_COMMUNITY .....	118
<b>Figura 73</b> Configuración de host.....	119
<b>Figura 74</b> Configuración de templates.....	120
<b>Figura 75</b> Verificación de host.....	121
<b>Figura 76</b> Interfaz latest data.....	122
<b>Figura 77</b> Interfaz gráfica .....	123
<b>Figura 78</b> Interfaz gráfica 2 .....	123
<b>Figura 79</b> Configuración de map.....	124
<b>Figura 80</b> Configuración de Router.....	125
<b>Figura 81</b> Configuración de estado del Router.....	126
<b>Figura 82</b> Topología de red en Map.....	127
<b>Figura 83</b> Comprobación de Funcionamiento .....	127
<b>Figura 84</b> Configuración de Screen .....	128
<b>Figura 85</b> Configuración de graph.....	129
<b>Figura 86</b> Verificación de Screen .....	129
<b>Figura 87</b> Interfaz Media types .....	130
<b>Figura 88</b> Interfaz de habilitación de correo .....	131
<b>Figura 89</b> User profile: Zabbix Administrator .....	132
<b>Figura 90</b> Bandwidth test (Running) .....	133
<b>Figura 91</b> Verificación de tráfico de red.....	134
<b>Figura 92</b> Dashboard .....	135
<b>Figura 93</b> Gmail.....	136
<b>Figura 94</b> Instalación de GNS3 .....	137

<b>Figura 95</b> <i>Instalación de VMware Workstation</i> .....	138
<b>Figura 96</b> <i>Interfaz web de Zabbix</i> .....	139
<b>Figura 97</b> <i>Instalación en el laboratorio</i> .....	140
<b>Figura 98</b> <i>Manual de implementación</i> .....	141
<b>Figura 99</b> <i>Guía de laboratorio de administración de red</i> .....	142

## Resumen

Este trabajo abarca la realización de una red corporativa simulada en el software GNS3 con dispositivos de RouterOS Mikrotik y se ejecutó la configuración de enrutamiento con el protocolo OSPF, entre dos sedes se estableció la conexión mediante el túnel de VPNs con IPsec donde esta red será monitoreada desde un servidor web Zabbix el cual se utilizó para llevar a cabo la monitorización y administración de la red creada, este servidor fue instalado en una máquina virtual Ubuntu 20.04 soportada en un simulador VMware Workstation pro donde primero se estableció los adaptadores de red y también se procedió a configurar en el panel de control del servidor web de Zabbix y por cada Router con su dirección ip se agregó un host y se estableció el protocolo SNMP, esto también se realizó en la herramienta de redes winbox donde se puede acceder a los routers activando la herramienta Romon y una vez dentro se habilito y configuro el protocolo SNMP para establecer la conexión directa entre la red corporativa y el servidor web Zabbix ya para comenzar a monitorear los routers principales viendo las gráficas, memoria, interfaces y la carga de CPU, Además para administrar se añadió un correo electrónico de Gmail con una cuenta personal donde llegara todas las notificaciones de problemas o fallos y las soluciones realizadas a la red o del mismo servidor web donde indicara la fecha y hora de la falla presentada.

Palabras clave:

- **SERVIDORES (INFORMÁTICA)**
- **MODEM**
- **REDES INFORMÁTICAS**
- **SISTEMAS OPERATIVOS**

## **Abstract**

This work covers the realization of a corporate network simulated in GNS3 software with RouterOS Mikrotik devices and the routing configuration was made with the OSPF protocol, the connection between two sites was established through a VPN tunnel with IPsec where this network will be monitored from a Zabbix web server, which was used to carry out the monitoring and administration of the network created, this server was installed on an Ubuntu 20.04 virtual machine supported on a VMware Workstation pro simulator where the network adapters were first set up and also proceeded to configure in the control panel of the Zabbix web server and for each Router with its ip address a host was added and the SNMP protocol was established, this was also done in the winbox network tool where you can access the routers by activating the Romon tool and once inside, the SNMP protocol was enabled and configured to establish a direct connection between the corporate network and the Zabbix web server to start monitoring the main routers by viewing the graphs, in addition, a Gmail e-mail address was added with a personal account where all notifications of problems or failures and the solutions made to the network or the web server itself, indicating the date and time of the failure, were sent.

Key words:

- **SERVERS**
- **MODEM**
- **COMPUTER NETWORKS**
- **OPERATING SYSTEMS**

## Capítulo I

### 1 Introducción

#### 1.1 Antecedentes

En la actualidad el monitoreo de redes es fundamental para un correcto funcionamiento, despliegue y mantenimiento de las redes corporativas por lo que habido un gran interés en la implementación de este tipo de sistemas como es el caso de:

Trabajo investigado por Fernández A. (2018) Cantabria-España, cuyo tema es: “Estudio e implementación de un entorno de gestión para la red privada del laboratorio docente de telemática”, llegando a concluir que la monitorización de cualquier red siempre resulta rentable si se busca la herramienta adecuada que mejor se adapte a cada tipo de infraestructura. En este caso se trataba de un entorno pequeño de investigación y docencia, por lo que era necesario que la plataforma fuera gratuita Zabbix cumplió estos requisitos con creces; logrando resultados que pueden ser de utilidad la instalación y comparación en detalle de los distintos sistemas de alertas que Zabbix provee.

(Fernandéz, 2018)

Trabajo investigado por Aquino J. (2017) San Salvador-El Salvador, cuyo tema es: “Manual de Instalación, Configuración de un Sistema de Gestión y Monitoreo de Redes Informáticas para Pequeñas y Medianas Empresas en El Salvador, utilizando software libre”, llegando a concluir que se analizaron de forma documental cinco diferentes herramientas de monitoreo de software libre MRTG, NAGIOS, CACTI, ZABBIX, MUNNIN; logrando resultados que Nagios Core es una buena propuesta de implementación para llevar acabo el monitoreo de una red. (Aquino & Martínez, 2017)

Por lo mencionado es importante que el laboratorio de telecomunicaciones cuente con un sistema virtual.

## **1.2 Planteamiento del problema**

La Universidad de las fuerzas Armadas ESPE sede Latacunga fue creado en 1987 en el centro de la ciudad, para albergar a 10.000 estudiantes (Bravo, 2014) donde la carrera de tecnología superior en Redes y Telecomunicaciones fue recientemente creada y como estudiantes se ha presenciado la falta de un laboratorio virtual para realizar prácticas y no contar con herramientas adecuadas para el monitoreo de redes, el cual se ha visto la necesidad de implementar un software de monitoreo de red para el aprendizaje de los estudiantes.

La carrera de tecnología superior en Redes y Telecomunicaciones no cuenta con todos los laboratorios necesarios para dicha carrera, además ha existido el requerimiento en las asignaturas de redes en contar con una herramienta que permita administrar redes que forme parte del laboratorio virtual para que los estudiantes puedan aprender la manipulación de estos sistemas, por esto es trascendental hacer uso de las bondades que otorga la ciencia y la tecnología en el ámbito de dispositivos eléctricos o electrónicos en el área de telecomunicaciones.

De no solucionarse seguirá el inconveniente de que los estudiantes no tengan un laboratorio virtual donde puedan realizar las prácticas de laboratorio además existirá deficiencia de conocimientos en el ámbito para monitorización de una red virtual.

Por lo expuesto es necesario implementar una simulación tanto de una red corporativa como de un sistema de monitoreo para que los estudiantes puedan hacer uso del mismo y profundizar sus conocimientos prácticos.

### **1.3 Justificación e importancia**

En la actualidad debido a la falta de un laboratorio virtual de telecomunicaciones se requiere implementar un sistema de monitoreo de red para poder manipular e ir verificando cada uno dentro del aula, de tal manera tanto como los docentes y estudiantes serán beneficiados ya que podrán realizar las prácticas de manera adecuada. Así como también: facilita el aprendizaje, clases más prácticas, monitoreo de red.

Se aprovecharán los resultados de aprendizaje en el área de monitoreo de redes virtuales y conocimientos tanto teóricos como prácticos con el debido proceso para la manipulación de las herramientas de monitorización.

Por lo dicho es importante que el laboratorio de telecomunicaciones cuente con una herramienta de monitoreo de red virtual para el respectivo aprendizaje, lo cual facilitara la manipulación y verificación de redes a medida que realizan las practicas los estudiantes irán adquiriendo conocimientos básicos de monitoreo de red.

## **1.4 Objetivos**

### **1.4.1 Objetivo general**

Implementar, administrar y monitorear una red corporativa simulada en el laboratorio de redes virtual de la Universidad de las Fuerzas Armadas ESPE Sede Latacunga mediante un servidor Zabbix

### **1.4.2 Objetivos específicos**

- Investigar acerca del servidor Zabbix, su implementación y funcionamiento para aprovechar al máximo en la administración y monitoreo de la red corporativa.
- Implementar una red corporativa con por lo menos 3 sitios remotos simulándola en GNS3 utilizando el sistema operativo RouterOS
- Implementar un servidor de administración y monitoreo de redes Zabbix en las computadoras del laboratorio de comunicaciones de la ESPEL
- Implementar un manual de funcionamiento del servidor Zabbix y una guía de laboratorio de la administración de la red corporativa simulada.

## **1.5 Alcance**

El presente trabajo de titulación consiste en implementar un servidor de administración de redes Zabbix en las computadoras del laboratorio de comunicaciones de la ESPEL, así como también simular una red corporativa que tenga por lo menos tres sitios remotos conectados por VPNs y cuente con las tecnologías y protocolos suficientes de una red de esta categoría. La simulación se la realizará en el software de simulación de redes GNS3 con el sistema operativo RouterOS de Mikrotik.

Se entregará un instructivo del uso del servidor Zabbix y una guía de laboratorio para la administración de la red simulada.

## Capítulo II

### 2 Marco Teórico

#### 2.1 Redes

Una red es el conjunto de varios dispositivos eléctricos los cuales están conectados entre sí, en el cual intercambian y comparten la información y recursos, por lo tanto, una red es un sistema que permite comunicarse con los distintos dispositivos que actúan como emisor y receptor de una manera alternada. (RedUsers, 2021)

##### 2.1.1 *Dispositivos*

Los dispositivos conectados a una red informática según RedUsers se clasifican en: los que gestionan el acceso y las comunicaciones en una red

Dispositivos de red: son aquellos que permiten el acceso a la información y la comunicación, como son los switches, routers, módem, etc.

Dispositivos de usuario final: son aquellos que se conectan a la red para acceder a la información o recursos, como es un ordenador, Tablet, celular. (2021, pág. 1)

##### 2.1.2 *Tipos de redes*

Según el sitio web CMM manifiesta que los tipos de redes se clasifican según la función del tamaño (grande, mediano y pequeño) y del alcance de ordenadores, donde las más importantes son:

### **2.1.2.1 Red de área local (LAN)**

Local Área Network (Red de área local) es una red que básicamente se utiliza en empresas. Es una red que consiste en conectar equipos dentro de un área geográfica pequeña, la cual permite un intercambio de datos y recursos entre sí. Una red de área local puede contener de 100 hasta 1000 usuarios.

### **2.1.2.2 Red de área metropolitana (MAN)**

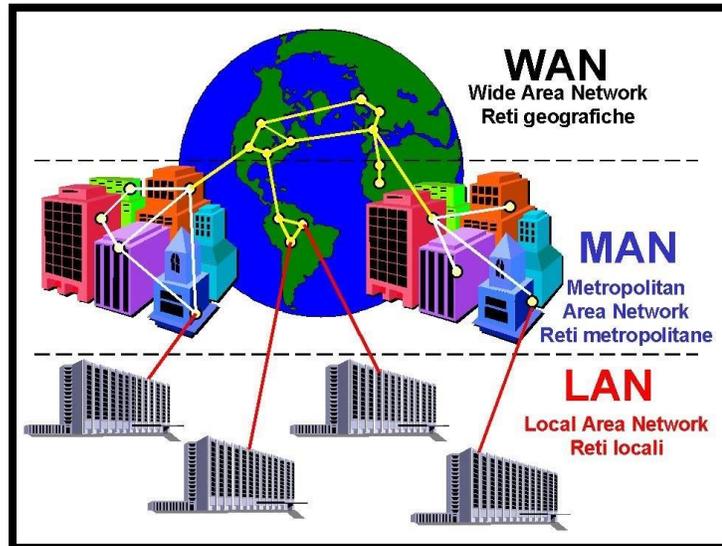
Metropolitan Area Network (Red de área metropolitana) es aquella red que tiene un alcance superior a lo local pero no internacional, un ejemplo de una red MAN son las redes de campus universitarios en la cual cada uno tiene sus sedes en diversos lugares de la ciudad.

### **2.1.2.3 Red de área amplia (WAN)**

Wide Area Network (Red de área amplia) son aquellas redes que se extienden por amplias áreas geográficas y conectan redes más pequeñas como la red LAN o la red MAN. Es una red que se utiliza en el sector profesional, en algunas ocasiones su uso es privado además es útil para los proveedores de internet porque brindan conexión de redes de una zona muy amplia. (2021, pág. 2)

## Figura 1

*Tipos de redes*



*Nota.* El gráfico representa los tipos de redes el cual las redes tienen como función habilitar la capacidad de conexión entre usuarios. Tomado de (Sites, 2018)

### 2.1.3 Topologías de redes

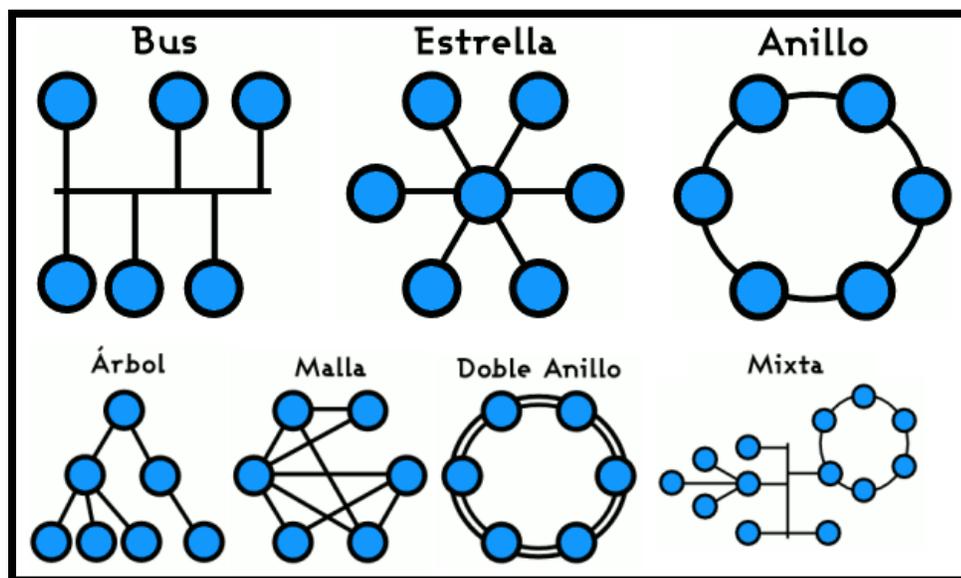
Según Rouse M. (2021) menciona que la topología de red es la forma en la que la red está diseñada para conectar computadoras e intercambiar datos entre sí ya sea físico o lógico, es decir es el procedimiento a tender el cableado que conectará a las computadoras que forman parte de una red.

#### 2.1.3.1 Tipos de topologías de red

Entre las principales topologías de red más utilizados son:

**Figura 2**

*Tipos de topologías de red*



*Nota.* El gráfico representa las diferentes formas de topologías de red y muestra la manera en que va estar el tendido de cableado. Tomado de (Rouse, 2021)

#### **2.1.3.1.1 Topología de Anillo**

Es una topología de red simple, donde las computadoras se encuentran conectadas entre sí en forma de un anillo. La información viaja en un solo sentido por lo que si un nodo deja de funcionar la red dejará de enviar información a las demás computadoras que se encuentran dentro, por lo tanto, es poco eficaz.

#### **2.1.3.1.2 Topología de árbol**

Es una topología de red sencilla, su conexión se lo realiza entre los nodos (terminales o computadoras) está adaptado en forma de árbol con una punta y una base que es parecida a una serie de redes en estrella interconectadas si un nodo falla no

presenta problemas entre los nodos siguientes, cuenta con un cable principal llamado Backbone el cual es el encargado de llevarla comunicación a todos los nodos de la red.

#### **2.1.3.1.3 Topología de bus**

La topología de bus tiene conectado los nodos (computadoras) a un circuito común (cable central), la información que se trasmite por el cable viaja en ambos sentidos a una velocidad aproximada de 10/100Mbps y tiene en sus dos extremos una resistencia (terminador). Pueden estar conectadas gran cantidad de computadoras al cable central (bus), si un computador falla la comunicación se mantienen por lo contrario si el cable central falla la red quedara inutilizada.

#### **2.1.3.1.4 Topología Estrella**

La topología estrella es una red sencilla de computadoras donde los nodos se encuentran conectados directamente a un punto central o host y se comunican a través de ese punto (conmutador, repetidor o concentrador) lo cual en la actualidad es muy utilizada y eficiente por lo que si un nodo falla la comunicación se mantiene por lo tanto depende del funcionamiento del host.

#### **2.1.3.1.5 Topología Malla**

La topología de malla es una red donde cada nodo está conectado a todos los nodos por lo cual permite transmitir la información de un nodo a otro por distintos caminos. A diferencia de las demás topologías no requiere de un nodo central con lo que se reduce el riesgo de fallas y si un nodo falla no implica la caída de toda la red.

(2021, pág. 1)

## **2.2 Implementación de red**

Según el sitio web (Pandora FMS, 2017) manifiesta que para implementar una red se debe tener en cuenta cada caso, analizando las necesidades de la empresa o institución identificando la capacidad de cada área y los niveles de conexión. Por eso es fundamental seguir estos objetivos:

- Elegir los recursos materiales
- Conocer las redes
- Conocer los dispositivos
- Pensar siempre en el cliente
- Revisar y evaluar la red

### **2.2.1 Elegir los recursos materiales**

Tener en cuenta las herramientas que se va a necesitar, incluyendo los recursos materiales. Para la administración de redes debe encargarse una persona que cuenta con formación y las certificaciones necesarias y así también ayudara a manejar el software de monitorización de la empresa.

### **2.2.2 Conocer las redes**

Como decía la famosa frase de Francis Bacon: "Scientia est potentia". O lo que es lo mismo: "saber es poder". Para poder administrar se debe conocer los recursos por eso es adecuado contar con mapas de red donde vamos a poder comprender las

capacidades, necesidades y recursos de la red y así facilitar las instalaciones de las redes.

Teniendo en cuenta el tamaño de la empresa la red va a variar, pero debemos conocer su funcionamiento y sus capacidades. Por eso debemos monitorear las redes y conocer al revés al derecho para evitar un gran número de problemas.

### **2.2.3 Conocer los dispositivos**

Es fundamental saber cómo funciona cada equipo que va ser monitorizado y adaptar las herramientas a los dispositivos por eso todos los dispositivos desde un Router, pasando por móviles y ordenadores para que en el caso de que uno de ellos falle saber que ocurre y poder corregir.

### **2.2.4 Pensar siempre en el cliente**

Desarrollar un software acorde a lo que el cliente pida siendo potente e innovador y como administrador de red es necesario mantener una red y apoyar a las partes interesadas. Tener la capacidad de visión global de toda la infraestructura detectando los problemas que contengan y así facilitar el trabajo a los clientes.

### **2.2.5 Revisar y evaluar la red**

Estar preparados para el continuo cambio de las redes que se va presentando día a día y saber mantener un correcto funcionamiento de las redes por eso hay que dedicarle tiempo y trabajo para evaluar el funcionamiento de manera constante y asegurarnos de que todo funcione correctamente. (2017, págs. 1,2)

## **2.3 Administración de red**

Administración de red es el proceso en el cual administra fallos y el rendimiento de la red utilizando herramientas y tecnologías para mantenerse al día con los requisitos empresariales. El principal objetivo de administrar una red es lograr que la red esté libre de errores.

### **2.3.1 Protocolos de administración de red**

Según el sitio web PANDORA FMS menciona que los protocolos de administración son los siguientes:

#### **2.3.1.1 ICMP**

ICMP (Internet Control Message Protocol) tiene la función de validar fallas y calcular ciertas métricas de rendimiento,

Los mensajes ICMP generalmente informan errores en el procesamiento de datagramas, para evitar la regresión infinita de mensajes sobre mensajes no se envían mensajes ICMP sobre mensajes ICMP. Los mensajes solo se envían sobre errores en el manejo del fragmento cero de datagramas fragmentados (el fragmento cero tiene el fragmento de compensación igual cero).

El lector puede leer las especificaciones detalladas del protocolo en el RFC792. El procedimiento que propone ICMP parte de la detección de una condición de error y él envió de mensaje reportando dicha condición.

Los mensajes contemplados por ICMP suelen clasificarse en dos categorías:

- Mensaje de error: utilizados para reportar un error en la transmisión de paquetes.
- Mensajes de control: utilizados para informar sobre el estado de los dispositivos.

Construcción de la cabecera de internet control message protocol, vinculada directamente con la IP y tiene la siguiente forma.

### Figura 3

#### *Funcionamiento ICMP*

	Bit 0–7	Bit 8–15	Bit 16–23	Bit 24–31
0	Tipo	Código	Suma de verificación	
32	Datos sobre la cabecera			

*Nota.* El gráfico representa la construcción de la cabecera del protocolo de mensajes de control de internet. Tomado de (Digital Guide , 2019, pág. 1)

#### 2.3.1.2 SNMP

SNMP (Simple Network Protocol) es un protocolo de capa de aplicación que abarca los ámbitos de fallas, rendimiento y acciones, pretende un esquema para reunir, organizar y comunicar información de administración de los dispositivos conformados en una red.

Este protocolo puede soportar un gran número de componentes de hardware:

Diversidad de dispositivos: enrutadores, switches, access points hasta dispositivos de usuarios finales como impresoras, escáneres y servidores.

Diversidad de marcas: las diferentes marcas de productos tienen que incluir soporte a SNMP.

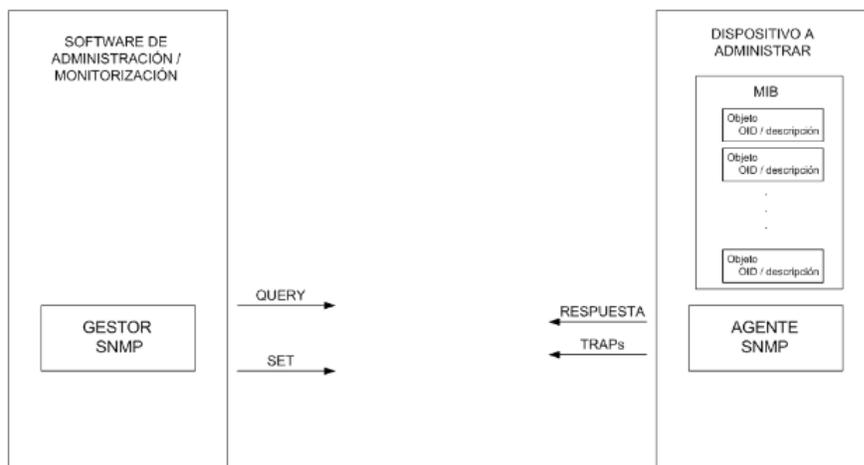
#### **2.3.1.2.1 Arquitectura SNMP**

La arquitectura de SNMP se basa en dos componentes básicos: los Agentes SNMP y los Administradores SNMP.

Los agentes SNMP son piezas de software que se utilizan en los elementos que van a ser administrados. Se encargan de reunir la data sobre el dispositivo en cuestión.

También pueden enviar al administrador SNMP.

Los administradores SNMP o llamados también gestores SNMP son como parte de una herramienta de administración o de monitorización en el que están diseñados para funcionar como consolas en el cual se centraliza toda la data captada y enviada por los agentes SNMP.

**Figura 4***Arquitectura SNMP*

*Nota.* El gráfico representa la arquitectura básica del protocolo SNMP en el cual está constituido por un agente y administrador. Tomado de (PANDORA FMS, 2019, págs. 1,2)

**2.3.1.3 WMI**

WMI (Windows Management Instrumentation) propone un modelo para poder representar, obtener, almacenar y compartir información de administración de hardware y software todo basado en Windows, tanto local como remoto, además está relacionado con la información de administración ya que WMI permite la ejecución de ciertas acciones.

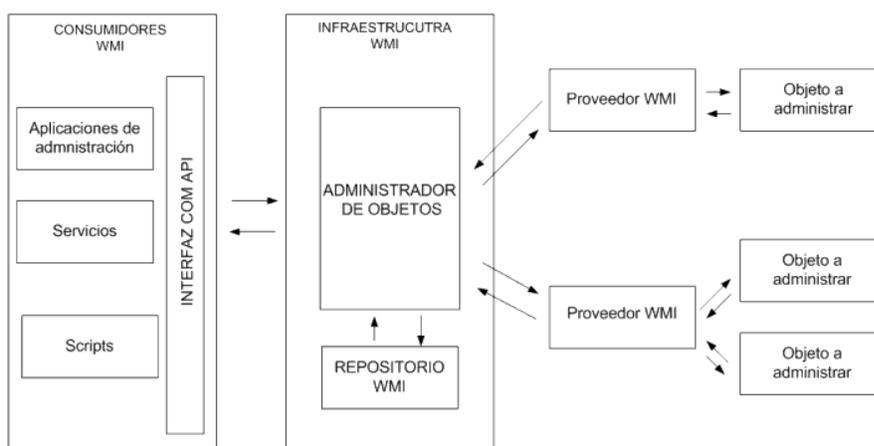
**2.3.1.3.1 Arquitectura de WMI**

WMI está compuesta por tres entidades fundamentales que son:

La arquitectura WMI está compuesta por tres entidades fundamentales. Veamos el siguiente diagrama: proveedor WMI, infraestructura WMI y aplicaciones de administración.

### Figura 5

#### Arquitectura de WMI



*Nota.* El gráfico representa la arquitectura WMI el cual está constituido por tres entidades fundamentales. Tomado de (PANDORA FMS, 2019)

**Proveedores WMI:** es una pieza la cual se encarga de obtener información de administración de uno o más objetos.

**Infraestructura WMI:** es la que actúa como intermediarios entre los proveedores y las herramientas de administración.

**Aplicación de administración:** son las aplicaciones, servicios o scripts la cual utiliza y procesa la información sobre los objetos administrados. (2019, pág. 1)

## 2.4 Monitoreo de red

Monitorizar una red consiste en observar, vigilar, tomar datos y analizar los resultados con el fin de proporcionar información a los administradores el cual permita solucionar problemas eficazmente o mejor aún, anticiparse a ellos. Con la monitorización de la red se toman datos como consumo de recursos, asignación de memoria, estado de memoria, parámetro de rendimiento, estado del dispositivo, rendimiento del sistema, etc. (Cardenas, 2017)

Según el sitio web Interpolados manifiesta que el monitoreo de una red está dividido en 4 fases que son:

- Definición de la información que se monitorea
- Acceso a la información
- Diseño de políticas de la información
- Procesamiento de la información

### 2.4.1 *Los tipos de monitoreo son:*

- Local. - se denomina monitoreo local cuando se realiza un monitoreo de área local dentro de una red interna del usuario.
- Remoto. - cuando se realiza el monitoreo desde un lugar remoto a la red como puede ser desde una estación remota que se encuentre a varios kilómetros de la red.

- Automático. - un dispositivo se encarga de monitorear y comunicar el estado en el que se encuentra.
- Manual. - una persona monitorea personalmente y comunica su estado.

## **2.5 Red corporativa**

Son redes que están compuestas por ordenadores o redes de área local propias de una entidad (empresa, firma, organismo, etc.) y unidades mediante enlaces privados o públicos, que contienen en el ámbito de su red las prestaciones de la red pública y las propias. (Telecomunicaciones, 2016)

### **2.5.1 Protocolo OSPF**

Según el sitio web IBM manifiesta que OSPF (Open Shortest Path First) es un protocolo de ruteo dinámico definido en la RFC 2328 para IPv4 y en la RFC 5340 para IPv6. En una red OSPF los direccionamientos de la misma área genera su propia base de datos de enlace-estado. Cumple la función de recolectar la información necesaria para armar la tabla de ruteo. (IBM, 2015)

#### **2.5.1.1 Características básicas de OSPF**

- ❖ Sistema autónomo
- ❖ Estándar y de especificación abierta
- ❖ Converge rápidamente
- ❖ Envía actualizaciones rápidas
- ❖ Se comunica utilizando multicast

- ❖ Soporta autenticación

### **2.5.1.2 Ventajas de OSPF**

- OSPF recalcula las rutas en poco tiempo cuando la topología de red cambia
- OSPF divide un sistema autónomo en áreas y las mantiene separadas para disminuir el tráfico de direccionamiento de OSPF.
- OSPF proporciona un direccionamiento multivía de coste equivalente.

### **2.5.2 Tunnel VPN**

Según (Ramirez, 2020) manifiesta que un túnel VPN o también llamando VPN es una conexión encriptada entre un equipo y el internet. Su conexión esta encriptada por lo cual nadie a lo largo del tunnel VPN podrá interceptar la información, monitorear ni alterar sus comunicaciones. El cual permite que el ordenador en la red envíe y reciba datos de la red compartida con toda la seguridad y políticas de gestión de una red privada, se lo realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas, cifrado o la combinación de ambos métodos.

Un ejemplo es la posibilidad de conectar dos o más sucursales de una empresa vinculando a internet el cual permite a los miembros de soporte técnico la conexión desde su casa a cualquier lugar ya sea un centro de cómputo o sea teletrabajo.

La conexión de túnel VPN es utilizada en empresas y entornos laborales con el objetivo de asegurar su información y tener unos parámetros de seguridad que evitan varias consecuencias que sean negativas para la empresa. (2020, pág. 1)

### **2.5.2.1 Funcionamiento de túnel de VPN con IPsec con dispositivos Mikrotik**

Esta configuración se utiliza para realizar conexiones entre oficinas remotas con una sede central específica de cualquier tipo de organización. El servidor VPN tiene un vínculo de manera permanente con Internet el cual acepta conexiones vía Internet provenientes de los sitios y establece el túnel VPN. Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor de Internet. (vpnMentor, 2021)

### **2.5.2.2 Mikrotik**

Mikrotik RouterOS es un sistema operativo y software un PC en un Router dedicado además está basado en el núcleo de un sistema operativo Linux el cual implementa una funcionalidad. Proporciona estabilidad, controles y flexibilidad para todo tipo de interfaces de datos y enrutamientos.

RouterOS es una de las mejores opciones que existe en el mercado para administrar redes con requerimientos de una administración avanzada. (Romero, 2018)

**Figura 6***RouterOS Mikrotik*

```

MikroTik 6.47 (stable)
MikroTik Login: admin
Password:

MMM      MMM      KKK
MMMM     MMMM     KKK
MMM MMMM MMM III  KKK KKK RRRRRR  000000  TTT      III  KKK KKK
MMM MM  MMM III  KKKKK  RRR RRR  000 000  TTT      III  KKKKK
MMM     MMM III  KKK KKK RRRRRR  000 000  TTT      III  KKK KKK
MMM     MMM III  KKK KKK RRR RRR  000000  TTT      III  KKK KKK

MikroTik RouterOS 6.47 (c) 1999-2020      http://www.mikrotik.com/

o you want to see the software license? [Y/n]: y

```

*Nota.* El gráfico representa el interfaz de Mikrotik RouterOS 6.47.

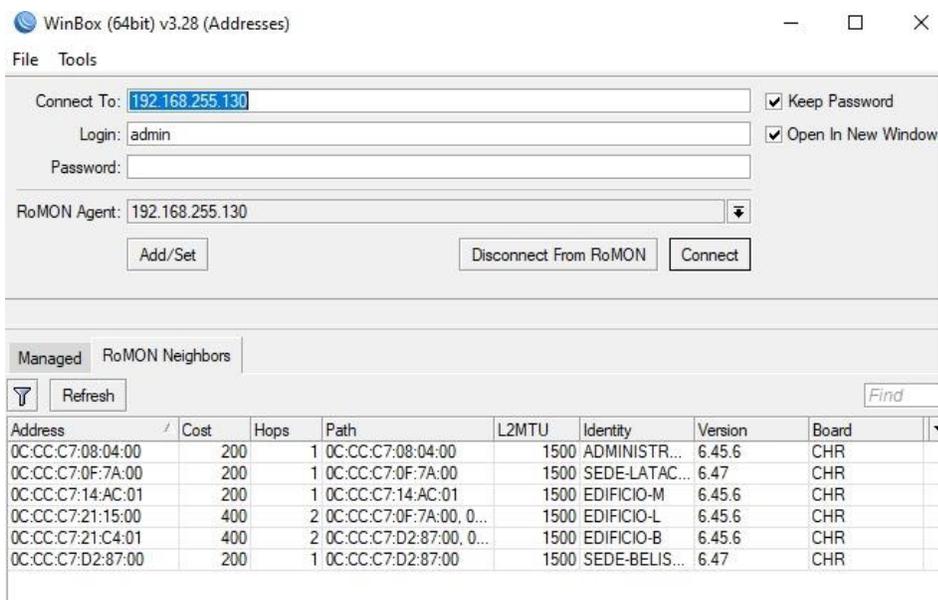
### 2.5.2.3 Herramienta Romon

Todos los dispositivos habilitados con Romon establecen un protocolo de reenvío de datos y generación de pared de capa MAC independiente por cada dispositivo. Romon funciona de manera independiente de la configuración de reenvío, su comunicación se basa en el ID de Romon que toma de la primera dirección MAC. Solo permite interfaces inalámbricas y similares a Ethernet, Romon es un protocolo patentado de Mikrotik.

(WirelessNetware, 2015)

## Figura 7

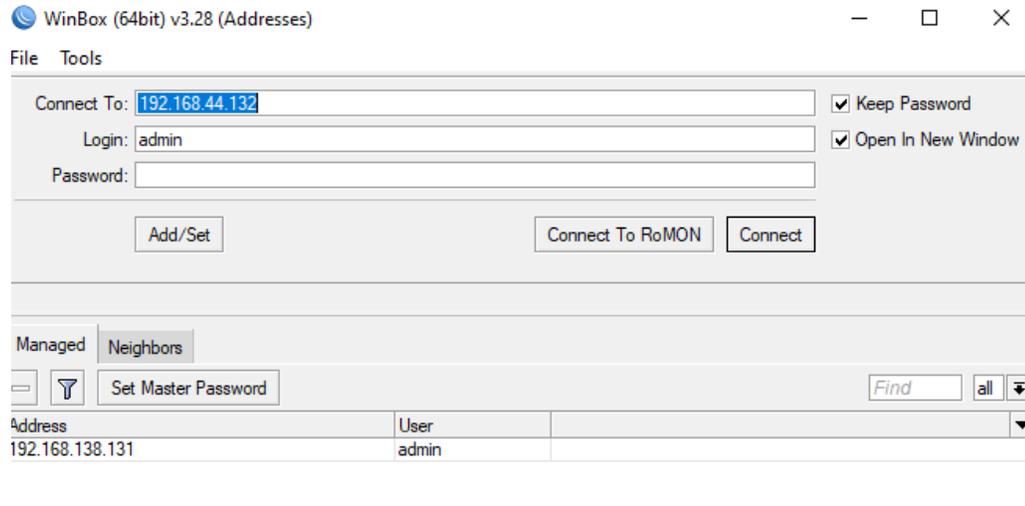
### Romon



*Nota.* El gráfico representa de Romon y las conexiones de todos los routers por Romon.

#### 2.5.2.4 Winbox

Según (Anrrango, 2020) Winbox es una aplicación que permite administrar Mikrotik RouterOS usando una interfaz gráfica. Tiene una tecnología para realizar conexión basada en el sistema operativo RouterOS. Permite a los usuarios realizar conexiones vía FTP, telnet y SSH el cual incluye crear aplicaciones personalizadas para monitorizar y administrar.

**Figura 8***Winbox*

*Nota.* El gráfico representa la interfaz de la herramienta de red Winbox.

## 2.6 Simulador de red

Es un software que permite al usuario diseñar un sistema de redes entre computadoras, switches, routers, impresoras, teléfonos, etc. Esto se realiza en un monitor haciendo conexiones mediante cables entre los dispositivos para luego realizar una prueba virtual de compatibilidad de conexión. (Blogspot, 2012)

### 2.6.1 GNS3

GNS3 es un simulador de red que permite emular diferentes topologías de red más o menos complejas y ejecutar simulaciones para particularizadas (Rejón, 2019).

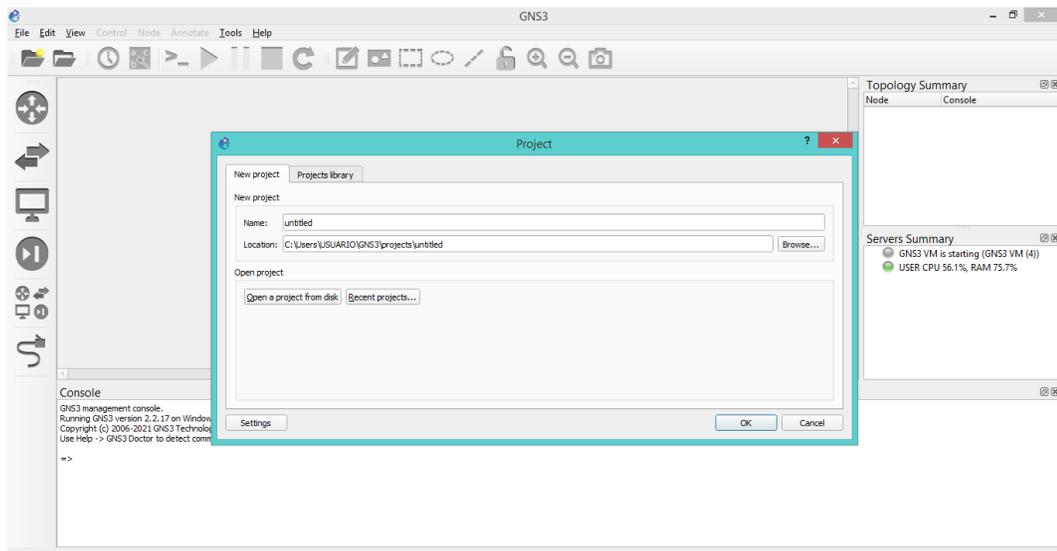
#### 2.6.1.1 Funciones de GNS3

- ✓ Simula redes en tiempo real para pruebas previstas a la implementación sin necesidad de hardware de red.

- ✓ En un entorno virtual prueba más de 20 proveedores de redes diferentes, sin riesgos: ejecuta y prueba rápido varios proveedores de hardware.
- ✓ Crea mapas de red dinámicos para la solución de problemas y pruebas de concepto.
- ✓ GNS3 se conecta a cualquier red real: aprovecha su hardware existente y amplía su laboratorio actual conectado sus topologías GNS3 directamente a él.
- ✓ Topologías y laboratorios personalizados dentro de GNS3 para capacitación en certificados de redes.

**Figura 9**

*Interfaz de GNS3*



*Nota.* El gráfico representa la interfaz del simulador de redes GNS3

## 2.7 Máquinas virtuales

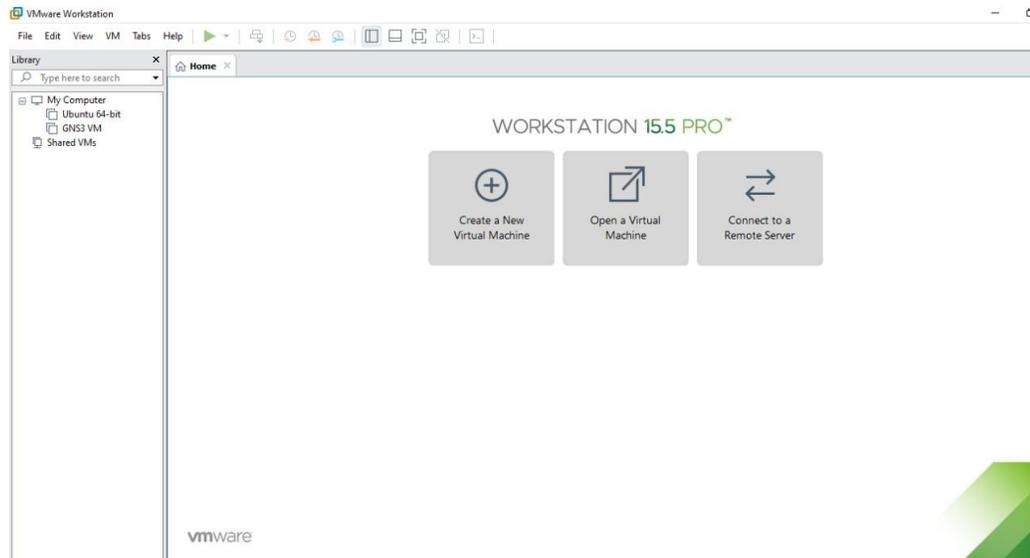
Una máquina virtual es aquel que funciona como un sistema informático virtual la cual tiene su propia CPU, memoria, interfaz de red y almacenamiento. Las máquinas

virtuales permiten que se ejecute diferentes sistemas operativos a la misma vez en una computadora, como una distribución de Linux. Cada sistema operativo funciona de la misma manera.

La tecnología de virtualización es aquella tecnología que le permite compartir un sistema con muchos entornos virtuales. Los recursos se dividen según las necesidades, desde el entorno físico hasta las VM. (Red had , 2021)

## **2.8 VMware**

VMware es una herramienta muy utilizada al momento de realizar una virtualización. El cual permite a los usuarios ejecutar máquinas virtuales. Cuando el simulador se ejecuta presenta características idénticas a las de una máquina física. Permite configurar varias máquinas virtuales en una sola máquina física al igual usarlas simultáneamente junto con las máquinas, en cada máquina virtual se puede ejecutar cualquier sistema operativo. (WebsDirect, 2016)

**Figura 10***VMWare Workstation*

*Nota.* El gráfico representa la interfaz de la herramienta utilizada para realizar virtualizaciones VMware Workstation 15.5 Pro.

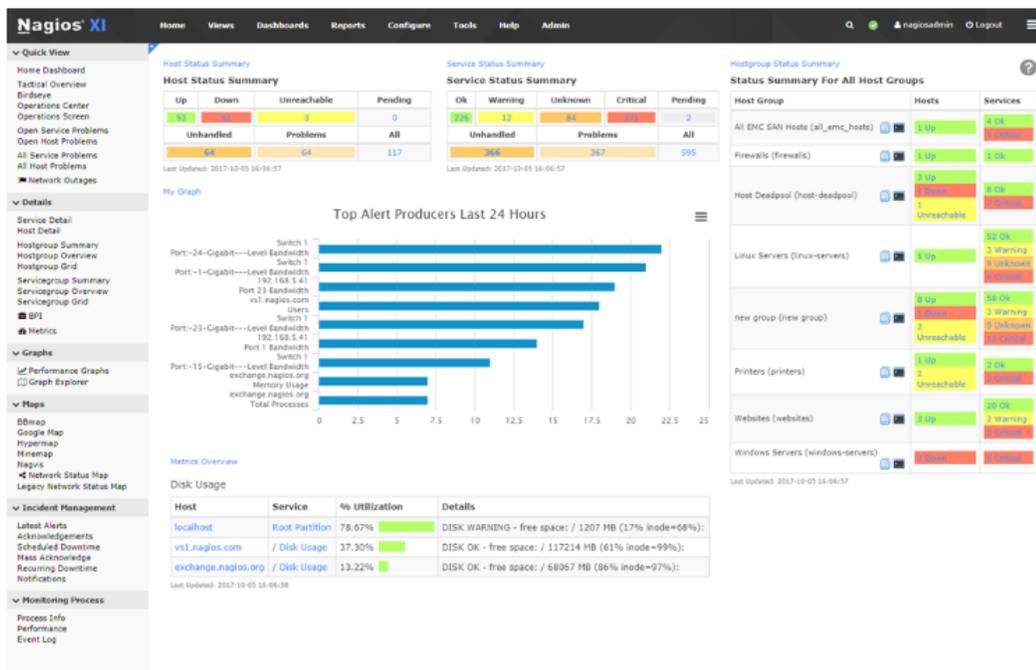
## 2.9 Herramientas de monitoreo de una red

### 2.9.1 Nagios

Nagios es una herramienta de monitorización de redes y de código abierto que controla los equipos y servicios (software), notificando el estado de los mismos, su característica principal es la monitorización de servicios de red (SMTP, POP3, HTTP, SNMP), en la monitorización de los recursos se puede ver (carga de procesador, uso de los discos, memoria, estado de los puertos). (Robledo, 2021)

Figura 11

Interfaz principal de Nagios



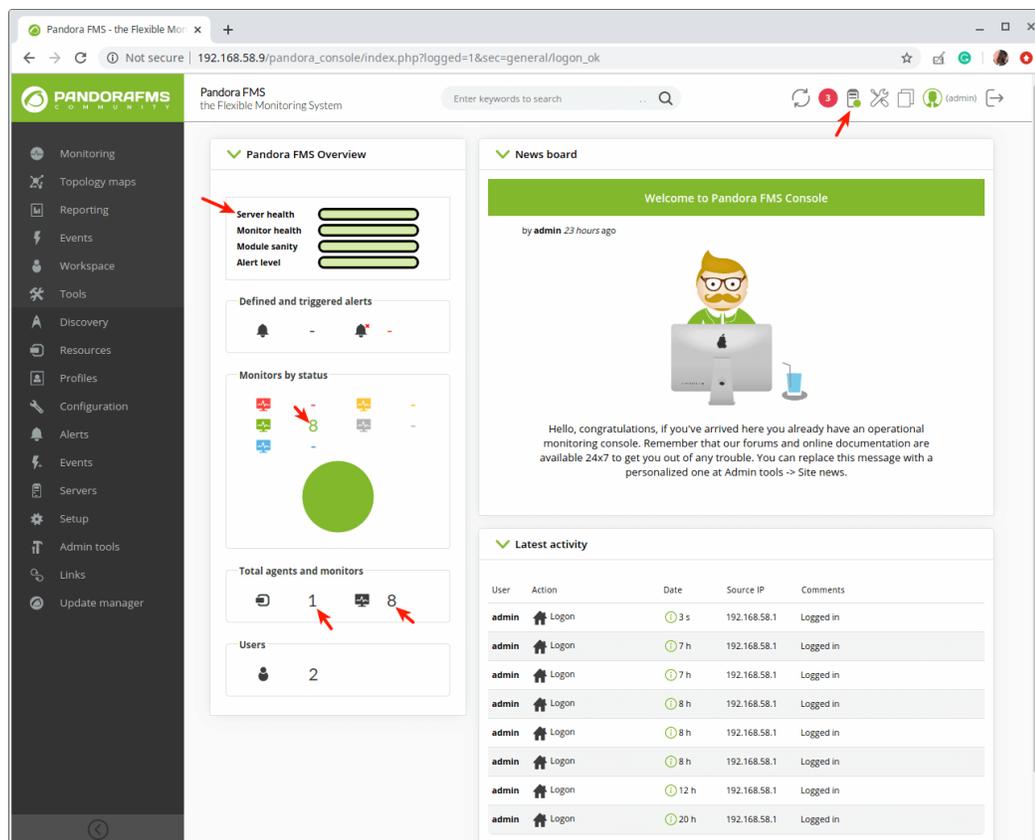
Nota. El gráfico representa la interfaz principal de Nagios. Tomado de (Open IT Networks, 2021)

## 2.9.2 Pandora FMS

Es una herramienta de monitorización de red que permite a los usuarios monitorizar desde 100 dispositivos hasta varias cantidades de miles, monitoreando todos los componentes de red desde una misma consola. Pandora FMS maneja entornos complejos y soluciones de redes remotas. (PANDORAFMS, 2020)

**Figura 12**

*Interfaz principal de Pandora FMS*



*Nota.* El gráfico representa la interfaz de la herramienta de monitoreo Pandora FMS.

Tomado de (Artica, 2021, pág. 1)

### 2.9.3 Zabbix

Trabajo investigado por la página programador clic manifiesta que Zabbix: es un software diseñado para monitorear y administrar mediante código abierto redes, sistemas operativos, aplicaciones y otros hardware de red. (Programerclick, 2020)

### **2.9.3.1 Servidor Zabbix**

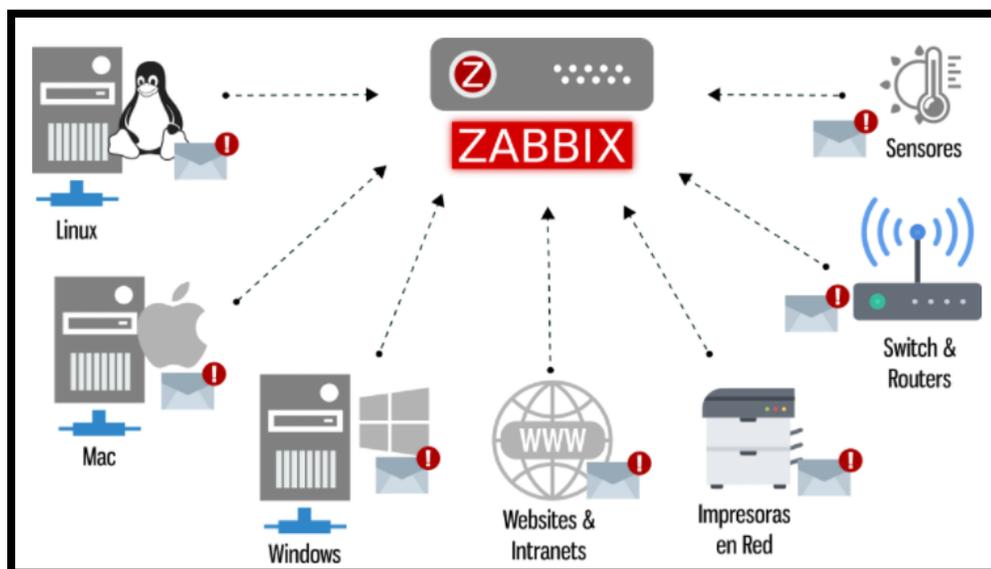
Es una herramienta el cual gestiona la red para la supervisión adecuada de la disponibilidad y el rendimiento de los dispositivos de red. (Petrucci, 2018)

### **2.9.3.2 Funcionamiento de Zabbix**

Zabbix se instala en un servidor Linux en donde se encargará de monitorear y recolectar información. Además, el servidor tiene una interfaz Web la cual se presenta de forma gráfica toda la información que va ir recolectando de todos los dispositivos que vayan a ser administrados por Zabbix. Cuenta con agentes para sistemas operativo como Linux, Mac y Windows los cuales se instalan en los servidores o sitios de trabajo que vayan a ser monitorizados. También esta permite observar el estado de impresoras, routers, switches, sensores de temperatura y humedad entre otros. (Hernandez J. , 2020)

**Figura 13**

*Funcionamiento de Zabbix*



*Nota.* El gráfico representa el funcionamiento generalizado de Zabbix el cual le permite monitorear. Tomado de Weebly (Hernandez J. , 2020, pág. 1)

### 2.9.3.3 Componentes de Zabbix

Zabbix consta de varios softwares principales, los cuales se describen a continuación.

#### 2.9.3.3.1 Servidor Zabbix

El servidor es el componente principal de Zabbix ya que el servidor puede comprobar de forma remota los servicios en red (como servidores web y servidores de correo) mediante comprobaciones de servicio sencillas, además los agentes informaran toda la información y las estadísticas de disponibilidad e integridad al servidor lo cual esto hace que el servidor sea un componente central ya que almacena todos los datos de configuración, estadísticos y operarios. Es una entidad del software Zabbix la que

alertara activamente a los administradores cuando se produzca problemas en cualquiera de los sistemas monitoreados. Es decir, es el componente central responsable de recibir la información del informe enviado por el agente, toda la configuración, las estadísticas de los datos y las operaciones de datos son organizadas por el servidor. (Hernandez J. , 2020)

#### **2.9.3.3.2 Agente Zabbix**

El agente Zabbix es el que recopila información operativa del sistema en el que se está ejecutando y reportara estos datos al servidor para su respectivo procesamiento. En caso de errores (como un disco duro que se ejecuta lleno un proceso de servicios bloqueado), el agente comunicara una alerta de la máquina en particular que está en error.

Los Agentes Zabbix son extremadamente eficientes debido al uso de llamadas nativa del sistema para recopilar información estadística.

Es decir, es implementado en el host monitoreado (cliente), es responsable de recopilar los datos del host monitoreado, como CPU, memoria, base de datos y otros datos y luego enviarlos al servidor. (Hernandez J. , 2020)

#### **2.9.3.3.3 Interfaz web**

Con el fin de permitir un fácil acceso a los datos de monitoreo y la configuración de Zabbix desde cualquier lugar y desde cualquier plataforma, se proporciona la interfaz basada en web. La interfaz es una parte del servidor, y normalmente (pero no necesariamente) se ejecuta en la misma máquina física que la que se ejecuta el servidor Zabbix. (Hernandez J. , 2020)

### 2.9.3.4 Funcionamiento de monitoreo en Zabbix

Figura 14

Monitoreo en Zabbix



*Nota.* El gráfico representa el funcionamiento de monitoreo en Zabbix. Tomado de (Hernandez J. E., Cosysco, 2021)

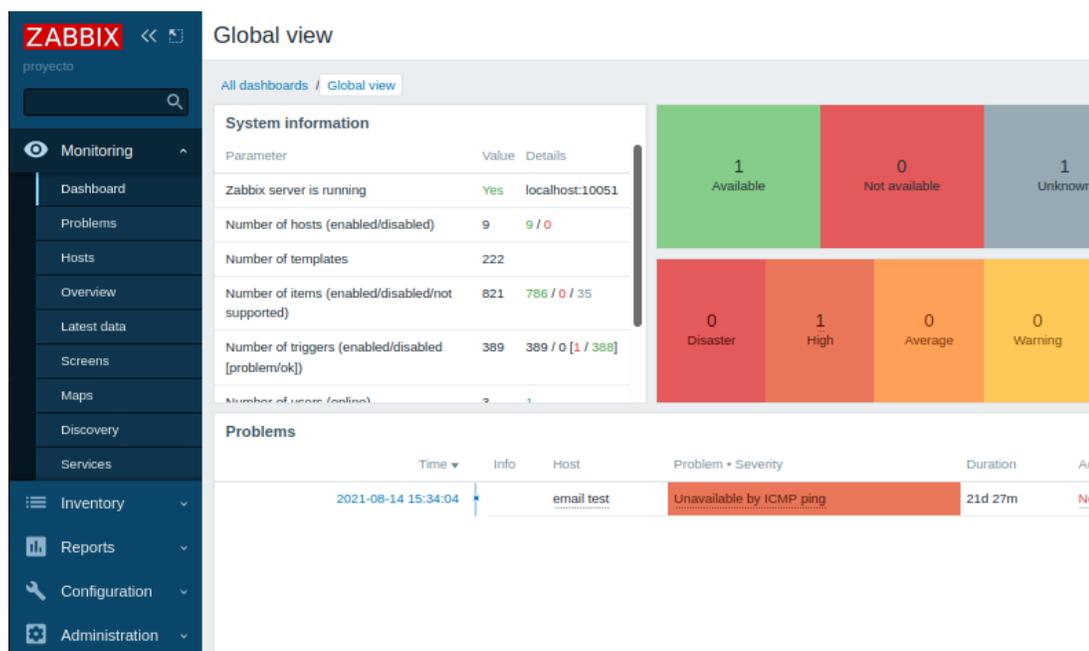
- 1) El agente Zabbix en el servidor o estación de trabajo a monitorear, el cual debe estar configurado para reportar al servidor recolector Zabbix de la red. En el caso de monitorear un switch, routers, impresoras o sensores de temperatura no se utiliza el agente.
- 2) En el servidor recolector Zabbix con la herramienta de administración web Frontend, se debe registrar los equipos y dispositivos que se desee monitorear.

- 3) El equipo que va ser monitoreado tendrá que ser registrado y recibirá el nombre de host.
- 4) Los hosts están compuestos por ítems los cuales son módulos que recogen datos del host y en el caso de hardware que obtiene del dispositivo.
- 5) Los ítems utilizan Key que son parámetros del servidor el cual nos permite especificar qué tipo de información se solicitara al agente Zabbix.
- 6) Los triggers en Zabbix son módulos que se crean a uno o múltiples ítems para analizar o comparar la información recolectada por los ítems con las condiciones que se vaya definiendo según lo que este monitorizándose.
- 7) Los triggers crean eventos que se reflejan en la herramienta de administración web donde muestra de forma gráfica y a través de iconos la situación del entorno.
- 8) Zabbix captura todas las situaciones y eventos dependiendo de su entorno puede enviar alertas vía correo electrónico o SM. (Cosysco, 2021, pág. 2)

## 2.10 Interfaz web de Zabbix

### Figura 15

*Panel de control del servidor web Zabbix*



*Nota.* El gráfico representa la interfaz principal del servidor web Zabbix con el panel de control.

Según el sitio web Zabbix manifiesta que: en la interfaz de Zabbix se puede encontrar los siguientes componentes:

### 2.10.1 Panel de control

En el panel de control en la parte izquierda y en la derecha el dashboard que está diseñado para mostrar los resúmenes de toda la información importante del sistema que se ha configurado. Además, se puede editar, compartir, crear, eliminar,

clonar el dashboard a nuestra preferencia donde también muestra los problemas que van presentando.

### **2.10.2 Problems**

En problemas es donde se muestra todos los errores que se van presentando en todo el sistema el cual se puede crear manualmente o automáticamente cuando estamos creando un host.

### **2.10.3 Host**

En los hosts se puede ver una lista completa de host creados donde detalla la información de la interfaz, también se puede ver el estado (habilitado, deshabilitado), los nombres y los últimos datos.

### **2.10.4 Screens**

En los screens de Zabbix los elementos como los gráficos tanto de las interfaces, CPU, memoria se los puede agrupar para mostrarlos en una sola pantalla resumidas. Un screen se lo crea básicamente como una tabla el cual tiene filas y columnas llamadas fresh.

### **2.10.5 Maps**

En Maps se puede visualizar los datos recopilados en Zabbix e integrar la topología de la red que se está monitoreando además se podrá integrar parámetros como el nombre, la IP, memoria y el disco.

### **2.10.6 Latest data**

Latest data muestra los datos más recientes del host supervisados, muestra el nombre del dispositivo, hora de última comprobación, último valor, cantidad de cambios, etiquetas y un enlace que se puede ver su respectivo gráfico.

### **2.10.7 Graphs**

Graphs son los gráficos que podemos crear o agregarlos a un template. Estos también se generan automáticamente cuando se crea un host donde podemos ver los gráficos de todas las interfaces, CPU, memoria, disco.

### **2.10.8 Ítems**

Los ítems son los encargados de recolectar la información de los equipos que van a ser monitoreados, la información recolectada puede ser el uso de CPU, disponibilidad, porcentajes de ancho de banda, etc.

### **2.10.9 Triggers**

Los triggers son expresiones que evalúan los datos recopilados por los ítems y representan el estado actual del sistema. Son condiciones que si sobrepasan el límite en zabbix será considerado como un problema.

### **2.10.10 Media types**

Media types es el medio de comunicación de los canales donde van a ser enviados las notificaciones y alertas de Zabbix, esto tipos de medio son correo electrónico, mensajes de texto, alertscripts personalizados y webhook. (2021, pág. 5)

## Capítulo III

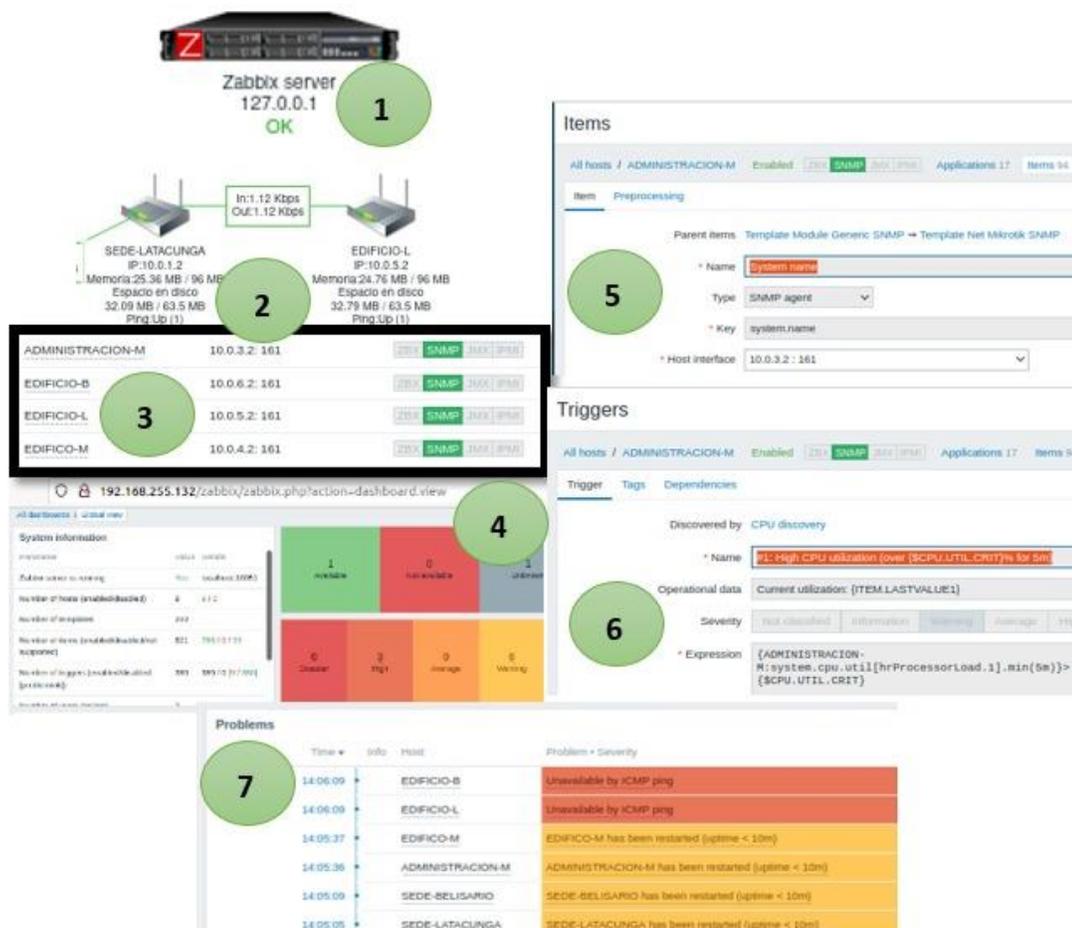
### 3 Desarrollo

#### 3.1 Servidor Zabbix

En la investigación del servidor Zabbix se comprendió que sirve para monitorear y administrar equipos o dispositivos de red, servidores, sistemas operativos donde puede ser añadido como Host activando el protocolo SNMP tanto en el servidor como en el dispositivo. Para llevar a cabo su implementación se verifico lo componentes a instalarse como el agente Zabbix, servidor Zabbix, interfaz web y la base de datos que son necesarios para su funcionamiento.

Figura 16

## Funcionamiento de Zabbix



*Nota.* El gráfico representa las funciones que hace cada componente para el monitoreo de un Router.

- 1) En el Servidor Zabbix se registran todos los Routers añadidos manualmente para ser monitoreados
- 2) Router es el dispositivo de red que será añadido como host al servidor
- 3) El agente SNMP se activa en el Router y en el servidor como Host que permitirá la administración.

- 4) La interfaz web es el panel de control de Zabbix donde muestra la información del sistema
- 5) Los ítems recolectan la información del Router como es la memoria, el tamaño del disco y la carga del CPU, el cual utiliza keys que son los parámetros que tiene el servidor.
- 6) Los triggers son los datos recopilados de los ítems el cual presenta el estado del sistema, donde se condiciona los parámetros creados en los ítems.
- 7) Las notificaciones son los problemas que se van presentando por las condiciones establecidas en los triggers, el cual se mostrara en el Dashboard.

### **3.2 Implementación de la red corporativa**

Para implementar la red corporativa se instaló el software VMware donde se utilizó el complemento GNS3/VM como servidor externo de todos los equipos de la red y el software GNS3 donde se simuló la red, se descargó, se importó el RouterOS Mikrotik y la imagen svg al software para comenzar con la realización de la red corporativa con los tres sitios remotos.

#### **3.2.1 Requisitos de instalación de VMware Workstation 15.5.1 Pro**

En la máquina física se procedió a instalar VMware Workstation 15.5.1 Pro con todas las configuraciones necesarias para realizar la instalación de nuestra máquina virtual.

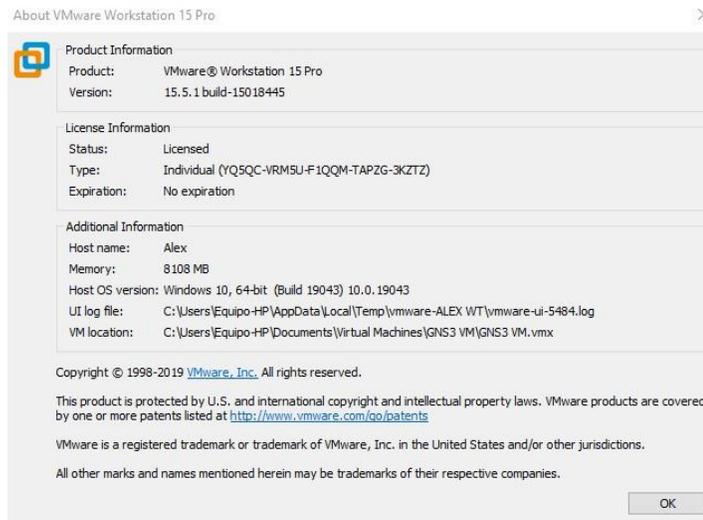
Requisitos del sistema:

- ✓ Memoria RAM: se requiere 2GB de RAM
- ✓ Disco Duro: 1,5 GB de espacio libre

- ✓ Procesador: Intel Pentium a 1,3GHz o superior
- ✓ Sistema operativo: Windows 8 o superior x64bits

## Figura 17

### *Características de instalación VMware Workstation 15.5.1 Pro*

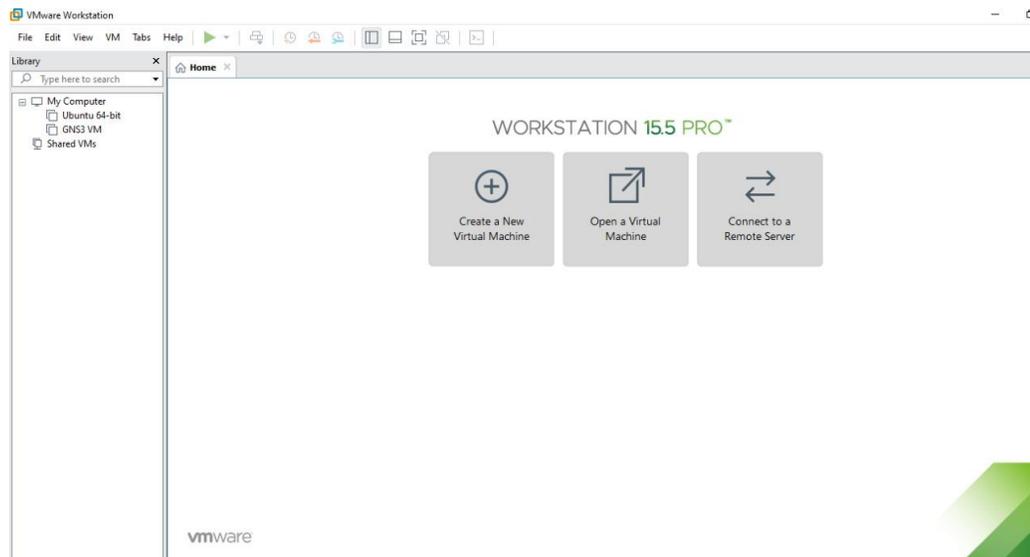


*Nota.* El gráfico representa la interfaz previa del producto de instalación VMware Workstation 15 Pro implementada en la máquina física.

### 3.2.1.1 Visualización de la interfaz VMware instalado

**Figura 18**

*Interfaz principal VMware*



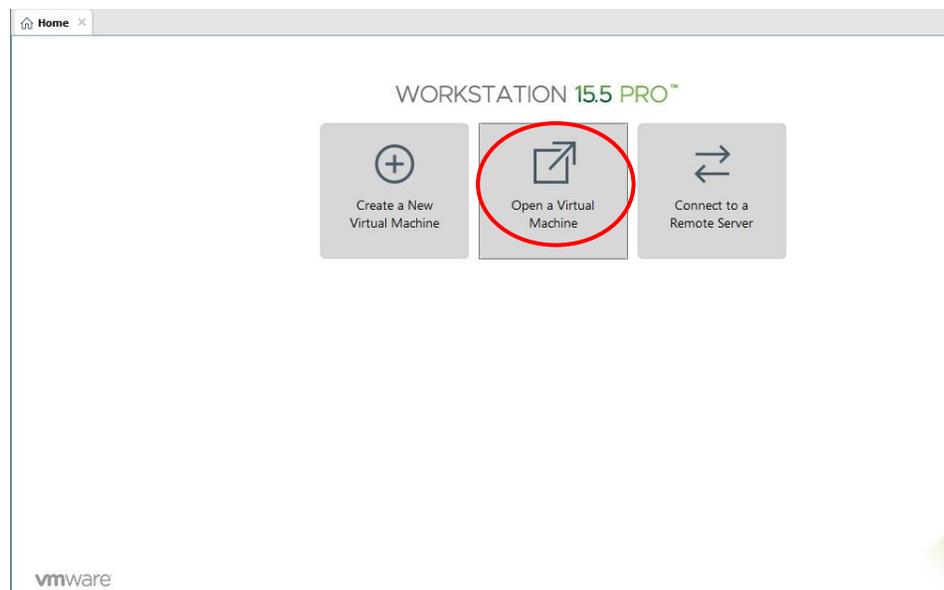
*Nota.* El gráfico representa la interfaz del menú principal de VMware Workstation 15.5 Pro.

### 3.2.1.2 Instalación GNS3/VMware en VMware Workstation

Una vez descargado el complemento GNS3/VM en el software VMware abrir el complemento de conexión con gns3 para encender como máquina virtual.

## Figura 19

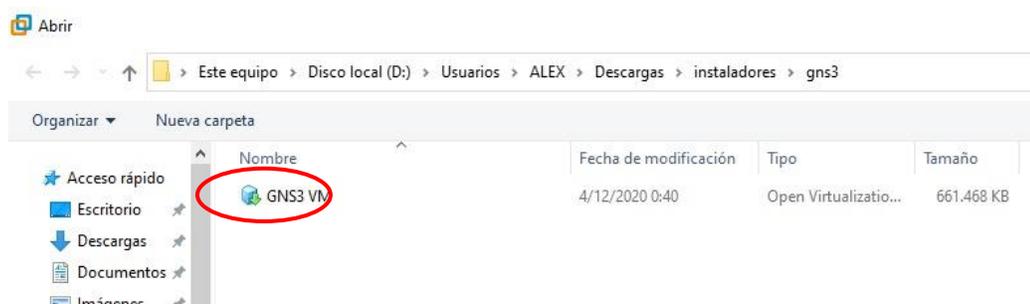
### Instalación GNS3/VM



*Nota.* El gráfico representa la interfaz previa de instalación de la máquina virtual GNS3/VM.

## Figura 20

### Selección de GNS3VM del escritorio



*Nota.* El gráfico representa la interfaz del complemento GNS3/ VM para la instalación en la dirección de descargas.

### **3.2.2 GNS3**

Se utilizó el software GNS3 simulación de dispositivos de red ya que cumple con las funciones que se requiere para simular una red corporativa el cual se debe contar con requisitos mínimos en la computadora.

#### **3.2.2.1 Requisitos mínimos GNS3**

- Sistema operativo: Windows 7 o superior
- Procesador: 2 o más núcleos
- Virtualización: habilitar desde el BIOS del computador
- Memoria: 4GB de RAM o superior
- Disco duro: 1GB de espacio libre
- Almacenamiento adicional para sistema operativo virtual

#### **3.2.2.2 Instalación GNS3**

Una vez descargado el archivo ejecutable de GNS3 de la página oficial, acceder a descargas y ejecutar el instalador para comenzar con la instalación el cual abra la interfaz de bienvenida del inicio de instalación.

## Figura 21

### Interfaz de bienvenida GNS3



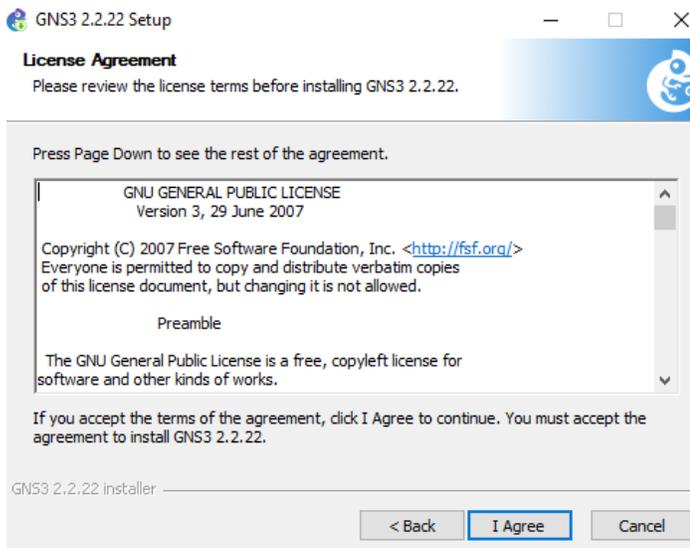
*Nota.* El gráfico representa el Setup de inicio de instalación de gns3 para iniciar la instalación.

### 3.2.2.3 Aceptación de licencia

Posteriormente aparecerá la pantalla como se muestra en la figura 22 lo cual hace referencia al acuerdo de licencia para poder continuar con la instalación de gns3.

## Figura 22

### Contrato de licencia



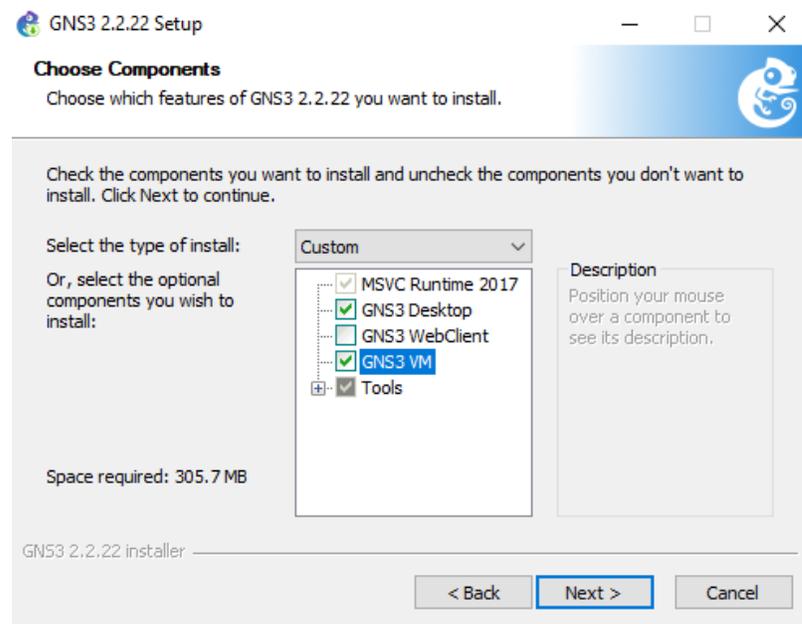
*Nota.* El gráfico representa la aceptación de licencia para continuar con la instalación de gns3.

#### 3.2.2.4 Selección de componentes

Se solicitará instalar los componentes en el simulador para su funcionamiento, en este paso se recomienda dejarlo todo por defecto para que no ocurra ningún problema y el software funcione de manera correcta.

## Figura 23

### Elegir componentes



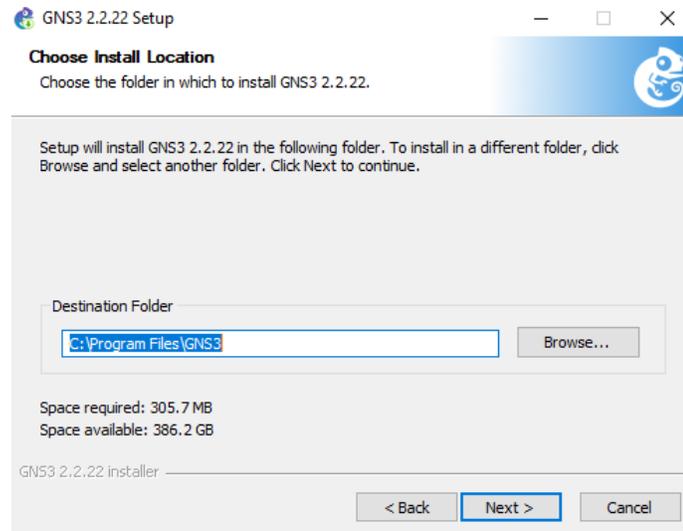
*Nota.* El gráfico representa la selección de componentes para el funcionamiento de gns3

### 3.2.2.5 Selección del destino de instalación

Establecer la carpeta de destino de la instalación como en este caso se lo dejo por defecto o si desea crear una carpeta donde se vaya a guardar todos los proyectos como se muestra en la figura 24.

## Figura 24

### *Ubicación de instalación*



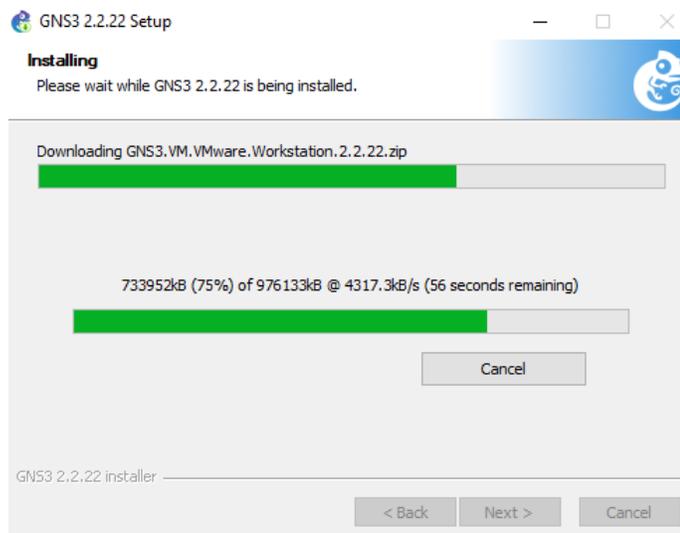
*Nota.* El gráfico representa el destino de instalación de gns3

### **3.2.2.6 Proceso de instalación de aplicaciones**

Se procederá a instalar todas las aplicaciones necesarias para el buen funcionamiento del programa además se complementará la copia de archivos para que sea una instalación exitosa.

## Figura 25

### Final de Instalación



*Nota.* El gráfico representa la finalización de copia de archivos y la descarga de archivos.

### 3.2.2.7 Finalización de instalación

Para finalizar la instalación se solicitará si desea marcar la opción para abrir el software GNS3 o finalizar la instalación lo cual estará listo para usar y comenzar con la red corporativa.

**Figura 26**

*Instalación completada*



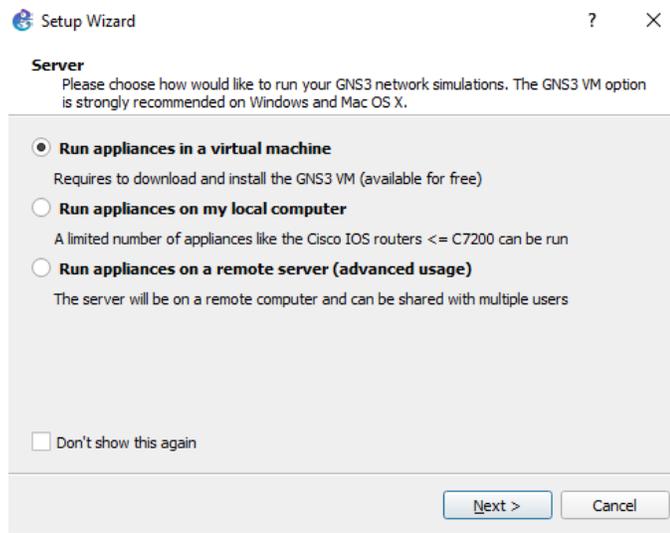
*Nota.* El gráfico representa la finalización de la instalación de gns3 e iniciar GNS3.

**3.2.2.8 Asistente de configuración**

Luego de la instalación se procedió a configurar la interfaz gráfica mediante setup wizard para poder colocar imágenes IOS además nos recomienda utilizar el GNS3/VM por el momento dar clic en cancel, ya que más adelante se mostrará como añadir el complemento.

## Figura 27

### Setup Wizard



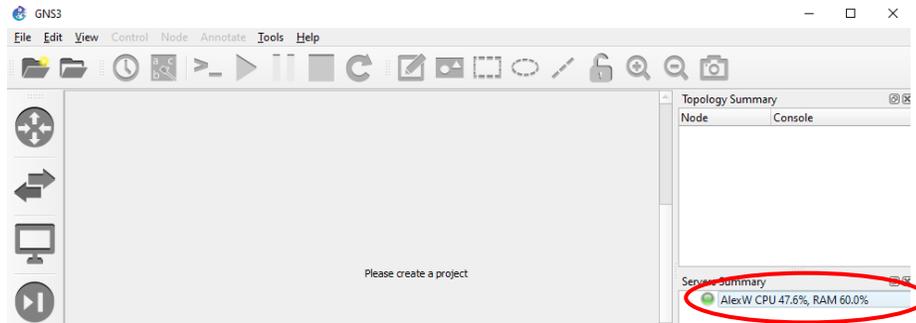
*Nota.* El gráfico representa la configuración de la interfaz gráfica mediante setup wizard

### 3.2.2.9 Visualización de la interfaz GNS3

Una vez abierto el software se puede observar que se utiliza como servidor de GNS3 los recursos de la máquina física, el cual los equipos de red no consumirán el procesador para realizar las simulaciones. GNS3/VM servirá como servidor externo para no sobrecargar la máquina física.

## Figura 28

### Interfaz de GNS3



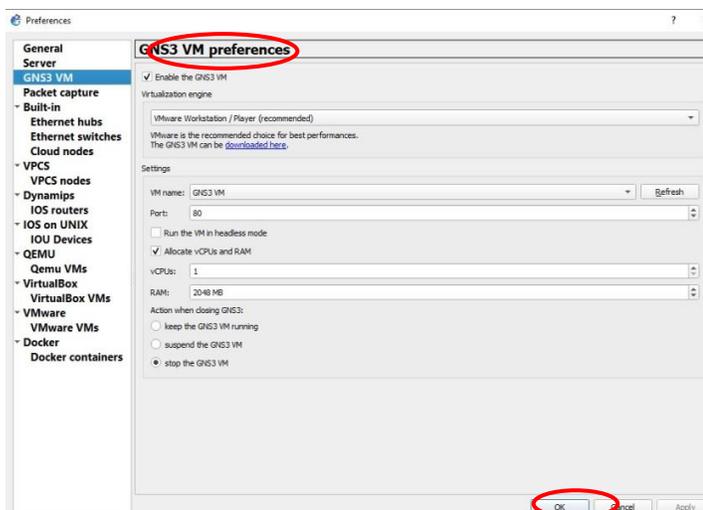
*Nota.* El gráfico representa la interfaz de GNS3 y la utilización del servidor de la máquina física en GNS3.

#### 3.2.2.10 Configuración general de GNS3/VM

En configuración general seleccionar GNS3VM y en settings VM name buscar el GNS3/VM que se instaló en VMware y habilitar el GNS3/VM y el resto dejar las configuraciones por defecto y dar clic en aplicar y aceptar para añadir.

**Figura 29**

*Preferencias de GNS3/VM*



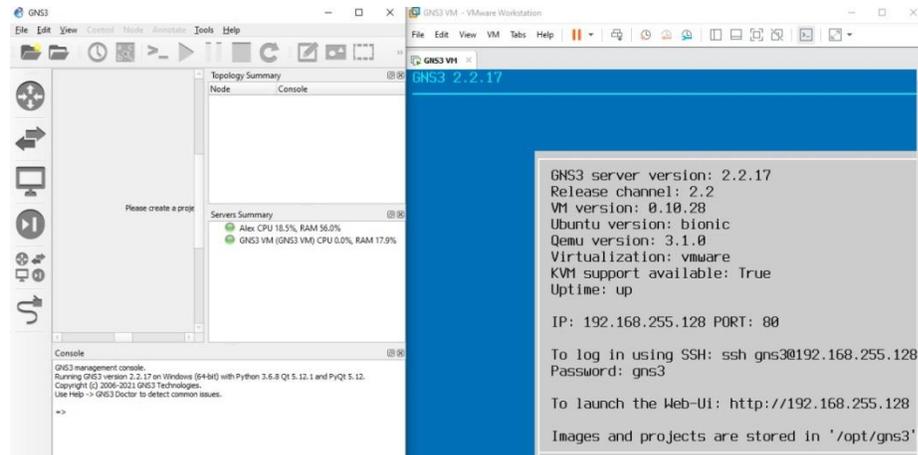
*Nota.* El gráfico representa la configuración del GNS3VM como servidor externo

### 3.2.2.11 Verificación de conexión de GNS3/VM

Una vez añadido GNS3/VM se encenderá y abrirá automáticamente el complemento habilitado y también en GNS3 se añadirá a servers summary y se encenderá de color verde mostrando que hay conexión entre gns3 y gns3/VMware.

**Figura 30**

*Interfaces de conexión entre GNS3 y VMware*



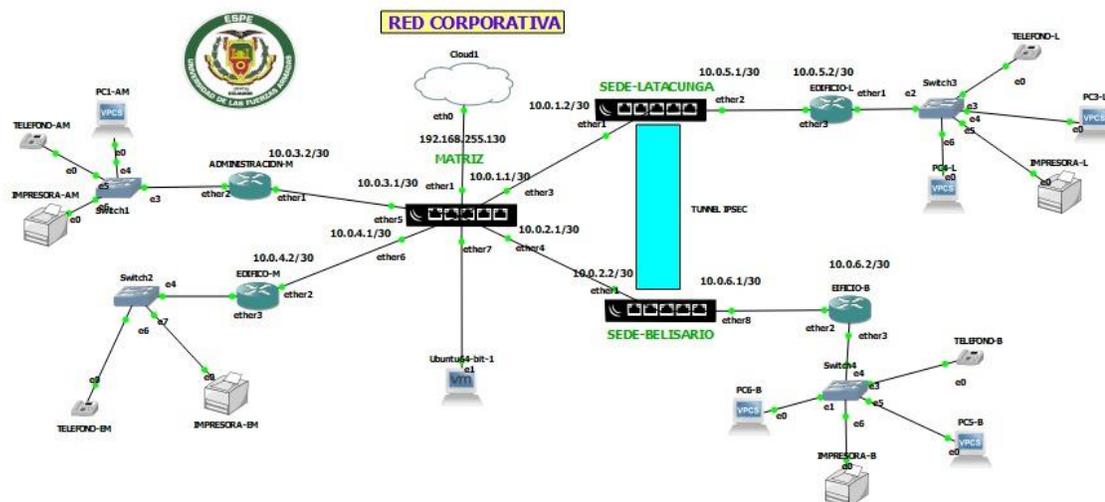
*Nota.* El gráfico representa la conexión del servidor externo GNS3/VM a GNS3

### **3.2.3 Creación de la red corporativa**

Se creó la red corporativa donde se añadió la nube, Routers y dispositivos de red, lo cual en el RouterOS Mikrotik matriz se accedió a la consola para verificar la dirección ip de red **192.168.255.130** con el cual se va a trabajar para comenzar hacer la tabla de direccionamiento.

Figura 31

Topología de red



Nota. El gráfico representa la estructura de la red corporativa con tres sitios remotos.

Figura 32

IP del RouterOS Mikrotik

```
[admin@MikroTik] > ip address
[admin@MikroTik] /ip address> print
Flags: X - disabled, I - invalid, D - dynamic
# ADDRESS NETWORK INTERFACE
0 D 192.168.255.130/24 192.168.255.0 ether1
```

Nota. El gráfico representa la verificación de la ip para trabajar en winbox.

**Tabla 1***Direccionamiento IP*

<b>Nombre</b>	<b>IP</b>	<b>Mascara</b>	<b>Gateway</b>	<b>Interfaces</b>
<b>Router-Matriz</b>	192.168.255.130	255.255.255.0	192.168.255.0	Ether1
	10.0.1.1	255.255.255.252	10.0.1.0	Ether3
	10.0.2.1	255.255.255.252	10.0.2.0	Ether4
	10.0.3.1	255.255.255.252	10.0.3.0	Ether5
	10.0.4.1	255.255.255.252	10.0.4.0	Ether6
	10.0.5.1	255.255.255.252	10.0.5.0	Ether2
	10.0.6.1	255.255.255.252	10.0.6.0	Ether8
	10.0.7.1	255.255.255.252	10.0.7.0	Ether7
<b>Router-Administración-M</b>	10.0.3.2	255.255.255.252	10.0.3.0	Ether1
	192.168.90.1	255.255.255.0	192.168.90.0	Ether2
	192.168.91.1	255.255.255.0	192.168.91.0	Ether3
<b>Router-Edificio-M</b>	10.0.4.2	255.255.255.252	10.0.4.0	Ether2
	192.168.100.1	255.255.255.0	192.168.100.0	Ether3
	192.168.101.1	255.255.255.0	192.168.101.0	Ether4
<b>Router-Sede-Latacunga</b>	10.0.1.2	255.255.255.252	10.0.2.0	Ether1
	10.0.5.1	255.255.255.252	10.0.5.0	Ether2
<b>Router-Edificio-L</b>	10.0.5.2	255.255.255.252	10.0.5.0	Ether3
	192.168.150.1	255.255.255.0	192.168.150.0	Ether1
	192.168.151.1	255.255.255.0	192.168.151.0	Ether2
<b>Router-Sede-Belisario</b>	10.0.2.2	255.255.255.252	10.0.2.0	Ether1
	10.0.6.1	255.255.255.252	10.0.6.0	Ether3
<b>Router-Edificio-B</b>	10.0.6.2	255.255.255.252	10.0.6.0	Ether2
	192.168.200.1	255.55.255.0	192.168.200.0	Ether3
	192.168.201.1	255.255.255.0	192.168.201.0	Ether4
<b>Teléfono-A</b>	192.168.90.10	255.255.255.0	192.168.90.1	Ether1
<b>Impresora-A</b>	192.168.90.11	255.255.255.0	192.168.90.1	Ether4
<b>PC1-A</b>	192.168.90.12	255.255.255.0	192.168.90.1	Ether5
<b>PC2-E</b>	192.168.100.10	255.255.255.0	192.168.100.1	Ether1
<b>Teléfono-E</b>	192.168.100.11	255.255.255.0	192.168.100.1	Ether2
<b>Impresora-E</b>	192.168.100.12	255.255.255.0	192.168.100.1	Ether3
<b>Impresora-L</b>	192.168.150.10	255.255.255.0	192.168.150.1	Ether6
<b>PC3-L</b>	192.168.150.11	255.255.255.0	192.168.150.1	Ether5
<b>PC4-L</b>	192.168.150.12	255.255.255.0	192.168.150.1	Ether4
<b>Teléfono-L</b>	192.168.150.13	255.255.255.0	192.168.150.1	Ether3
<b>Impresora-B</b>	192.168.200.10	255.255.255.0	192.168.200.1	Ether1
<b>PC6-B</b>	192.168.200.11	255.255.255.0	192.168.200.1	Ether2
<b>Teléfono-B</b>	192.168.200.12	255.255.255.0	192.168.200.1	Ether3
<b>PC5-B</b>	192.168.200.13	255.255.255.0	192.168.200.1	Ether5

*Nota.* Esta tabla muestra todas las direcciones Ip establecidas para la configuración de la red.

### 3.2.3.1 Configuración de la herramienta Romon

Posteriormente se realizó la configuración de la herramienta Romon en todos los Routers que conforman la red, se accedió a la consola y con el comando **/tool romon** y **enable** se habilitó Romon. Además, se procedió a cambiar el nombre a cada Router con el comando **/system identity**.

#### Figura 33

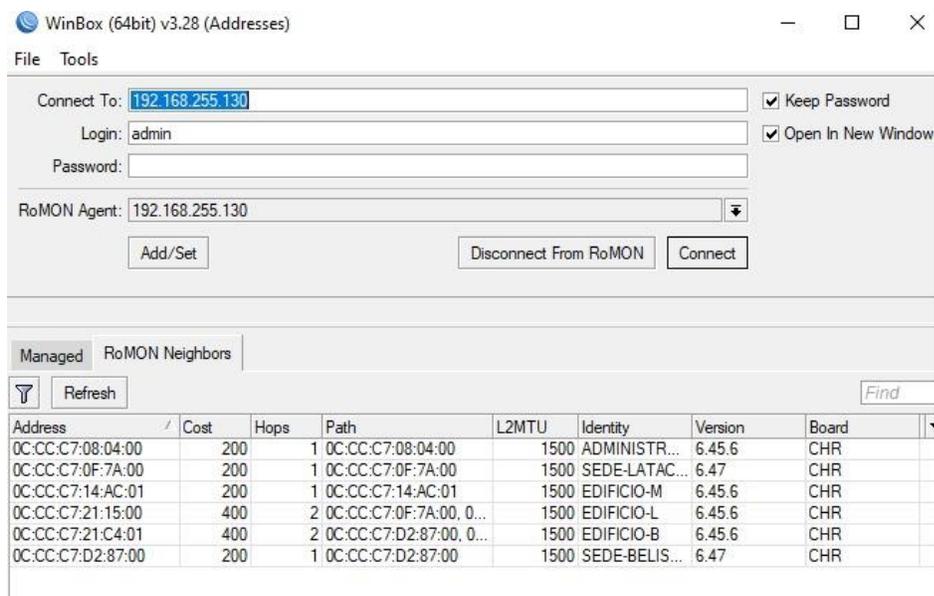
*Configuración de Romon y nombre de los Routers*

```
[admin@MikroTik] > system identity
[admin@MikroTik] /system identity> edit name
[admin@ADMINISTRACION-M] /system identity>
[admin@ADMINISTRACION-M] /system identity> ..
[admin@ADMINISTRACION-M] /system> ..
[admin@ADMINISTRACION-M] > tool romon
[admin@ADMINISTRACION-M] /tool romon> print
  enabled: no
    id: 00:00:00:00:00:00
  secrets:
[admin@ADMINISTRACION-M] /tool romon> edit
value-name: enable
[admin@ADMINISTRACION-M] /tool romon> print
  enabled: yes
    id: 00:00:00:00:00:00
  secrets:
    current-id: 0C:DD:13:88:99:01
[admin@ADMINISTRACION-M] /tool romon> []
```

*Nota.* El gráfico representa la habilitación de herramienta Romon en todos los RouterOS.

**Figura 34**

Conexión a la herramienta Romon



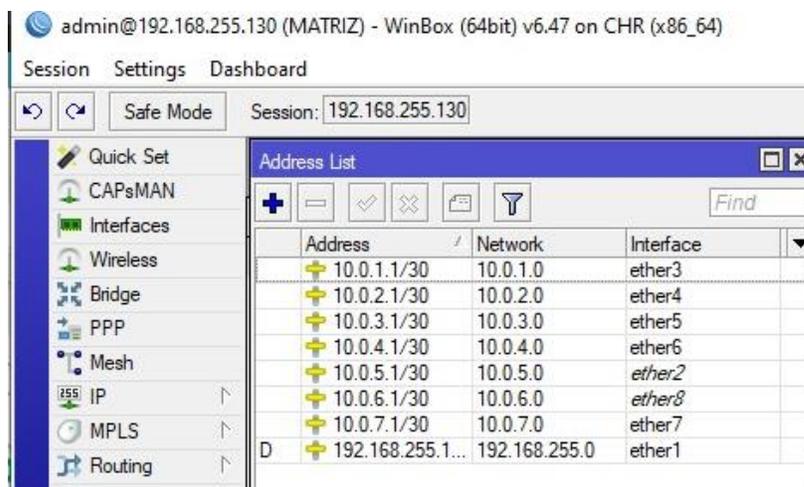
*Nota.* El gráfico representa las direcciones Mac habilitadas en Romon.

### 3.2.3.2 Configuración IP

A continuación, se procedió a ingresar las direcciones ip correspondiente a todos los routers de la red, teléfonos, computadoras e impresoras junto con el Gateway. Se realizó ping en las computadoras para verificar su conectividad.

## Figura 35

*Lista de direcciones de IP Matriz*



*Nota.* El gráfico representa las direcciones ip agregadas en el Router Matriz con sus interfaces.

## Figura 36

*Configuración de ip y Gateway*

```
TELEFONO-AM> ip 192.168.90.10/24 192.168.90.1
Checking for duplicate address...
TELEFONO-AM : 192.168.90.10 255.255.255.0 gateway 192.168.90.1

TELEFONO-AM> ping 192.168.91.1

84 bytes from 192.168.91.1 icmp_seq=1 ttl=64 time=2.288 ms
84 bytes from 192.168.91.1 icmp_seq=2 ttl=64 time=0.689 ms
84 bytes from 192.168.91.1 icmp_seq=3 ttl=64 time=0.557 ms
84 bytes from 192.168.91.1 icmp_seq=4 ttl=64 time=1.612 ms
84 bytes from 192.168.91.1 icmp_seq=5 ttl=64 time=1.657 ms

TELEFONO-AM> save
Saving startup configuration to startup.vpc
. done

TELEFONO-AM> █
```

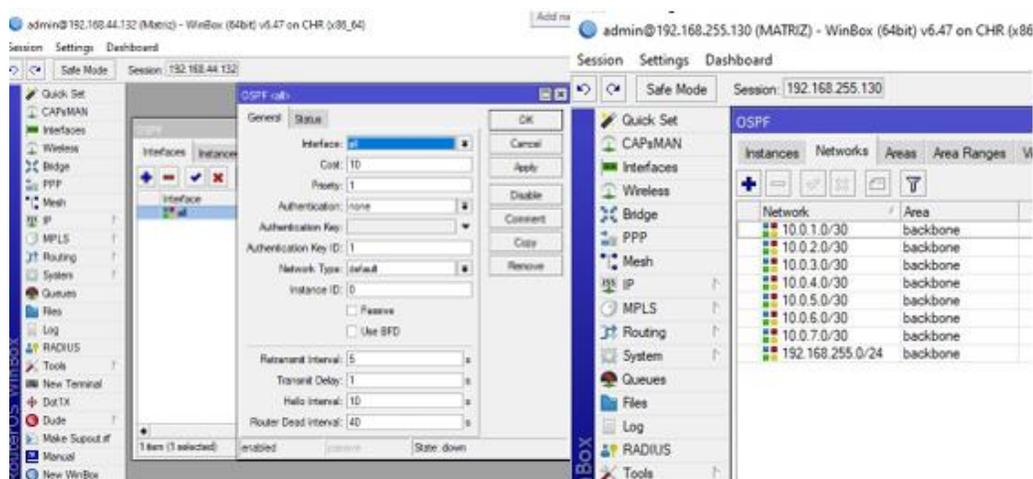
*Nota.* El gráfico representa la configuración de la dirección ip y verificación de conectividad.

### 3.2.3.3 Configuración del protocolo OSPF

Se realizó la configuración del protocolo OSPF en todos los Routers que componen la red, se agregó la interface en el cual se configuró de manera predeterminada, ya creada la interface ingresar cada una de las puertas de enlace en networks. Configurado OSPF se verificó la conexión entre computadoras de extremo a extremo.

**Figura 37**

*Configuración protocolo OSPF*



*Nota.* El gráfico representa la configuración del protocolo OSPF e ingresando las puertas de enlace.

**Figura 38***Comprobación de conectividad*

```
PC5-B> ip 192.168.200.10/24 192.168.200.1
Checking for duplicate address...
PC5-B : 192.168.200.10 255.255.255.0 gateway 192.168.200.1

PC5-B> ping 192.168.201.1

84 bytes from 192.168.201.1 icmp_seq=1 ttl=64 time=0.619 ms
84 bytes from 192.168.201.1 icmp_seq=2 ttl=64 time=0.615 ms
84 bytes from 192.168.201.1 icmp_seq=3 ttl=64 time=1.049 ms
84 bytes from 192.168.201.1 icmp_seq=4 ttl=64 time=1.142 ms
84 bytes from 192.168.201.1 icmp_seq=5 ttl=64 time=0.953 ms

PC5-B> ping 10.0.2.2

84 bytes from 10.0.2.2 icmp_seq=1 ttl=63 time=6.284 ms
84 bytes from 10.0.2.2 icmp_seq=2 ttl=63 time=1.348 ms
84 bytes from 10.0.2.2 icmp_seq=3 ttl=63 time=3.242 ms
84 bytes from 10.0.2.2 icmp_seq=4 ttl=63 time=1.172 ms
84 bytes from 10.0.2.2 icmp_seq=5 ttl=63 time=2.503 ms

PC5-B> save
Saving startup configuration to startup.vpc
. done
```

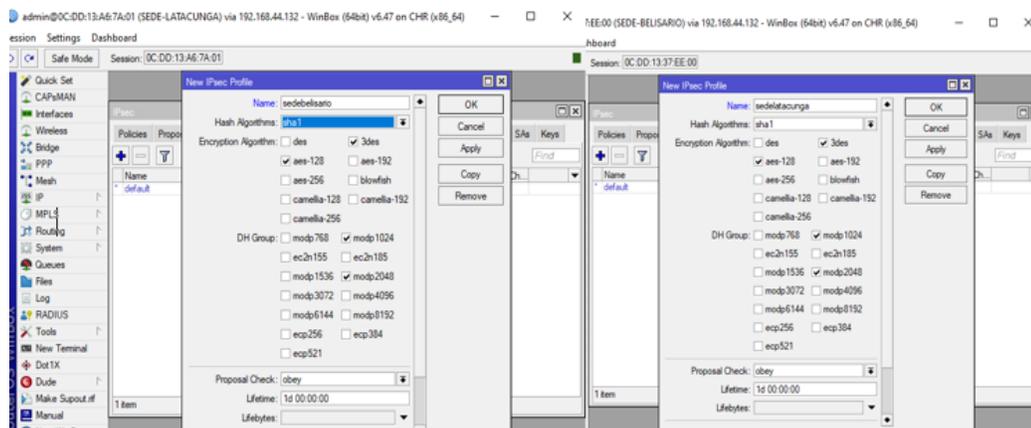
*Nota.* El gráfico representa la conexión de extremo a extremo realizando ping con la ip 10.0.2.2.

**3.2.3.4 Configuración de IPsec**

Se efectuó la configuración de IPsec entre los routers Sede Latacunga y Sede Belisario en el cual se inició configurando perfiles, posteriormente configuramos peers los cuales son los puntos de conexión que va existir entre Sede Latacunga y Sede Belisario.

**Figura 39**

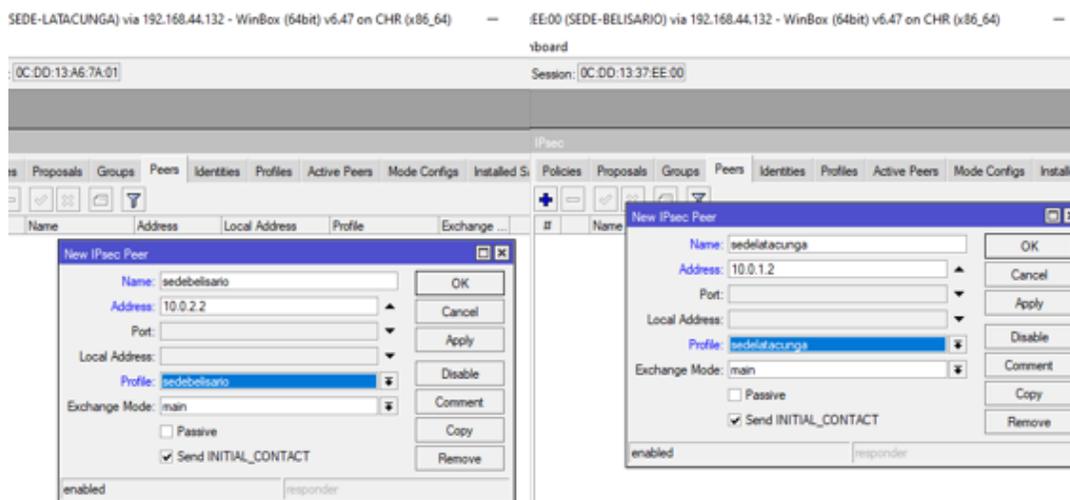
*Configuración Ipsec en los routers*



*Nota.* El gráfico representa la configuración de perfiles por IPsec en los routers Sede Latacunga y Sede Belisario.

**Figura 40**

*Configuración peers de IPsec*



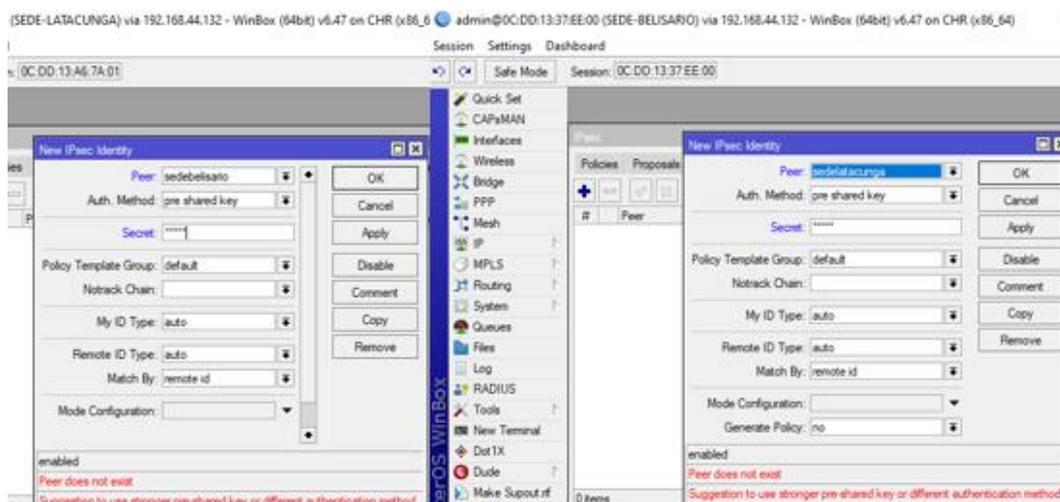
*Nota.* El gráfico representa la configuración de los peers el cual son los puntos de conexión que va existir entre sede Latacunga y sede Belisario.

### 3.2.3.5 Agregación de peers

Agregar peer de sede Latacunga a sede Belisario y peer de sede Belisario a sede Latacunga para que puedan ser identificados entre si mediante el tunnel IPsec, posteriormente agregar proposals a cada Router y activar el túnel, introducir direcciones ip de la red en new ip policy. Finalmente se realizó la verificación de IPsec creada.

**Figura 41**

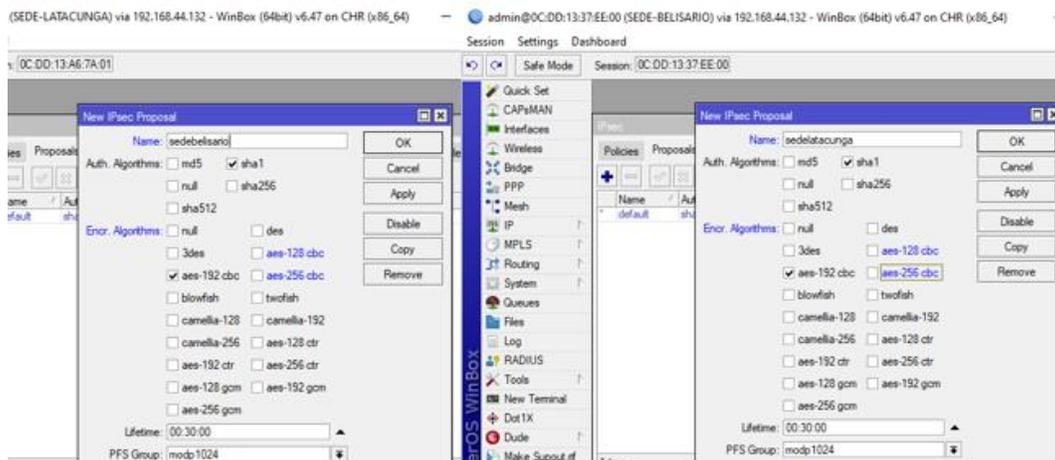
*Creación de IPsec Identity*



*Nota.* El gráfico representa la creación de un nuevo IPsec Identity tanto en la sede Latacunga como en sede Belisario.

Figura 42

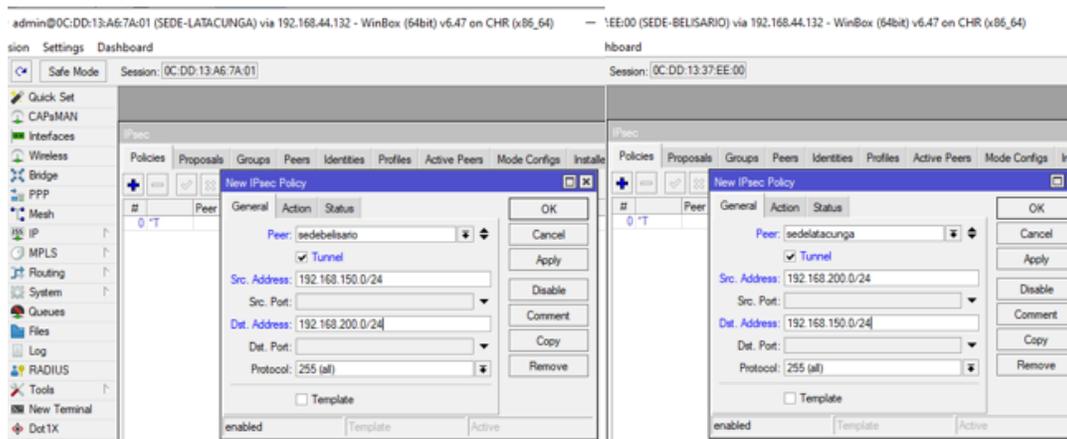
## Creación de propuesta IPsec



*Nota.* El gráfico representa la creación de una nueva IPsec propuesta a cada una de las sedes que van a estar en red mediante IPsec.

Figura 43

## Creación de política de IPsec



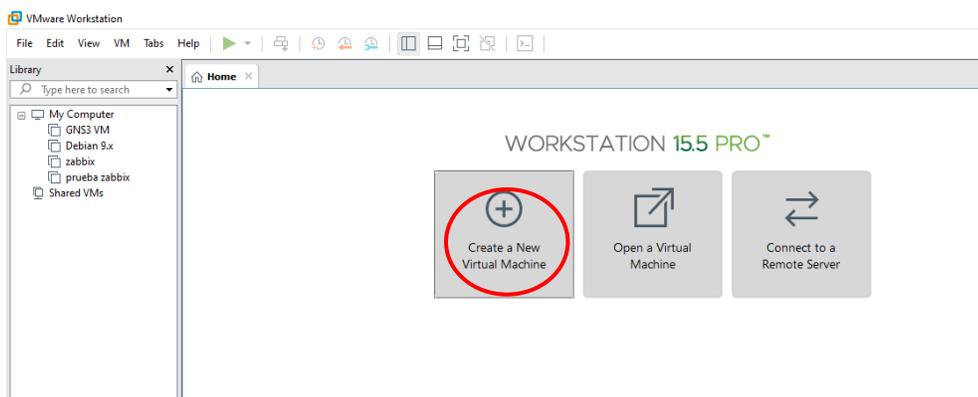
*Nota.* El gráfico representa la creación de una nueva política, activación del tunnel e ingreso de cada IP.

### 3.2.4 Instalación de la máquina virtual Ubuntu en VMware

En la interfaz principal de VMware seleccionar el enlace create a new virtual Machine para comenzar con la instalación de la máquina virtual.

#### Figura 44

*Interfaz principal de VMware*



*Nota.* El gráfico representa la creación de la nueva máquina virtual.

### 3.2.5 Asistente de instalación

En esta interfaz de asistente da la bienvenida para la creación de una nueva máquina virtual, aquí elegir la instalación típica o una personalizada y en este caso elegir la typical ya que es recomendable por la asistencia y dar clic en next para continuar.

**Figura 45**

*Ventana de asistente de creación*



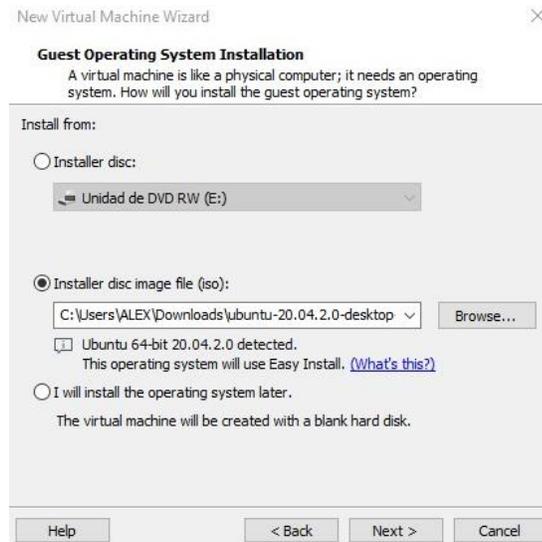
*Nota.* El gráfico representa la bienvenida de la creación de la nueva máquina virtual.

### **3.2.6 Selección de imagen ISO**

Una vez descargada la imagen ISO de la página oficial de Ubuntu, seleccionar de opción archivo de imagen de disco y hacer clic en el botón examinar para agregar el archivo Ubuntu, dar clic en next.

**Figura 46**

*Ventana de selección imagen ISO*



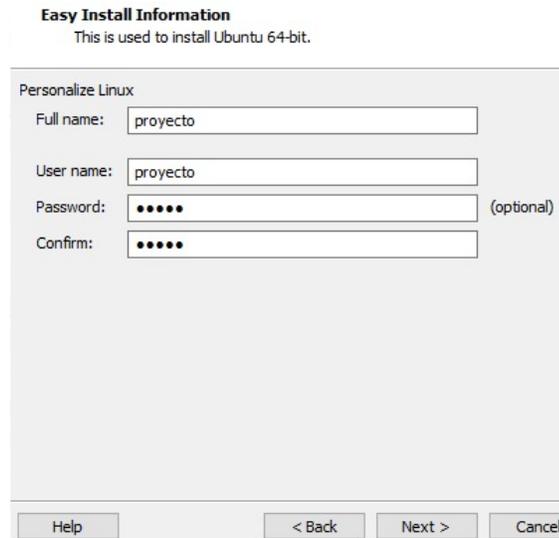
*Nota.* El gráfico representa la selección de la imagen ISO Ubuntu.

### **3.2.7 Configuración de usuario**

En la siguiente pantalla rellenar todos los datos como su nombre completo, nombre de usuario y una contraseña, una vez llenado los datos necesarios dar clic en siguiente para continuar.

## Figura 47

### Creación de usuario y contraseña



**Easy Install Information**  
This is used to install Ubuntu 64-bit.

Personalize Linux

Full name:

User name:

Password:  (optional)

Confirm:

Help < Back Next > Cancel

*Nota.* El gráfico representa la configuración de datos de usuario.

### **3.2.8 Ubicación de instalación de la máquina virtual**

Establecer el nombre de la máquina o dejar por defecto como en este caso, elegir la ubicación predeterminada o la carpeta de instalación creada de la máquina virtual y dar clic en next.

**Figura 48**

*Ventana de ubicación de instalación*

**Name the Virtual Machine**  
What name would you like to use for this virtual machine?

Virtual machine name:  
Ubuntu 64-bit

Location:  
C:\Users\ALEX\Documents\Virtual Machines\Ubuntu 64-bit

The default location can be changed at Edit > Preferences.

< Back 

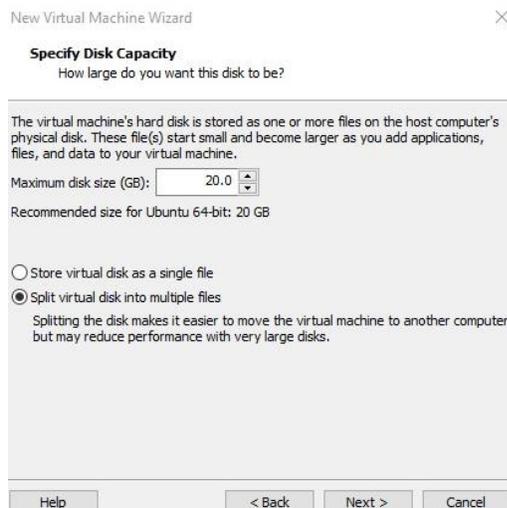
*Nota.* El gráfico representa la creación del nombre de la máquina virtual y la selección de ubicación de la instalación.

### **3.2.9 Configuración tamaño de disco**

En esta interfaz dejar los ajustes por defecto (20GB) o agregar más espacio de disco si prefiere, la instalación predeterminada de Ubuntu solo ocupara entre 4,5 y 5 GB, dar clic en next.

## Figura 49

### Configuración de tamaño del disco virtual



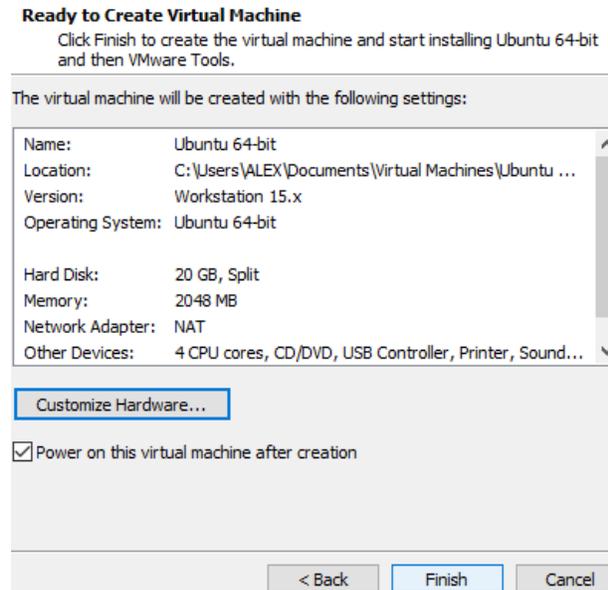
*Nota.* El gráfico representa la configuración del tamaño del disco virtual.

### 3.2.10 Resumen de las configuraciones de la máquina virtual

En esta ventana se podrá editar las opciones como la memoria RAM, la cantidad de procesadores, el uso compartido de dispositivos. En este caso se configuró 2 de RAM y dos de procesadores y marcar la opción power on para encender la máquina virtual después de la creación dar clic en finish.

## Figura 50

### Configuración general de la máquina virtual



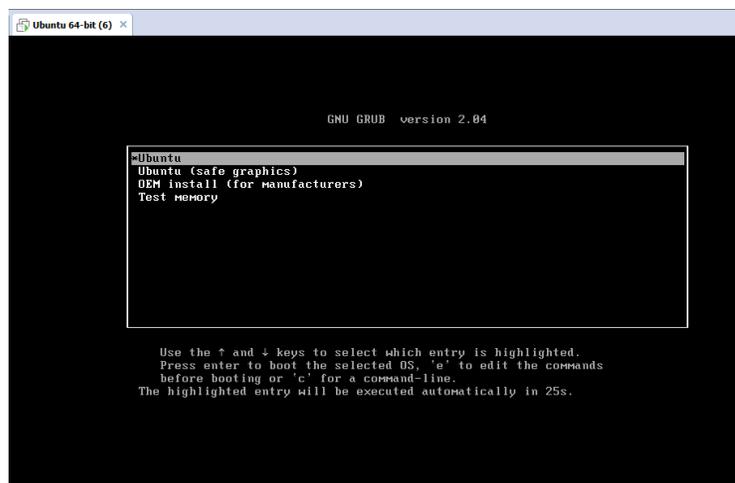
*Nota.* El gráfico representa la configuración personalizada del hardware a la máquina virtual.

### 3.2.11 Inicio de instalación de la máquina virtual Ubuntu

Una vez terminado de configurar todas las especificaciones del hardware virtual se abrirá automáticamente el menú de inicio de instalación de la máquina virtual ubuntu seleccionar install ubuntu y enter.

**Figura 51**

*Ventana de inicialización de instalación*



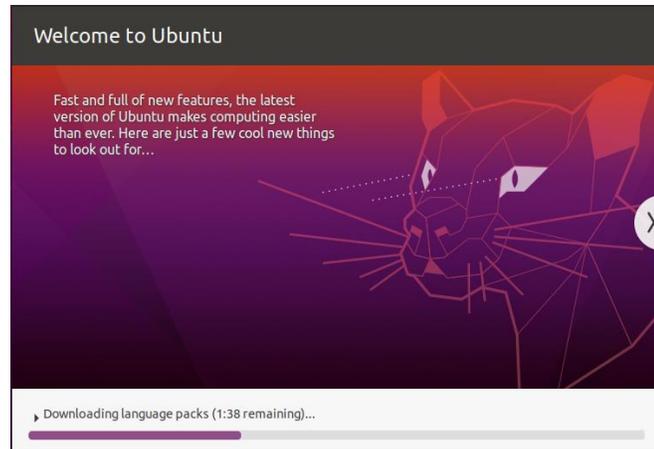
*Nota.* El gráfico representa la interfaz principal de inicio de instalación de la máquina virtual Ubuntu.

### 3.2.11.1 Visualización del proceso de instalación

Interfaz de bienvenida del proceso de instalación de la máquina virtual de Ubuntu, esperar unos minutos mientras se instala todos los paquetes necesarios para la funcionalidad de Ubuntu.

## Figura 52

### *Interfaz de bienvenida Ubuntu*



*Nota.* El gráfico representa la descarga e instalación de los paquetes de Ubuntu.

### **3.2.11.2 Iniciar sesión en Ubuntu**

Interfaz de inicio de sesión de Ubuntu con el nombre de usuario creado como proyecto e ingresar la contraseña para acceder a la máquina virtual.

**Figura 53**

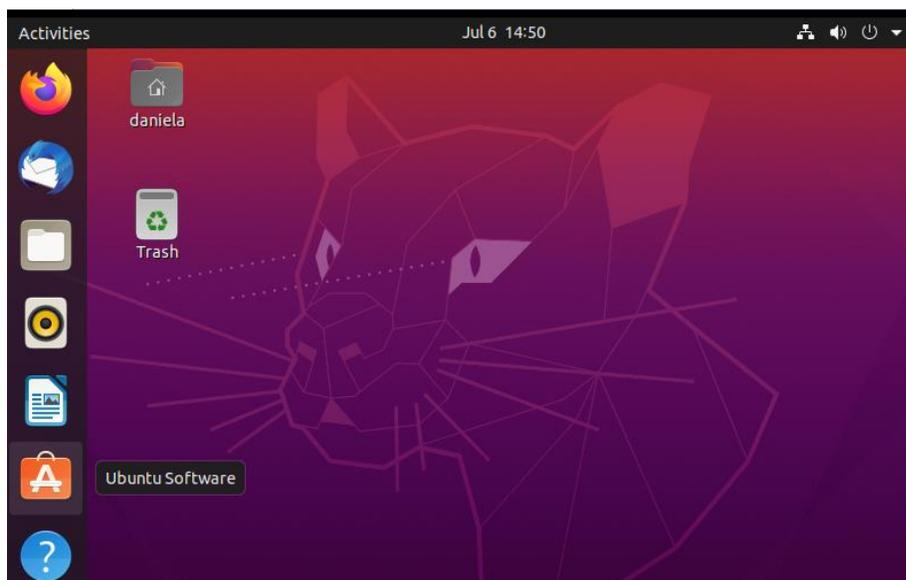
*Interfaz de inicio de sesión*



*Nota.* El gráfico representa el ingreso a la máquina virtual Ubuntu con el usuario proyecto.

**Figura 54**

*Interfaz menú principal de Ubuntu*



*Nota.* El gráfico representa la interfaz principal de la máquina virtual Ubuntu.

### 3.3 Instalación del servidor Zabbix en la máquina virtual Ubuntu

En conclusión, al momento de elegir la mejor plataforma de monitoreo entre Nagios, Zabbix y Pandora FMS se escogió Zabbix debido a su fácil implementación donde se puede administrar mediante una interfaz web además posee una gran cantidad de pantallas y gráficos que se pueden crear de una manera sencilla.

Todas estas y más características se demuestra en la Tabla 1 de forma detallada para dar una visión global de las tres plataformas.

**Tabla 2**

*Comparación de las herramientas de monitoreo*

<b>Herramientas</b>	<b>Nagios</b>	<b>Zabbix</b>	<b>Pandora FMS</b>
<b>Características y requerimientos</b>			
<b>Monitoreo de red</b>	X	X	X
<b>Monitoreo de servidores</b>	X	X	X
<b>Monitoreo de aplicaciones</b>	X	X	X
<b>Monitoreo de máquinas virtuales</b>	X	X	X
<b>Monitoreo de base de datos</b>	X	X	X
<b>Temperatura de seguridad</b>	X	X	X
<b>Monitoreo de correo electrónico</b>	X	X	X
<b>Monitoreo de rendimiento de PC</b>	X		
<b>Instalación en Linux</b>	X	X	X
<b>Dificultad de instalación</b>	X		X
<b>Verificación de correo electrónico</b>	X	X	X
<b>Facilidad de uso</b>		X	X
<b>Graficas</b>	X	X	X
<b>Mapas</b>	X	X	
<b>Administración SNMP</b>	X	X	X

*Nota.* Esta tabla representa la comparación de características y requerimientos de las herramientas de monitoreo

### 3.3.1 Requisitos de instalación del servidor web Zabbix

Zabbix requiere una memoria física de 128 MB y 256 MB de espacio libre en disco, disponer de un sistema operativo Linux. La cantidad de memoria de disco depende de la cantidad de hosts y parámetros que se van a monitorizar.

#### 3.3.1.1 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 55

*Página oficial de Zabbix*



*Nota.* El gráfico representa la selección de la versión y componentes a instalar de Zabbix.

#### 3.3.1.2 Instalación del repositorio de Zabbix

En el terminal de la máquina virtual de Ubuntu 20.04 ingresar al root con el comando **sudo su** e ingresar la contraseña creada en el usuario para entrar al root. Instalar el

repositorio de Zabbix el cual hay que copiar y ejecutar los enlaces para descargar los paquetes que contiene la información de repositorio de Zabbix para Ubuntu 20.04 e instalar el paquete, posteriormente actualizar la lista de los repositorios ya creados.

## Figura 56

### Instalación del repositorio de Zabbix

```

root@ubuntu:/home/daniela# wget https://repo.zabbix.com/zabbix/5.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_5.0-1+focal_all.deb
2021-07-08 14:34:55 -- https://repo.zabbix.com/zabbix/5.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_5.0-1+focal_all.deb
Resolving repo.zabbix.com (repo.zabbix.com)... 178.128.6.101, 2604:a880:2:d0::2062:d001
Connecting to repo.zabbix.com (repo.zabbix.com)|178.128.6.101|:443... connected
root@ubuntu:/home/daniela# dpkg -i zabbix-release_5.0-1+focal_all.deb
Selecting previously unselected package zabbix-release.
(Reading database ... 182804 files and directories currently installed.)
Preparing to unpack zabbix-release_5.0-1+focal_all.deb ...
Unpacking zabbix-release (1:5.0-1+focal) ...
Setting up zabbix-release (1:5.0-1+focal) ...
root@ubuntu:/home/daniela# apt update
Hit:1 http://security.ubuntu.com/ubuntu focal-security InRelease
Hit:2 http://us.archive.ubuntu.com/ubuntu focal InRelease
Get:3 http://repo.zabbix.com/zabbix/5.0/ubuntu focal InRelease [4,930 B]
Hit:4 http://us.archive.ubuntu.com/ubuntu focal-updates InRelease
Hit:5 http://us.archive.ubuntu.com/ubuntu focal-backports InRelease
Get:6 http://repo.zabbix.com/zabbix/5.0/ubuntu focal/main Sources [1,196 B]
Get:7 http://repo.zabbix.com/zabbix/5.0/ubuntu focal/main amd64 Packages [3,218 B]
Fetched 9,344 B in 2s (5,351 B/s)

```

*Nota.* El gráfico representa la instalación de los paquetes del repositorio de Zabbix.

### 3.3.1.3 Instalación del servidor, la interfaz y el agente de Zabbix

Instalar el servidor, la interfaz y el agente de Zabbix y el fronted web con el soporte de la base de datos MySQL y el agente Zabbix que permitirá recoger datos sobre el estado del servidor. Cuando se esté ejecutando preguntara si quiere continuar y presionar yes para continuar.

Figura 57

*Instalación de Zabbix server, frontend y agent*

```

root@ubuntu:/home/daniela# apt install zabbix-server-mysql zabbix-frontend-php
zabbix-apache-conf zabbix-agent
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils fonts-dejavu
  fonts-dejavu-extra fping libapache2-mod-php libapache2-mod-php7.4 libapr1
  Rhythmbox l1 libaprutil1-dbd-sqlite3 libaprutil1-ldap liblua5.2-0 libodbc1
  libonig5 libopenipmi0 mysql-client mysql-client-8.0 mysql-client-core-8.0
1 upgraded, 43 newly installed, 0 to remove and 506 not upgraded.
Need to get 20.1 MB of archives.
After this operation, 137 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://repo.zabbix.com/zabbix/5.0/ubuntu focal/main amd64 zabbix-server-my
sql amd64 1:5.0.14-1+focal [2,886 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu focal/main amd64 libapr1 amd64 1.6.5-1
ubuntu1 [91.4 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu focal/main amd64 libaprutil1 amd64 1.6
.1-4ubuntu2 [84.7 kB]

```

*Nota.* El gráfico representa la ejecución del zabbix server, agent y frontend.

### 3.3.1.4 Instalación de la Base de Datos

Para poder usar Zabbix, instalar una base de datos para almacenar los datos que el servidor recogerá de los agentes, primero ingresar al host de la base de datos con la contraseña **password**. Después crear una base de datos MySQL y completar la información básica adecuada para Zabbix, también crear un usuario para la base de datos y establecer una contraseña o dejarlo por defecto.

**Figura 58**

*Instalación y creación de la base de datos*

```
root@ubuntu:/home/daniela# sudo apt-get install mysql-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
root@ubuntu:/home/daniela# mysql -uroot -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 8
Server version: 8.0.25-0ubuntu0.20.04.1 (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 (0.01 sec))

mysql> create user zabbix@localhost identified by 'password';
(query OK, 0 rows affected (0.03 sec))

mysql> grant all privileges on zabbix.* to zabbix@localhost;
(query OK, 0 rows affected (0.01 sec))

mysql> quit;
bye
root@ubuntu:/home/daniela#
```

*Nota.* El gráfico representa la creación de usuario y la base de datos MySQL.

### 3.3.1.5 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 59

### Configuración del host del servidor Zabbix

```
root@ubuntu:/home/daniela# zcat /usr/share/doc/zabbix-server-mysql*/create.sql.gz | mysql -uzabbix -p zabbix
Enter password:
root@ubuntu:/home/daniela#
```

*Nota.* El gráfico representa la importación del esquema y los datos iniciales de la configuración realizada en la base de datos.

### 3.3.1.6 Configuración de la Base de Datos para el servidor Zabbix

Para utilizar la base de datos del servidor Zabbix establecer la contraseña de la base de datos en el archivo de configuración del servidor. Abrir el archivo de configuración con el comando `sudo nano`. Modificar el parámetro **DBpassword=password**, posteriormente guardar los cambios realizados.

## Figura 60

### Interfaz de configuración de la base de datos

```
root@ubuntu:/home/daniela# sudo nano /etc/zabbix/zabbix_server.conf
root@ubuntu:/home/daniela#
# DBUser=
DBUser=zabbix
### Option: DBPassword
# Database password.
# Comment this line if no password is used.
#
# Mandatory: no
# Defaults:
DBPassword=password
### Option: DBSocket
^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text    ^J Justify
^X Exit       ^R Read File  ^L Replace    ^U Paste Text ^T To Spell
```

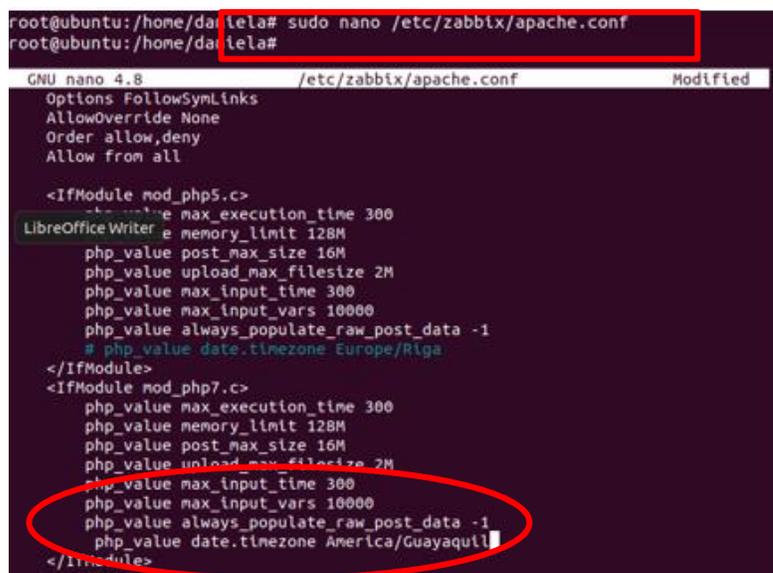
*Nota.* El gráfico representa la configuración de la base de datos para servidor Zabbix.

### 3.3.1.7 Configuración PHP para Zabbix Fronted

La interfaz web de Zabbix requiere algunos ajustes especiales al servidor Zabbix en php posteriormente acceder al directorio que está ubicado en **etc/zabbix** el cual contiene los ajustes de php donde se debe configurar la zona horaria estándar.

**Figura 61**

*Configuración PHP para fronted de Zabbix*



```

root@ubuntu:/home/daniela# sudo nano /etc/zabbix/apache.conf
root@ubuntu:/home/daniela#

GNU nano 4.8 /etc/zabbix/apache.conf Modified
Options FollowSymLinks
AllowOverride None
Order allow,deny
Allow from all

<IfModule mod_php5.c>
    php_value max_execution_time 300
    LibreOfficeWriter e 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>

```

*Nota.* El gráfico representa la configuración de la zona horaria adecuada.

### 3.3.1.8 Iniciación y restauración del agente y el servidor

Ejecutar los comandos restart el cual reiniciara el servidor de Zabbix y los procesos de agent para aplicar la nueva configuración realizada y con el comando enable para habilitar el sistema para su inicialización.

**Figura 62**

*Inicialización del sistema*

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

*Nota.* El gráfico representa la inicialización y habilitación del proceso del servidor Zabbix.

### 3.3.1.9 Instalación de la herramienta de red y verificación IP

Ejecutar el comando **apt install** para instalar las herramientas de red necesarias.

Verificar la dirección Ip con la cual se va trabajar para ingresar al servidor Zabbix y luego ejecutar con el comando **ifconfig**.

Figura 63

*Instalación de herramientas de red*

```

root@ubuntu:/home/daniel# apt install net-tools
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
 net-tools
0 upgraded, 1 newly installed, 0 to remove and 246 not upgraded.
Need to get 196 kB of archives.

root@ubuntu:/home/proyecto# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> ntu 1500
    inet 192.168.255.132 netmask 255.255.255.0 broadcast 192.168.255.255
    inet6 fe80::7db2:7dc7:e7fa:61f0 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:11:69:83 txqueuelen 1000 (Ethernet)
    RX packets 60558 bytes 79041689 (79.0 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 25934 bytes 2273048 (2.2 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ens38: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> ntu 1500
    inet 192.168.164.130 netmask 255.255.255.0 broadcast 192.168.164.255
    inet6 fe80::e7b1:9a6c:a7bc:245c prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:11:69:8d txqueuelen 1000 (Ethernet)
    RX packets 225 bytes 22262 (22.2 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 511 bytes 49569 (49.5 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

*Nota.* El gráfico representa la verificación de la dirección Ip del servidor web de Zabbix.

### 3.3.1.10 Inicio de instalación de la interfaz web del servidor

Instalación de la interfaz web de Zabbix (frontend) ingresando con la dirección ip:

**192.168.255.132** y el nombre del servidor en la url del navegador Firefox que tiene por defecto la máquina virtual Ubuntu.

**Figura 64**

*Interfaz de bienvenida Zabbix*



*Nota.* El gráfico representa como ingresar con la dirección Ip y nombre del servidor al Zabbix.

### 3.3.1.1 Verificación de pre-requisitos

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.

**Figura 65***Interfaz de verificación*

	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

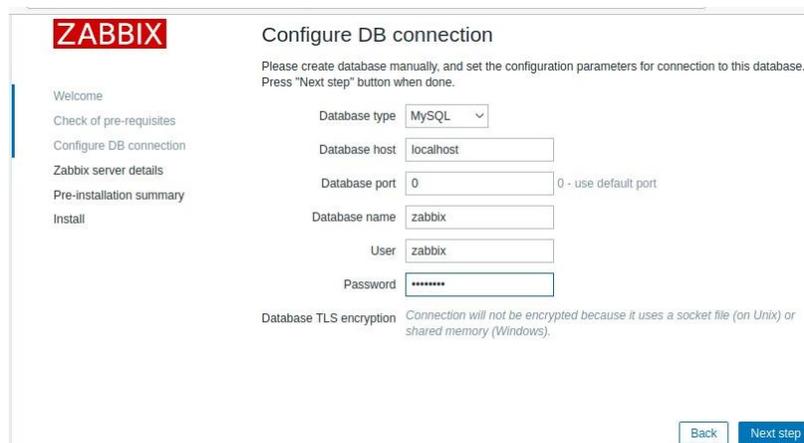
*Nota.* El gráfico representa el chequeo de prerrequisitos de instalación de Zabbix.

### 3.3.1.12 Configuración de conexión de la base de datos

Interfaz de configuración de conexión de la base de datos donde se verifica las configuraciones ya realizadas en el proceso de instalación de Zabbix e introducir el nombre de la base de datos, el usuario y establecer la contraseña **password**.

## Figura 66

### Configuración de conexión de la base de datos

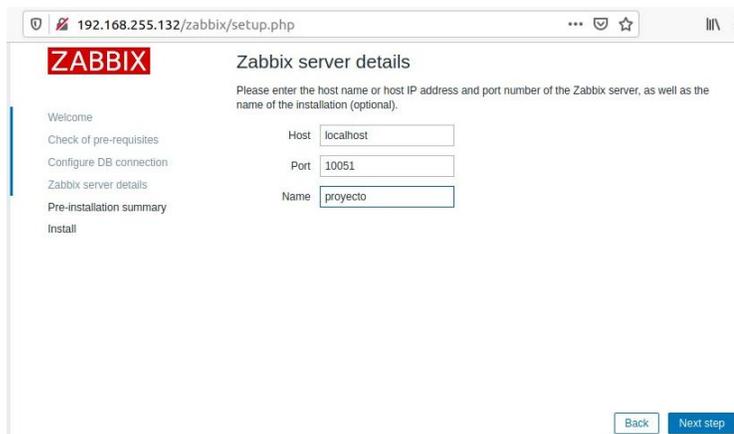


The screenshot shows the Zabbix installation wizard's 'Configure DB connection' step. On the left is a navigation menu with options: Welcome, Check of pre-requisites, Configure DB connection (highlighted), Zabbix server details, Pre-installation summary, and Install. The main area is titled 'Configure DB connection' and includes the Zabbix logo. Below the title, it says: 'Please create database manually, and set the configuration parameters for connection to this database. Press "Next step" button when done.' The form contains the following fields: 'Database type' (a dropdown menu set to 'MySQL'), 'Database host' (text input 'localhost'), 'Database port' (text input '0' with a note '0 - use default port'), 'Database name' (text input 'zabbix'), 'User' (text input 'zabbix'), and 'Password' (password input field with masked characters). At the bottom, there is a note about 'Database TLS encryption' stating 'Connection will not be encrypted because it uses a socket file (on Unix) or shared memory (Windows)'. At the bottom right, there are two buttons: 'Back' and 'Next step'.

*Nota.* El gráfico representa la verificación de configuración de conexión de la base de datos predeterminada.

#### 3.3.1.13 Detalles del servidor Zabbix

En los detalles del servidor Zabbix dejar las opciones y sus valores predeterminados o crear un nombre de la interfaz web para poder distinguir un servidor de otro en caso de tener varios servidores de monitorización o como en este caso asignar el nombre de proyecto.

**Figura 67***Interfaz Zabbix server details*

The screenshot shows a web browser window with the address bar displaying "192.168.255.132/zabbix/setup.php". The page title is "ZABBIX" in a red box, followed by "Zabbix server details". Below the title, there is a instruction: "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)". There are three input fields: "Host" with the value "localhost", "Port" with the value "10051", and "Name" with the value "proyecto". At the bottom right, there are two buttons: "Back" and "Next step".

Host	localhost
Port	10051
Name	proyecto

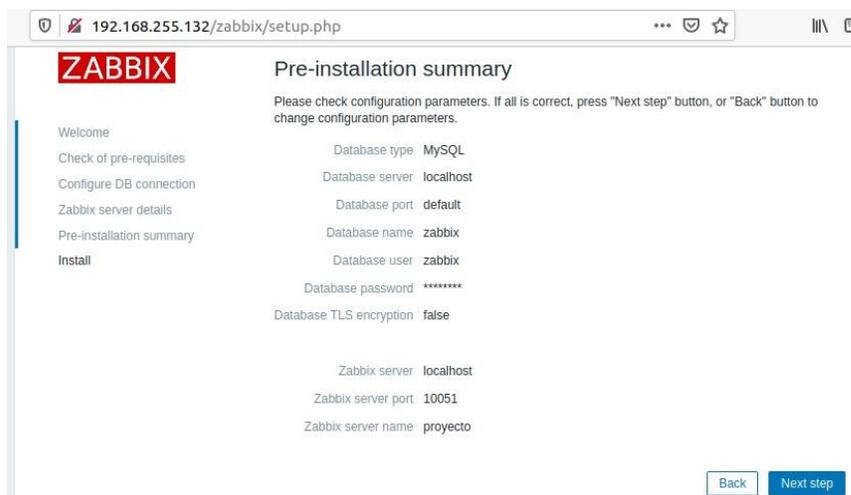
*Nota.* El gráfico representa la configuración predeterminada del servidor y asignación del nombre.

### 3.3.1.14 Resumen de la preinstalación

Interfaz previa resumida de la preinstalación que se va a proceder a realizar donde debemos verificar que todo predeterminado o acorde a como se configuró para poder continuar con la instalación.

## Figura 68

### Resumen de preinstalación



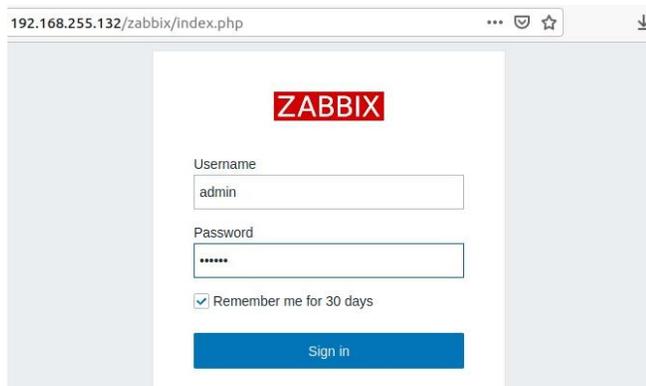
*Nota.* El gráfico representa el resumen de la preinstalación del servidor Zabbix.

### 3.3.1.15 Inicio de sesión

Una vez finalizado el proceso de instalación de Zabbix se abrirá automáticamente la interfaz de inicio de sesión y acceder al frontend o interfaz web del servidor con nombre de usuario **Admin** y la contraseña **zabbix**.

**Figura 69**

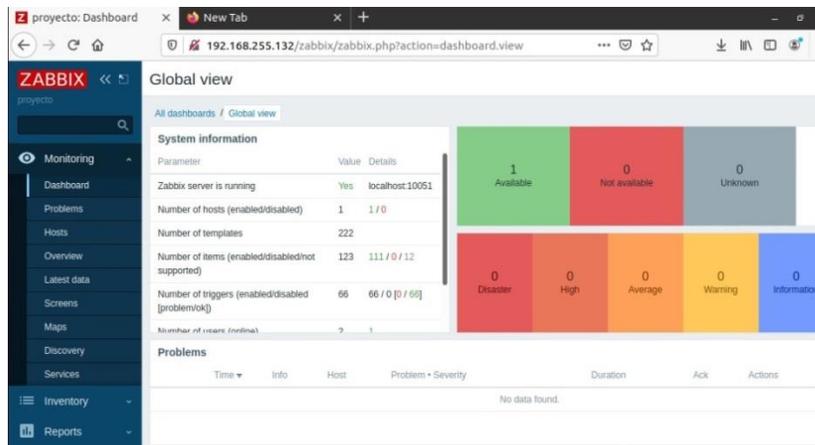
*Interfaz de inicio de sesión*



*Nota.* El gráfico representa el ingreso de usuario y contraseña para iniciar sesión en el servidor web de Zabbix.

**3.3.1.16 Panel de control de la interfaz web de Zabbix**

Finalmente se podrá verificar la interfaz web del servidor con su principal panel de control y estará listo para hacer uso de los componentes para el monitoreo de red, también se verá el sistema de información de los parámetros establecidos.

**Figura 70***Panel de control principal*

*Nota.* El gráfico representa el panel de control del servidor web Zabbix y el sistema de información de los parámetros.

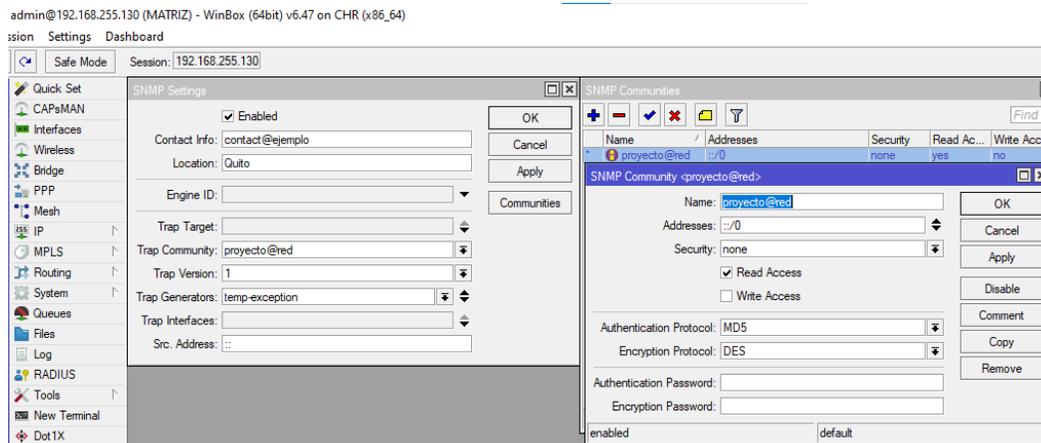
### 3.4 Monitoreo de la red corporativa simulada

#### 3.4.1 *Habilitación protocolo SNMP*

En la herramienta de red winbox se procedió activar el protocolo SNMP de todos los RouterOS Mikrotik que conforman la red, realizar todas las configuraciones necesarias para que funcione de manera correcta y establecer la conexión de SNMP con el servidor web Zabbix.

**Figura 71**

*Configuración protocolo SNMP*

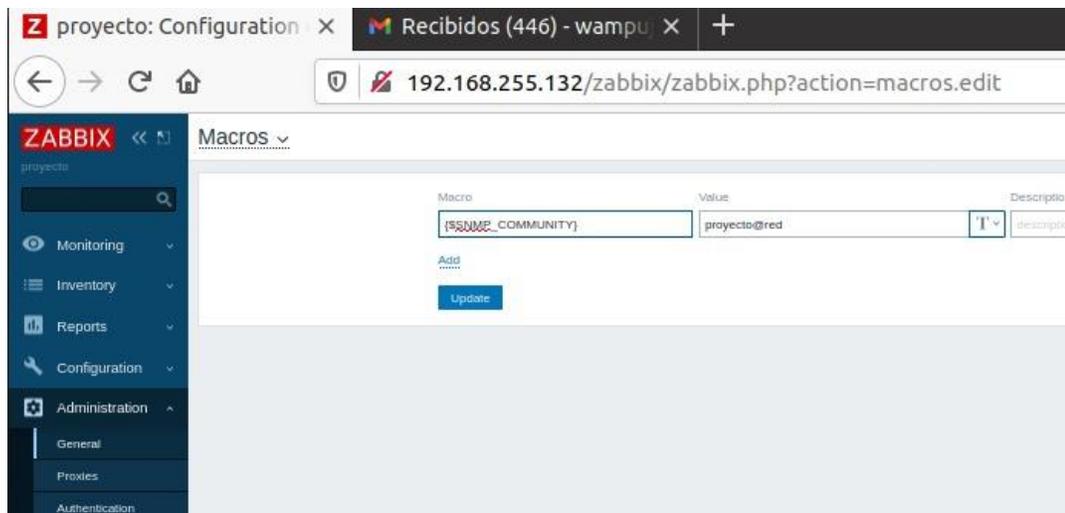


*Nota.* El gráfico representa la configuración del protocolo SNMP para el buen funcionamiento de la red.

En el panel de control del servidor Zabbix de administración dar clic en la pestaña general donde dirige a la ventana de Macros para configurar el SNMP\_COMMUNITY creado en la herramienta de winbox y en value agregar el nombre creado proyecto@red, actualizar para añadir la macro. Esto permitirá crear un host ya con el protocolo SNMP COMMUNITY.

**Figura 72**

Configuración SNMP\_COMMUNITY



*Nota.* El gráfico representa la configuración de la Macro SNMP COMMUNITY.

### 3.4.1.1 Creación del host

En el panel de control de Zabbix ir a configuración luego a host y en la parte derecha dar clic en create host y añadir el nombre del host matriz, se agregó los groups, donde se escogió el protocolo SNMP y se estableció la dirección ip **192.168.255.130** y las demás configuraciones por defecto. Dar clic en la pestaña templates y en link new templates crear un nuevo templates, agregar el host a monitorear.

**Figura 73***Configuración de host*

projecto: Configuration x Recibidos (446) - wampu x +

192.168.255.132/zabbix/hosts.php?form=create&groupids[0]=9

ZABBIX

Hosts

Host Templates IPMI Tags Macros Inventory Encryption

\* Host name: MATRIZ

Visible name: MATRIZ

\* Groups: Templates/Network devices x Virtual machines x Select

\* Interfaces

Type	IP address	DNS name	Connect to	Port
SNMP	192.168.255.130		IP DNS	161

\* SNMP version: SNMPv2

\* SNMP community: [SNMP\_COMMUNITY]

Use bulk requests

Add

Description

Monitored by proxy: (no proxy)

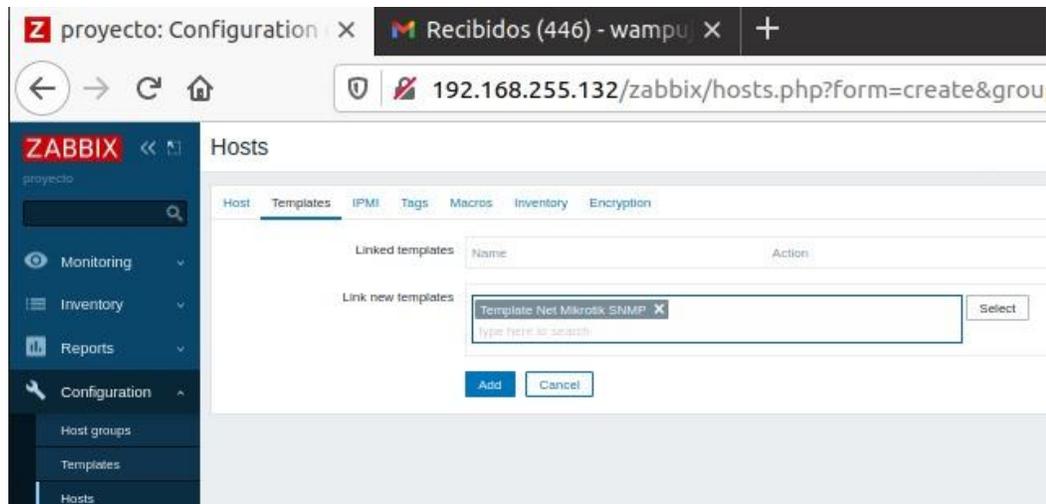
Enabled

Add Cancel

*Nota.* El gráfico representa la creación del host y el protocolo SNMP para la conectividad.

**Figura 74**

*Configuración de templates*



*Nota.* El gráfico representa la selección del template Net Mikrotik SNMP.

### 3.4.1.2 Verificación de host creados

Una vez creado y configurado todos los routers como host dirigirse a monitoring y seleccionar la pestaña host se mostrará todos los hosts creados para monitorear y administrar. Después de unos segundos se establecerá la conexión SNMP donde se podrá ver que SNMP está de color verde el cual significa que está habilitado.

## Figura 75

### Verificación de host

The screenshot shows the Zabbix 'Hosts' configuration page. The interface includes a search form with fields for Name, Host groups, IP, DNS, and Port. There are also filters for Status (Any, Enabled, Disabled) and Severity (Not classified, Information, Warning, Average, High, Disaster). A table below the form lists the following hosts:

Name	Interface	Availability	Tags	Problems	Status	Latest data	Problems	Graphs	Screens
ADMINISTRACION.M	10.0.3.2: 161	25% <span>SNMP</span> <span>add</span> <span>print</span>			Enabled	Latest data	Problems	Graphs 11	Screens 1
EDIFICIO-B	10.0.6.2: 161	25% <span>SNMP</span> <span>add</span> <span>print</span>			Enabled	Latest data	Problems	Graphs 11	Screens 1
EDIFICIO-L	10.0.5.2: 161	25% <span>SNMP</span> <span>add</span> <span>print</span>			Enabled	Latest data	Problems	Graphs 11	Screens 1
EDIFICIO-M	10.0.4.2: 161	25% <span>SNMP</span> <span>add</span> <span>print</span>			Enabled	Latest data	Problems	Graphs 11	Screens 1
email test	192.168.30.1: 10050	25% <span>SNMP</span> <span>add</span> <span>print</span>		1	Enabled	Latest data	Problems 1	Graphs	Screens
MATRIZ	192.168.255.130: 161	25% <span>SNMP</span> <span>add</span> <span>print</span>			Enabled	Latest data	Problems	Graphs 11	Screens 1
SEDE-BELISARIO	10.0.2.2: 161	25% <span>SNMP</span> <span>add</span> <span>print</span>			Enabled	Latest data	Problems	Graphs 11	Screens 1
SEDE-LADACUNGA	10.0.1.2: 161	25% <span>SNMP</span> <span>add</span> <span>print</span>			Enabled	Latest data	Problems	Graphs 11	Screens 1

*Nota.* El gráfico representa todos los hosts habilitados con el protocolo SNMP.

### 3.4.1.3 Latest data del Router

En el buscador ingresar el nombre de host matriz y dar clic donde se abrirá a una nueva ventana del host matriz y nuevamente clic en la pestaña latest data o también se buscara directamente desde el panel de control en monitoring y latest data para acceder y dando clic allí se desplegará toda la información que tiene el equipo RouterOS Mikrotik.

Figura 76

*Interfaz latest data*

Host	Name	Last check	Last value
MATRIZ	<b>CPU (1 Item)</b>		
	#1: CPU utilization	2021-08-18 16:47:02	0 %
MATRIZ	<b>General (6 Items)</b>		
	SNMP traps (fallback)		
	System contact details	2021-08-17 23:00:02	contact@ejemplo
	System description	2021-08-17 23:00:02	RouterOS CHR
	System location	2021-08-18 01:00:02	Quito
	System name	2021-08-18 01:00:02	MATRIZ
	System object ID	2021-08-18 16:45:02	iso.3.6.1.4.1.14988.1
MATRIZ	<b>Interface ether1() (9 Items)</b>		
	Interface ether1(): Bits received	2021-08-18 16:45:02	1.23 Kbps
	Interface ether1(): Bits sent	2021-08-18 16:45:02	1.3 Kbps
	Interface ether1(): Inbound packets discarded	2021-08-18 16:45:02	0
	Interface ether1(): Inbound packets with errors	2021-08-18 16:45:02	0
	Interface ether1(): Interface type	2021-08-17 23:00:02	ethernetGsmacd (0)
	Interface ether1(): Operational status	2021-08-18 16:47:02	up (1)
	Interface ether1(): Outbound packets discarded	2021-08-18 16:45:02	0

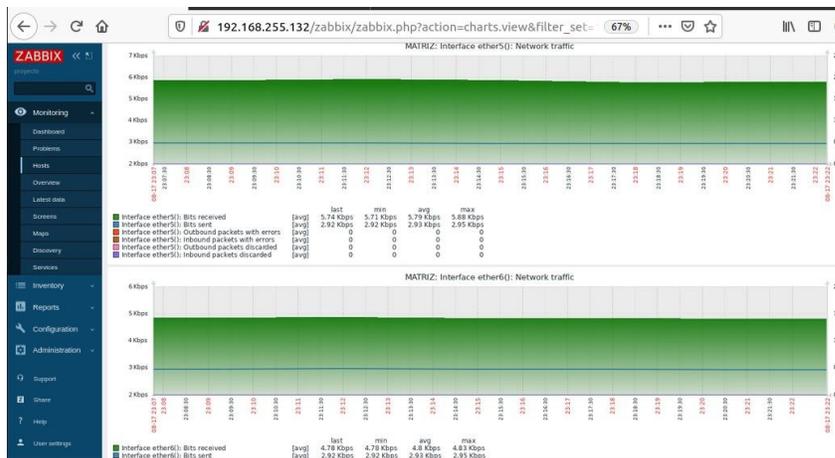
*Nota.* Este gráfico representa la verificación de información del RouterOS Mikrotik Matriz.

#### 3.4.1.4 Verificación de gráficas

En el buscador de Zabbix insertar el nombre del host que se desea monitorear para ver sus estadísticas como las gráficas de las interfaces, del CPU, utilización de la memoria y el tamaño del disco utilizado donde también se podrá ver los bits enviados y recibidos en tiempo real.

Figura 77

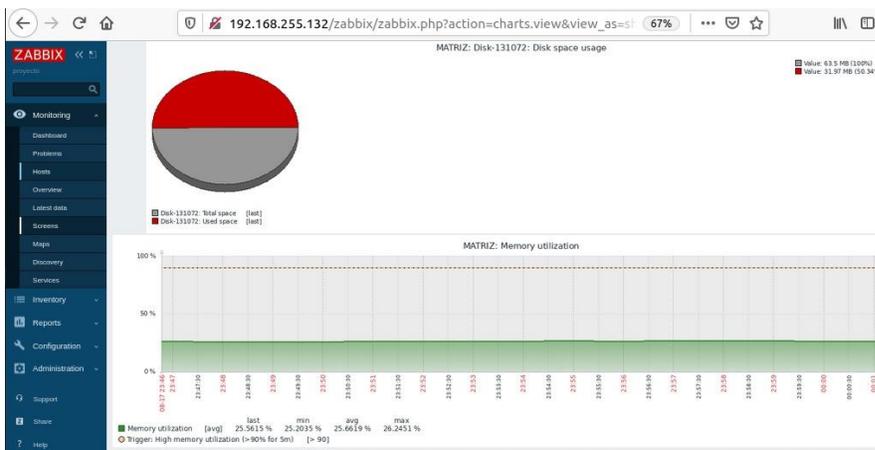
Interfaz gráfica



Nota. El gráfico representa la verificación de los bits enviados están de color azul y los bits recibidos color verde en las interfaces.

Figura 78

Interfaz gráfica 2



Nota. El gráfico representa el tamaño del disco usado y el espacio de memoria usado.

### 3.4.1.5 Creación de Maps

En monitoring -Maps se creó un nuevo mapa y se llenó los datos necesarios como nombre map y aplicar cambios si requiere o dejar por defecto lo cual para ingresar al map creado dar clic en el nombre map y se desplegara la ventana vacía para agregar los equipos.

**Figura 79**

*Configuración de map*

Network maps

Map Sharing

\* Owner Admin (Zabbix Administrator) Select

\* Name MAP

\* Width 800

\* Height 600

Background image No image

Automatic icon mapping <manual> show icon mappings

Icon highlight

Mark elements on trigger status change

Display problems Expand single problem Number of problems Number of problems and expand most critical one

Advanced labels

Map element label type Label

Map element label location Bottom

Problem display All

Minimum severity Not classified Information Warning Average High Disaster

Show suppressed problems

URLs

Name	URL
<input type="text"/>	<input type="text"/>

Add

Add Cancel

*Nota.* El gráfico representa la creación de un nuevo mapa de red de Zabbix administrador.

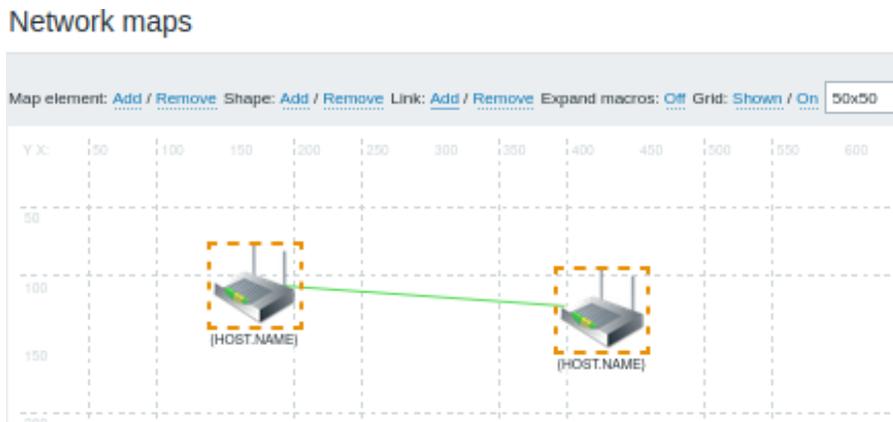
### 3.4.1.6 Creación de elementos

En la ventana principal de maps añadimos los routers principales en Map element add y se conectó como es debido la Matriz la nube de Internet y para guardar los cambios de

configuración realizada dar clic en update para no perder los cambios realizados y para seguir configurando dar clic en edit map.

## Figura 80

### Configuración de Router



*Nota.* El gráfico representa la conexión entre los Router.

### 3.4.1.7 Configuración de equipos en maps

En la configuración del equipo dar clic e ingresar los datos necesarios, el cual se asignará un estado o información del dispositivo donde se copiará las keys de los ítems dependiendo de cada host y se podrá visualizar el nombre del Router, ip, espacio de memoria, espacio en disco y el ping.

**Figura 81***Configuración de estado del Router*

Map element

Type

Label

```
{HOST.NAME}
IP:{HOST.IP}
Memoria:{MATRIZ-vm.memory.used[hrStorageUsed.Memory].last(2)} /
{MATRIZ-vm.memory.total[hrStorageSize.Memory].last(2)}
Espacio en disco
{MATRIZ-ifs.fs.used[hrStorageSize.131072].last(2)} /
{MATRIZ-ifs.fs.total[hrStorageSize.131072].last(2)}
Ping:{MATRIZ-icmp.ping.last(2)}
```

Label location

\* Host

Application

Automatic icon selection

Icons

Default	<input type="text" value="Router_(64)"/>
Problem	<input type="text" value="Default"/>
Maintenance	<input type="text" value="Default"/>
Disabled	<input type="text" value="Default"/>

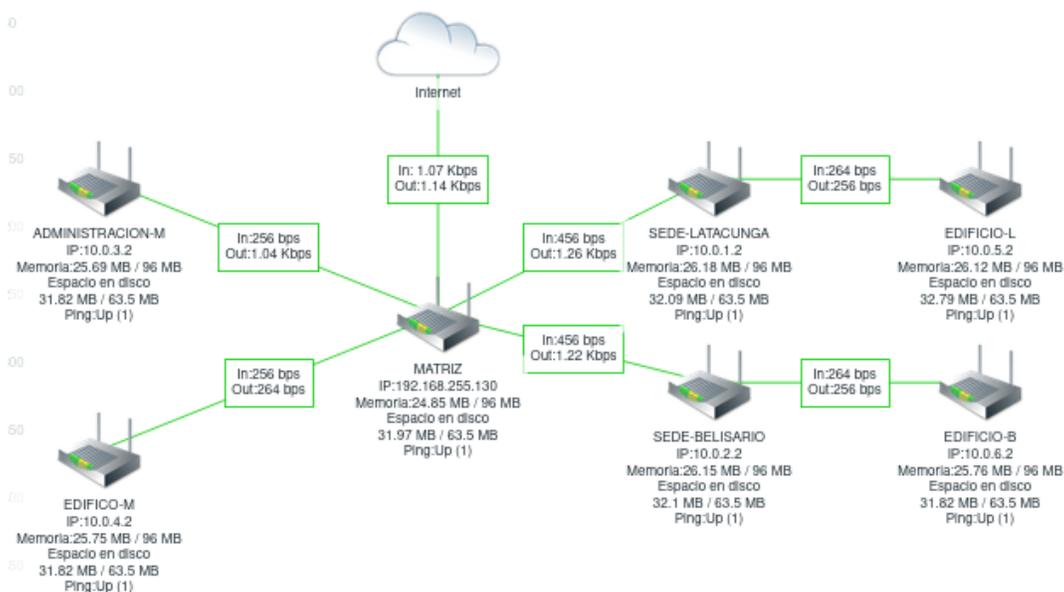
*Nota.* El gráfico representa la configuración del Router mediante las keys.

**3.4.1.8 Creación de topología**

Una vez configurado todos los Router y establecido la conexión guardar e ingresar nuevamente para ver las configuraciones realizadas a cada Router y mostrará información añadida y si la mayoría de los parámetros asignados esta funcional el estado del equipo será **Ok**. Comprobar el ping apagando el router Administración-M y Edificio-L para verificar el estado no disponible.

**Figura 82**

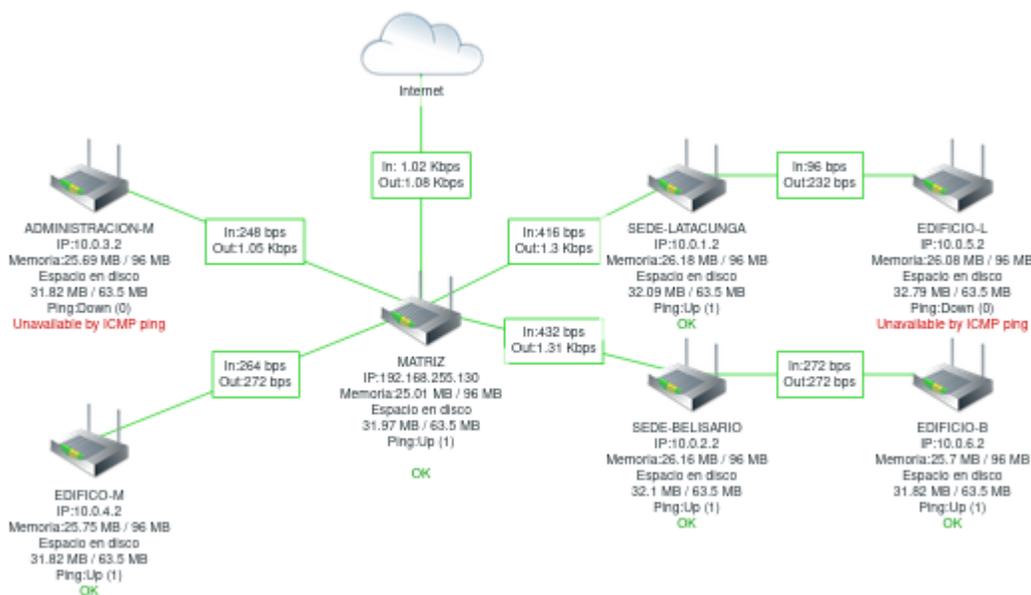
*Topología de red en Map*



*Nota.* El gráfico representa la conexión y configuración realizada a la topología.

**Figura 83**

*Comprobación de Funcionamiento*



*Nota.* El gráfico representa la verificación de ICMP ping no disponible.

### 3.4.1.9 Creación screen

En monitoring- screen crear un nuevo screen y configurar asignando un nombre red y lo demás dejar por defecto ya que podrá añadir o borrar los espacios de columnas y filas manualmente en la interfaz y clic en add.

#### Figura 84

##### Configuración de Screen

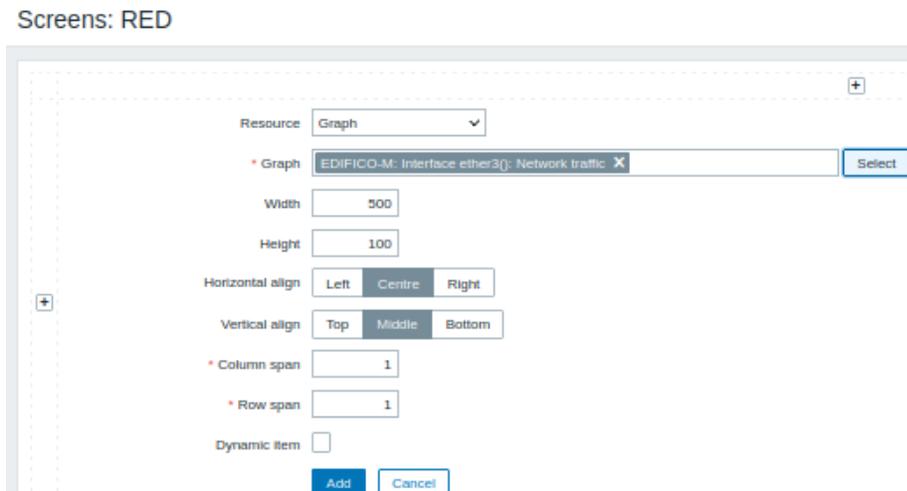
*Nota.* El gráfico representa la creación de un nuevo Screens de Zabbix administration.

### 3.4.1.10 Configuración Screens Red

Para añadir las capturas de pantalla dar clic en change y se desplegará la venta de configuración donde se asignara un host y el graph que quiere mostrar que puede ser las interfaces, memoria, tamaño del disco y CPU load. Se puede agregar todos los hosts tanto en columna como fila, (+) para añadir otra fila y (-) para descartar, y se podrá ver las gráficas añadida al Screen.

**Figura 85**

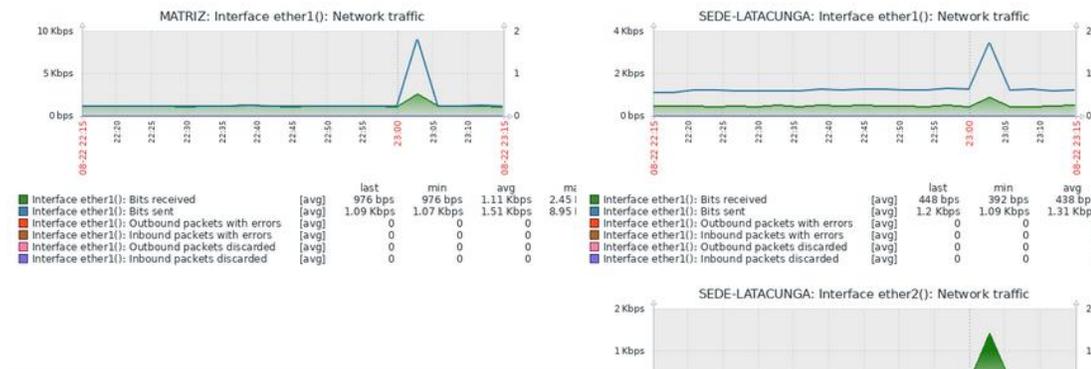
*Configuración de graph*



*Nota.* El gráfico representa la configuración de graph Edificio-M interfaces.

**Figura 86**

*Verificación de Screen*



*Nota.* El gráfico representa la verificación de los screen añadidos con sus gráficos y datos.

### 3.4.1.11 Creación de notificaciones por Gmail

Ahora en administración dirigirse a media types para editar en email el correo electrónico de Gmail que se va a utilizar, cambiar el puerto de SMTP server y en SMTP email agregar un correo de Gmail `wampujami@gmail.com` y en username agregar nuevamente el correo junto con la contraseña, actualizar para guardar las configuraciones.

**Figura 87**

*Interfaz Media types*

*Nota.* El gráfico representa la confirmación de gmail para la administración de la red.

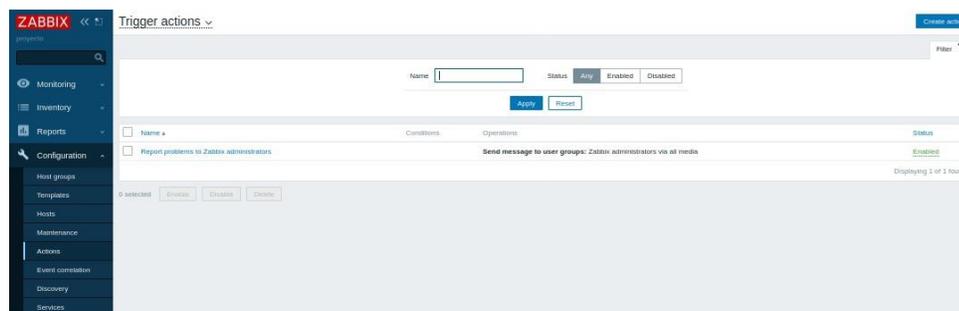
### 3.4.1.12 Habilitación trigger actions

En configuración en la pestaña actions en la parte derecha de la interfaz el estado del envío de mensaje el cual esta desactivado y activar dando clic en disable. En la pestaña

de user settings dar clic en media y añadir el correo de gmail que se agrago anteriormente y ahí se enviaran las notificaciones del servidor web de zabbix y actualizar para añadir.

## Figura 88

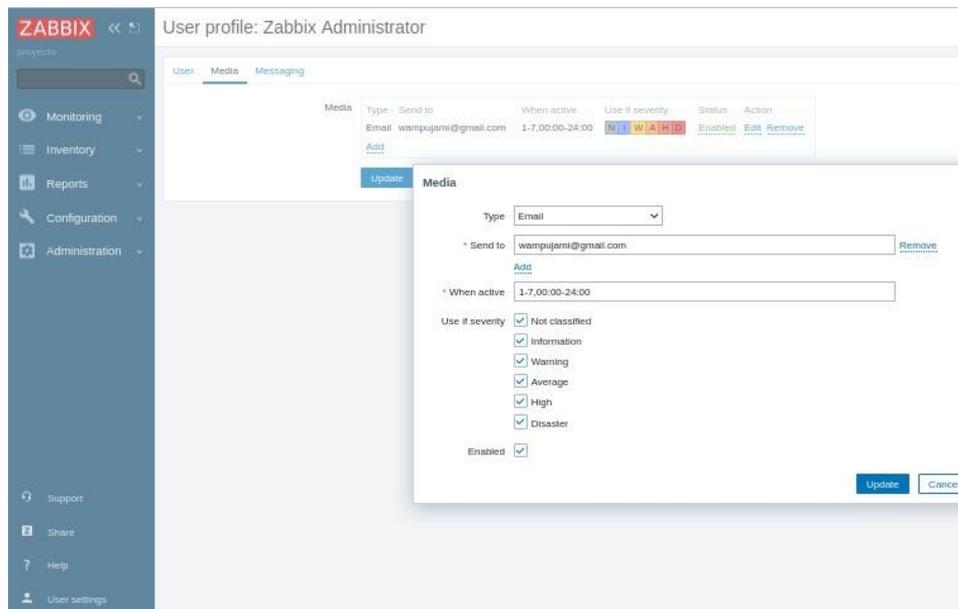
*Interfaz de habilitación de correo*



*Nota.* El gráfico representa la habilitación del envío de mensajes.

## Figura 89

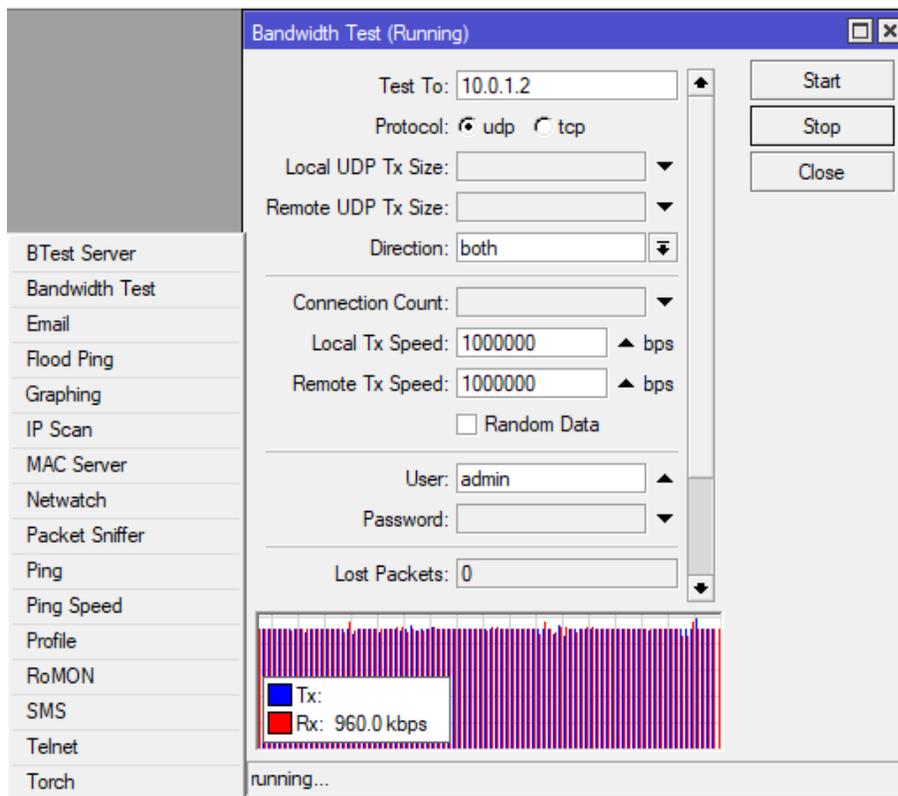
User profile: Zabbix Administrator



*Nota.* El gráfico representa la configuración de Gmail el cual recibirá las notificaciones del servidor web.

### 3.4.1.13 Configuración de tráfico de red

En la herramienta de red winbox acceder al bandwidth test para agregar el ancho de banda 1M para ocasionar tráfico en la dirección ip 10.0.1.2 de sede Latacunga y se visualizó mediante las gráficas el incremento de ancho de banda de 970 kbps.

**Figura 90***Bandwidth test (Running)*

*Nota.* El gráfico representa la configuración del ancho de banda para ocasionar el tráfico de red.

**Figura 91**

Verificación de tráfico de red



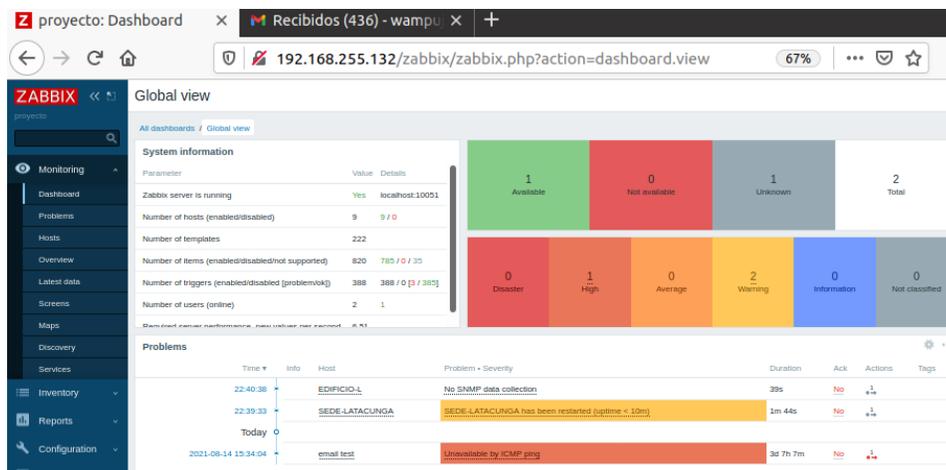
*Nota.* El gráfico representa el tráfico de red de 970 kbps en sede Latacunga.

### 3.4.1.14 Comprobación de notificaciones por Gmail

En el dashboard 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 correo electrónico de Gmail agregado.

## Figura 92

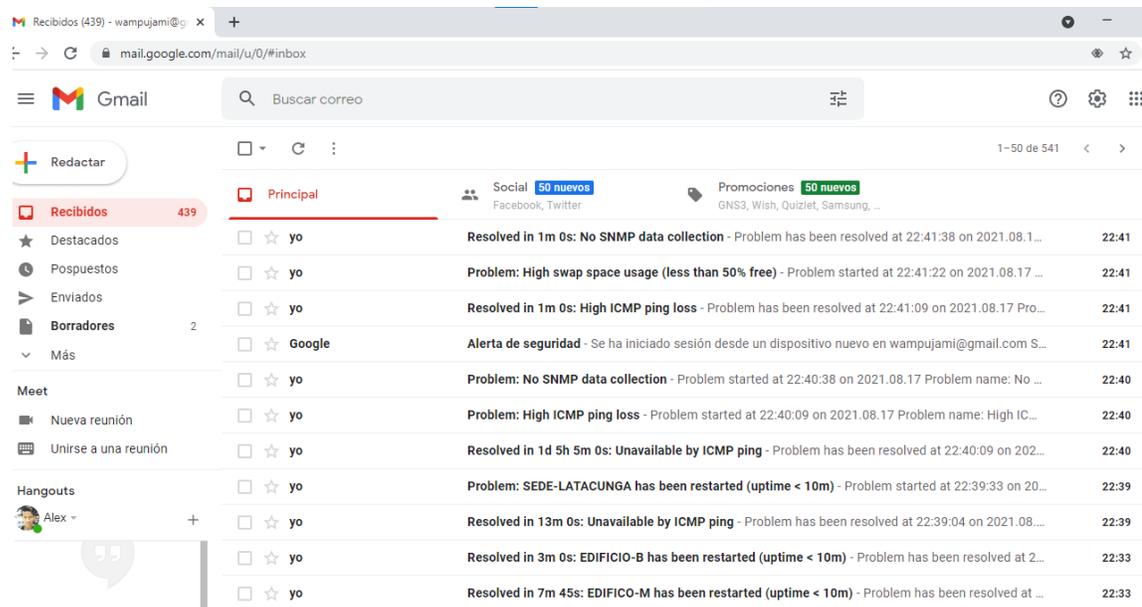
### Dashboard



*Nota.* El gráfico representa las notificaciones de los errores que se presentan en el servidor Zabbix.

## Figura 93

### Gmail



*Nota.* El gráfico representa las notificaciones del problema de activación del protocolo SNMP.

## 3.5 Implementación del servidor Zabbix en las computadoras del laboratorio de comunicaciones de la ESPEL

### 3.5.1 Características de la computadora

Sistema Operativo: Windows 7 Professional 64 bits

Procesador: Intel Core i7-4770 CPU @ 3.40GHz

Memoria: 4096MB RAM

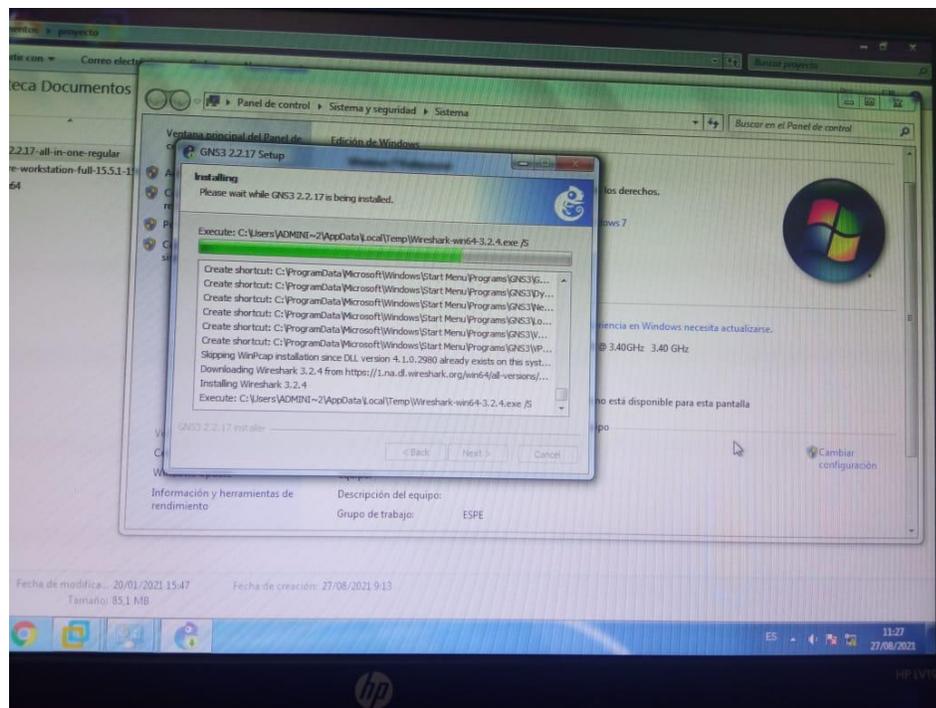
Espacio del disco local C: 265 GB

### 3.5.1.1 Instalación de los simuladores GNS3, VMware

Se procedió a instalar los simuladores para luego abrir las exportaciones realizadas del gns3vm, la red corporativa y la máquina virtual Ubuntu y comenzar con el monitoreo de red.

**Figura 94**

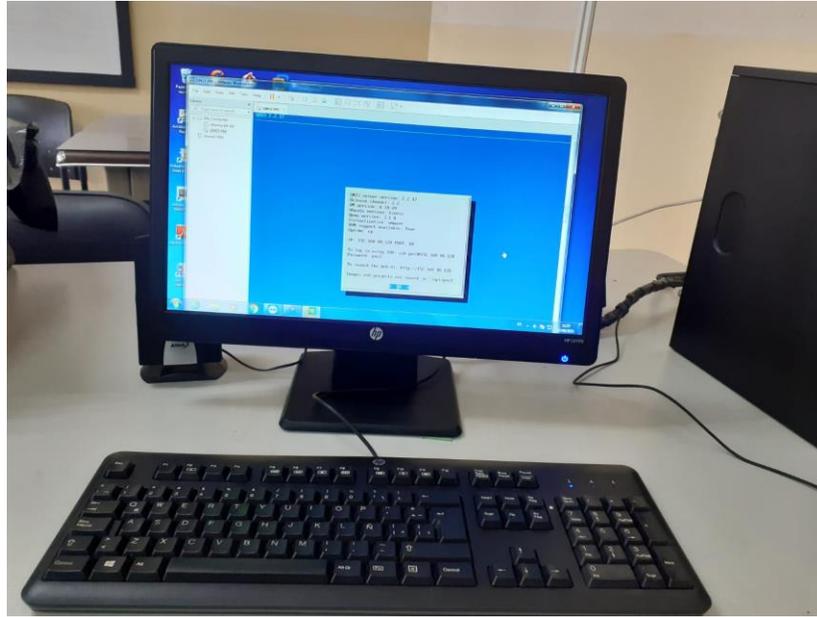
*Instalación de GNS3*



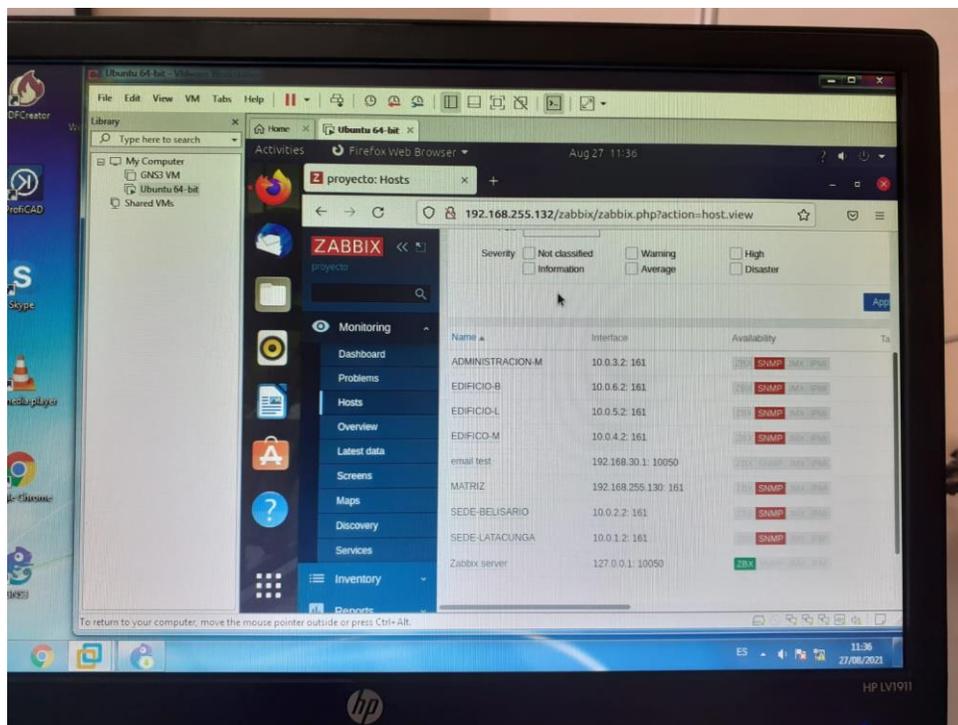
*Nota.* El gráfico representa la instalación de GNS3 en la computadora del laboratorio.

**Figura 95**

*Instalación de VMware Workstation*



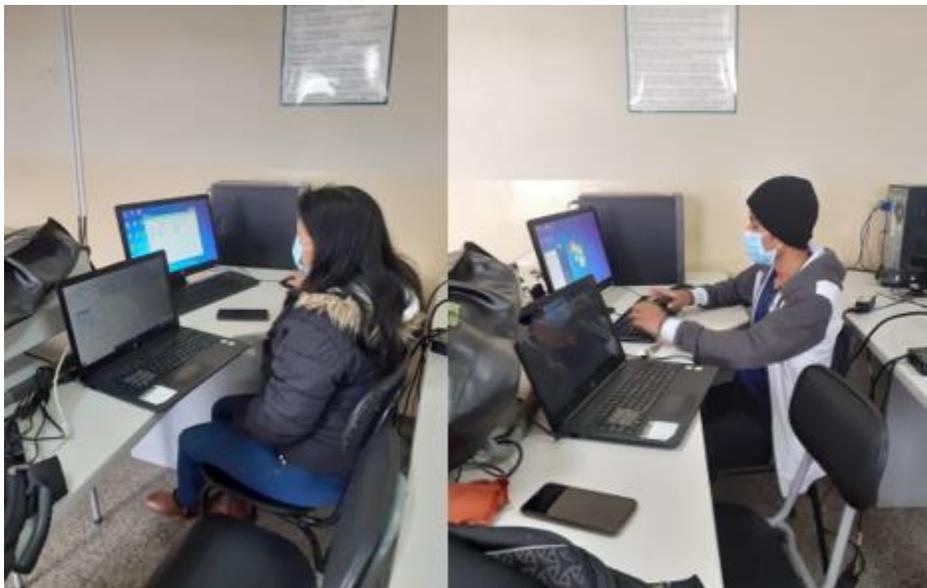
*Nota.* El gráfico representa la instalación de VMware Workstation 15.5.

**Figura 96***Interfaz web de Zabbix*

*Nota.* El gráfico representa el panel de control de Zabbix en la máquina virtual Ubuntu.

**Figura 97**

*Instalación en el laboratorio*



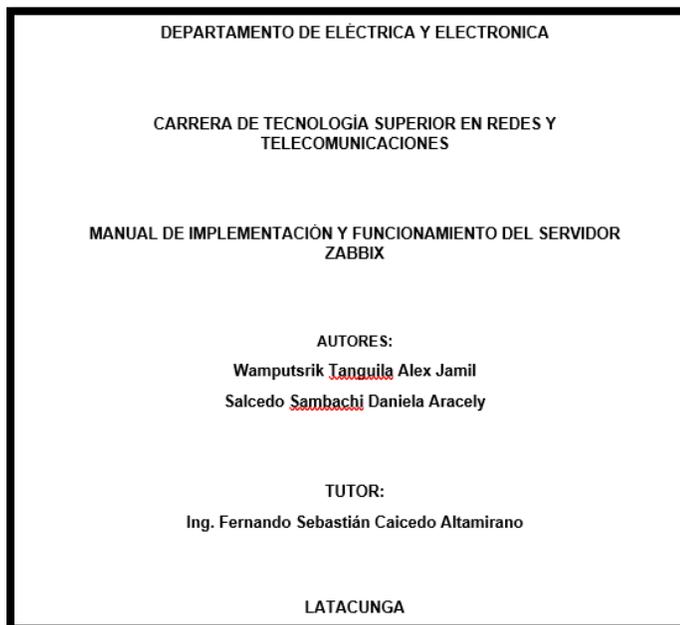
*Nota.* Este gráfico representa la implementación del servidor en las computadoras del laboratorio de comunicaciones de la ESPEL.

### **3.6 Implementación del manual del servidor Zabbix y guía de laboratorio de la administración de red**

Se realizó el manual de implementación donde muestra los pasos a seguir para llevar a cabo la instalación de la máquina virtual ubuntu en el software VMware, el servidor zabbix en la terminal de Ubuntu, la interfaz web del servidor en el navegador firefox y el funcionamiento de los componentes de la interfaz del servidor web Zabbix, el cual se encuentra en Anexo 1. Además se realizó una guía que mostrará paso a paso las diferentes configuraciones a realizarse para el monitoreo de la red corporativa simulada, lo cual constará con la activación del protocolo SNMP, creación de host, screens, maps, notificación por Gmail y todo lo necesario para llevar a cabo la administración de la red, el cual se encuentra en Anexo 2.

**Figura 98**

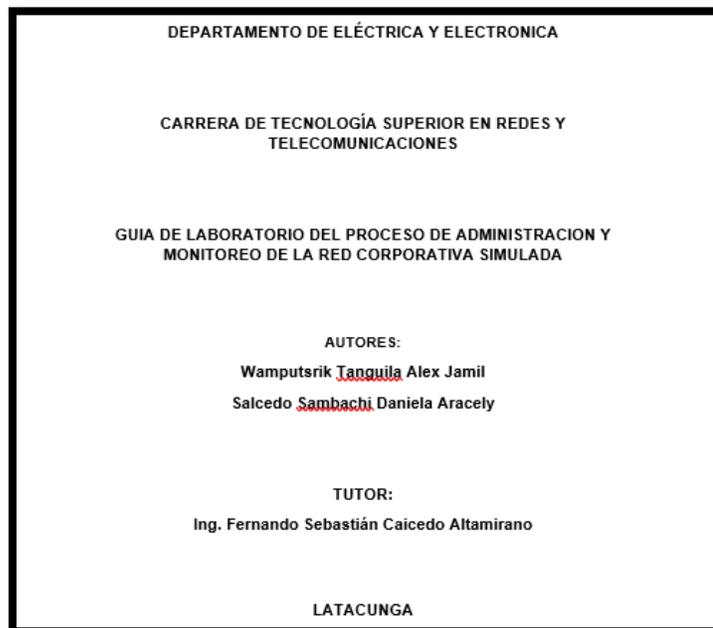
*Manual de implementación*



*Nota.* El gráfico representa el manual de implementación del servidor web Zabbix.

**Figura 99**

*Guía de laboratorio de administración de red*



*Nota.* El gráfico representa la guía del laboratorio de monitoreo y administración de la red corporativa.

## Capítulo IV

### 4 Conclusiones y recomendaciones

#### 4.1 Conclusiones

- Se realizó las investigaciones sobre el servidor Zabbix y se concluyó que sirve para monitorear y administrar el estado de diferentes equipos de red como servidores, hardware de red y aplicaciones, su implementación se llevó a cabo en la máquina virtual Ubuntu 20.04 exitosamente. Para administrar el equipo de red se habilita el agente SNMP.
- Se implementó una red corporativa con tres sitios remotos utilizando RouterOS de Mikrotik donde se hizo las configuraciones básicas para tener conexión entre toda la red, se aplicó el enrutamiento OSPF se realizó la conexión VPN mediante el túnel IPSEC entre sede Latacunga y sede Belisario.
- Se implementó el servidor web Zabbix en la computadora del laboratorio de comunicaciones de la ESPEL el cual será útil para la impartición de clases a los estudiantes ya que podrán realizar las prácticas de monitoreo y administración de red.
- Se realizó un manual de instalación y del funcionamiento principal del servidor web Zabbix detallando paso a paso su instalación en la máquina virtual Ubuntu, además se realizó una guía del laboratorio para administrar la red corporativa simulada y se pudo verificar los equipos que estas siendo monitoreadas.

## 4.2 Recomendaciones

- Se recomienda investigar bien sobre la implementación del servidor web Zabbix ya que al momento de instalar la última versión del servidor Zabbix no son compatibles con la máquina virtual o vienen con errores internos.
- Se recomienda realizar una tabla de enrutamiento de todas las direcciones de ip utilizadas en la red corporativa para identificar cada uno de los dispositivos de red y saber arreglar el problema de fallos de conectividad que se presente en la red sabiendo el direccionamiento de ip.
- Se recomienda revisar las características de las computadoras en las que se va a instalar todos los simuladores para que funcionen de manera correcta sin ningún problema, ya que para correr todos los programas la máquina virtual se queda con lag por falta de recursos en el equipo.
- Se recomienda tener en cuenta todos los requerimientos técnicos que el servidor Zabbix necesita para que funcione de manera correcta ya que el uso de la memoria dependerá de los hosts o parámetros que se vayan a monitorizar en el servidor.

## Bibliografía

- WORDPRESS. (26 de Julio de 2018). *Interpolados*. Recuperado el 18 de Agosto de 2021, de <https://interpolados.wordpress.com/2018/07/26/monitoreo-de-redes/>
- Anrrango, R. (27 de Agosto de 2020). *Configurar Mikrotik, Wireless*. Recuperado el 30 de Junio de 2021, de <https://configurarmikrotikwireless.com/blog/mikrotik-routeros-para-que-sirve.html>
- Aquino, J., & Martínez, K. (2017). *Manual de Instalación, Configuración de un Sistema de Gestión y Monitoreo de Redes*. Recuperado el 05 de Julio de 2021, de <http://biblioteca.utec.edu.sv/siab/virtual/tesis/941001022.pdf>
- Artica. (2021). *PANDORA FMS*. Recuperado el 10 de Julio de 2021, de <https://artica.es/pandorafms/>
- Blogspot. (15 de Julio de 2012). *Simuladores de redes*. Recuperado el 18 de Agosto de 2021, de <https://simuladoresredes.blogspot.com/2012/07/algunos-simuladores-de-redes.html#comment-form>
- Bravo, K. (Diciembre de 2014). *Repositorio Espe*. Recuperado el 07 de Julio de 2021, de <http://repositorio.espe.edu.ec/xmlui/handle/21000/9210>
- Cárdenas, A. (27 de Junio de 2017). *Sistema de monitoreo ZABBIX*. Recuperado el 05 de Julio de 2021, de <http://repositorio.ug.edu.ec/bitstream/redug/19823/1/B-CINT-PTG.169%20Cardenas%20Freire%20Anny%20Ivonne.pdf>
- Cardenas, A. (2017). *Zabbix sistema de monitoreo*. Recuperado el 29 de Junio de 2021, de <http://repositorio.ug.edu.ec/bitstream/redug/19823/1/B-CINT-PTG.169%20Cardenas%20Freire%20Anny%20Ivonne.pdf>
- CMM. (9 de Enero de 2021). *CMM Benchmark*. Recuperado el 5 de Julio de 2021, de <https://es.ccm.net/contents/257-tipos-de-redes>
- Digital Guide . (5 de Marzo de 2019). *IONOS* . Recuperado el 8 de Julio de 2021, de <https://www.ionos.es/digitalguide/servidores/know-how/que-es-el-protocolo-icmp-y-como-funciona/>
- Fernández, A. (2018). *Estudio e implementación de un entorno de gestión para la red privada del laboratorio docente de telemática*. Cantabria. Recuperado el 20 de Junio de 2021, de <https://repositorio.unican.es/xmlui/bitstream/handle/10902/14184/409473.pdf?sequence=1&isAllowed=y>
- Flores, I. (Abril de 2015). *Wix*. Recuperado el 30 de Junio de 2021, de <https://mejiafloresitzel.wixsite.com/dreamweaver/single-post/2015/05/04/qu%C3%A9-son-sitios-remotos-en-dreamweaver>

- Hernandez, J. (19 de Octubre de 2020). *Weebly*. Recuperado el 29 de Junio de 2021, de Weebly: [http://911-ubuntu.weebly.com/zabbix\\_como\\_funciona/conoce-la-estructura-de-zabbix-y-como-usarlo](http://911-ubuntu.weebly.com/zabbix_como_funciona/conoce-la-estructura-de-zabbix-y-como-usarlo)
- Hernandez, J. E. (7 de Febrero de 2021). *Cosysco*. Recuperado el 18 de Agosto de 2021, de [http://911-ubuntu.weebly.com/zabbix\\_como\\_funciona/conoce-la-estructura-de-zabbix-y-como-usarlo](http://911-ubuntu.weebly.com/zabbix_como_funciona/conoce-la-estructura-de-zabbix-y-como-usarlo)
- Hernandez, J. E. (7 de Febrero de 2021). *Cosysco*. Recuperado el 20 de Junio de 2021, de Estructura de zabbix: [http://911-ubuntu.weebly.com/zabbix\\_como\\_funciona/conoce-la-estructura-de-zabbix-y-como-usarlo](http://911-ubuntu.weebly.com/zabbix_como_funciona/conoce-la-estructura-de-zabbix-y-como-usarlo)
- IBM. (2015). *OSPF (Open Shortest Path First)*. Recuperado el 28 de Junio de 2021, de <https://www.ibm.com/docs/es/i/7.3?topic=routing-open-shortest-path-first>
- Interpolados. (26 de Julio de 2018). *Blog de wordpress.com*. Recuperado el 29 de Junio de 2021, de <https://interpolados.wordpress.com/2018/07/26/definicion-y-objetivos-de-la-administracion-de-redes/>
- Mardones, J. (2014). *Implementación de plataforma de monitoreo Zabbix para sistemas de telecomunicaciones Telsur*. Valdivia. Recuperado el 23 de Junio de 2021, de <http://cybertesis.uach.cl/tesis/uach/2014/bmfci.41i/doc/bmfci.41i.pdf>
- OnyxSystems. (2016). *OnyxSystem*. Recuperado el 29 de Junio de 2021, de <https://www.onyxsystems.es/que-es-un-servidor.html>
- Open IT Networks. (29 de Julio de 2021). *Nagios*. Recuperado el 5 de Agosto de 2021, de <https://www.openitnet.com/index.php/software/nagios/nagios-xi>
- Pandora FMS. (17 de Julio de 2017). *Administracion de redes*. Recuperado el 8 de Julio de 2021, de <https://pandorafms.com/blog/es/administracion-de-redes/#:~:text=Administraci%C3%B3n%20de%20redes%3A%205%20pasos%20para%20asegurar%20el,cliente.%205%20Revisa%20y%20eval%C3%BAa%20de%20manera%20continua>
- PANDORA FMS. (16 de Mayo de 2019). *PANDORAFMS.COM*. Recuperado el 8 de Julio de 2021, de <https://pandorafms.com/blog/es/protocolos-de-administracion-de-redes/>
- PANDORAFMS. (17 de Agosto de 2020). *Herramienta de monitorización*. Recuperado el 10 de Agosto de 2021, de <https://pandorafms.com/blog/es/monitorizacion-de-red/>
- Petruti, C.-M. (2018). Solución de gestión automática en la nube utilizando Zabbix. *IEEE*, 2. doi:10.1109 / ROEDUNET.2018.8514142
- Programerclick. (2020). *Sistema de monitoreo Zabbix*. Recuperado el 25 de Junio de 2021, de <https://programerclick.com/article/36601455850/>
- Programmerclick.com. (2021). *Programador click*. Recuperado el 29 de Junio de 2021, de <https://programerclick.com/article/26201210521/>

- Ramirez, I. (29 de Enero de 2020). *Xataka*. Recuperado el 25 de Julio de 2021, de <https://www.xataka.com/basics/que-es-una-conexion-vpn-para-que-sirve-y-que-ventajas-tiene>
- Red had . (2021). *Virtualizacion* . Recuperado el 19 de Agosto de 2021, de <https://www.redhat.com/es/topics/virtualization/what-is-a-virtual-machine>
- RedUsers. (2021). *Copyright RedUsers*. Recuperado el 5 de Julio de 2021, de <https://www.redusers.com/noticias/que-es-una-red-informatica/>
- Rejón, J. (14 de Mayo de 2019). *munro telematico*. Recuperado el 30 de Junio de 2021, de <https://www.mundotelematico.com/simulador-de-red-gns3/>
- Robledo, J. C. (26 de Febrero de 2021). *NORTH NETWORKS*. Recuperado el 20 de Julio de 2021, de <https://www.north-networks.com/que-es-nagios/>
- Rodrigo, A. (22 de Marzo de 2021). *MikrotikWireless*. Recuperado el 10 de Julio de 2021, de <https://configurarmikrotikwireless.com/blog/conceptos-winbox-configurar-mikrotik.html>
- Romero, D. (20 de Abril de 2018). *Institutowisp*. Recuperado el 19 de Agosto de 2021, de <https://institutowisp.com/conceptos-basicos-sobre-mikrotik-que-todo-operador-de-telecomunicaciones-debe-conocer/>
- Rouse, M. (2021). *TechTarget*. Recuperado el 8 de Julio de 2021, de <https://searchdatacenter.techtarget.com/es/definicion/Topologia-de-red>
- Sites. (2018). *Redes de computadoras*. Recuperado el 5 de Julio de 2021, de <https://sites.google.com/site/haymepicounaiguanaverde/tipos-de-redes>
- Telecomunicaciones. (17 de Septiembre de 2016). *Red corporativa*. Recuperado el 29 de Junio de 2021, de <https://glosarios.servidor-alicante.com/telecomunicaciones/red-corporativa>
- Tokio New School. (2021). *Tokio*. Recuperado el 25 de Junio de 2021, de <https://www.tokioschool.com/noticias/caracteristicas-principales-monitoreo-red/>
- vpnMentor. (2021). *VPN*. Recuperado el 29 de Julio de 2021, de <https://es.vpnmentor.com/blog/diferentes-tipos-de-vpn-y-cuando-usarlas/#section-8>
- WebsDirect. (s.f.).
- WebsDirect. (2016). *Tecnosas*. Recuperado el 18 de Julio de 2021, de <https://www.tecnosas.es/que-es-vmware-y-para-que-sirve/>
- WirelessNetwork. (2015). *Romon router management*. Recuperado el 25 de Julio de 2021, de <https://tvoip.ca/romon-router-management-overlay-network/>
- Zabbix. (2021). *Documentación Zabbix*. Recuperado el 20 de Agosto de 2021, de <https://www.zabbix.com/documentation/current/manual/definitions>

Zoho corp. (2021). *ManageEngine*. Recuperado el 25 de Junio de 2021, de <https://www.manageengine.com/es/network-monitoring/network-management.html>

## **Anexos**