Universidad Nacional de Loja

Facultad de la Energía, las Industrias y los Recursos Naturales no Renovables

Carrera de Ingeniería en Sistemas

Implementación de un Sistema de Administración de Red (NMS) para los clientes ISP de la empresa Red Nueva Conexión

Implementation of a Network Management System (NMS) for the ISP clients of the company Red Nueva Conexión

Trabajo de Titulación previo a la obtención del título de Ingeniero en Sistemas

AUTOR:

Ruben Dario Lozano Lozano

DIRECTOR:

Ing. Mario Enrique Cueva Hurtado Mg. Sc.

Loja – Ecuador

2023

Certificación

Loja, 07 de septiembre de 2023

Ing. Mario Enrique Cueva Hurtado Mg. Sc.
DIRECTOR DE TRABAJO DE TITULACIÓN

CERTIFICO:

Que he revisado y orientado todo el proceso de elaboración del Trabajo Titulación denominado: **Implementación de un Sistema de Administración de Red (NMS) para los clientes ISP de la empresa Red Nueva Conexión**, previo a la obtención del título de **Ingeniero en Sistemas**, de la autoría del estudiante **Ruben Dario Lozano Lozano**, con **cédula de identidad** Nro.**1900826569**, una vez que el trabajo cumple con todos los requisitos exigidos por la Universidad Nacional de Loja, para el efecto, autorizo la presentación del mismo para su respectiva sustentación y defensa.

Firmado digitalmente
por MARIO ENRIQUE
CUEVA HURTADO

Ing. Mario Enrique Cueva Hurtado Mg. Sc.
DIRECTOR DE TRABAJO DE TITULACIÓN

Autoría

Yo, **Ruben Dario Lozano Lozano**, declaro ser autor del presente Trabajo de Titulación denominado: **Implementación de un Sistema de Administración de Red (NMS) para los clientes ISP de la empresa Red Nueva Conexión**, y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos, de posibles reclamos y acciones legales, por el contenido del mismo. Adicionalmente acepto y autorizo a la Universidad Nacional de Loja la publicación de mi Trabajo de Titulación, en el Repositorio Digital Institucional – Biblioteca Virtual.

Firma: Firmado electrónicamente por: RUBEN DARIO LOZANO LOZANO

Cédula de identidad: 1900826569

Fecha: 21 de septiembre de 2023

Correo electrónico: rdlozanol@unl.edu.ec

Teléfono: +593 98 905 5780

Carta de Autorización por parte del autor, para consulta, reproducción parcial o total y/o, publicación electrónica del texto completo, del Trabajo de Titulación.

Yo, **Ruben Dario Lozano Lozano**, declaro ser autor del Trabajo de Titulación denominado: **Implementación de un Sistema de Administración de Red (NMS) para los clientes ISP de la empresa Red Nueva Conexión**, como requisito para optar por el título de **Ingeniero en Sistemas**, autorizo al sistema Bibliotecario de la Universidad Nacional de Loja para que, con fines académicos, muestre la producción intelectual de la Universidad, a través de la visibilidad de su contenido en el Repositorio Institucional.

Los usuarios pueden consultar el contenido de este trabajo en el Repositorio Digital Institucional, en las redes de información del país y del exterior, con las cuales tenga convenio la Universidad.

La Universidad Nacional de Loja, no se responsabiliza por plagio o copia del Trabajo de Titulación que realice un tercero.

Para constancia de esta autorización, en la ciudad de Loja, a los veintiún días del mes de septiembre de dos mil veintitrés.

Firma: 

Autor: Ruben Dario Lozano Lozano

Cédula de identidad: 1900826569

Dirección: Loja, Pedro Vicente Maldonado y Francisco de Caldas

Correo electrónico: rdlozanol@unl.edu.ec

Teléfono: +593 98 905 5780

DATOS COMPLEMENTARIOS:

Director del Trabajo de Titulación: Ing. Mario Enrique Cueva Hurtado Mg. Sc.

Dedicatoria

A ti mamá, por tu apoyo incondicional.

Ruben Dario Lozano Lozano

Agradecimiento

Agradezco a Dios por permitirme culminar esta etapa de mi vida profesional.

A mi madre por ser mi pilar fundamental en mi vida, a mis hermanas por su apoyo y consejos en este proceso.

A mi director de Trabajo de Titulación Ing. Mario Cueva por su excelente asesoría y guía durante el desarrollo de la presente investigación.

Finalmente, mi profundo agradecimiento a la planta docente de la carrera de Ingeniería en Sistemas de la Universidad Nacional de Loja, por impartir sus conocimientos durante esta etapa.

Ruben Dario Lozano Lozano

Índice de contenidos

Índice de Tablas:

Índice de Figuras:

Índice de Anexos:

1. Título

Implementación de un Sistema de Administración de Red (NMS) para los clientes ISP de la empresa Red Nueva Conexión

2. Resumen

En la actualidad, conocer la disponibilidad de los equipos de Telecomunicaciones es un componente importante, más aún cuando se trata de Proveedores de Servicio de Internet (ISP). La empresa “Red Nueva Conexión” brinda servicios de soporte técnico y consultoría de telecomunicaciones, actualmente administra la red de borde de 35 ISP, por lo que debe conocer los problemas o inconvenientes que surjan en los dispositivos de borde de los ISP. Los problemas de red de estas 35 empresas han sido reportados a través de llamadas telefónicas por el personal técnico de cada ISP, para lo cual se creaba un ticket para recibir atención posteriormente. Por tal razón surge la necesidad de implementar un sistema de Administración de Red (NMS) para los clientes ISP que permita monitorear y alertar los incidentes ocurridos en los 35 ISP al personal de TI de forma oportuna. Para cumplir con este objetivo se consideraron 3 fases. En la primera se realizó el análisis de tres soluciones NMS Open Source; en la segunda se configuró el Sistema de Administración de Red y los agentes en los equipos de los ISP y en la tercera se verificó el funcionamiento del NMS. Para el desarrollo de este trabajo se analizaron tres herramientas NMS Open Source, seleccionando a Zabbix como NMS por su escalabilidad y adaptabilidad; Zabbix monitorea 100 dispositivos Mikrotik que componen la infraestructura de los 35 Proveedores de Servicios de Internet (ISP). Para ello se utilizó la plantilla Mikrotik SNMP compuesta por 19 ítems de monitoreo y 10 disparadores (triggers) preconfigurados que establecen puntos de referencia específicos para la generación de alertas que indican la severidad (alta, media, advertencia e informativa). Se monitoreó los dispositivos durante los meses de junio y julio, registrando 9114 eventos. Los ISP con mayores problemas de red fueron Flashnet y Yaneznet recibiendo alertas altas (60) como “ping indisponible por ICMP” y alertas medias (151) de “Enlace Caído” respectivamente. Estas notificaciones fueron enviadas en tiempo real mediante correo electrónico y un bot de Telegram configurado para la comunicación; lo que permitió a los administradores de red identificar el equipo afectado, determinar cuándo comenzó el problema y evaluar su gravedad; reduciendo el tiempo de detección de incidentes y mejorando así la atención hacia cada ISP personalizada.

Palabras Clave: *Open Source, SNMP, monitoreo, Zabbix*

2.1. Abstract

Nowadays, knowing the availability of telecommunications equipment is a relevant component, even more so when dealing with Internet Service Providers (ISPs); the company "Red Nueva Conexión" provides technical support and telecommunications consulting services and currently manages the edge network of 35 ISPs, so it must know the problems or inconveniences that arise in the ISP's edge devices, we reported the network problems of these 35 companies through phone calls by the technical staff of each ISP, for which we created a ticket to receive attention later. For this reason, the need arose to implement a Network Management System (NMS) for ISP clients that would allow monitoring and alerting IT personnel of incidents occurring in the 35 ISPs opportunely. To meet this objective, we considered 3 phases. In the first phase, we analyzed three open-source NMS solutions; in the second phase, we configured the Network Management System and agents in the ISP equipment; and in the third phase, we verified the operation of the NMS for the development of this work, we analyzed three Open Source NMS tools, selecting Zabbix as the NMS for its scalability and adaptability; Zabbix monitors 100 Mikrotik devices that make up the infrastructure of the 35 Internet Service Providers (ISPs). For this purpose, we used the Mikrotik SNMP template, consisting of 19 monitoring items and 10 preconfigured triggers that set specific benchmarks to generate alerts indicating severity (high, medium, warning, and informative); we kept track of the devices during June and July by recording 9114 events. The ISPs with the most network problems were Flashnet and Yaneznet, receiving high alerts (60) as "ping unavailable by ICMP" and medium alerts (151) as "Link Down", respectively; we sent these notifications in real-time via email and a Telegram bot configured for communication; allowing network administrators to identify the affected equipment, determine when the problem started and assess its severity; reducing incident detection time and thus improving the attention towards each personalized ISP.

Keywords: *Open Source, SNMP, monitoring, Zabbix*

3. Introducción

En los últimos años, el crecimiento acelerado de las redes de telecomunicaciones ha transformado la forma de comunicarse y acceder a la información. Sin embargo, este avance tecnológico ha venido acompañado de un desafío igualmente significativo; la complejidad en la administración de estas grandes redes. Según la agenda de transformación digital 2022-2025 [1], fomentar la introducción de soluciones tecnológicas de hardware y software es un factor clave en la automatización de procesos. La importancia de mantener los servicios de telecomunicaciones siempre disponibles se ha vuelto fundamental en un mundo donde la conectividad es parte de la vida cotidiana.

Los proveedores de servicio de Internet aprovisionan del servicio a la población urbana y rural de las distintas ciudades del Ecuador. Por ello es primordial el monitoreo y la administración de redes para asegurar el funcionamiento y disponibilidad de los servicios que ofrecen. Por lo que surge la siguiente pregunta de investigación. ¿Implementar un Sistema de Administración de Red (NMS) en la empresa “Red Nueva Conexión” permitirá monitorear y alertar los incidentes ocurridos en los 35 ISP al personal de TI de forma oportuna? En base a ello se planteó el siguiente trabajo de titulación que tiene como objetivo principal implementar un sistema de administración de red (NMS) para clientes ISP, utilizando el protocolo SNMP en la empresa “Red Nueva Conexión”. Y con el fin de cumplir este objetivo se plantearon 3 objetivos específicos, el primero “Analizar tres herramientas NMS Open Source para ISP”, el segundo, “Configurar el Sistema de Administración de Red (NMS) y los agentes en los ISP” y finalmente el tercero, “Verificar el funcionamiento del NMS”.

Para el desarrollo del trabajo de Titulación se analizaron tres herramientas Open Source; se seleccionó Zabbix como herramienta NMS, posteriormente se obtuvo la información de la infraestructura de red de los ISP; se instaló el servidor NMS y se configuró el servicio SNMP en los routers Mikrotik de los ISP, habilitando el puerto 161 UDP. Finalmente se verificó el funcionamiento del NMS, con la obtención de las gráficas de monitoreo, además el envío de alertas en tiempo real mediante correo electrónico y Telegram.

El presente Trabajo de Titulación sigue una estructura organizativa que comprende varias secciones esenciales. Comenzando con el Marco Teórico, donde se establecen los fundamentos necesarios para esta investigación, seguidamente de la sección de Metodología, que explica detalladamente el proceso, contexto, recursos y participantes involucrados. Posteriormente se presentan los Resultados con toda la información relevante obtenida en este Trabajo de Titulación, en la sección de Discusión se analizan los resultados obtenidos. Además de las Conclusiones, respaldadas por los hallazgos obtenidos. Finalmente, se indican

las Recomendaciones, con el objetivo de contribuir al conocimiento y a futuras investigaciones en el área de estudio.

4. Marco Teórico

4.1. Proveedor de servicios de Internet (ISP)

Los proveedores de servicios de Internet (ISP) son entidades tanto privadas como públicas. Estos entes desempeñan un papel crucial al ofrecer conectividad y acceso a Internet, así como facilitar la interconexión de los usuarios, ya sean particulares o empresas que buscan acceder a la red [2]. Un ISP establece la conexión de sus usuarios a Internet mediante diversas tecnologías, tales como DSL, Cablemódem, GSM, Dial-up, Wifi, Fibra Óptica, entre otras. Además de brindar conectividad, muchos ISP también ofrecen una variedad de servicios relacionados con Internet, como correo electrónico, alojamiento web, registro de dominios y servidores, entre otros [3].

4.2. Administración de redes

La administración de redes es un conjunto de técnicas destinadas a mantener una red operativa, eficiente, segura, constantemente monitoreada y debidamente planificada y documentada. Se trata principalmente de operar, monitorear, mantener y controlar los elementos tecnológicos de una infraestructura para asegurar que funcione de acuerdo con los objetivos de la organización [4].

4.2.1. Administrador de red

Un administrador de redes requiere de la habilidad para supervisar, comprobar, sondear, configurar y controlar los componentes de hardware y software de una red, además las tareas que realiza un administrador dependen del tipo de organización, tamaño, número de usuarios, tipo de red y responsabilidades asignadas [5]. Las principales son:

- Planeación
- Diseño
- Implementación
- Monitoreo
- Respuesta a fallas, seguimiento y solución
- Seguridad física y lógica

4.3. Protocolo Simple de Administración de Red o SNMP

SNMP fue desarrollado para su uso como herramienta de gestión de red e interconexión de redes que operan sobre TCP/IP. Es el protocolo de administración de redes estándar usado en Internet. Este protocolo define la comunicación de un administrador con un agente. Es un

protocolo de gestión de red que permite obtener: información de dispositivos, memoria libre, uso de CPU, detección de errores, establecer alarmas, estado de funcionamiento. SNMP está formado por tres componentes básicos[6].

4.4. Elementos básicos de SNMP (Simple Network Management Protocol)

Para que el NMS se encargue de la gestión de la red y este pueda obtener información de los elementos de la red, es necesario que estos elementos cuenten con un sistema que permita su comunicación con la estación de gestión. Este software se denomina agente [7].

Un sistema de gestión de red está compuesto por [8]:

- **Administrador de SNMP. -** El administrador de SNMP forma parte de un sistema de administración de red (NMS). El administrador de SNMP ejecuta software de administración SNMP.
- **Agentes SNMP (nodo administrado). -** El agente SNMP reside en los clientes de dispositivo de red, como los switches, los routers, los servidores, los firewalls y las estaciones de trabajo, cuentan con un módulo de software de agente SMNP.
- **Base de información de administración (MIB). -** Las MIB almacenan datos sobre el funcionamiento del dispositivo y están diseñadas para estar disponibles para los usuarios remotos autenticados.

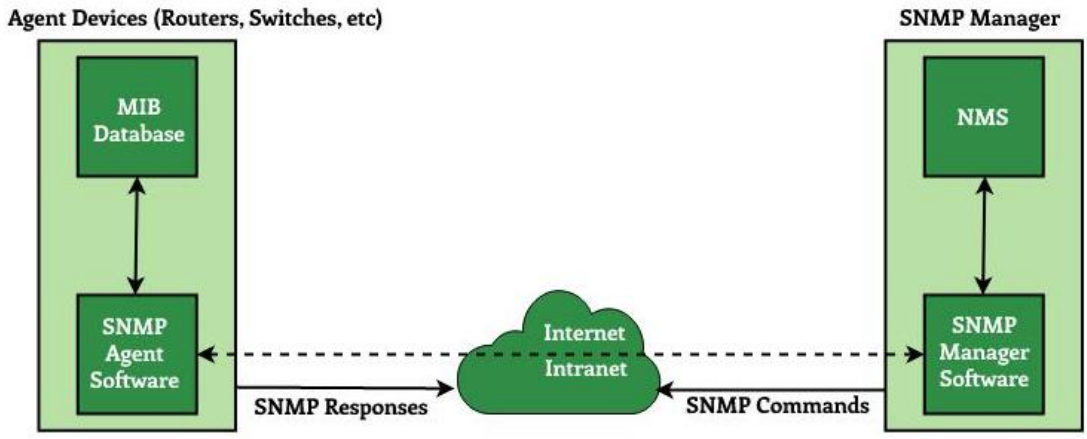


Figura 1. Arquitectura SNMP[9]

4.5. Versiones de SNMP

- **Versión 1:** Surge en el año de 1990 como primera versión, no posee seguridad solo se basa en comunidades.

- **Versión 2:** Se publica 1996 como un nuevo estándar. Los cambios fundamentalmente son la mejora de las prestaciones de intercambio de información de gestión y la implementación de seguridad.
- **Versión 3:** Tiene el mismo formato que la versión 2, pero añade una serie de capacidades de seguridad y un marco que hace posible su uso junto con las PDUs de SNMPv2 con mayor seguridad y administración.

4.6. Sistemas de Administración de red (NMS)

Según Stalling [6], un sistema de gestión de redes se define como un conjunto de herramientas que permiten supervisar y controlar la red de manera integrada, abarcando tanto el software como el hardware. Su objetivo es lograr que toda la red se presente como una entidad unificada.

Un Sistema de administración de red (NMS) se refiere a una aplicación o conjunto de aplicaciones que brindan a los administradores de red la capacidad de administrar los diferentes componentes de una red. Un NMS permite a los administradores operar, monitorear, mantener y controlar los elementos tecnológicos de una red para garantizar que funcione según lo diseñado y de acuerdo con los objetivos de la organización [10].

4.7. Herramientas de NMS Open Source más populares

4.7.1. Cacti

Cacti está diseñado para ser una solución gráfica completa basada en el marco de RRDtool a su vez Cacti está bajo la licencia GNU GPL [11]. Su objetivo es facilitar el trabajo de un administrador de red al ocuparse de todos los detalles necesarios para crear gráficos significativos. Esta solución recopila datos a través de múltiples métodos y crea plantillas con gráficos avanzados con los que podrás obtener reportes visuales de datos como: temperatura, velocidad, voltaje, número de impresiones, etc.

A continuación, se detalla las características principales:

1. **Recopilación de datos:** Utiliza el protocolo SNMP (Simple Network Management Protocol) para recopilar datos de los dispositivos de red. Puede monitorear una amplia gama de métricas, como ancho de banda, uso de CPU, memoria, tráfico de red, entre otros.
2. **Gráficos y visualización:** Una de las principales fortalezas es su capacidad para generar gráficos claros y personalizables. Puedes crear gráficos históricos y en tiempo real para

visualizar el rendimiento de los dispositivos de red. Estos gráficos son altamente personalizables y se pueden ajustar según tus necesidades.

3. **Gestión de dispositivos:** Permite administrar y organizar los dispositivos de red a monitorear.

4. **Alertas y notificaciones:** Ofrece la capacidad de establecer umbrales y generar alertas cuando los valores monitoreados superan o caen por debajo de ciertos límites. Esto te permite recibir notificaciones y tomar medidas proactivas para solucionar problemas de red.

5. **Personalización:** Es altamente personalizable y extensible en cuanto a plantillas de gráficos y ajustar la apariencia de la interfaz de usuario según las preferencias.

6. **Comunidad:** Tiene una comunidad activa de usuarios que desarrollan complementos para ampliar la funcionalidad.

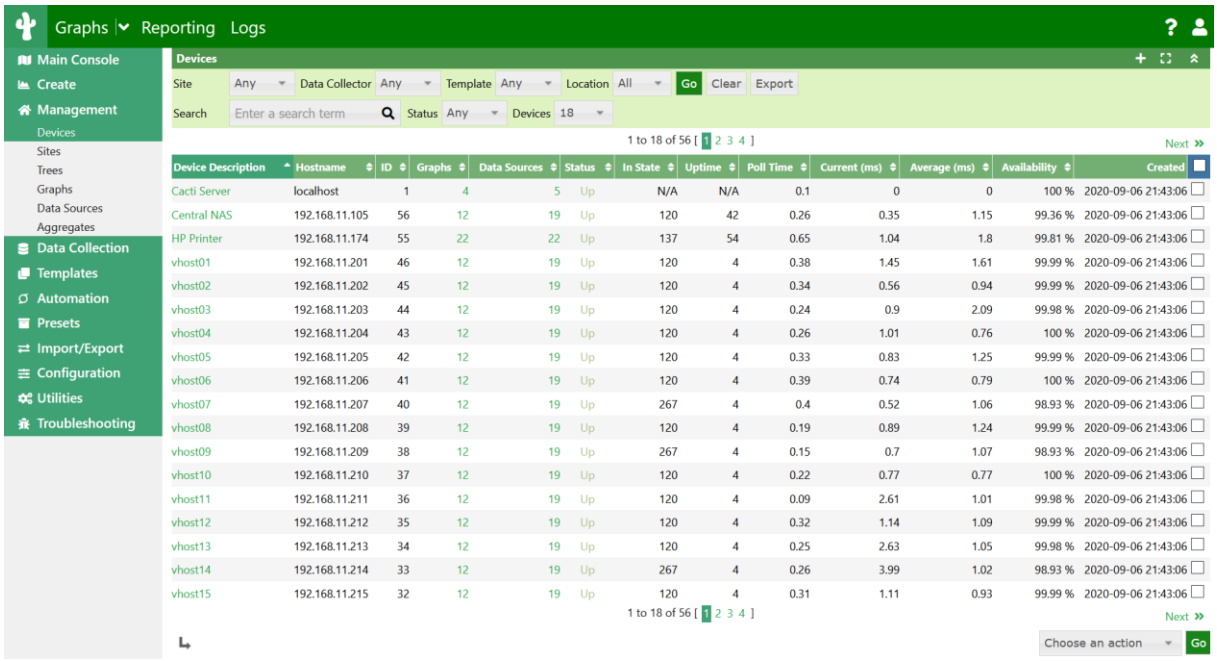


Figura 2. Cacti interfaz web

4.7.2. Nagios Core

Nagios Core es la versión central y original de Nagios, que es una aplicación de monitoreo de red de código abierto y gratuito. Es una herramienta de monitoreo de infraestructura que permite monitorear hardware, software, aplicaciones, servicios de datos, almacenamiento, servicios web, herramientas intercomunicación [12]. De igual manera es un sistema de

monitorización de máquinas y servicios diseñado para ayudar a los administradores a tener siempre el control de su red. Las principales características de Nagios Core son [13]:

1. **Arquitectura:** Se basa en una arquitectura cliente-servidor. El servidor Nagios Core es responsable de realizar el monitoreo y generar alertas, mientras que los clientes (también conocidos como agentes) son los dispositivos o servicios que están siendo monitoreados.
2. **Monitoreo de servicios y hosts:** Permite el monitoreo de servicios y hosts en tiempo real. Además, puede supervisar servicios como HTTP, FTP, SSH, SMTP, así como también el estado general de los hosts.
3. **Configuración flexible:** Utiliza archivos de configuración en formato texto plano para definir hosts, servicios, umbrales de rendimiento, reglas de notificación y otras opciones de monitoreo. Esto proporciona una gran flexibilidad y capacidad de personalización.
4. **Alertas y notificaciones:** Puede enviar alertas y notificaciones cuando se detectan problemas o se superan umbrales de rendimiento. Se pueden configurar reglas de notificación para enviar alertas por correo electrónico, SMS o ejecutar scripts personalizados.
5. **Escalabilidad:** Se puede escalar para adaptarse a entornos pequeños o grandes. Además de se puede configurar una configuración distribuida o utilizar instancias múltiples para monitorear diferentes partes de la infraestructura.
6. **Paneles y gráficos:** Proporciona paneles y gráficos incorporados.
7. **Complementos:** Con el uso de complementos se pueden ampliar la funcionalidad básica de Nagios Core y agregar características adicionales con la versión de pago.
8. **Comunidad:** Tiene una comunidad altamente activa, la cual se encarga del desarrollo de complementos y extensiones, así como de ayuda en foros.

Nagios Core ha sido utilizado durante muchos años como una solución confiable y escalable para el monitoreo de infraestructuras de TI. Aunque Nagios Core proporciona una funcionalidad sólida pero limitada, ya que también existen otras variantes y productos basados en Nagios que ofrecen características adicionales y una interfaz de usuario más moderna, como Nagios XI y Naemon[13].

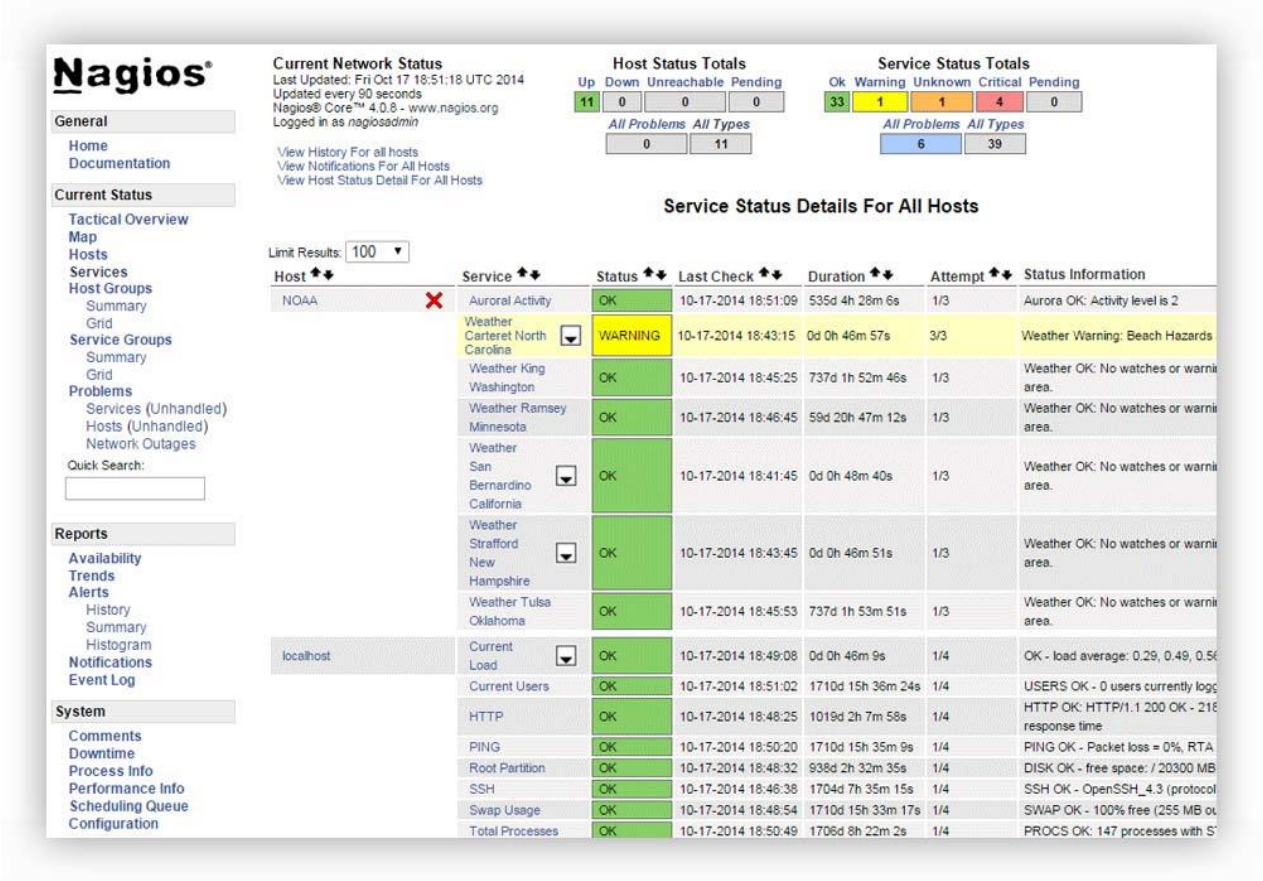


Figura 3. Nagios Core [14]

4.7.3. Zabbix

Zabbix fue creado por Alexei Vladishev, y actualmente está siendo activamente desarrollado y soportado por Zabbix SIA. Zabbix es una solución open source de monitoreo de clase empresarial [15]. Es un software que monitorea numerosos parámetros de una red y de la salud e integridad de distintos dispositivos, utiliza un mecanismo flexible de notificación que permite a los usuarios configurar alertas para cualquier evento. Esto permite una rápida reacción a los problemas de los dispositivos, además ofrece reportes y visualizaciones de los datos de calidad, basados en los datos recolectados y almacenados. También, ofrece características avanzadas de monitoreo, alertas y visualización, que incluso, algunas de las mejores aplicaciones comerciales de este tipo no ofrecen. Algunas de las características comunes de Zabbix incluyen [16]:

1. **Monitoreo integral:** Permite el monitoreo integral de dispositivos, servidores, redes y servicios. Puede supervisar métricas de rendimiento como uso de CPU, memoria, ancho de banda, latencia de red, entre otros.

2. **Recopilación de datos**: Recopila datos utilizando varios métodos, como SNMP, IPMI, JMX, agentes Zabbix o verificaciones de red. Esto permite un monitoreo eficiente y completo de los recursos de la infraestructura.

3. **Alertas y notificaciones:** Zabbix ofrece un sistema de alertas y notificaciones altamente configurable. Puedes establecer umbrales y condiciones para generar alertas y recibir notificaciones a través de diferentes canales, como correo electrónico, SMS o mensajes instantáneos.

4. **Visualización de datos:** Proporciona una interfaz gráfica para visualizar datos de monitoreo en tiempo real y generar informes históricos. También se puede crear gráficos personalizados, paneles de control y mapas de red para tener una visión clara del estado de la infraestructura.

5. **Automatización y escalabilidad:** Es altamente escalable y se puede implementar en entornos pequeños y grandes. Puede gestionar miles de dispositivos y escalar horizontalmente mediante la distribución de tareas en servidores proxy y de front-end.

6. **Configuración flexible:** Ofrece una configuración flexible a través de su interfaz web. También se puede personalizar la configuración de monitoreo, crear plantillas reutilizables y definir acciones personalizadas para eventos específicos.

7. **Seguridad:** Cuenta con funciones de seguridad robustas, como autenticación de usuarios, control de acceso basado en roles y cifrado de datos. Esto ayuda a garantizar la integridad y confidencialidad de los datos de monitoreo.

Figura 4. Zabbix [15]

Zabbix puede desempeñar un papel importante en monitorear la infraestructura de TI, tanto para pequeñas organizaciones con pocos servidores como para grandes empresas con una multitud de servidores.

4.8. Trabajos relacionados

Según [17] en su trabajo de titulación titulado “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 la cual recomienda tener en cuenta todos los requisitos técnicos que el servidor Zabbix necesita para funcionar correctamente porque el uso de memoria dependerá de los hosts o parámetros que se estén monitoreando en el servidor. En este estudio, se simuló la implementación de una red corporativa con tres sitios remotos utilizando RouterOS de Mikrotik.

Milton Intriago [18] señala, que en su investigación realizó una comparativa de siete herramientas NMS de las cuales escogió cuatro para pruebas de implementación, luego de hacer pruebas por cinco días cada sistema para determinar su nivel de cumplimiento con base en parámetros obtenidos en estudios similares. Él plantea que Nagios fue el sistema que se adaptó a las necesidades de la empresa, según los criterios evaluados, además menciona que los sistemas de monitoreo pudieron detectar apagones de varios equipos y niveles elevados de consumo de recursos de hardware en otros, lo que le permitió establecer un plan de mejoras con estrategias para la optimización de la red de datos.

Reyes y Duffaut [19] en su estudio “Influencia del software Zabbix para el monitoreo de infraestructura de TI en la SUNARP Zona Registral N° XI - Sede Ica”, demostraron que el software Zabbix mejoró el tiempo promedio de detección de falla y la disponibilidad operacional, influyendo de manera positiva sobre el monitoreo de la infraestructura de TI de la Zona Registral Nº XI – Sede Ica.

Garcia y Roa [20] en su trabajo “Diseño de una herramienta de monitoreo y control de servidores utilizando como eje principal CACTI. Aplicado a una pyme mediana” implementaron Cacti como herramienta NMS ya que es una herramienta que mantiene un historial del consumo de interfaces de red, la cual facilita por medio de los gráficos detectar los comportamientos anómalos en la red y en los consumos de CPU y memoria RAM de los equipos.

5. Metodología

Para el desarrollo del presente trabajo de titulación se aplicó la investigación tecnológica, y experimental, las cuales permitieron llevar a cabo una investigación objetiva, y de esta manera dar solución a los problemas de "Red Nueva Conexión" con la implementación de un sistema de administración de red (NMS) que le permita estar al tanto de los eventos que ocurren en los equipos de los clientes ISP que se encuentran distribuidos en diferentes ciudades del Ecuador.

5.1. Área de estudio

El presente trabajo de titulación se lo realizó en la Facultad de la Energía las Industrias y los Recursos Naturales No Renovables (FEIRNNR) de la UNL, en la carrera de Ingeniería en Sistemas dentro de su línea de investigación: Redes de Ordenadores y Telecomunicaciones. Además de la colaboración del Ing. Manuel Tandazo CEO de "Red Nueva Conexión", empresa que opera en el cantón Pueblovieo de la provincia de Los Ríos; que brindó las facilidades para el desarrollo del Trabajo de Titulación (Ver Anexo 1), donde se implementó un NMS para alertar de manera oportuna al departamento de TI de "Red Nueva Conexión" los eventos que ocurren en los equipos de borde de los ISP que administra en las diferentes provincias del Ecuador.

5.2. Proceso

El cumplimiento del objetivo general del trabajo de titulación se llevó a cabo a través de un proceso dividido en tres fases, alineadas con los tres objetivos específicos.

Fase 1: Analizar tres herramientas NMS Open Source para ISP

Se realizó un análisis de tres Sistemas de Administración de Red (NMS) Open Source basándose en trabajos relacionados, para determinar la herramienta que se ajusta a la necesidad de la empresa, así como la revisión de los fundamentos teóricos. (Ver sección 6.1.1)

Se realizó una tabla comparativa para seleccionar la herramienta NMS adecuada para la gestión de los equipos de los ISP (Ver sección 6.1.2).

Fase 2: Configurar el sistema de administración de red NMS y los agentes en los ISP

Se obtuvo la información de la infraestructura de los ISP que se va a monitorear (ver la sección 6.2.1).

Se seleccionó el hardware necesario para instalar Zabbix, (Ver la sección 6.2.2.).

Se realizó la instalación y configuración del NMS, bajo la plataforma Ubuntu Server 22.04 en la cual se configuraron los grupos de host correspondientes a cada ISP, (Ver la sección 6.2.3.).

Se realizó la configuración del protocolo SNMP en los dispositivos Mikrotik pertenecientes a cada ISP, configurando la comunidad SNMP y activando el servicio SNMP en los dispositivos, (Ver la sección 6.2.4.).

Fase 3: Verificar el funcionamiento del NMS

Se obtuvo información de los equipos gestionados por en NMS mediante los agentes SNMP. Como: gráficas de consumo de CPU, memoria RAM y ancho de banda de las interfaces WAN (Ver la sección 6.3.1.).

Se configuró las alertas para notificar al personal de TI los eventos que ocurren en los equipos de los ISP (Ver la sección 6.3.2.).

Se creó un manual de usuario para uso de administrador de red indicando las funciones principales del NMS (Ver la sección 6.3.3. y Anexo 8).

5.3. Recursos

5.3.1. Recursos Científicos

Para el desarrollo del Trabajo de Titulación se utilizó los siguientes recursos científicos:

Método Experimental. – este método permitió implementar un sistema de monitoreo de red, en un ambiente real, pues se utilizaron dispositivos en producción de la red de la empresa como enrutadores, conmutadores y servidores, de los ISP.

Método deductivo. – Permitió la comprensión de conceptos en el ámbito de la gestión de redes, la implementación de sistemas de administración de red (NMS) y el uso del protocolo SNMP.

Estudio de casos. - Permitió la investigación sobre el funcionamiento e implementación de los Sistemas Administración de Red, usando el protocolo SNMP para el monitoreo de los dispositivos que conforman la red. Con este conocimiento se pudo determinar el ambiente adecuado para su correcta configuración e implementación.

Revisión y Seguimiento. - Se utilizó para recopilar información relacionada a la aceptación del proyecto, así como la efectividad del mismo al implementarlo en un entorno real.

5.3.2. Recursos Técnicos

Entrevista: permitió obtener los requerimientos para seleccionar la herramienta NMS.

Encuesta: permitió evaluar la satisfacción de los administradores de Red de los ISP, respecto a las notificaciones de los incidentes ocurridos.

5.3.3. Recursos de hardware y software

5.3.3.1. Hardware

Servidor Dell PowerEdge R720: este equipo fue el servidor que proporcionó la Empresa para instalar el NMS.

Laptop Toshiba Satellite C55-B: Fue utilizada para las investigaciones y configuración del servidor.

5.3.3.2. Software

Draw.io: se utilizó para realizar el diagrama de red (NMS y agentes).

Mendeley: se utilizó para la gestión de fuentes bibliográficas.

OpenVPN: permitió establecer una comunicación VPN con la red interna de la empresa Red Nueva Conexión.

MobaXterm: permitió establecer las conexiones SSH con el servidor.

5.4. Participantes

El proyecto de titulación fue ejecutado por Ruben Dario Lozano Lozano, estudiante de la Carrera de Ingeniería en Sistemas, con la dirección del Ing. Mario Enrique Cueva Hurtado, Docente de la Universidad Nacional de Loja, además de la colaboración del Ing. Manuel Ignacio Tandazo Mera, CEO de la empresa “Red Nueva Conexión”.

6. Resultados

Para el desarrollo de este trabajo de titulación, se establecieron tres fases, cada una estuvo definida por un objetivo específico y compuesta por varias actividades que se llevaron a cabo durante el proceso de investigación. Esta metodología permitió la selección e implementación exitosa de un sistema de administración de red (NMS) en la empresa "Red Nueva Conexión". Este sistema fue destinado a la gestión de los equipos pertenecientes a los 35 clientes ISP, con el propósito de monitorear los eventos que acontecen en los dispositivos de estas infraestructuras.

6.1. Objetivo 1: Analizar tres herramientas NMS Open Source para ISP.

En el desarrollo de esta fase fue importante para obtener información relevante y necesaria sobre los sistemas de administración de red utilizados por los ISP. Esto permitió seleccionar el sistema de administración de red (NMS) más adecuado para su implementación en la empresa Red Nueva Conexión. A continuación, se detalla el proceso:

6.1.1. Análisis de tres herramientas NMS Open Source para ISP.

Los sistemas de administración de red también conocidos como NMS son populares entre las pequeñas y grandes empresas, así como en los proveedores de servicio de internet (ISP) ya que permiten centralizar el monitoreo y administración de dispositivos de red, de servidores (Linux, Windows, Unix), enrutadores, conmutadores y de todo aquello que este en la capacidad de intercambiar información en la red, permitiendo reducir de esta manera los costos relacionados con la administración y supervisión de la infraestructura de red. Para ello se analizó 7 trabajos relacionados de la Tabla 1; muestra los Sistemas más usados para la implantación de NMS; los cuales son Cacti, Nagios Core y Zabbix, todas ellas herramientas Open Source.

Tabla 1.Trabajos relacionados que utilizaron NMS Open Source

Trabajo relacionado	NMS Analizados	Características destacadas de los NMS seleccionados	NMS Implementado
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 [17].	Nagios, Pandora, Zabbix	• Zabbix: Fácil instalación, interfaz web intuitiva, facilidad de personalización de gráficos. Fácil escalabilidad. • Nagios: Su instalación y configuración es compleja. • Pandora: la versión libre es limitada, no cuenta con soporte.	Zabbix
Comparativa entre herramientas de monitoreo de red de computadoras	Zabbix, Nagios, Pandora,	• Zabbix: Fácil instalación.	Nagios

aplicadas a la empresa puerto atún [18].	FMS, y PRTG	• Nagios: Instalación compleja, se utilizó plugins para envío de alertas • Pandora FMS: monitoreo básico y equipos limitados en la versión gratuita. • PRTG: solo admite hasta 100 host en la versión gratuita.	
Influencia del software Zabbix para el monitoreo de infraestructura de TI en la SUNARP Zona Registral N° XI - Sede Ica [19]	Zabbix	• Zabbix influyó de forma positiva sobre el monitoreo de la infraestructura de TI. Fácil escalabilidad para el crecimiento de la infraestructura	Zabbix
Evaluación de herramientas de monitoreo para mejorar la seguridad de la red de datos[21].	Zabbix, PRTG, Nagios, Pandora FMS, OpenNMS, Dude y Cacti	• Nagios: Tiene soporte, permite monitorear los recursos de los dispositivos. • Zabbix: Facilidad de uso, monitoreo de ancho de banda en tiempo real. • PRTG: Detección de ICMP, alertas por correo electrónico. • Pandora FMS: monitoreo básico de red en su versión gratis. • Open NMS: soporte técnico limitado, gráficos limitados. • Dude: software limitado, gráficos sin personalización. • Cacti: Monitoreo básico de red y de recursos, necesita agregar plugins para su personalización.	Nagios, Zabbix
Implantación de un sistema de monitoreo para la infraestructura de red de datos de la UFPS Sede Cúcuta y Campos Elíseos [22].	Nagios, Cacti, Zabbix	• Nagios: En su versión gratuita tiene funcionalidades limitada. • Zabbix: herramienta completa, facilidad de configuración desde la interfaz gráfica. • Cacti: Los gráficos son muy limitados.	Zabbix
Diseño de una herramienta de monitoreo y control de servidores utilizando como eje principal CACTI. Aplicado a una pyme mediana[20].	Cacti	• Cacti: Permite obtener gráficas, alertas por correo electrónico usando plugins.	Cacti
Implementación de un sistema de monitoreo para el análisis de la disponibilidad, capacidad, calidad y latencia de enlaces corporativos de última milla[23] .	Cacti Nagios	• Cacti: Permite un fácil monitoreo usando ICMP y SNMP. • Nagios: Permite el monitoreo de recurso de red y el envío de alertas mediate Correo electrónico.	Cacti, Nagios

6.1.2. Selección de una herramienta NMS para ISP.

En la Tabla 2, se muestra la comparación detallada de las características de los tres Sistemas de Gestión de Red (NMS) considerados para este objetivo.

Tabla 2. Características de 3 Sistemas de administración de red (NMS) Open Source.

Características	Cacti	Nagios Core	Zabbix
Escalabilidad	Maneja entornos de tamaño moderado a grande. Puede generar cuellos de botella debido a la arquitectura centralizada.	Admite distribución de carga. Es escalable, ya que cuenta con opciones de distribución de carga y sondas de monitoreo distribuidas.	Permite distribución de carga. Es altamente escalable, con arquitectura distribuida y configuración de servidores proxy.
Flexibilidad y personalización	Limitada	Limitada	Alta
Monitoreo en tiempo real	Si	Sí	Sí
Alertas	Tiene limitado soporte para alertas nativas	Ofrece alertas basadas en umbrales y condiciones	Ofrece alertas flexibles y personalizables basadas en umbrales y condiciones
Generación de informes	Limitada	Limitada	Sí
Interfaz de usuario	Interfaz gráfica intuitiva y fácil de usar.	Interfaz de usuario basada en texto y configuración a través de archivos de configuración.	Interfaz de usuario intuitiva y amigable con capacidades avanzadas de configuración.
Comunidad y soporte	Activa	Activa	Activa
Integración con protocolos comunes (SNMP, ICMP, etc.)	Sí	Sí	Sí
Costo	Gratuito	Gratuito, con opción a Pago	Gratuito
Gestión de dispositivos	Enfocado en monitoreo y generación de gráficos de rendimiento.	Enfocado en el monitoreo de estado y disponibilidad.	Enfocado en el monitoreo y gestión integral de dispositivos.
Plantillas y configuración centralizada	Permite la creación de plantillas para dispositivos y gráficos.	Puede utilizar plantillas y configuraciones centralizadas mediante complementos y extensiones	Ofrece una gestión centralizada de configuraciones mediante plantillas, herencia de configuraciones y plantillas de descubrimiento
Automatización de tareas	No	Sí	Sí
Integración con proveedores de servicios en la nube	No tiene integración nativa con proveedores de servicios en la nube	No tiene integración nativa con proveedores de servicios en la nube	Ofrece integración nativa con algunos proveedores de servicios en la nube, como AWS, Azure y Google Cloud Platform

API y soporte de integración	No cuenta con una API dedicada para la automatización	Ofrece una API para la automatización de tareas	Proporciona una API completa y documentada para la automatización de tareas
Notificaciones por múltiples canales (email, SMS, etc.)	No	Sí	Sí
Seguridad	Proporciona autenticación de usuarios básica basada en nombres de usuario y contraseñas. No incluye funciones de seguridad avanzadas, como autenticación de dos factores (2FA) o autenticación basada en certificados	Se basa en la seguridad a través de la protección de su entorno de instalación y acceso a través de la red. No proporciona una autenticación integrada, pero se puede utilizar junto con herramientas externas	Avanzada Proporciona funciones de seguridad avanzadas, como autenticación de dos factores (2FA), autenticación basada en certificados y cifrado de datos en tránsito utilizando SSL/TLS. También ofrece funciones de seguridad adicionales, como la gestión de usuarios y grupos, control de acceso basado en roles y registro de auditoría.
Autenticación	Utiliza un sistema de autenticación interno y no es compatible directamente con otros sistemas de autenticación, como LDAP o Active Directory.	No proporciona un sistema de autenticación nativo, pero se puede configurar para trabajar con herramientas externas	Admite múltiples opciones de autenticación, incluyendo autenticación interna, autenticación basada en LDAP y autenticación basada en Active Directory.

En la Tabla 3, se presentan los requisitos para el NMS, los cuales fueron obtenidos a través de una entrevista con el administrador de Red (ver Anexo 2). Estos requisitos fueron elementos esenciales para la selección de una herramienta de Administración de Red (NMS) adecuada para los Proveedores de Servicios de Internet (ISP).

Tabla 3. Requerimientos del NMS

Requerimientos	**Características**
Escalabilidad	La plataforma debe ser capaz de adaptarse y expandirse para cumplir con la creciente demanda y las cambiantes necesidades de los clientes. Dado que cada ISP posee redes de diversos tamaños y complejidades, la solución debe ser capaz de gestionar considerables cantidades de dispositivos y servicios.
Flexibilidad y personalización	Se requiere una solución que posibilite la fácil personalización y adaptación de los paneles de control, alertas e informes para satisfacer de manera individualizada los requisitos de cada ISP.
Monitoreo en tiempo real y alertas.	Se necesita recibir alertas y notificaciones en tiempo real cuando surjan problemas en la red de los ISP.

Visualización de datos	Debe tener capacidad de obtener información detallada por ello se seleccionó una herramienta que ofrece funciones sólidas de generación de informes y visualización de datos.
Comunidad y soporte	Debe tener una comunidad activa de usuarios y un buen soporte técnico, facilita obtener ayuda, compartir conocimientos y resolver problemas.

En la Tabla 4, se llevó a cabo una calificación acorde a los requisitos obtenidos en relación a la herramienta de Administración de Red (NMS), siendo 1 cumple y 0 no cumple. Cada requisito fue evaluado y calificado con el propósito de medir cómo cada NMS cumplía con los criterios específicos establecidos en la entrevista con el administrador de red.

Tabla 4. Comparación de los NMS

Factores	**NMS**		
	Cacti	**Nagios Core**	**Zabbix**
Escalabilidad	1	1	1
Flexibilidad y personalización	0	0	1
Monitoreo en tiempo real y alertas	1	1	1
Informes y generación de datos	1	1	1
Comunidad y soporte	1	1	1

Esta evaluación proporcionó una base sólida para comparar y tomar decisiones sobre la selección de la herramienta más adecuada para satisfacer las necesidades de la empresa respecto a los proveedores de servicios de Internet (ISP).

Se seleccionó Zabbix como Sistema de Administración de Red (NMS) debido a su escalabilidad, capacidad para adaptarse a diversos entornos, flexibilidad en la personalización y una interfaz intuitiva. Además, Zabbix ofrece funciones de monitoreo en tiempo real, alertas personalizables con varias opciones de mensajería instantánea, generación de informes y una comunidad activa de usuarios, lo cual es esencial para brindar soporte.

6.2. Objetivo 2: Configurar el Sistema de administración de red (NMS) y los agentes en los ISP

En esta fase, se recopiló información detallada sobre la infraestructura de red y los dispositivos utilizados por los proveedores de servicios de Internet (ISP) permitiendo obtener una visión completa de la configuración y topología de la red, contribuyendo así a un despliegue eficiente del sistema Zabbix y a una gestión efectiva de los eventos de monitoreo.

Paralelamente, se procedió a la instalación y configuración del sistema Zabbix, después de seleccionar el hardware adecuado para su implementación. El sistema fue instalado en el servidor Proxmox designado por la empresa tanto para los propósitos actuales como para futuros servicios. Adicionalmente, se habilitó el servicio SNMP en los dispositivos Mikrotik de los 35 proveedores de servicios de Internet (ISP).

6.2.1. Obtener información de la infraestructura de red de los ISP.

Por medio de entrevista con el administrador de red de la empresa Red Nueva Conexión se identificó los equipos de borde y distribución de los 35 ISP, obteniendo un total de 100 equipos que se detallan en la Tabla 5, cada uno de estos equipos es accesible por el Sistema de Administración de Red Zabbix a través de su IP Pública.

Tabla 5. Equipos de los 35 ISP

#	ISP	CIUDAD	NODO	IP PÚBLICA	EQUIPO
1	AMG	Vinces	Vinces	45.185.163.xxx	CCR1036-12G-4S
	AMG	Vinces	El Rosario	200.24.130.xxx	RB4011iGS+
	AMG	Vinces	Estero de En medio	177.234.230.xxx	CCR1036-8G-2S+
	AMG	Vinces	Punta del Este	177.234.245.xxx	RB4011iGS+
2	AccesNet	Cuenca	Borde-Accessnet	45.71.202.xxx	CCR1036-12G-4S
	AccesNet	Baños	Accessnet-1	45.225.107.xxx	CCR1036-12G-4S
	AccesNet	Cuenca	Accessnet-2	200.24.157.xxx	CCR1072-8S+
3	CalcetaTV	Calceta	Core Calceta TV	200.24.153.xxx	CCR1036-8G-2S+
4	FiberPlus	Chambo	Core Radio	45.224.22.xxx	CCR1036-8G-2S+
	FiberPlus	Chambo	Core Fibra Chambo	45.224.22.xxx	CCR1072-8S+
	FiberPlus	Chambo	Core MOLOGOC	45.224.22.xxx	CCR1036-8G-2S+
5	Covirnet	Pajan	Core Pajan	157.100.55.xxx	CCR2004-16G-2S+
6	OptikNet	Cuenca	Shucay	45.164.64.xxx	RB4011iGS+
	OptikNet	Cuenca	El Verde	45.164.64.xxx	RB4011iGS+
7	FiberHome	Patate	El Triunfo	201.219.11.xxx	RB4011iGS+
	FiberHome	Patate	Patate	177.234.250.xxx	CCR1036-8G-2S+
8	FrancoNet	Samborondón	La Victoria	200.24.155.xxx	RB4011iGS+
	FrancoNet	Samborondón	Santa Martha	200.24.132.xxx	CCR1036-12G-4S
	FrancoNet	Samborondón	Samborondón	157.100.52.xxx	CCR1036-12G-4S
	FrancoNet	Samborondón	San Lorenzo	45.185.163.xxx	CCR1072-8S+
9	GlobalNet	Ponce enrique	Ponce enrique	45.71.202.xxx	CCR1036-8G-2S+
	GlobalNet	Ponce Enrique	Tendales	200.24.150.xxx	CCR1036-8G-2S+

	GlobalNet	Santa rosa	Santa rosa	200.24.148.xxx	CCR1072-8S+
	GlobalNet	Ponce enrique	Bella rica	200.24.150.xxx	CCR1036-8G-2S+
10	HCNET	Guayaquil	Guasmo	157.100.52.xxx	CCR1072-8S+
	HCNET	Guayaquil	Guasmo	157.100.52.xxx	CCR1036-12G-4S
11	Interdatos	3 postes	3 postes	200.24.130.xxx	CCR1036-12G-4S
	Interdatos	Babahoyo	Babahoyo Fibra	177.234.244.xxx	CCR1072-8S+
	Interdatos	Babahoyo	Babahoyo Babahoyo	200.24.130.xxx	CCR1036-8G-2S+
	Interdatos	Jujan	Jujan	45.70.196.xxx	CCR1036-8G-2S+
12	Interlive	Quito	Quito	45.229.87.xxx	CCR1072-8S+
	Interlive	Balzar	Balzar	45.229.87.xxx	CCR1036-8G-2S+
	Interlive	Guayaquil	Guayaquil	179.0.41.xxx	CCR1072-8S+
	Interlive	El empalme	El empalme	179.0.41.xxx	RB4011iGS+
13	Red Nueva Conexión	Puebloviejo	Puebloviejo-Oficina	179.0.41.xxx	RB4011iGS+
	Red Nueva Conexión	Puebloviejo	Puebloviejo	179.0.41.xxx	CCR1036-8G-2S+
14	FlashNET	Babahoyo	El Volante	177.234.244.xxx	RB4011iGS+
	FlashNET	Babahoyo	San Vicente	177.234.244.xxx	CCR1036-12G-4S
	FlashNET	Babahoyo	La Corona	177.234.244.xxx	CCR1036-12G-4S
	FlashNET	Babahoyo	Los Cilos	177.234.244.xxx	CCR1072-8S+
	FlashNET	Babahoyo	La Teresa	177.234.245.xxx	CCR1036-8G-2S+
15	MegaConnection	Zamora	Zamora	157.100.56.xxx	CCR1036-8G-2S+
	MegaConnection	Gualaquiza	Gualaquiza	45.225.88.xxx	CCR1072-8S+
	MegaConnection	Loja	Loja	177.234.251.xxx	CCR1036-8G-2S+
16	Meganet	Pajan	Pajan	200.24.154.xxx	CCR1072-8S+
	Meganet	Vergeles	Vergeles	200.24.131.xxx	RB4011iGS+
	Meganet	Guayaquil	OLT2	177.234.197.xxx	RB4011iGS+
	Meganet	Guayaquil	OLT3	177.234.197.xxx	CCR1036-8G-2S+
	Meganet	Guayaquil	OLT1	177.234.197.xxx	RB4011iGS+
	Meganet	Cascol	Cascol	200.24.152.xxx	CCR1036-12G-4S
17	MontufarNET	San Gabriel	Montufar	177.234.213.xxx	CCR1036-12G-4S
	MontufarNET	Bolívar	Bolívar	177.234.213.xxx	CCR1072-8S+
18	Red RonaldNet	Pedro Carbo	Estacada	157.100.55.xxx	CCR1036-8G-2S+
19	S&E	Quinsalomas	Quinsalomas	45.185.162.xxx	CCR1036-8G-2S+
	S&E	La mana	La mana	167.250.180.xxx	CCR1072-8S+
	S&E	La mana	La mana-II	167.250.180.xxx	CCR1036-8G-2S+

20	SWTelecom	La julia	La julia	177.234.244.xxx	CCR1072-8S+
	SWTelecom	Pueblonuevo	Pueblonuevo	177.234.245.xxx	CCR1036-12G-4S
	SWTelecom	Babahoyo	El salto	177.234.244.xxx	CCR1036-12G-4S
	SWTelecom	Montalvo	Montalvo	177.234.244.xxx	CCR1072-8S+
	SWTelecom	Yaguachi	Yaguachi	177.234.208.xxx	CCR1036-8G-2S+
	SWTelecom	San juan	San juan	45.185.162.xxx	CCR1036-8G-2S+
	SWTelecom	Babahoyo	Barreiro	160.20.167.xxx	CCR1072-8S+
21	Servi.Inter-1	Ricaurte	Ricaurte	45.71.37.xxx	CCR1036-8G-2S+
	Servi.Inter-1	Puebloviejo	Puebloviejo	45.70.236.xxx	CCR1072-8S+
22	Servi.Inter	Zapotal	Zapotal	45.70.14.xxx	CCR1036-12G-4S
	Servi.Inter	Ventanas	Ventanas	157.100.53.xxx	CCR1036-12G-4S
23	Servinet	Lomas de Sargentillo	San Lorenzo	200.24.131.xxx	CCR1072-8S+
24	TV Santana	Santana	Santana	45.224.21.xxx	CCR1036-8G-2S+
25	YanezNet	Santa lucia	Santa lucia	160.20.166.xxx	CCR1036-8G-2S+
	YanezNet	Fátima	Fátima	45.185.163.xxx	CCR1072-8S+
	YanezNet	Coloradal	Coloradal	45.185.163.xxx	CCR1036-8G-2S+
26	Velocinet	Puerto Quito	Provincias unidas	177.234.199.xxx	CCR1072-8S+
	Velocinet	Shushufindi	Shushufindi	177.234.199.xxx	CCR1036-12G-4S
	Velocinet	28 de mayo	28 de mayo	177.234.199.xxx	CCR1036-12G-4S
	Velocinet	Shushufindi-II	Shushufindi-II	177.234.199.xxx	CCR1072-8S+
	Velocinet	Yamanunca	Yamanunca	177.234.199.xxx	CCR1036-8G-2S+
27	APCOM	Ventanas	Ventanas	45.70.14.xxx	CCR1036-8G-2S+
28	Arenanet	Arenillas	Arenillas	200.24.149.xxx	CCR1072-8S+
29	San Miguel Net	Salcedo	Salcedo	45.70.198.xxx	CCR1036-8G-2S+
30	Teleing	Guayaquil	Urdesa	200.24.135.xxx	CCR1072-8S+
31	Producomsnet	Pangui	Bayanes	157.100.56.xxx	CCR1036-12G-4S
	Producomsnet	Pangui	Pangui	157.100.56.xxx	CCR1036-12G-4S
	Producomsnet	Pangui	Pangui-AAA	157.100.56.xxx	CCR1072-8S+
	Producomsnet	Pangui	Tundayme	157.100.56.xxx	CCR1036-8G-2S+
	Producomsnet	Pangui	Pangui-Radio	157.100.56.xxx	CCR1036-8G-2S+
32	JipiTV	Jipijapa	Jipijapa	45.70.239.xxx	CCR1072-8S+
33	Ultranet	Puerto quito	Puerto Quito	177.234.212.xxx	CCR1036-8G-2S+
	Ultranet	Puerto quito	Las palmas f.o	177.234.212.xxx	CCR1072-8S+

	Ultranet	Puerto quito	Las palmas radio	177.234.212.xxx	CCR1009-7G-1C-1S+
	Ultranet	Puerto quito	Marianitas	177.234.247.xxx	CCR1009-7G-1C-1S+
	Ultranet	Puerto quito	Mirador	177.234.212.xxx	CCR1009-7G-1C-1S+
	Ultranet	Puerto quito	Salazar	200.24.146.xxx	CCR1009-7G-1C-1S+
34	Fibratel	Santo domingo	Balle hermoso	45.225.104.xxx	RB4011iGS+
	Fibratel	Santo domingo	Congoma	45.225.104.xxx	CCR1009-7G-1C-1S+
	Fibratel	Santo domingo	Santo domingo	45.225.104.xxx	CCR1009-7G-1C-1S+
	Fibratel	Santo domingo	Toachi	177.234.217.xxx	CCR1009-7G-1C-1S+
35	RizzoNet	Bolivar	Las Naves	45.70.200.xxx	RB4011iGS+

Además, en la tabla anterior se indicó el modelo de cada equipo Mikrotik utilizado por los Proveedores de Servicio de Internet (ISP). Para obtener información detallada acerca de cada uno de estos equipos, se dispone de los datasheet correspondientes en el Anexo 4.

6.2.1.1. Infraestructura de red, entre el sistema de administración de red y los ISP

En la Figura 5 se detalló la representación gráfica de la infraestructura de "Red Nueva Conexión", destacando su interconexión con los 35 proveedores de servicios de Internet (ISP) mediante direcciones IP públicas, proporcionando una comprensión clara y visual de la distribución de la red.

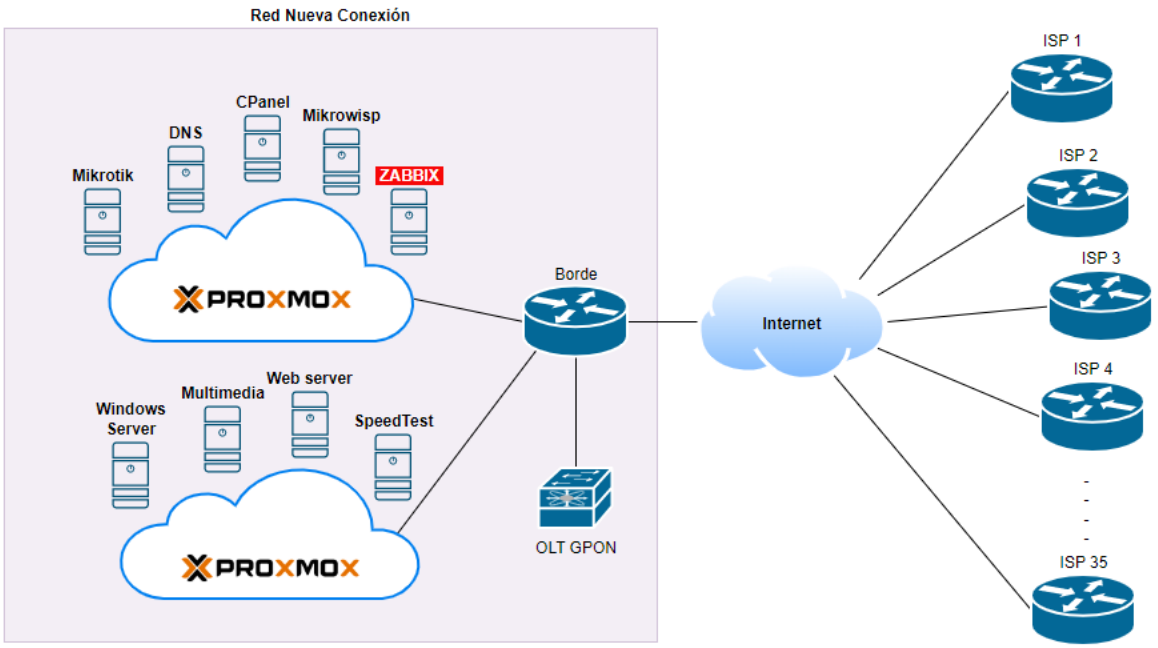


Figura 5. Topología de conexión de Zabbix y los 35 ISP

6.2.2. Seleccionar el hardware necesario para la instalación del NMS.

De acuerdo a la página oficial de Zabbix se establecen los siguientes requisitos mínimos de hardware para instalar el servidor asumiendo una plataforma Linux/BSD/Unix. Estos parámetros pueden variar de acuerdo a la cantidad de host y métricas que se vayan a monitorizar. La Tabla 6 indica el número de núcleos de CPU, la cantidad de memoria RAM y el tipo de base de datos que se puede utilizar.

Tabla 6. Requerimientos mínimos Zabbix [24]

Tamaño	Núcleos de CPU/Memoria	Base de datos	Cantidad de métricas
Pequeño	2 / 8 GB	Servidor MySQL, Servidor Percona, Servidor MariaDB, PostgreSQL	1000
Mediano	4 / 16 GB	Servidor MySQL, Servidor Percona, Servidor MariaDB, PostgreSQL	10000
Grande	16 / 64 GB	Servidor MySQL, Servidor Percona, Servidor MariaDB, PostgreSQL, Oracle	100000
Muy grande	32 / 96 GB	Servidor MySQL, Servidor Percona, Servidor MariaDB, PostgreSQL, Oracle	1000000

A continuación, en la Tabla 7 se detallan las características de hardware del servidor proporcionado por la empresa en el cual se instaló el Sistema de administración de Red (NMS). Este servidor cuenta con Proxmox instalado, lo que permite la virtualización de servidores.

Tabla 7. Características del servidor DELL con Proxmox

Características	Especificaciones técnicas de PowerEdge R720 [25]
Procesador	32 x Intel(R) Xeon(R) CPU E5-2650 0 @ 2.00GHz (2 Sockets)
Memoria RAM	192 GB
Almacenamiento	8 TB

Para el cálculo del hardware necesario para los 100 dispositivos Mikrotik se utilizó los parámetros de la plantilla Mikrotik SNMP que cuenta con 19 items y 10 triggers, se utilizó la fórmula "1 métrica = 1 elemento + 1 trigger + 1 gráfico" [24] como una referencia para el cálculo aproximado de la carga de trabajo total que se generará en servidor Zabbix.

Cálculo de Items

$$\boldsymbol{items} = N°items + N°host$$

$$\boldsymbol{items} = 19 * 100$$

$$\boldsymbol{items} = 1900$$

Se obtuvo un total de 1900 items por cada host (router).

Cálculo de Triggers

$$\boldsymbol{triggers} = N°triggers + N°host$$

$$\boldsymbol{triggers} = 10 * 100$$

$$\boldsymbol{triggers} = 1000$$

Se obtuvo un total de 1000 triggers por cada host (router).

Cálculo de Gráficos (se gráfica cada ítem)

$$\boldsymbol{gráficos} = N°gráficas + N°host$$

$$\boldsymbol{gráficos} = 19 * 100$$

$$\boldsymbol{gráficos} = 1900$$

Se obtuvo un total de 1900 gráficas por cada host (router).

Cálculo de Métricas

$$\boldsymbol{Métricas\ Totales} = ítems + triggers + gráficos$$

$$\boldsymbol{Métricas\ Totales} = 1900 + 1000 + 1900$$

$$\boldsymbol{Métricas\ Totales} = 4800$$

Basándose en el cálculo de ítems, triggers y graficas se obtuvo un total de 4800 métricas, por lo que se necesitó una solución de tamaño mediano. Se procedió a la creación de una máquina virtual con el propósito de instalar Ubuntu Server. Las especificaciones técnicas de la máquina virtual se detallaron en la Figura 6.

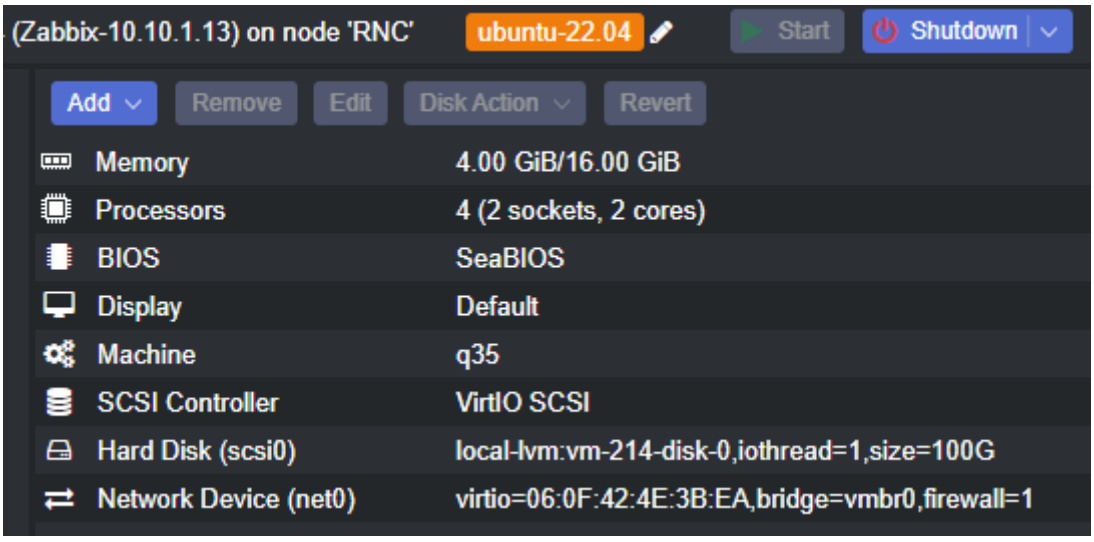


Figura 6. Máquina Virtual para el NMS Zabbix

6.2.3. Configuración del servidor NMS.

Luego de la instalación de Zabbix (Ver Anexo 3) se configuró el NMS para supervisar los equipos de los ISP. Para una gestión adecuada se creó un grupo de hosts para cada ISP, en los cuales están vinculados los hosts que pertenecen a cada ISP.

6.2.3.1. Creación de grupos de host por ISP

Para crear un grupo de host se seleccionó **Configuration → Host groups → Create host group** y se digitó el nombre del grupo (ver figura 7). De igual manera se creó los 35 grupos necesarios para asignar en estos los hosts de cada ISP.

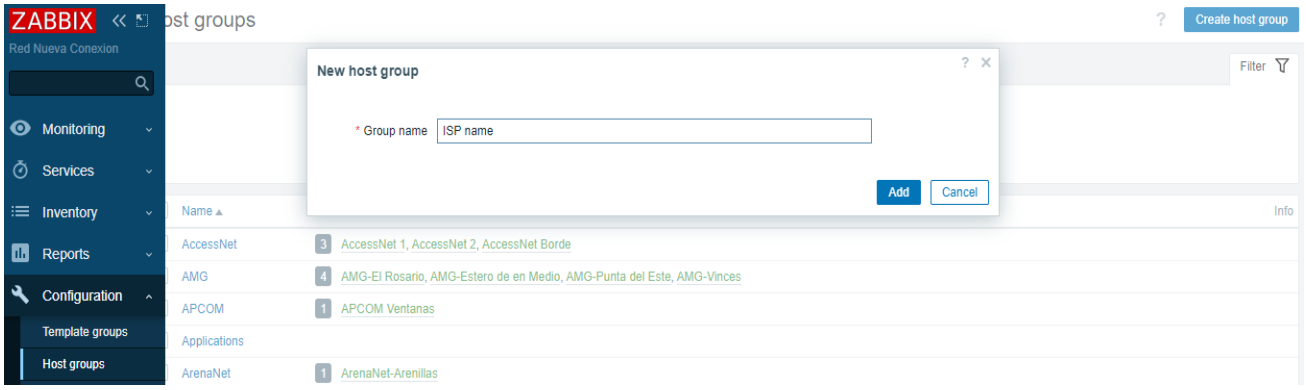


Figura 7. Creación de grupo de hosts

6.2.3.2. Creación de host y asignación a los grupos

Para esto se selecciona **Configuration → Hosts → Create host** y se ingresa la información descrita en la Tabla 8.

Tabla 8. Parámetros obligatorios en la creación de host

Parámetro		Descripción
Host name		Ingresar un nombre único para el host
Templates		Permite seleccionar la plantilla de monitoreo para cada dispositivo dependiendo de la marca.
Host groups		Seleccionar el grupo de ISP al que pertenece.
Interfaces		Se debe seleccionar SNMP
	IP address	Dirección IP del equipo a supervisar.
	Connect to	Seleccionar la opción IP
	Port	Utiliza el puerto 161 para el agente SNMP
	Default	Debe ir marcada ya que será la interfaz predeterminada.
Enabled		Se debe marcar la casilla de verificación para que el host esté activo y se pueda supervisar.

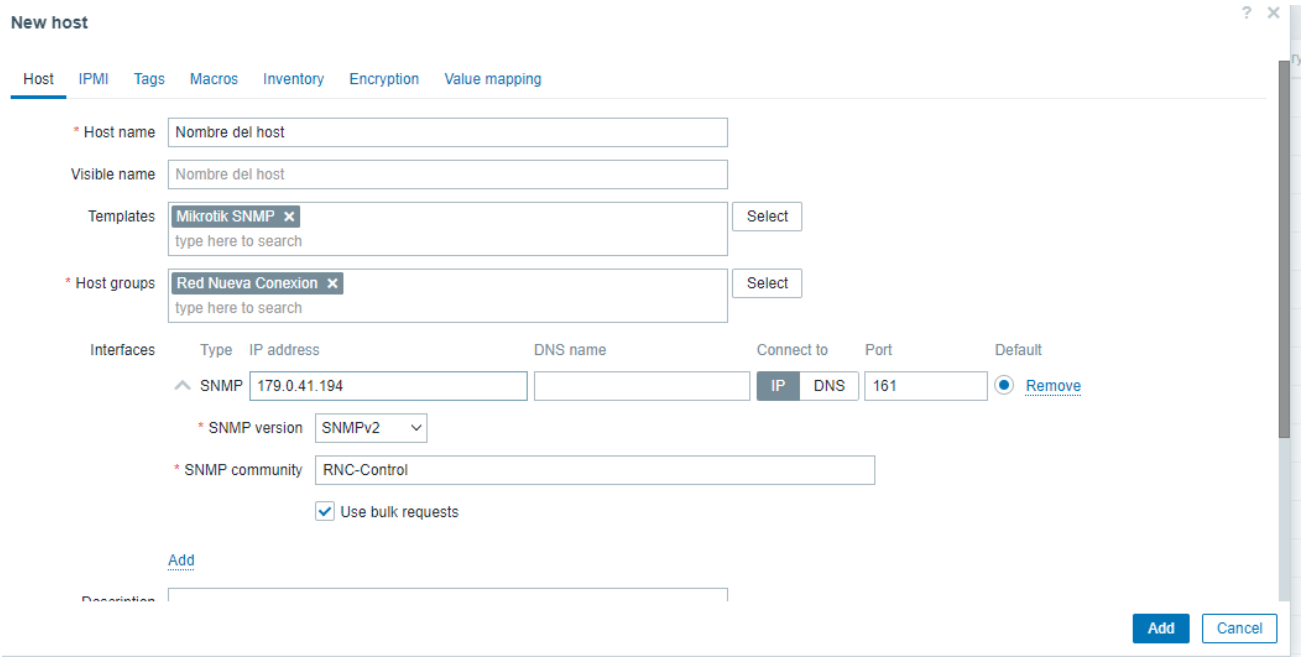


Figura 8. Crear host en Zabbix

Es importante destacar que el procedimiento y la configuración mencionada anteriormente se aplicó de manera uniforme a todos los equipos Mikrotik.

6.2.3.3. Plantilla Mikrotik SNMP

Se implementó la plantilla Mikrotik SNMP proporcionada por Zabbix. Esta plantilla se adapta para monitorear dispositivos Mikrotik utilizando el protocolo SNMPv2. La plantilla incluye 19 elementos que capturan diversas métricas y 10 disparadores que generan alertas en caso de condiciones anómalas, ver tabla 9.

Tabla 9. Items y Triggers de la Plantilla SNMP

Item	Tipo	Trigger	Severidad
Firmware version	SNMP agent	Firmware has changed	Information
Hardware model name	SNMP agent		
Hardware serial number	SNMP agent	Device has been replaced	Information
ICMP loss	Simple check	Unavailable by ICMP ping	High
ICMP ping	Simple check	High ICMP ping loss	Warning
ICMP response time	Simple check	High ICMP ping response time	Warning
Memory utilization	Calculated	High memory utilization	Average
Operating system	SNMP agent	Operating system description has changed	Information
SNMP agent availability	Zabbix internal	No SNMP data collection	Warning
SNMP traps (fallback)	SNMP trap		
System contact details	SNMP agent		
System description	SNMP agent		

System location	SNMP agent		
System name	SNMP agent	System name has changed	Information
System object ID	SNMP agent		
Total memory	SNMP agent		
Uptime (hardware)	SNMP agent	Host has been restarted	Warning
Uptime (network)	SNMP agent	Host has been restarted	Warning
Used memory	SNMP agent		

En la figura 10, se describen los 19 elementos específicos de la plantilla Mikrotik SNMP, que recopilan información relevante de los dispositivos, como uso de CPU, memoria, ancho de banda.

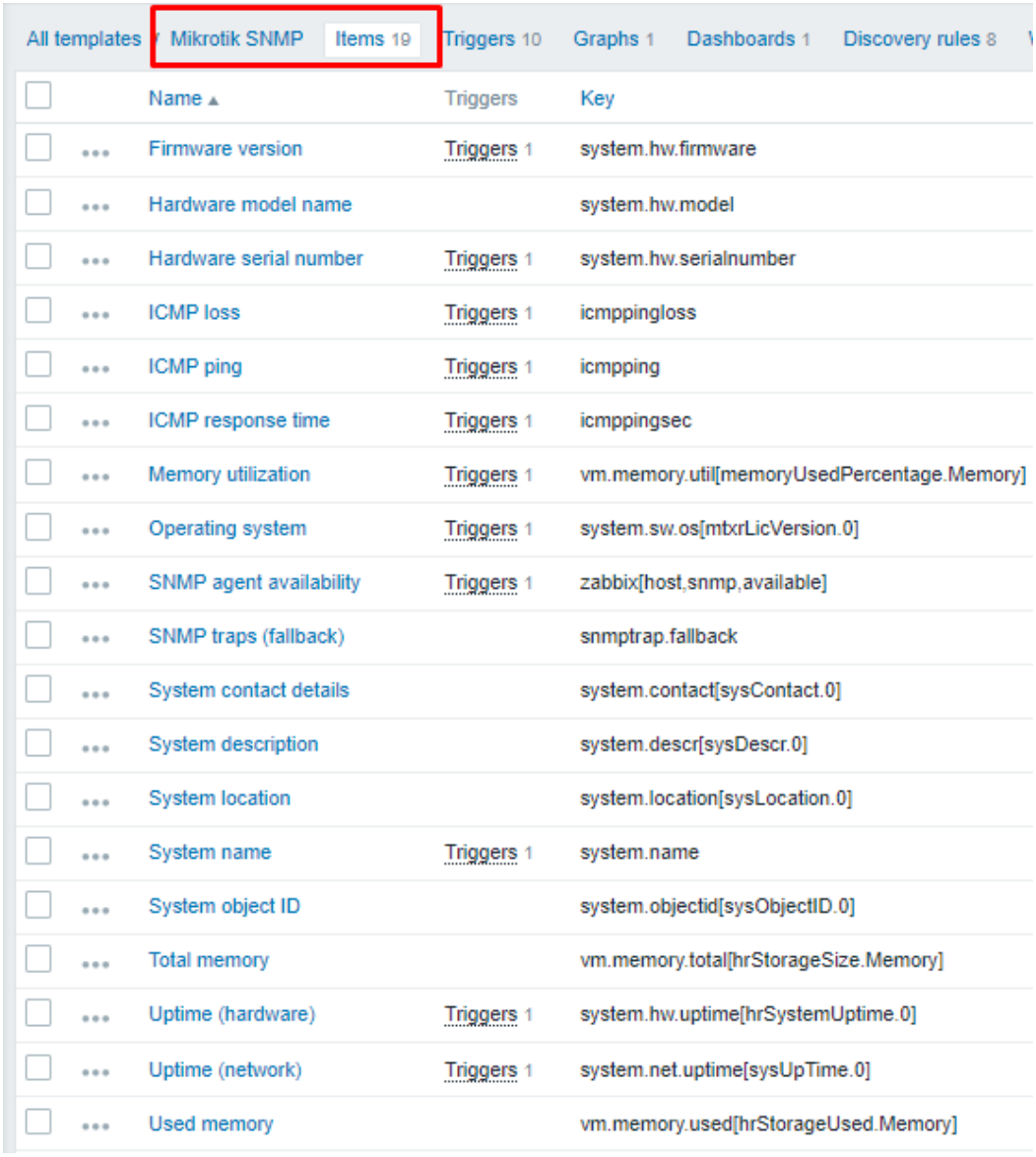
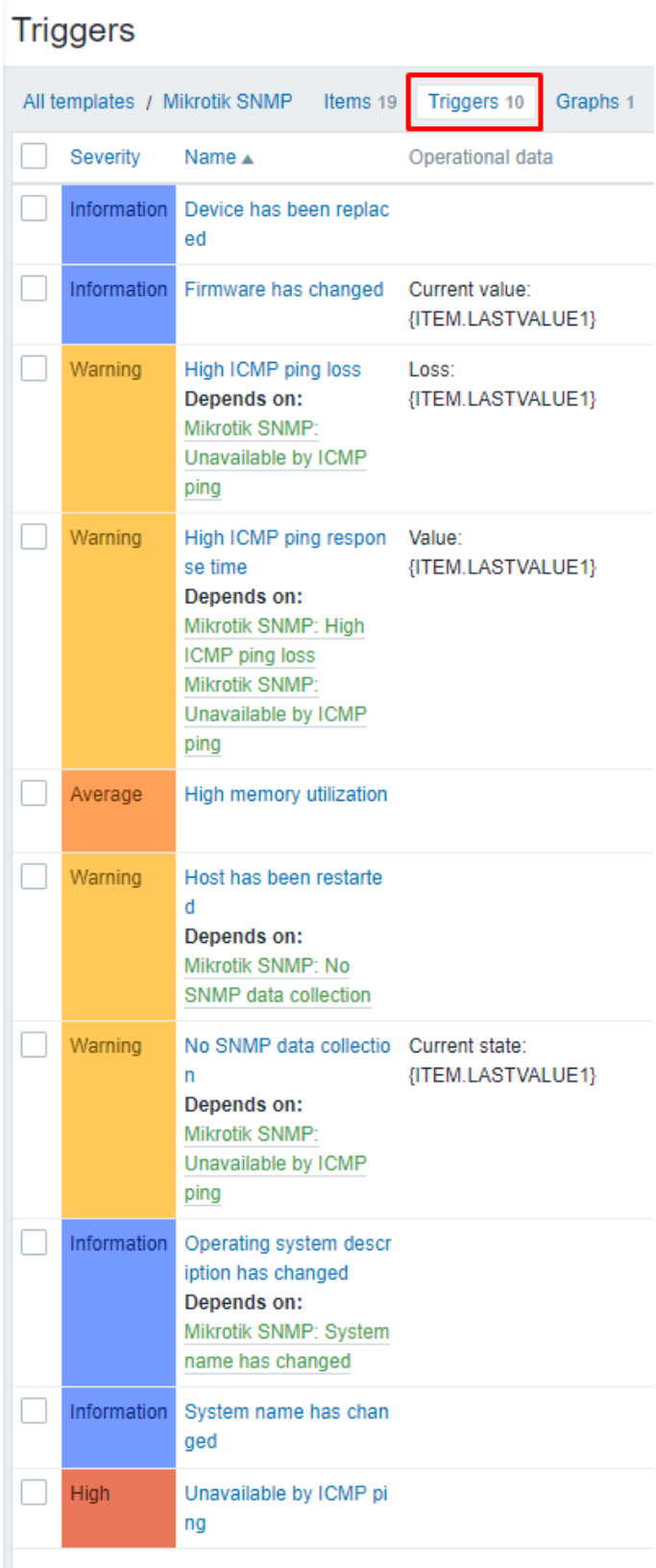


Figura 9. Items Plantilla Mikrotik SNMP

Además, en la figura 10 se muestra los 10 disparadores de la plantilla SNMP Mikrotik que generan alertas en situaciones críticas.



Triggers

All templates / Mikrotik SNMP Items 19 Triggers 10 Graphs 1

Severity	Name ▲	Operational data
Information	Device has been replaced	
Information	Firmware has changed	Current value: {ITEM.LASTVALUE1}
Warning	High ICMP ping loss **Depends on:** Mikrotik SNMP: Unavailable by ICMP ping	Loss: {ITEM.LASTVALUE1}
Warning	High ICMP ping response time **Depends on:** Mikrotik SNMP: High ICMP ping loss Mikrotik SNMP: Unavailable by ICMP ping	Value: {ITEM.LASTVALUE1}
Average	High memory utilization	
Warning	Host has been restarted **Depends on:** Mikrotik SNMP: No SNMP data collection	
Warning	No SNMP data collection **Depends on:** Mikrotik SNMP: Unavailable by ICMP ping	Current state: {ITEM.LASTVALUE1}
Information	Operating system description has changed **Depends on:** Mikrotik SNMP: System name has changed	
Information	System name has changed	
High	Unavailable by ICMP ping	

Figura 10. Triggers Plantilla Mikrotik SNMP

6.2.4. Configurar los agentes en los routers de los ISP usando el protocolo SNMP. Configuración SNMP en Mikrotik

La activación y ajuste del servicio SNMP en un enrutador Mikrotik fue realizada mediante el uso de SSH y la herramienta gráfica Winbox. En este contexto, se procedió a ingresar al enrutador y se configuró el servicio correspondiente con los permisos adecuados.

6.2.4.1. Configuración SNMP mediante consola SSH o Telnet

La figura 11, indica el script utilizado para la configuración del servicio SNMP en los enrutadores Mikrotik de los ISP:

```
/snmp community
add addresses=205.[redacted] name=RNC-Control
/snmp
set contact="soporte@rednuevaconexion.net" enabled=yes
location=Vinces trap-community=RNC-Control trap-version=2
```

Figura 11. Script SNMP Mikrotik

6.2.4.2. Activación mediante Winbox

Para acceder al enrutador se hace mediante la IP pública del mismo usando las credenciales de acceso, estas deben tener privilegios de administrador:

1. Acceso al router Mikrotik

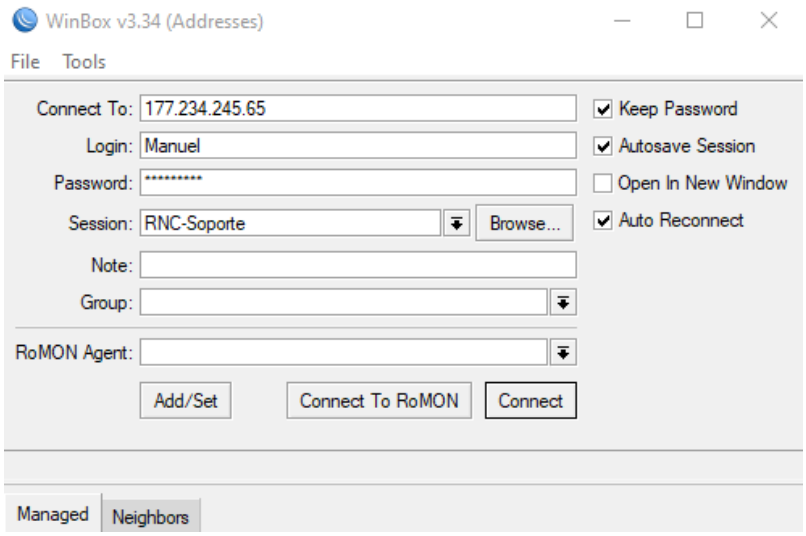


Figura 12. Login de Winbox

2. Creación de la comunidad SNMP

Se selecciona **IP → SNMP → Communities**, en la que se crea la comunidad SNMP, ver figura 13.

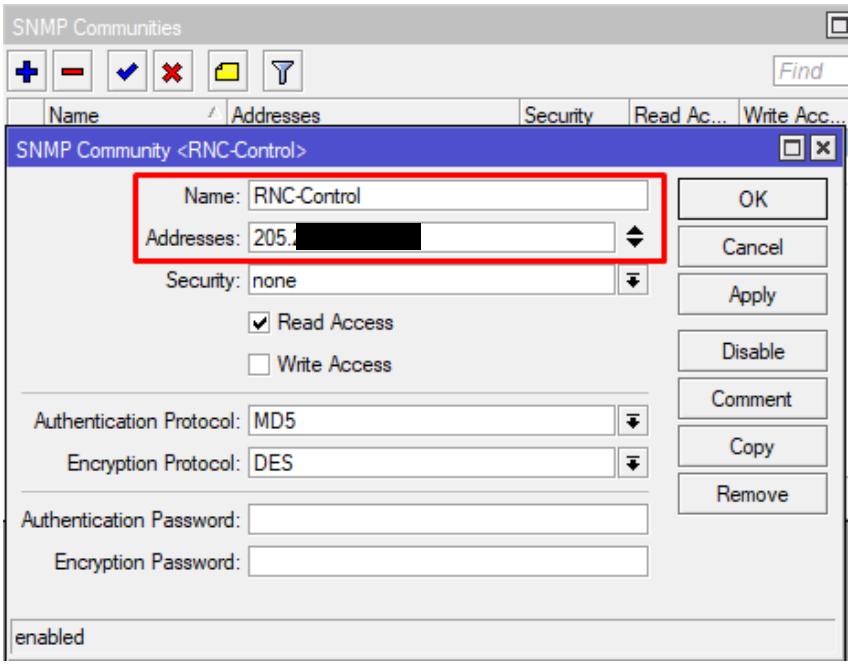


Figura 13. Configuración comunidad SNMP Mikrotik

3. Configuración SNMP

En esta ventana se debe habilitar el SNMP e ingresar la información de contacto, así como la ubicación del dispositivo, ver figura 14.

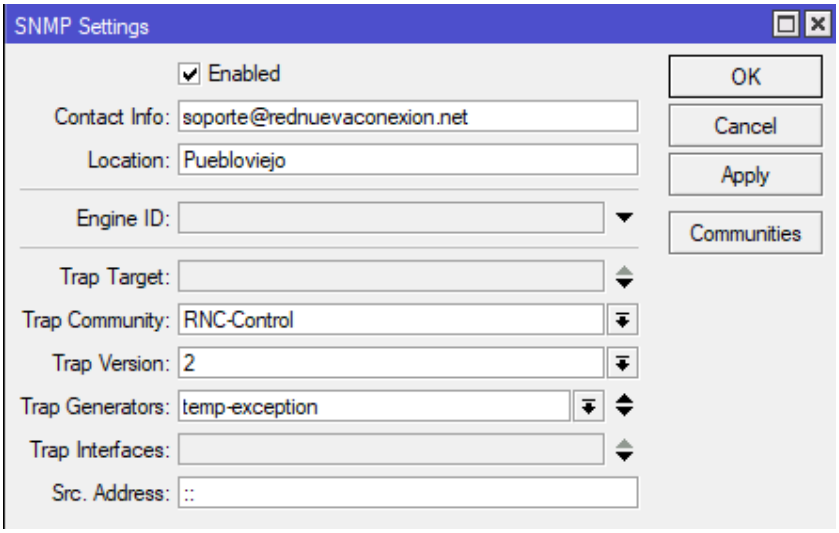


Figura 14. Habilitar SNMP con Winbox

En la Figura 15, se exhiben los dispositivos Mikrotik que están disponibles para el monitoreo mediante el Protocolo SNMP 161 puerto y están siendo gestionados por Zabbix. Esta representación visual proporciona una visión concreta de la supervisión activa de estos dispositivos en el entorno del sistema implementado.

Name ▲	Interface		Availability
InterLive Buena Fe	45.	61	SNMP
InterLive El Empalme	45.	:161	SNMP
InterLive Guayaquil	45.	161	SNMP
Interlive Portete	45.	161	SNMP
JipiTV-Jipijpa	45.	161	SNMP
Manaphi Fast - Charapoto	45.	161	SNMP
MegaConnection Gualaquiza	45.	:161	SNMP
MegaConnection Loja	177.	:161	SNMP
MegaConnection Zamora	157.	:161	SNMP
Meganet Cascol	200.	161	SNMP
Meganet Guayaquil - OLT1	177.	:161	SNMP
Meganet Guayaquil - OLT2	177.	:161	SNMP
Meganet Guayaquil - OLT3	177.	:161	SNMP
Meganet Pajan	200.	:161	SNMP
Meganet Vergeles	200.	:161	SNMP
Producomsnet-Bayanes	157.	:161	SNMP
Producomsnet-El Pangui	157.	161	SNMP
Producomsnet-El Pangui - AAA	157.	:161	SNMP
Producomsnet-EL Pangui Radio	157.	:161	SNMP
Producomsnet-Tundayme	157.	:161	SNMP
RizzoNet - Las Naves	45.	161	SNMP
RNC-PuebloViejo-PuebloViejo	205.	:161	SNMP
RNC PuebloViejo-Oficina	205	161	SNMP

Figura 15. Hosts agregados a Zabbix usando SNMP

La Figura 16, presenta el total de dispositivos incorporados utilizando tanto el protocolo SNMP como el Agente Zabbix. Esta representación ofrece una visión clara de la distribución de los dispositivos bajo supervisión y destaca el enfoque integral de la implementación.

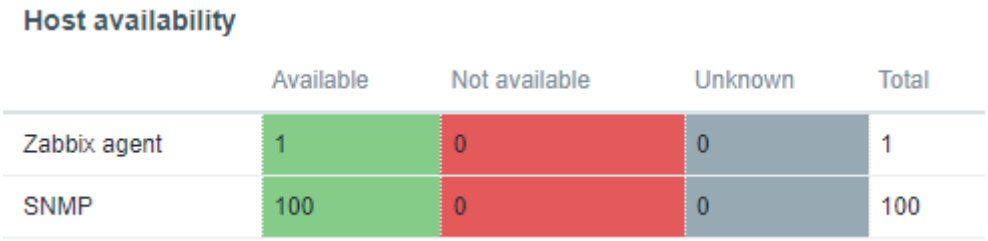


Figura 16.Total de dispositivos gestionados por Zabbix.

Adicionalmente se configuró en los dispositivos Mikrotik el firewall: **Filter Rules** (Figura 17) para permitir el acceso del protocolo SNMP únicamente a las direcciones IP que estén en la lista Acceso-SNMP.

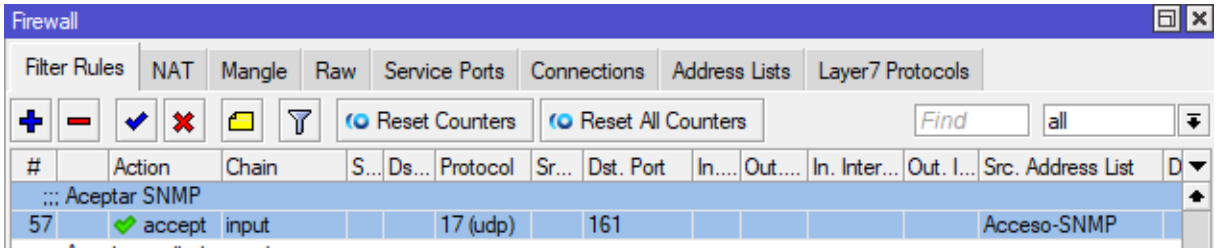


Figura 17. Regla de Firewall para permitir la lista Acceso-SNMP

En la Figura 18 se muestran las direcciones IP agregadas al **Address List** Acceso-SNMP.

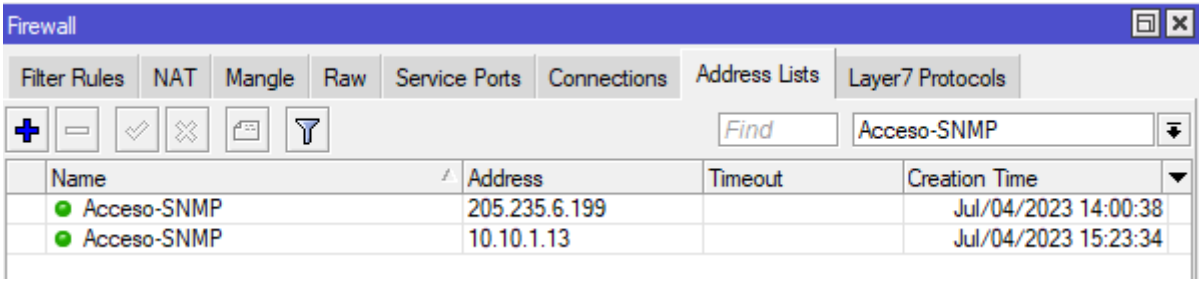


Figura 18. Direcciones IP con acceso a SNMP

La configuración de SNMP y Firewall en los equipos Mikrotik se realizó de manera uniforme en los 100 dispositivos.

6.3. Objetivo 3: Verificar el funcionamiento del NMS

En esta fase, se recopiló información de los dispositivos administrados por el NMS utilizando agentes SNMP. Esto incluyó datos como las gráficas de utilización de la CPU, la memoria y el ancho de banda de la interfaz WAN de cada uno de los hosts. Además, se configuraron alertas para notificar al personal de TI de “Red nueva Conexión” acerca de los eventos ocurridos en los 100 equipos de los ISP. Para lograr esto, se estableció un mecanismo de notificación que comprendió canales de comunicación como correo electrónico y mensajería instantánea. Específicamente, se creó un bot dedicado en la plataforma de Telegram para facilitar la entrega de estas notificaciones. Cada ISP cuenta de su propio grupo en esta plataforma (ver Anexo 6), dirigiendo a cada grupo las notificaciones relativas a los eventos de sus dispositivos.

6.3.1. Obtener gráficas de monitoreo del consumo de CPU, memoria y ancho de banda.

En la figura 19, se muestra información respecto al ancho de banda de la interfaz WAN correspondiente al router de borde del ISP RNC en la que indica el consumo máximo de 957.53 Mbps de ancho de banda durante el mes de junio y julio.

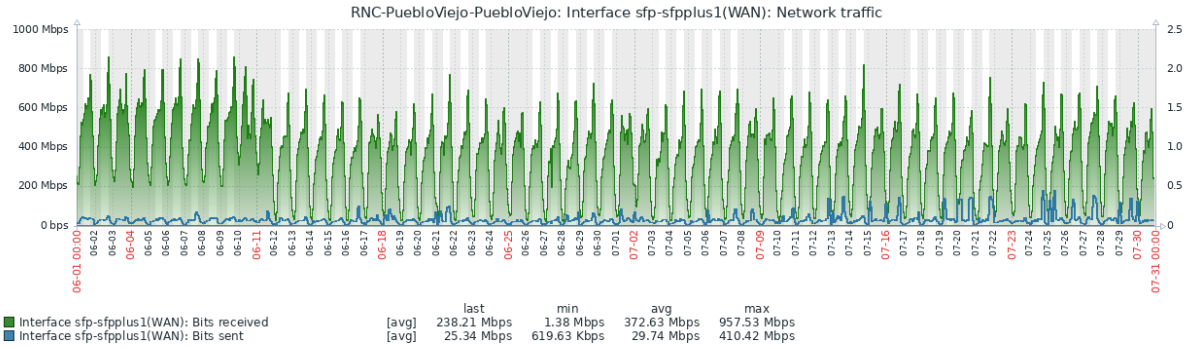


Figura 19. Ancho de banda – Red Nueva Conexión

En la figura 20, se observa el rendimiento de memoria del router de borde de RNC, durante los meses de junio y julio donde su consumo máximo es del 8.46% y un mínimo de 7.03 % del total de la memoria RAM.

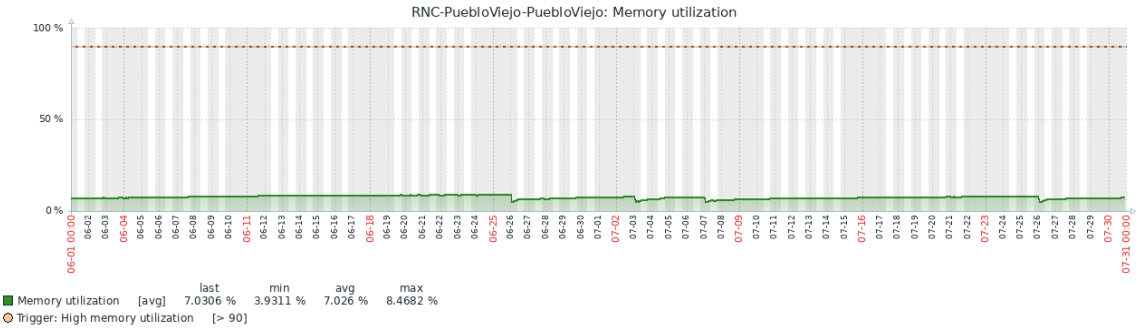


Figura 20. Rendimiento de Memoria RAM - Red Nueva Conexión

En la figura 21, se observa el consumo de CPU del router de borde de RNC durante los meses de junio y julio indicando un consumo máximo del 37%, además se observó el incremento de uso de CPU al mismo tiempo que existió mayor consumo de ancho de banda los primeros 11 días de junio.

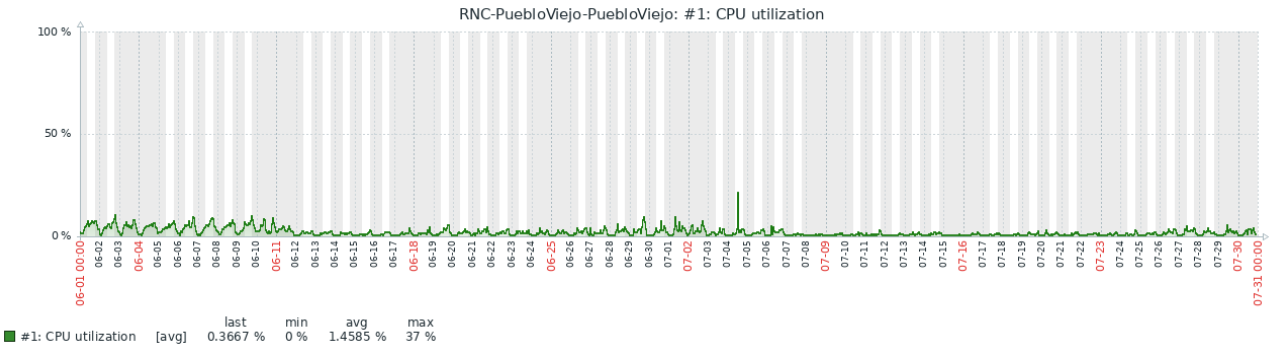


Figura 21. Consumo de CPU – Red Nueva Conexión

6.3.1.1. Eventos más recurrentes

En la figura 22, se obtuvo la información de los eventos más recurrentes en los 35 Proveedores de Servicio de Internet (ISP) durante los meses de junio y julio. Se obtuvo que el ISP YanezNet registra 196 eventos “Interface Ether9(): Link down” con una severidad “Average” (media).

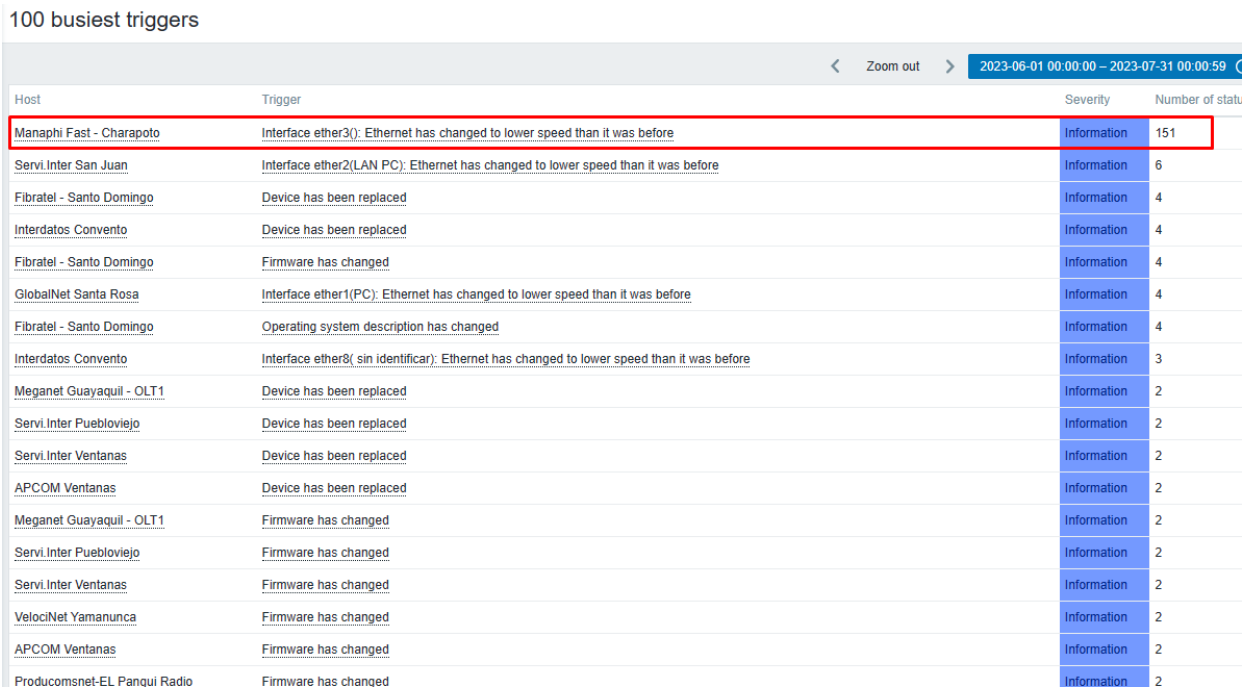
100 busiest triggers

Zoom out | 2023-06-01 00:00:00 – 2023-07-31 00:00:59

Host	Trigger	Severity	Number of status changes
YanezNet Fatima	Interface ether9(): Link down	Average	196
Manaphi Fast - Charapoto	Interface ether3(): Ethernet has changed to lower speed than it was before	Information	151
SWTelecom Pueblonuevo	Interface WisphubVPN(WispHub VPN): Link down	Average	124
CovirNet Pajan	Host has been restarted	Warning	116
Servi.Inter Zapotal	Interface ether3(JORGI QUINTO): Link down	Average	116
Interlive Portete	Interface ether4(PC): Link down	Average	116
Interlive Portete	Interface ether5(): Link down	Average	113
Manaphi Fast - Charapoto	Interface ether3(): Link down	Average	104
YanezNet Coloradal	Interface ether10(): High bandwidth usage	Warning	100
VelociNet Provincias Unidas	Interface wlan2(WIFI 2.4): Link down	Average	100
UltraNet Marianitas	High ICMP ping loss	Warning	90
FrancoNet La Victoria	CPU: Temperature is above warning threshold	Warning	88
FlashNet El volante	Interface ether4(ROUTER CASA): Link down	Average	70
FlashNet La Teresa	Host has been restarted	Warning	68
VentumNet Tingo	Interface ether3(NODO): Link down	Average	68
Teleing - Urdesa	Interface ether6(PC): Link down	Average	68
InterDatos 3 Postes	Interface ether8(Niguito 2 Puertas): Link down	Average	68

Figura 22. Top 100 Triggers más utilizados

En la figura 23, se indica el evento 151 notificaciones del evento “Cambio de velocidad del puerto Ethernet” con severidad informativa.



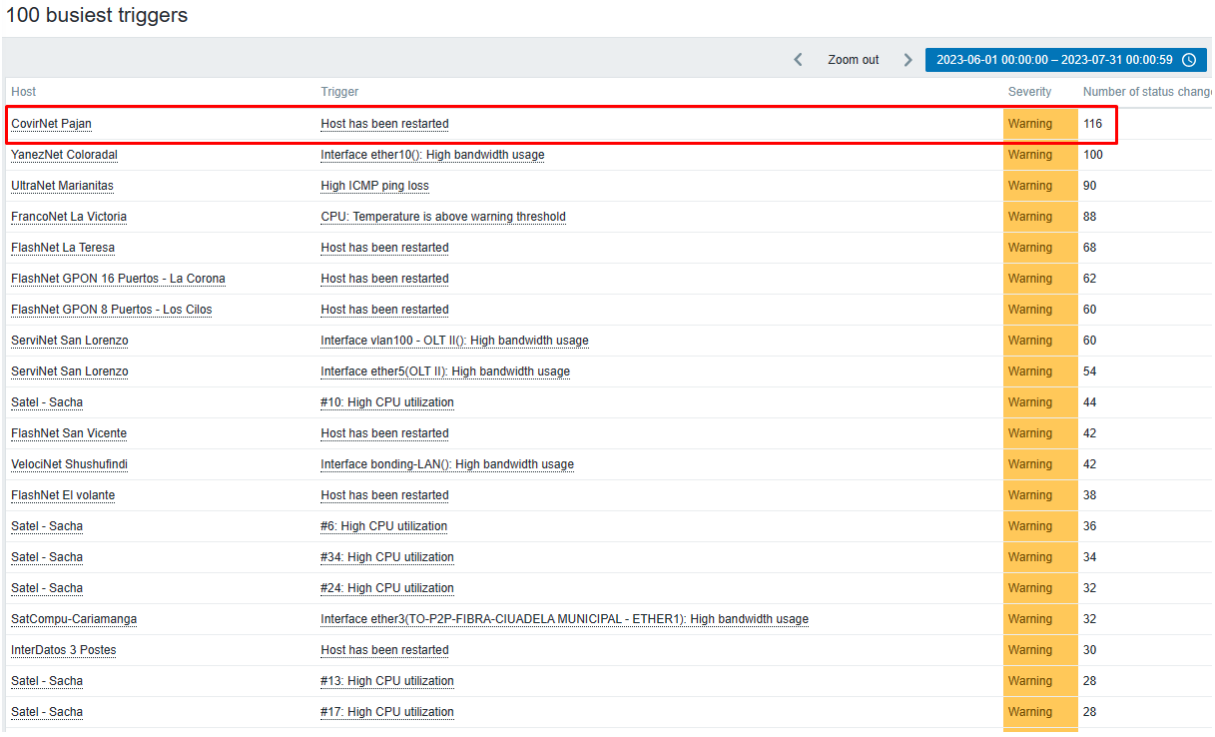
100 busiest triggers

Zoom out | 2023-06-01 00:00:00 – 2023-07-31 00:00:59

Host	Trigger	Severity	Number of statu
Manaphi Fast - Charapoto	Interface ether3(): Ethernet has changed to lower speed than it was before	Information	151
Servi.Inter San Juan	Interface ether2(LAN PC): Ethernet has changed to lower speed than it was before	Information	6
Fibratel - Santo Domingo	Device has been replaced	Information	4
Interdatos Convento	Device has been replaced	Information	4
Fibratel - Santo Domingo	Firmware has changed	Information	4
GlobalNet Santa Rosa	Interface ether1(PC): Ethernet has changed to lower speed than it was before	Information	4
Fibratel - Santo Domingo	Operating system description has changed	Information	4
Interdatos Convento	Interface ether8(sin identificar): Ethernet has changed to lower speed than it was before	Information	3
Meganet Guayaquil - OLT1	Device has been replaced	Information	2
Servi.Inter Puebloviejo	Device has been replaced	Information	2
Servi.Inter Ventanas	Device has been replaced	Information	2
APCOM Ventanas	Device has been replaced	Information	2
Meganet Guayaquil - OLT1	Firmware has changed	Information	2
Servi.Inter Puebloviejo	Firmware has changed	Information	2
Servi.Inter Ventanas	Firmware has changed	Information	2
VelociNet Yamanunca	Firmware has changed	Information	2
APCOM Ventanas	Firmware has changed	Information	2
Producomsnet-EL Pangui Radio	Firmware has changed	Information	2

Figura 23. Evento Severidad Informativa

La figura 24, indica las 116 notificaciones del evento “el host ha sido reiniciado” con Severidad “Warning” en el ISP Covirnet durante los meses de junio y julio del 2023.



100 busiest triggers

Zoom out | 2023-06-01 00:00:00 – 2023-07-31 00:00:59

Host	Trigger	Severity	Number of status chang
CovirNet Pajan	Host has been restarted	Warning	116
YanezNet Coloradal	Interface ether10(): High bandwidth usage	Warning	100
UltraNet Marianitas	High ICMP ping loss	Warning	90
FrancoNet La Victoria	CPU: Temperature is above warning threshold	Warning	88
FlashNet La Teresa	Host has been restarted	Warning	68
FlashNet GPON 16 Puertos - La Corona	Host has been restarted	Warning	62
FlashNet GPON 8 Puertos - Los Cilos	Host has been restarted	Warning	60
ServiNet San Lorenzo	Interface vlan100 - OLT II(): High bandwidth usage	Warning	60
ServiNet San Lorenzo	Interface ether5(OLT II): High bandwidth usage	Warning	54
Satel - Sacha	#10: High CPU utilization	Warning	44
FlashNet San Vicente	Host has been restarted	Warning	42
VelociNet Shushufindi	Interface bonding-LAN(): High bandwidth usage	Warning	42
FlashNet El volante	Host has been restarted	Warning	38
Satel - Sacha	#6: High CPU utilization	Warning	36
Satel - Sacha	#34: High CPU utilization	Warning	34
Satel - Sacha	#24: High CPU utilization	Warning	32
SatCompu-Cariamanga	Interface ether3(TO-P2P-FIBRA-CIUADELA MUNICIPAL - ETHER1): High bandwidth usage	Warning	32
InterDatos 3 Postes	Host has been restarted	Warning	30
Satel - Sacha	#13: High CPU utilization	Warning	28
Satel - Sacha	#17: High CPU utilization	Warning	28

Figura 24. Evento Severidad Warning

La figura 25 indica los eventos con severidad “Average”, destacando el problema de “enlace caído” notificado 116 veces al ISP Yaneznet en los meses de junio y julio del 2023.

100 busiest triggers

Zoom out | 2023-06-01 00:00:00 – 2023-07-31 00:00:59

Host	Trigger	Severity	Number of status chan
YanezNet Fatima	Interface ether9(): Link down	Average	196
SWTelecom Pueblonuevo	Interface WisphubVPN(WispHub VPN): Link down	Average	124
Servi.Inter Zapotal	Interface ether3(JORGI QUINTO): Link down	Average	116
Interlive Portete	Interface ether4(PC): Link down	Average	116
Interlive Portete	Interface ether5(): Link down	Average	113
Manaphi Fast - Charapoto	Interface ether3(): Link down	Average	104
VelociNet Provincias Unidas	Interface wlan2(WIFI 2.4): Link down	Average	100
FlashNet El volante	Interface ether4(ROUTER CASA): Link down	Average	70
VentumNet Tingo	Interface ether3(NODO): Link down	Average	68
Teleing - Urdesa	Interface ether6(PC): Link down	Average	68
InterDatos 3 Postes	Interface ether8(Niguito 2 Puertas): Link down	Average	68
RonalNet Pedro Carbo - Estacada	Interface ether5(HOSPOT RONALD): Link down	Average	64
FlashNet La Teresa	Interface vpnmikrowisp(): Link down	Average	56
Interdatos Convento	Interface ether10(): Link down	Average	52
FlashNet El volante	Interface Volante(): Link down	Average	52
FlashNet San Vicente	Interface SanVicente(): Link down	Average	48
ServiNet San Lorenzo	Interface l2tp-mikrowisp(): Link down	Average	42
Satel - Chaco	Interface ether2(PC): Link down	Average	40
InterLive Balzar	Interface vpnmikrowisp(): Link down	Average	40

Figura 25. Evento Severidad Average

La figura 26, indica las 60 notificaciones del evento “indisponibilidad del Ping ICMP” con severidad “High” en el ISP Flashnet.

100 busiest triggers

Zoom out | 2023-06-01 00:00:00 – 2023-07-31 00:00:59

Host	Trigger	Severity	Number of status changes
FlashNet El volante	Unavailable by ICMP ping	High	60
FrancoNet La Victoria	CPU: Temperature is above critical threshold	High	24
InterDatos 3 Postes	Unavailable by ICMP ping	High	24
InterDatos Babahoyo Fibra	Unavailable by ICMP ping	High	20
InterDatos Babahoyo Babahoyo	Unavailable by ICMP ping	High	20
Interdatos Convento	Unavailable by ICMP ping	High	18
VentumNet Pilalo	Unavailable by ICMP ping	High	17
CalcetaTV	Unavailable by ICMP ping	High	16
YanezNet Fatima	Unavailable by ICMP ping	High	16
Satel - Chaco	Unavailable by ICMP ping	High	16
Fibratel - Santo Domingo	Unavailable by ICMP ping	High	15
SWTelecom Montalvo	Unavailable by ICMP ping	High	14
VelociNet Yamanunca	Unavailable by ICMP ping	High	14
HCNET Safando	Unavailable by ICMP ping	High	14
FiberPlus Mologoc	Unavailable by ICMP ping	High	12
SE La Mana II	Unavailable by ICMP ping	High	12
SWTelecom Pueblonuevo	Unavailable by ICMP ping	High	12
UltraNet Marianitas	Unavailable by ICMP ping	High	12
UltraNet Salazar	Unavailable by ICMP ping	High	12

Figura 26. Evento Severidad High

La figura 27, indica el inventario de dispositivos que se obtuvo con el NMS, como la versión del Sistema Operativo, modelo y nombre de los routers. Esta información es esencial para una gestión eficiente de los recursos, ya que permitió a los administradores de red conocer rápidamente la distribución, modelos y versiones del sistema operativo de los routers en toda la infraestructura.

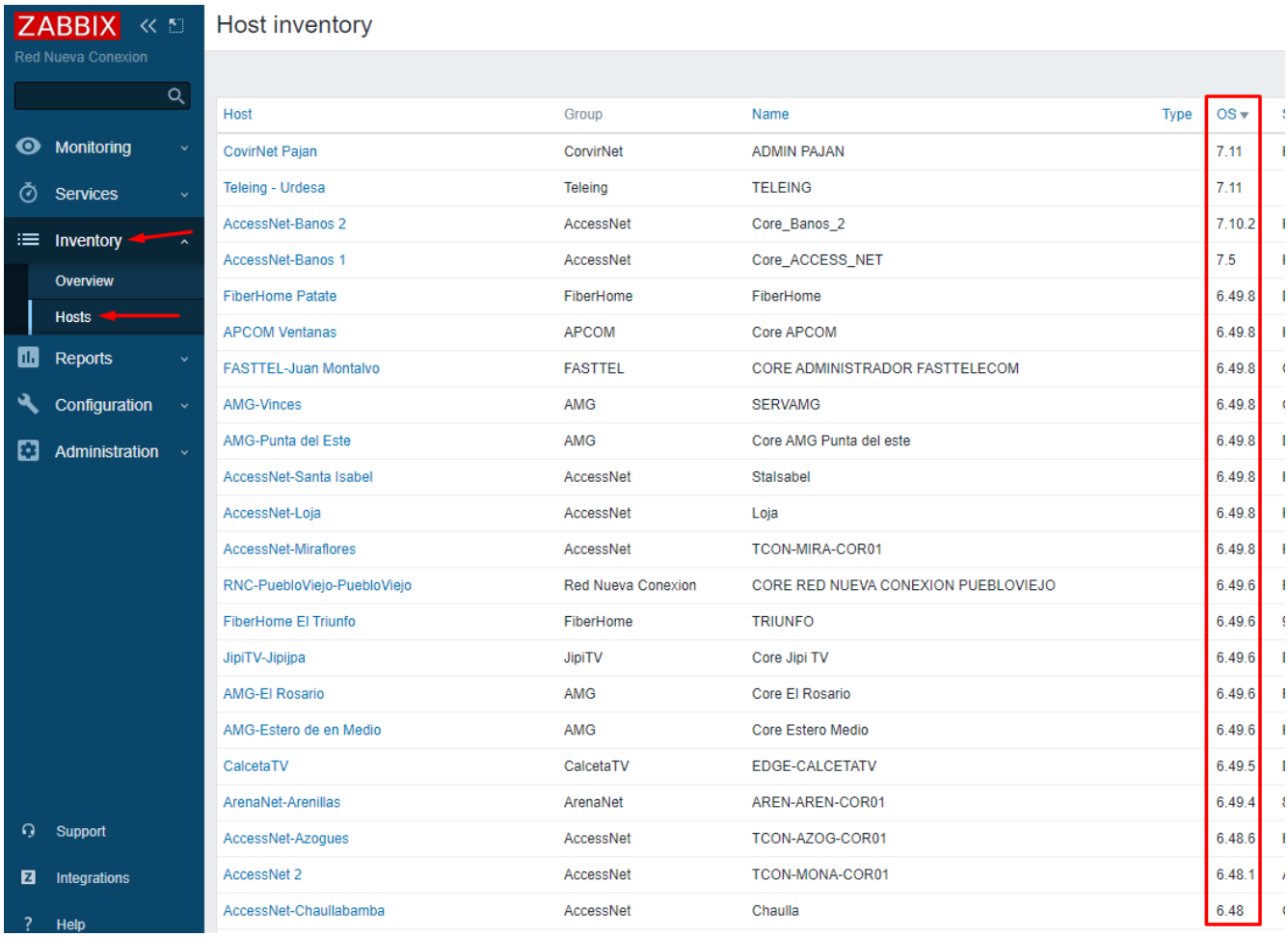


Figura 27. Host inventory

La figura 28, se indica el dashboard creado para el ISP FiberHome, indicando el monitoreo de la pérdida de ping, latencia, memoria usada, CPU y tráfico de la interfaz WAN.

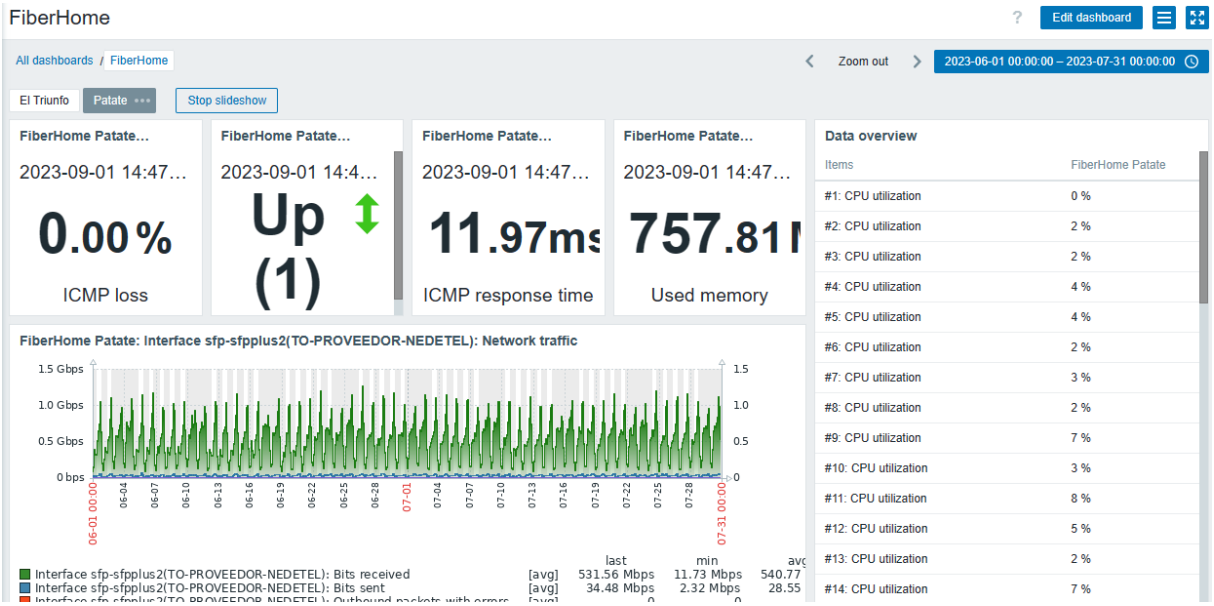


Figura 28. Dashboard ISP FiberHome

La figura 29, indica el mapa de red creado para el ISP Red Nueva Conexión, exponiendo su topología de red y los equipos monitoreados.

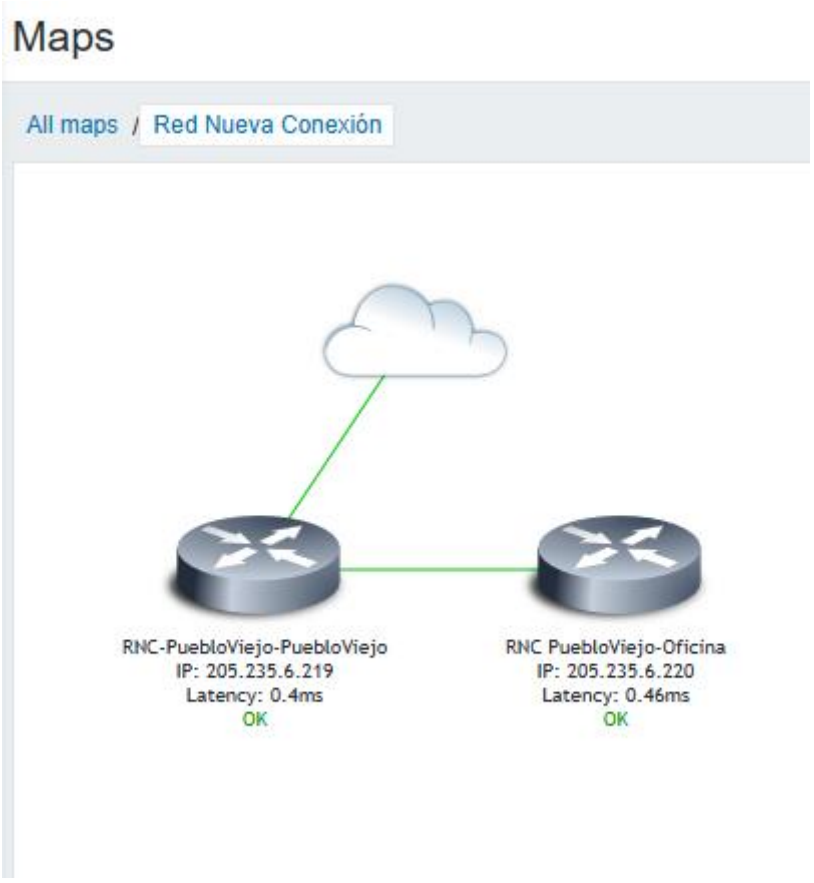


Figura 29. Mapa de Red- ISP Red Nueva Conexión

6.3.1.2. Zabbix gestionando los 100 dispositivos

En la figura 30, se indica el consumo de recursos de CPU del servidor Zabbix durante los meses de junio y julio con un promedio del 19.34 %

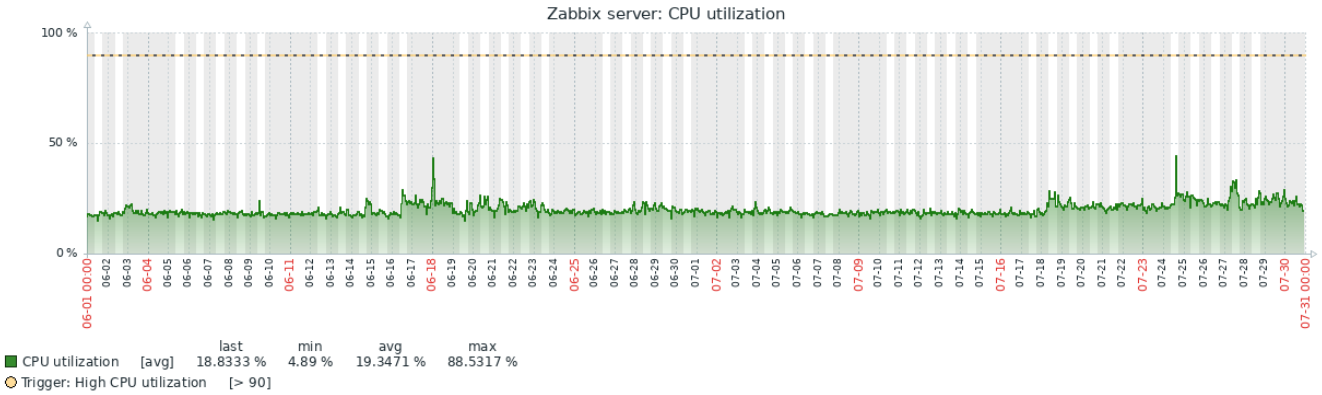


Figura 30. CPU del Servidor Zabbix con 100 dispositivos

La figura 31, representa un consumo promedio del 15.24% de Memoria RAM durante el periodo de junio a julio.

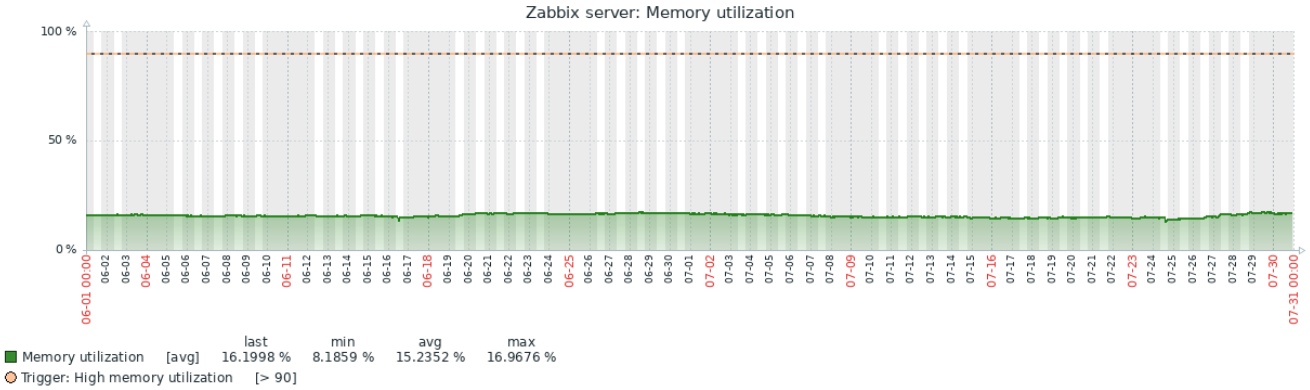


Figura 31. RAM del Servidor Zabbix con 100 dispositivos

6.3.2. Configurar el envío de alertas a los administradores por correo electrónico y una herramienta de mensajería instantánea (Telegram).

En las Figuras 32, se evidencia la notificación enviada por correo electrónico. Esta notificación detalla que la interfaz ether4 (RED_CRISTOBAL_COLON) del ISP Fibratel – Santo Domingo ha experimentado un estado de "Link down", a las 11:16:56 horas del 23 de agosto de 2023,

con una severidad "Average" (media) con identificador ID 15472344, el cual facilita el seguimiento y la identificación precisa del evento ocurrido en este ISP.

Figura 32. Notificación de evento por Correo

En las Figuras 33, se indica la notificación enviada por Telegram, detallando que la interfaz ether4 (RED_CRISTOBAL_COLON) del ISP Fibratel – Santo Domingo ha experimentado un estado de "Link down", a las 11:16:56 horas del 23 de agosto de 2023, con una severidad "Average" (media) con identificador ID 15472344.

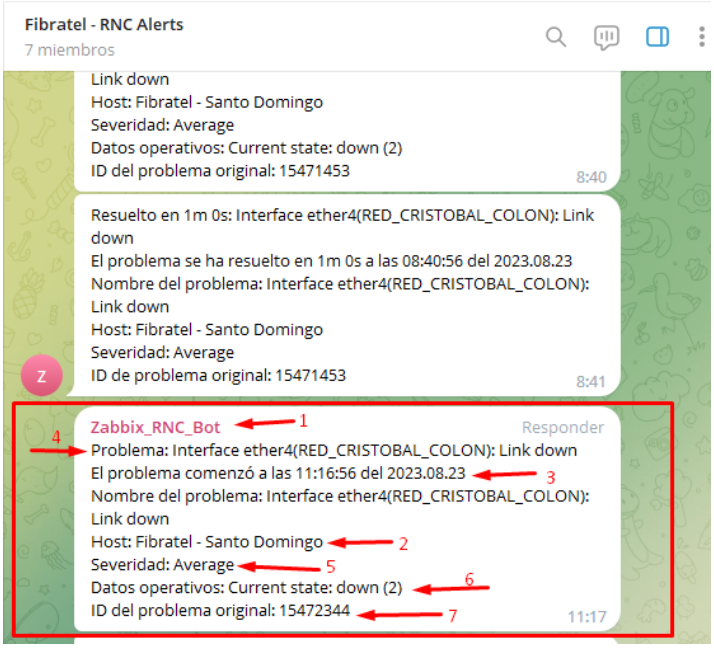


Figura 33. Notificación enviada al grupo de Telegram del ISP Fibratel.

En la Figura 34, se presenta una captura de pantalla del equipo Mikrotik del ISP Fibratel - Santo Domingo y se confirma la información enviada, tanto por correo electrónico como por Telegram, que fue enviado de manera inmediata en que ocurrió el evento. Esta evidencia del registro en el log del equipo Mikrotik, demuestra de manera visual la eficacia y la rapidez del sistema de notificación implementado, asegurando una respuesta instantánea ante los eventos críticos.

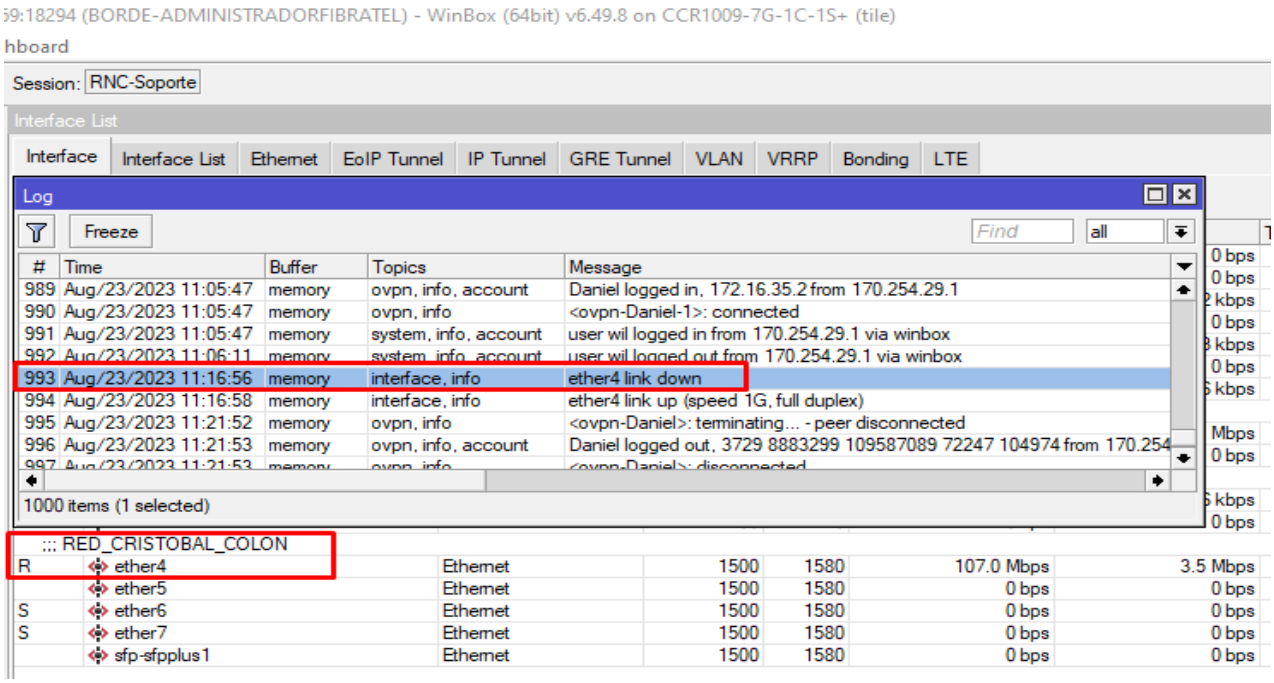


Figura 34. Log Mikrotik – ISP Fibratel Santo Domingo

En el anexo 6 encuentran todos los grupos de Telegram que fueron creados para recibir las notificaciones de los incidentes de host de cada ISP.

6.3.2.1. Encuesta de satisfacción, respecto a las notificaciones por Correo Electronico y Telegram.

La encuesta fue efectuada a los 35 ISP que reciben soporte de la empresa Red nueva Conexion.

1. **¿Recibe notificaciones de eventos a través de Correo o Telegram de manera oportuna?**

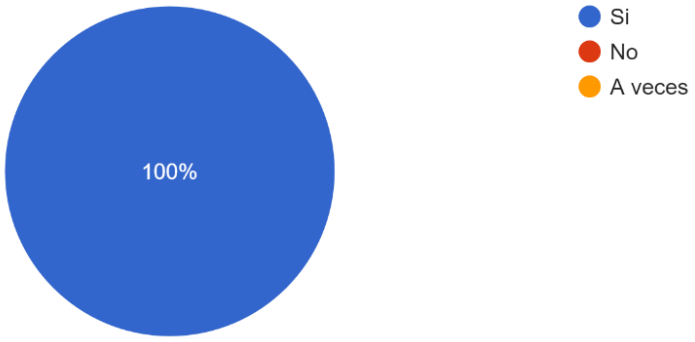


Figura 35. Resultado - Pregunta 1

La figura 35, indico que el 100% de los encuestados sugiere que el sistema de notificaciones a través de correo y Telegram está funcionando de manera eficiente y efectiva, cumpliendo su propósito de proporcionar información oportuna sobre eventos.

2. **¿El contenido de las notificaciones de eventos es claro y comprensible?**

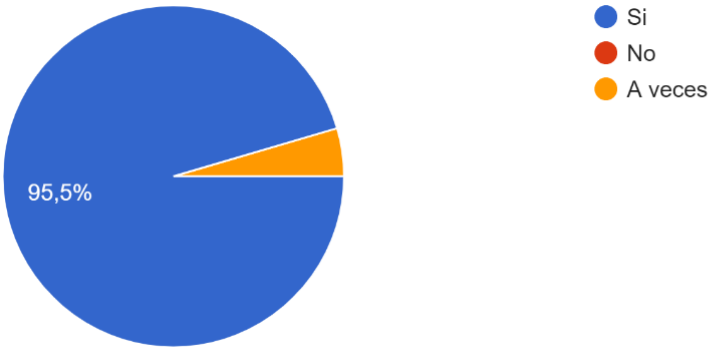


Figura 36. Resultado - Pregunta 2

La respuesta a esta pregunta (figura 36) indicó que el 95.5 % de los participantes perciben que el contenido de las notificaciones que reciben es fácil de entender y brinda información clara sobre los eventos en cuestión, esto gracias a que tienen conocimientos técnicos.

3. **¿Las notificaciones de eventos le permiten abordar problemas técnicos y operativos?**

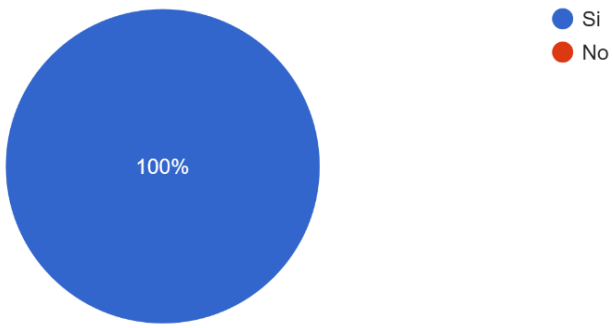


Figura 37. Resultado - Pregunta 3

Respecto a la pregunta 3 (figura 37) el 100 % de los participantes respondió que las notificaciones tuvieron un impacto altamente positivo al permitir abordar problemas técnicos y operativos.

4. **¿Cuándo sucede un evento en la red, el Sistema de Administración de Red (NMS) le notifica inmediatamente?**

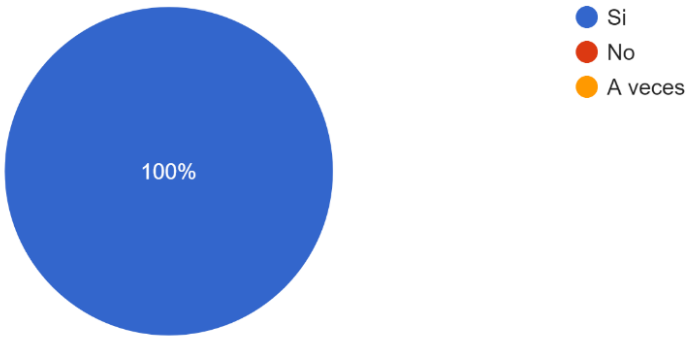


Figura 38. Resultado - Pregunta 4

La respuesta afirmativa del 100% (figura 38) de los participantes refleja la eficacia del Sistema de Administración de Red (NMS) en la notificación inmediata de eventos.

5. **¿Las notificaciones de eventos le permiten tomar medidas preventivas para evitar interrupciones del servicio?**

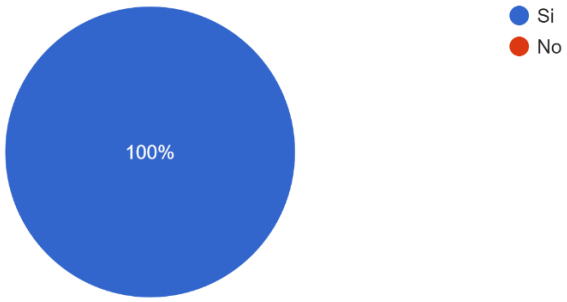


Figura 39. Resultado - Pregunta 5

La respuesta afirmativa del 100% de los participantes en la pregunta 5 (figura 39) indica que las notificaciones de eventos permiten tomar medidas preventivas para evitar interrupciones del servicio.

6. **¿Cuánto tiempo le tomaba detectar los problemas, antes de la implementación de nuestras notificaciones por correo y Telegram?**

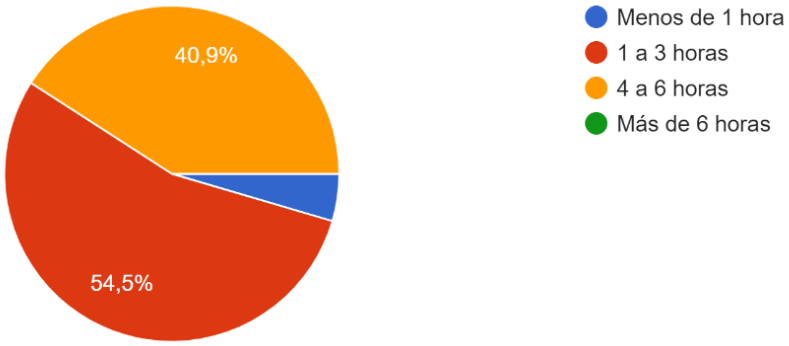


Figura 40. Resultado - Pregunta 6

La figura 40, muestra el resultado de la pregunta 6, en la cual el 54.5% de los encuestados informó que requería de 1 a 3 horas para detectar problemas. El 40.9 % un tiempo mayor de 4 a 6 horas en detectar inconvenientes, y tan solo un 4.6 % de los participantes le tomaba entre 1 hora detectar los eventos ocurridos en su ISP.

6.3.3. Realizar un manual de usuario del NMS para uso del administrador de red.

Para finalizar esta actividad se realizó el manual de usuario del sistema con el objetivo de describir el uso de Zabbix como Sistema de Administración de Red, el manual completo se lo puede observar en el Anexo 7.

En el Anexo 8 y 9, se encuentra el oficio de la entrega del manual de usuario, y la certificación de la Implementación del NMS a la Empresa Red Nueva Conexión.

Red Nueva Conexión
Conectándote al Mundo

Manual de usuario del NMS Zabbix

Implementación de un Sistema de Administración de Red (NMS) para los clientes ISP de la empresa Red Nueva Conexión.

Zabbix

Universidad Nacional de Loja

7. Discusión

La implementación de un Sistema de Administración de Red (NMS) para los clientes ISP de la empresa Red Nueva Conexión, se basa en el cumplimiento de cada objetivo específico planteado que se detallan a continuación:

7.1. Objetivo 1: Analizar tres herramientas NMS Open Source para ISP.

Para el cumplimiento del primer objetivo, se realizó un análisis comparativo a tres sistemas de Administración de Red de código abierto (NMS): Cacti, Nagios Core y Zabbix. El propósito de esta evaluación consistió en analizar las capacidades y limitaciones de cada NMS, en función de las necesidades respecto a la gestión de redes de los ISP.

Con respecto a Cacti, es un NMS que se enfoca en la visualización de datos de rendimiento mediante gráficos ilustrativos. Esta característica resultó sumamente útil para obtener una comprensión rápida de la red. Sin embargo, esta fortaleza no abarca las complejidades de entornos y redes complejas que demandan una capacidad de alertas en tiempo real y la capacidad de adaptarse a nuevas condiciones y requerimientos.

Por otro lado, Nagios Core es destacado por su monitoreo de la disponibilidad y generación de alertas, además su estructura modular permite adaptarse a las peculiaridades de las redes. Sin embargo, cabe señalar que su enfoque en la disponibilidad podría llevar limitaciones cuando se trata de rendimiento y escalabilidad.

Finalmente, Zabbix surgió como una solución equilibrada por sus características, como el monitoreo en tiempo real, la emisión de alertas, la escalabilidad y la flexibilidad. Además de su capacidad de adaptación a entornos de constante cambio y su fácil personalización se consolidaron como un NMS sólido para ISP. Este enfoque se relacionó directamente con los requerimientos obtenidos en la entrevista con el administrador de Red.

7.2. Objetivo 2: Configurar el Sistema de Administración de Red (NMS) y los agentes en los ISP.

Para el cumplimiento de este objetivo, se recopiló la información de la infraestructura de los 35 ISP. Esta fase involucró la identificación de los equipos como servidores, switch o enrutadores. La información que se obtuvo; permitió visualizar un panorama completo de la topología de red y los 100 dispositivos que necesitaban monitoreo constante.

Posteriormente se seleccionó el hardware para la implementación del NMS Zabbix en el servidor Proxmox de la empresa. Esto tiene ventajas en cuanto a la escalabilidad y flexibilidad que Proxmox ofrece para alojar aplicaciones críticas. El hardware consta de 4 CPU, 16 GB de memoria RAM y 100GB de almacenamiento. Conforme a los requerimientos de rendimiento y capacidad de almacenamiento, como se indicó en la sección 6.2.2. de resultados.

En cuanto a la instalación de Zabbix (ver anexo 3), se configuró los elementos cruciales, como base de datos usando María DB, creación de usuarios, grupos de host y uso de la plantilla SNMP Mikrotik, que consta de 19 elementos (items) como: el uso de CPU, la memoria RAM, la carga de la interfaz, el tráfico de red y otros parámetros relevantes. La plantilla está preconfigurada para recopilar información en intervalos regulares y mantener un registro histórico. Además, la plantilla incluye 10 disparadores (triggers) que son fundamentales para la detección y notificación de eventos críticos. Estos disparadores se activan automáticamente cuando los valores medidos superan los umbrales preconfigurados.

Respecto a la configuración del SNMP en los dispositivos Mikrotik de los ISP, se estableció la comunidad RNC-Control y se configuró reglas de firewall en los Mikrotik para garantizar que únicamente se comuniquen con el NMS Zabbix. Se establecieron reglas que filtran y permiten únicamente el tráfico UDP en el puerto 161, garantizando que solo las comunicaciones SNMP estén habilitadas y que cualquier otro tipo de tráfico no autorizado o potencialmente peligroso se restrinja de manera efectiva.

7.3. Objetivo 3: Verificar el funcionamiento del NMS

Esta fase se enfocó en la verificación del funcionamiento del Sistema de Administración de Red (NMS) Zabbix y en la realización de actividades de configuración avanzada. Se llevaron a cabo acciones específicas para asegurar la plena operatividad del sistema. Adicionalmente, se extrajeron gráficas de consumo de ancho de banda de la WAN de cada dispositivo, así como de la utilización de la CPU y la memoria RAM de los hosts, lo que permitió a los administradores de red obtener una visión clara y precisa del rendimiento.

Para fortalecer la capacidad de respuesta ante eventos críticos, se procedió con la configuración de notificaciones de eventos. Esto se logró a través de dos canales principales: correo electrónico y Telegram. Para el correo electrónico se utilizó el correo: **monitoreo@rednuevaconexion.net** y para Telegram se creó el Bot **@Zabbix_RNC_Bot** y se configuraron grupos de Telegram para cada ISP en los que se recibieron las alertas sobre eventos ocurridos en los dispositivos. Esto permitió dar respuesta a la pregunta de investigación, al enviar notificaciones de manera inmediata y oportuna, aumentando la agilidad en la detección y solución de problemas.

Para obtener una comprensión completa de la percepción de los usuarios y su experiencia con las notificaciones, se llevó a cabo una encuesta de satisfacción, que constó de seis preguntas específicas sobre el uso de NMS; y su influencia en la detección de eventos y en la adopción de medidas preventivas por parte de los administradores de red. De acuerdo a las preguntas 1 y 4 de la encuesta se identificó que el 100% de los ISP participantes recibió las notificaciones en tiempo real mediante correo electrónico y Telegram. Además, según los resultados de la pregunta 3 y 5 resaltan que se mejoró en un 100% la identificación de problemas técnicos y operativos de los ISP, así como la toma de medidas preventivas para evitar interrupciones de servicio, mejorando significativamente la detección de los incidentes, que anteriormente se demoraba de 1 a 6 horas como lo indica en la pregunta 6 de la encuesta.

Además, se desarrolló un manual de usuario destinado al administrador de red de la empresa con el objetivo de proporcionar una guía sobre el uso de Zabbix.

8. Conclusiones

La implementación del Sistema de Administración de Red (NMS) Zabbix en la empresa Red Nueva Conexión, proporcionó una plataforma centralizada que brinda información en tiempo real sobre el estado y el rendimiento de la red de los 35 ISP, permitiendo conocer los eventos oportunamente en base a las incidencias detectadas.

El análisis de las soluciones NMS Open Source Cacti, Nagios Core y Zabbix, permitió identificar a Zabbix como la opción óptima para enfrentar los desafíos de la gestión de red. La escalabilidad permitió agregar 100 hosts Mikrotik, con capacidad de expandirse a 200 host con 9600 métricas. La adaptabilidad permitió la creación de dashboards personalizados basados en widgets, gráficas personalizables, mapas de red y manejo de usuarios basados en roles, visibilidad de la información.

Se implementó el NMS Zabbix en un entorno de red, alojado en un servidor Dell R720, con Ubuntu Server como sistema operativo y Proxmox como plataforma de virtualización. La infraestructura virtualizada tiene 4 CPU, 16 GB de RAM y 100 GB de almacenamiento. Con estas características Zabbix gestiona exitosamente 100 dispositivos Mikrotik que componen la infraestructura de los proveedores de servicios de Internet (ISP); involucrando un total de 30,306 ítems y 16,126 disparadores (triggers). El consumo promedio del hardware durante los meses de junio y julio fue del 19.34% de procesador, 15.24% de memoria RAM y de 10.6GB de almacenamiento; es decir aproximadamente un 20% de la capacidad del servidor.

Se utilizó la plantilla Mikrotik SNMP que ofrece Zabbix para el monitoreo de equipos de esta marca. La plantilla tiene 19 ítems de monitoreo y 10 disparadores (triggers) preconfigurados que establecen puntos de referencia específicos para la generación de alertas, lo que garantiza que se notifique de inmediato cuando se superan los límites críticos. Además, el uso de la plantilla permitió el ahorro de tiempo y errores de configuración en los hosts.

Durante los meses de junio y julio, el NMS registró 9114 eventos en los 100 dispositivos de los ISP. Los mensajes críticos detectados fueron: “ping indisponible por ICMP” con 60 notificaciones y “Enlace Caído (Link down)” con 196 notificaciones; en los ISP Flashnet y Yaneznet respectivamente. Siendo los ISP con mayores problemas. El mensaje de advertencia detectado fue “el host ha sido reiniciado” con 116 notificaciones en el ISP Covirnet. Finalmente, el mensaje informativo “Ethernet ha cambiado a una velocidad más baja” con 151 notificaciones en el ISP Manaphifast.

La comunicación en tiempo real mediante correo electrónico y Telegram permitió la interacción de la empresa Red Nueva Conexión y sus clientes ISP, mediante notificaciones que facilitan a los administradores de red comprender rápidamente el incidente, identificar el equipo

afectado, determinar cuándo comenzó el problema y evaluar su gravedad; reduciendo el tiempo de detección de incidentes en los equipos Mikrotik; a una comunicación en tiempo real, mejorando la atención hacia cada uno de los ISP.

9. Recomendaciones

Configurar Zabbix para vincularlo con sistemas de Tickets, para que los incidentes notificados sean asignados directamente al personal técnico.

Integrar Zabbix con Grafana para visualizar la información obtenida por Zabbix en gráficas más interactivas.

Monitorear dispositivos en marcas como cisco o Huawei haciendo uso de las plantillas de Zabbix, puesto que solo se utilizó la plantilla de equipos Mikrotik.

10. Bibliografía

[1] Ministerio de Telecomunicaciones y Sociedad de la Información, «Agenda de Transformación Digital del Ecuador 2022-2025», 2022, Accedido: 2 de septiembre de 2023. [En línea]. Disponible en: https://www.arcotel.gob.ec/wp-content/uploads/2022/08/Agenda-transformacion-digital-2022-2025.pdf

[2] D. I. Karyabwite Coordinador y R. Hill, «Manual sobre redes basadas en el Protocolo Internet (IP) y asuntos conexos», 2005, Accedido: 6 de junio de 2023. [En línea]. Disponible en: www.itu.int/ITU-T/special-projects/ip-policy/fi

[3] F. P. Baño, S. R. Lascano, F. A. Viscaino, y W. V. Culque, «Propuesta de un proveedor de servicios de internet de banda ancha utilizando la red eléctrica Proposal for a broadband internet service provider using the electrical network».

[4] Luis Molero, «Introducción a la Gestión de Redes», *Universidad "Dr. Rafael Belloso Chacín"*, vol. 2010.

[5] M. T. I. C. Alberto y R. Hernández, «Administración de redes», 2019. Accedido: 27 de junio de 2023. [En línea]. Disponible en: http://ri.uaemex.mx/bitstream/handle/20.500.11799/108337/secme-25150_1.pdf?sequence=1

[6] William. Stallings, J. M. López Soler, y A. Prieto Espinosa, *Comunicaciones y redes de computadores*. Prentice Hall, 2000.

[7] López Angel, *Protocolos de Internet*, Alfaomega. Mexico, 2003.

[8] «8.2.1.1 Introducción a SNMP». https://www.sapalomera.cat/moodlecf/RS/4/course/module8/8.2.1.1/8.2.1.1.html (accedido 13 de junio de 2023).

[9] «SNMP Enumeration - GeeksforGeeks». https://www.geeksforgeeks.org/snmp-enumeration/ (accedido 13 de junio de 2023).

[10] CIC Consulting Informático, «Network Management System - CIC Consulting Informático», 30 de agosto de 2017. https://www.cic.es/que-es-un-nms-network-management-system/ (accedido 11 de junio de 2023).

[11] The Cacti Group, «Cacti® - The Complete RRDTool-based Graphing Solution». https://www.cacti.net/ (accedido 11 de mayo de 2023).

[12] F. Fahreza y M. Rifqi, «Nagios Core Optimization By Utilizing Telegram as Notification of Disturbance», *Journal of Applied Science, Engineering, Technology, and Education*, vol. 2, n.º 2, pp. 121-135, nov. 2020, doi: 10.35877/454RI.asci2259.

[13] «Nagios Core. Download Nagios Core For Free Here.» https://www.nagios.org/projects/nagios-core/ (accedido 13 de junio de 2023).

[14] «www.openitnet.com | Nagios Core». https://www.openitnet.com/index.php/software/inst-software-libre/nagios-core (accedido 13 de junio de 2023).

[15] Zabbix LLC, «Zabbix features overview», 2023. https://www.zabbix.com/la/features (accedido 11 de junio de 2023).

[16] Zabbix SIA, «Zabbix Manual». https://www.zabbix.com/documentation/6.2/en/manual (accedido 11 de mayo de 2023).

[17] S. Sambachi, D. Aracely, W. Tanguila, y A. Jamil, «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», Universidad de las Fuerzas Armadas ESPE, Latacunga, 2021.

[18] Intriago Cedeño Milton Luyely, «Comparativa entre herramientas de monitoreo de red de computadoras aplicadas a la Empresa Puerto Atún», Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix Lopéz, Calceta, 2019.

[19] C. A. Duffaut Misajel y R. E. Reyes Ramirez, «Influencia del software Zabbix para el monitoreo de infraestructura de TI en la SUNARP Zona Registral N° XI - Sede Ica», *Repositorio Institucional - UCV*, 2021, Accedido: 3 de agosto de 2023. [En línea]. Disponible en: https://repositorio.ucv.edu.pe/handle/20.500.12692/67190

[20] Garcia Salas Jorge Stteven y Roa Piñeros Camilo Andres, «Diseño de una herramienta de monitoreo y control de servidores utilizando como eje principal CACTI. Aplicado a una pyme mediana», Universidad Cooperativa De Colombia, Bogota, 2020. Accedido: 6 de junio de 2023. [En línea]. Disponible en: https://repository.ucc.edu.co/server/api/core/bitstreams/5d68b3fb-20be-4a6a-b8e3-785ce8884c53/content

[21] Intriago Cedeño Milton Luyely, Carrera Sánchez Freddy Andrés, Morejón López Eduardo, y Pita Valencia Josselyn Stefanía, «Evaluación de herramientas de monitoreo para mejorar la seguridad de la red de datos», *Revista Interdisciplinaria de Humanidades, Educación, Ciencia y Tecnología*, 2022. Accedido: 6 de junio de 2023. [En línea]. Disponible en: https://www.cienciamatriarevista.org.ve/index.php/cm/article/view/1053/1753

[22] L. Rios Epalza, «Implantación de un sistema de monitoreo para la infraestructura de red de datos de la UFPS sede Cúcuta y Campos

Elíseos», *http://alejandria.ufps.edu.co/descargas/tesis/1151177.pdf*, 2020, doi: 10.1/JQUERY.MIN.JS.

[23] Vega Picon Guillermo Eduardo, «Implementación de un sistema de monitoreo para el análisis de la disponibilidad, capacidad, calidad y latencia de enlaces corporativos de última milla.», 2018. Accedido: 7 de agosto de 2023. [En línea]. Disponible en: http://repositorio.ucsg.edu.ec/handle/3317/11890

[24] Zabbix SIA., «2 Requirements». https://www.zabbix.com/documentation/6.2/en/manual/installation/requirements (accedido 18 de junio de 2023).

[25] Dell Inc., «PowerEdge R720», 2014, Accedido: 19 de julio de 2023. [En línea]. Disponible en: www.dell.com/QRL/Server/PER720

11. Anexos

Anexo 1. Certificado de colaboración de Red Nueva Conexión.

Red Nueva Conexión
Conectándote al Mundo

Puebloviejo, 21 de abril de 2023

Ing. Manuel Ignacio Tandazo Mera
Gerente de Red Nueva Conexión

CERTIFICA:

Que, Red Nueva Conexión colaborará y brindara todas las facilidades de acceso a la red, así como a su infraestructura; además, asumirá los costos del hardware (servidor) necesario para la **Implementación de un Sistema de Administración de Red (NMS) para los clientes ISP de la empresa Red Nueva Conexión**, que el señor **Ruben Dario Lozano Lozano** con **C.I. 1900826569**, implementará en el centro de datos de la empresa, con la finalidad de monitorear la infraestructura de red; proyecto que servirá como Trabajo de Titulación, que será presentado para los fines legales pertinentes y optar al Título de Ingeniero en Sistemas.

Es cuanto puedo indicar en honor a la verdad, facultando al interesado hacer uso del presente documento para los fines que estime conveniente.

Atentamente,

MANUEL IGNACIO TANDAZO MERA
Firmado digitalmente por MANUEL IGNACIO TANDAZO MERA
Fecha: 2023.09.07 11:14:06 -05'00'

Ing. Manuel Tandazo Mera
C.I. 1206535450
Gerente - Red Nueva Conexión

Anexo 2. Entrevista al personal administrativo

Tabla 10. Entrevista

Objetivo:	Obtener información necesaria para seleccionar el NMS
Entrevistado:	Administrador de red, Técnico de soporte
Preguntas	

1. **¿Existe algún sistema para monitorear los ISP que gestiona?**
   Actualmente no tenemos ningún sistema de monitoreo.
2. **¿Conoce o ha escuchado de alguna de estas herramientas de monitoreo de red?**
   Si, y conociendo los beneficios que estos sistemas ofrecen se necesita implementar en la empresa.
3. **¿Cuenta con presupuesto para la implementación de sistema de monitoreo?**
   No, el sistema debe ser de licencia libre es decir Open Source. La empresa dispone de un servidor para que se pueda implementar este sistema.
4. **¿Qué dispositivos, enlaces, recursos y servicios se requieren monitorear?**
   Se desea monitorear los router de borde de las empresas ISP que administra Red nueva Conexión, y conocer el estado la disponibilidad de estas, el ancho de banda de las interfaces de red (WAN), además conocer el uso de memoria RAM y de CPU.
5. **¿Cuáles son las características de hardware de los dispositivos a monitorear?**
   Todos los routers que se administra en los ISP son de la marca Mikrotik.
6. **¿Cuáles son los requerimientos que la herramienta de monitoreo debe poseer como aplicación?**
   El sistema de debe permitir el monitoreo en tiempo real de todos los recursos de los routers de las empresas ISP. Debe tener una interfaz web intuitiva que permita una fácil personalización y adaptable para visualizar la información de los dispositivos, para satisfacer de manera individual los requisitos de cada ISP. Se necesita recibir alertas y notificaciones en tiempo real de los incidentes de las redes de los ISP.
   ,

Anexo 3. Instalación de Zabbix

Para la instalación de Zabbix se debe disponer de un sistema operativo instalado, en este caso se lo realizó sobre Ubuntu server 22.04.

1. **Descarga de Zabbix**

   Se debe acceder a la página oficial de Zabbix y en la sección descargas seleccionar la versión de Zabbix que se desea instalar, el sistema operativo en este caso Ubuntu, la versión del SO 22.04, componentes de Zabbix en este caso el server, frontend y agente, la base de datos MySQL y el servidor web Apache.

Figura 41. Página de descarga de Zabbix

2. **Instalación del repositorio de Zabbix sobre Ubuntu Server 22.04**

Acceder mediante consola al servidor usando una cuenta con privilegios de root e instalar el repositorio para esto se ejecuta los siguientes comandos y posteriormente actualizar los repositorios.

```
# wget https://repo.zabbix.com/zabbix/6.2/ubuntu/pool/main/z/zabbix-release/zabbix-release_6.2-4%2Bubuntu22.04_all.deb
# dpkg -i zabbix-release_6.2-4+ubuntu22.04_all.deb
# apt update
```

3. **Instalación del servidor, la interfaz web y el agente de Zabbix**

Se instala el servidor, la interfaz web, el agente Zabbix y el frontend web con soporte de base de datos MySQL

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

4. **Crear la base de datos**

Se procede a la creación de una base de datos que servirá para almacenar los datos que este servidor recogerá de los agentes.

```
# mysql -uroot -p
password
mysql> create database zabbix character set utf8mb4 collate utf8mb4_bin;
mysql> create user zabbix@localhost identified by 'password';
mysql> grant all privileges on zabbix.* to zabbix@localhost;
mysql> set global log_bin_trust_function_creators = 1;
mysql> quit;
```

5. **Importación del esquema y los datos iniciales**

Importación del esquema SQL

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

Deshabilitar la opción log_bin_trust_function_creators

```
# mysql -uroot -p
password
mysql> set global log_bin_trust_function_creators = 0;
mysql> quit;
```

6. **Configuración de la base de datos**

Para la configuración de la base datos se debe editar el archivo **/etc/zabbix/zabbix_server.conf** y en la línea **DBPassword=password** ingresar la contraseña de la base de datos creada anteriormente.

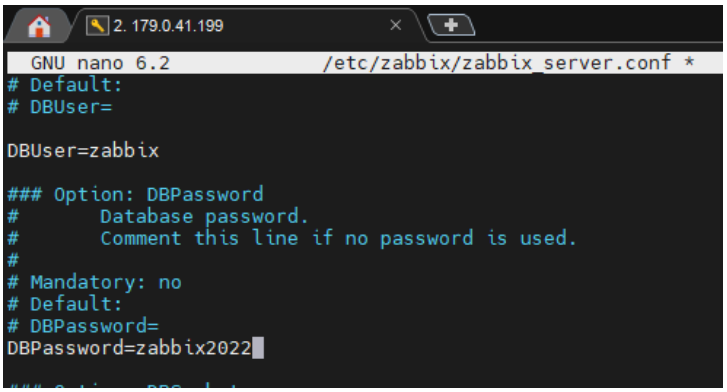


Figura 42. Configuración base de datos Zabbix

7. Iniciar los procesos del agente y servidor Zabbix

En este paso se inician los procesos del agente y del servidor Zabbix para que inicien con el sistema.

```
# systemctl restart zabbix-server zabbix-agent apache2
# systemctl enable zabbix-server zabbix-agent apache2
```

8. Configuración de la interfaz web de Zabbix

Se abre navegador web y se digita la dirección IP del servidor en este caso **http://direccion-IP/zabbix** y se escoge el idioma a usar.

Figura 43. Interfaz de bienvenida de Zabbix

9. Verificación de los prerrequisitos

En la Figura 44, se indica la verificación de los requisitos del servidor web Zabbix, hay que verificar que todos estén en OK para seguir con la instalación.

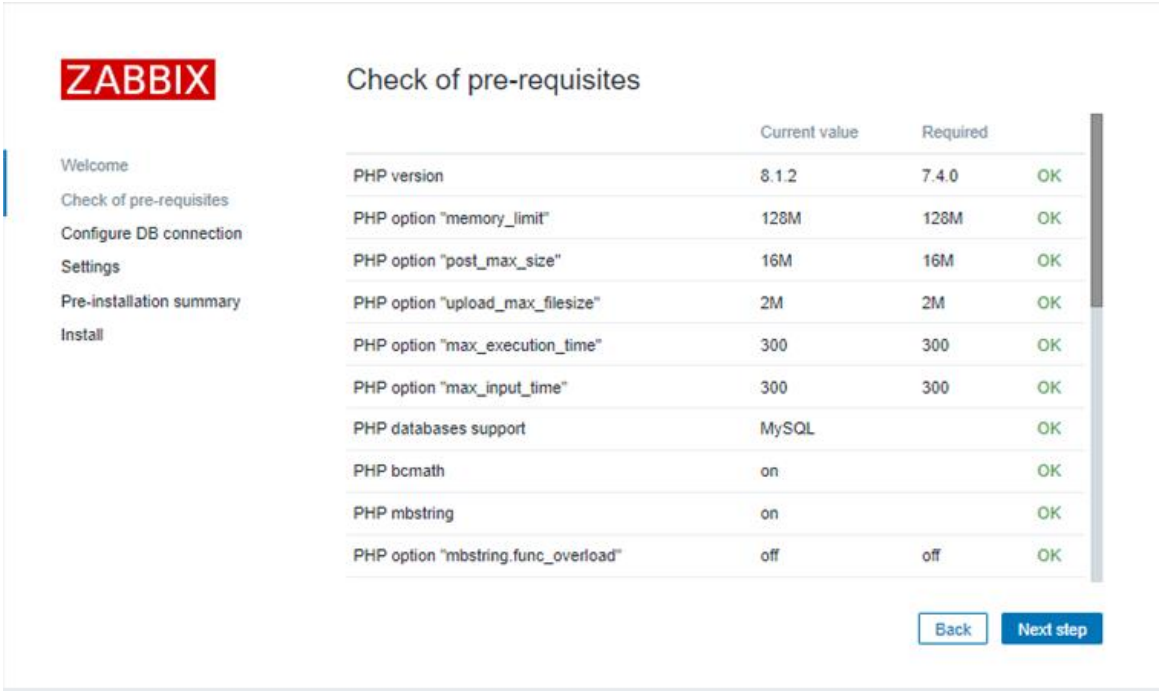


Figura 44. Verificación de Prerrequisitos

10. Configuración de la conexión a la base de datos

En esta pantalla se ingresa el nombre de la base de datos previamente creada, así como el usuario y contraseña de la misma.

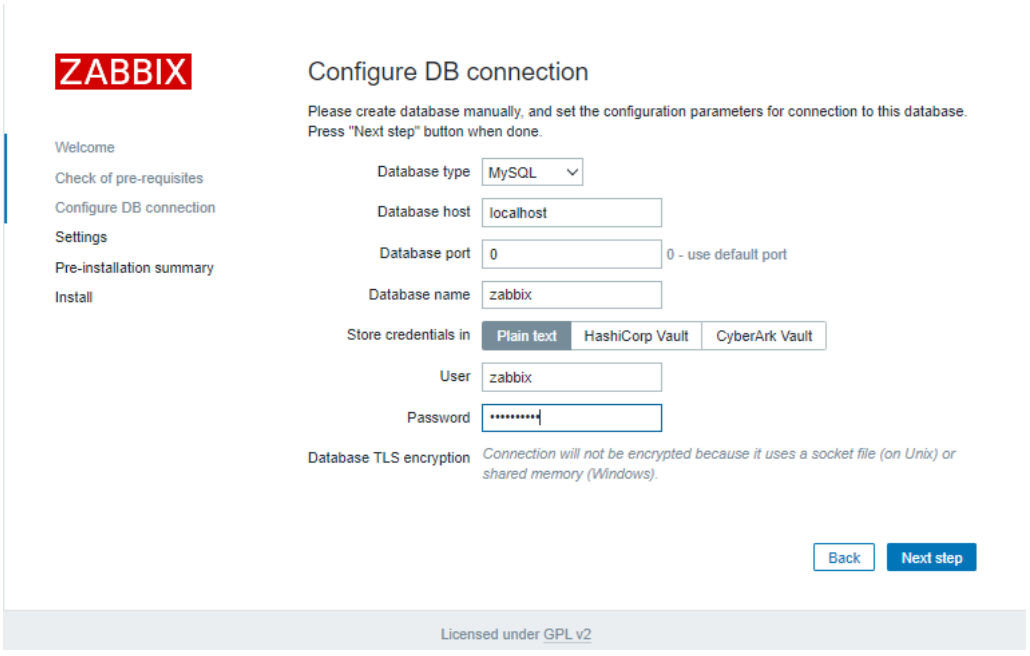


Figura 45. Configuración de conexión a la DB

11. Ajustes del servidor

En este paso se configura el nombre del servidor Zabbix, la zona horaria y el tema por defecto.

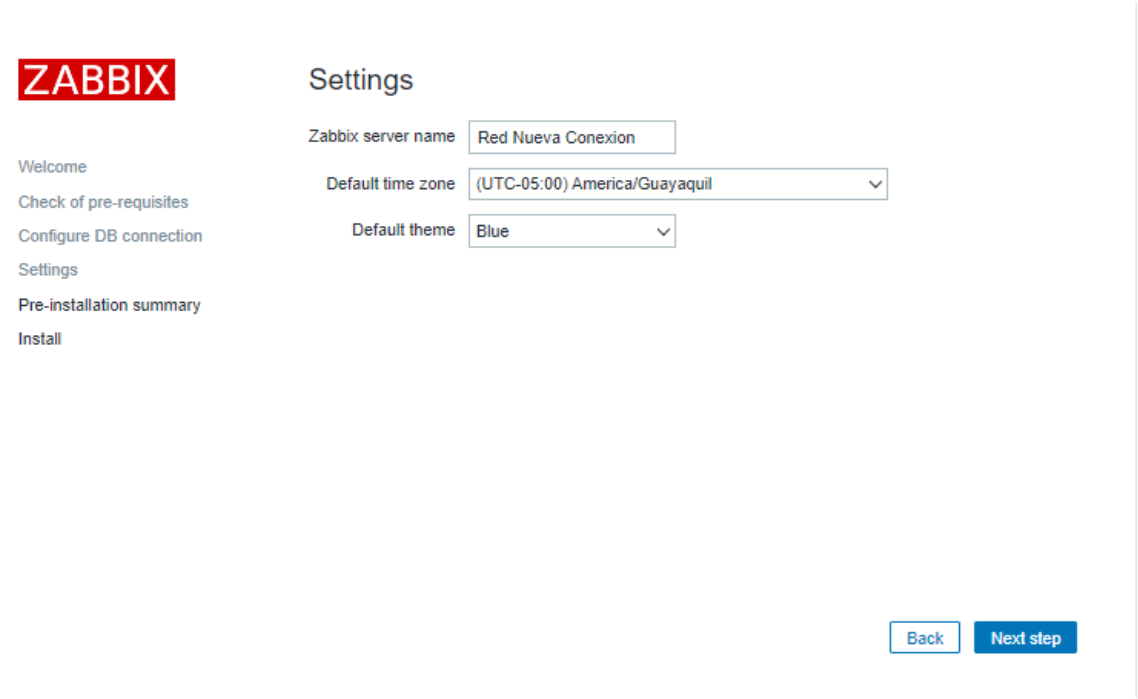


Figura 46. Ajustes del servidor

12. Resumen de la Preinstalación

Esta pantalla indica de forma resumida todos los parámetros configurados para el frontend de Zabbix.

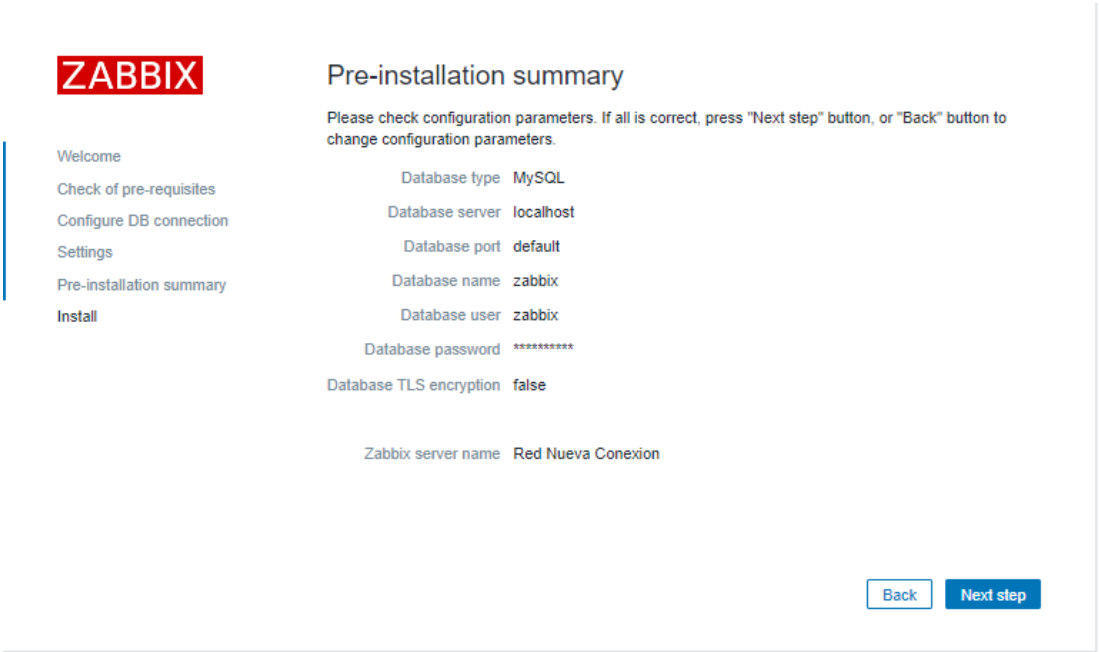


Figura 47. Confirmación de la preinstalación

13. Instalación finalizada del Frontend

Esta pantalla indica que la instalación del frontend de Zabbix ha sido instalada correctamente.

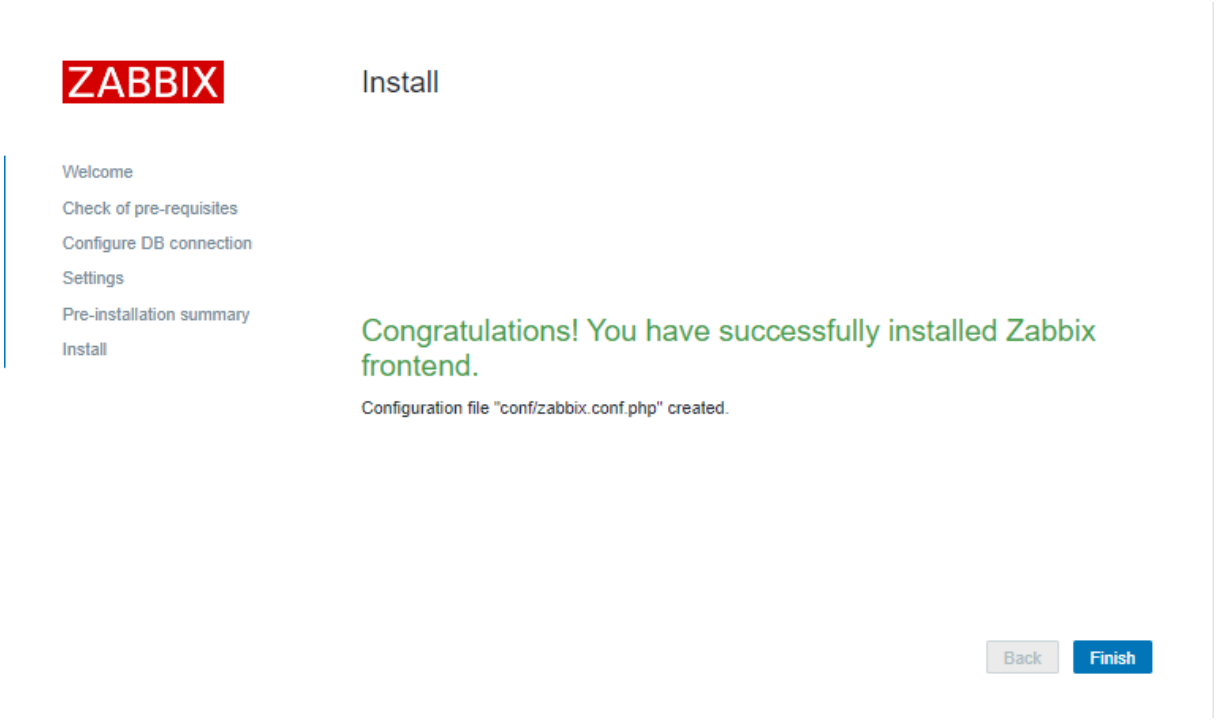


Figura 48. Instalación del frontend de Zabbix

14. Inicio de sesión

Una vez finalizada la instalación de Zabbix se muestra la pantalla de inicio de sesión, a la cual se accede con las siguientes credenciales por defecto: Usuario: Admin y la contraseña: zabbix.

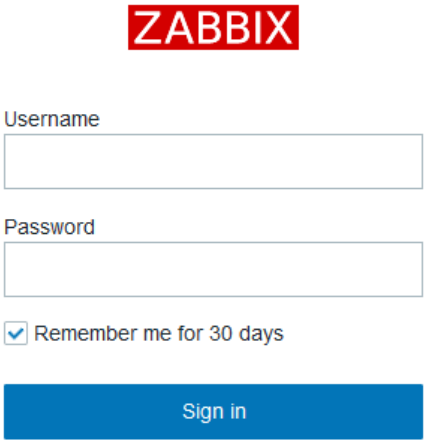


Figura 49. Página de Acceso a Zabbix

Anexo 4. Datasheet del servidor y equipos Mikrotik

Feature	PowerEdge R720 technical specification
Form factor	2U rack
Processors	Intel® Xeon® processor E5-2600 or E5-2600 v2 product families
Processor sockets	2
Internal interconnect	2 x Intel QuickPath Interconnect (QPI) links; 6.4GT/s; 7.2GT/s; 8.0GT/s
Cache	2.5MB per core; core options: 4, 6, 8, 10, 12
Chipset	Intel C602
Memory[1]	Up to 768GB (24 DIMM slots): 2GB/4GB/8GB/16GB/32GB DDR3 up to 1866MT/s
I/O slots	**6 PCIe slots:** • 1 x16 full-length, full-height • 3 x8 full-length, full-height • 3 x8 half-length, half-height • 1 x16 full-length, full-height (optional)
RAID controller	**Internal controllers:** PERC S110 (SW RAID) PERC H310 PERC H710 PERC H710P **External HBAs (RAID):** PERC H810 **External HBAs (non-RAID):** 6Gbps SAS HBA LSI 9207-8i HBA
Drive bays	Up to eight 3.5" drives or up to sixteen 2.5" drives
Maximum internal storage[1]	32TB
Hard drives	**Hot-plug hard drive options:** 2.5" PCIe SSD, SAS SSD, SATA SSD, SAS (15K, 10K), nearline SAS (7.2K), SATA (7.2K), SAS 512n (15K) 3.5" SAS (15K), nearline SAS (7.2K), SATA (7.2K); Self-encrypting drives available
Embedded NIC	Broadcom® 5720 quad-port 1GbE Base-T (no TOE or iSCSI offload) Broadcom 57800S dual-port 10GbE Base-T with 2 x 1GbE (TOE and iSCSI offload available on 10GbE ports Broadcom 57800S dual-port 10GbE SFP+ with 2 x 1GbE (TOE and iSCSI offload available on 10GbE ports Broadcom 57840S quad-port 10GbE SFP+ Rack NDC (NPAR1.0, SRIOV, DCB, iSCSI and FCoE offloads and CEM) Intel I350 quad-port 1GbE Base-T (no TOE or iSCSI offload) Intel X540 dual-port 10GbE Base-T with 2 x 1GbE (FCoE capability enabled on the 10GbE ports)
Power supplies	Titanium efficiency, hot-plug redundant 750W AC power supply (200-240VAC only); auto-ranging Platinum efficiency, hot-plug redundant 495W, 750W or 1100W AC power supply; 1100W DC power supply (-48VDC)
Availability	High-efficiency, hot-plug, redundant power supplies; hot-plug drive bays; TPM; dual internal SD support; hot-plug, redundant fan; optional bezel; information tag; ECC memory, interactive LCD screen; extended thermal support; ENERGY STAR® compliant; switch independent partitioning
Remote management	iDRAC7 with Lifecycle Controller Express (default), iDRAC7 Enterprise (upgrade option) 8GB vFlash media (upgrade option), 16GB vFlash media (upgrade optional)
Systems management	IPMI 2.0 compliant Dell OpenManage Essentials Dell OpenManage Mobile Dell OpenManage Power Center Dell OpenManage Integrations: • Dell OpenManage Integration Suite for Microsoft® System Center • Dell OpenManage Integration for VMware® vCenter™ Dell OpenManage Connections: • HP Operations Manager, IBM Tivoli® Netcool®, and CA Network and Systems Management • Dell OpenManage Plug-in for Oracle Database Manager
Rack support	ReadyRails™ II sliding rails for tool-less mounting in 4-post racks with square or unthreaded round holes or tooled mounting in 4-post threaded hole racks, with support for optional tool-less cable management arm. ReadyRails static rails for tool-less mounting in 4-post racks with square or unthreaded round holes or tooled mounting in 4-post threaded and 2-post (Telco) racks.
Operating systems	Microsoft® Windows Server® 2012 R2 (includes Hyper-V®) Microsoft Windows Server 2012 (includes Hyper-V) Microsoft Windows Server 2008 R2 SP1, x64 (includes Hyper-V) Microsoft Windows Small Business Server 2011 Novell® SUSE® Linux Enterprise Server Red Hat® Enterprise Linux® **Virtualization options:** Citrix® XenServer® VMware vSphere® ESXi™ Red Hat Enterprise Virtualization® For more information on the specific versions and additions, visit Dell.com/OSsupport.

Global services and support

Reduce IT complexity, lower costs and eliminate inefficiencies by making IT and business solutions work harder for you. You can count on Dell for end-to-end solutions to maximize your performance and uptime. A proven leader in Servers, Storage and Networking, Dell Enterprise Solutions and Services deliver innovation at any scale. And if you're looking to preserve cash or increase operational efficiency, Dell Financial Services has a wide range of options to make technology acquisition easy and affordable. Contact your Dell Sales Representative for more information.

Learn More at Dell.com/PowerEdge.

March 2014 | Version 5.0
Dell_PowerEdge_R720_SpecSheet

Figura 50. Datasheet Servidor PowerEdge R720

MikroTik CCR1072-1G-8S+

Specifications

Product code	CCR1072-1G-8S+
CPU nominal frequency	1 GHz
CPU core count	72
Size of RAM	16 GB
Storage	128 MB Onboard NAND, also see *expansion*
10/100/1000 Ethernet ports	1
Power supply	2x IEC C14 standard connectors 110/220V (Two redundant PSU)
Supported input voltage	12 V
CPU temperature monitor	Yes
PCB temperature monitor	Yes
Voltage Monitor	Yes
Current monitor	Yes
Dimensions	443 x 315 x 44 mm, weight: 3.8 kg, weight with packaging: 5.125 kg
License level	6
Operating System	RouterOS
CPU	Tilera Tile-Gx72 CPU
Max Power consumption	125 W
Display	Color LCD, touchscreen
SFP	8x 10G Ethernet SFP+ cages (Mini-GBIC; SFP module not included), DDMI support
Expansion	1x microUSB 2.0, 1x regular USB 2.0, full size Smart Card slot, microSD slot, 2x M.2 slots with x4 PCIE 2.0, Key-M, module size support: 2242,2260,2280
Serial port	RJ45
Suggested price	$3,050

Included

2x IEC cords

Screw and feet kit

Rackmount ears

Figura 51. Datasheet CCR 1072-1g-8s+

Specifications

Product code	CCR2216-1G-12XS-2XQ
CPU	AL73400 2 GHz
CPU architecture	ARM 64bit
CPU core count	16
Size of RAM	16 GB
RAM type	DDR4
Storage	128 MB, NAND
Number of 1G Ethernet ports	1
Number of 25G SFP28 ports	12
Number of 100G QSFP28 ports	2
Number of M.2 slots	2
Operating system	RouterOS (License level 6)
Switch chip model	98DX8525
Switch connection to CPU	4x25 Gbps
Dimensions	443 x 367 x 44 mm
Operating temperature	-20°C to +60°C

Powering

Number of AC inputs	2
AC input range	100-240 V
Power adapter nominal voltage	12 V
Power adapter nominal current	12.5 A
Max power consumption (without attachments)	80 W
Max power consumption	121 W

Included parts

2 Power cords | Rackmount ears | Rackmount rear support ears | Cable managment bracket | Fastening set

Figura 52. Datasheet CCR2216-1G-12XS-2XQ

MikroTik

Specifications

Product code	CCR2116-12G-4S+
CPU	AL73400 2 GHz
CPU architecture	ARM 64bit
CPU core count	16
Size of RAM	16 GB
RAM type	DDR4
Storage	128 MB, NAND
Number of 1G Ethernet ports	13
Number of 10G SFP+ ports	4
Number of M.2 slots	1
Operating system	RouterOS (License level 6)
Switch chip model	98DX3255
Dimensions	443 x 199 x 44 mm
Operating temperature	-20°C to +60°C

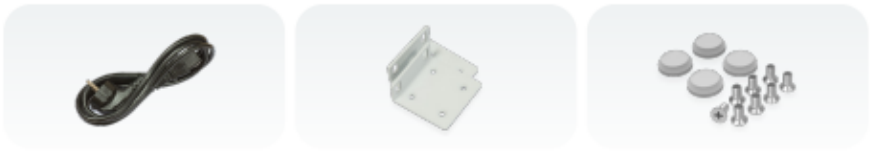
Powering

Number of AC inputs	2
AC input range	100-240 V
Power adapter nominal voltage	12 V
Power adapter nominal current	10.8 A
Max power consumption (without attachments)	60 W
Max power consumption	72 W

Certification & Approvals

Certification	CE, FCC, IC

Included parts



2 Power cords | Rackmount bracket white | Fastening set

Figura 53. Datasheet CCR2116-12G-4S+

MikroTik CCR1036-8G-2S+

Specifications

Product code	CCR1036-8G-2S+	CCR1036-8G-2S+EM
CPU	36 cores TLR4-03680 1.2 GHz	
RAM	4 GB	8 GB
Storage	NAND 1 GB	
Dimensions	443 x 193 x 44 mm	
Operating temperature	-20°C .. +60°C tested	
Operating system	RouterOS	
License level	6	

Interfaces

10/100/1000 Ethernet ports	8
1G/10G SFP+ ports	2
M.2 slots	1 PCIe x4
Memory card slots	1 microSD
USB ports	1 USB type A
Serial ports	1 RJ45

Powering

Supported input voltage	100 V - 240 V
Number of AC inputs	2
Max power consumption	73 W

Other

CPU temperature monitor	Yes
PCB temperature monitor	Yes

Figura 54. Datasheet CCR1036-8G-2S+

MikroTik CCR1016-12S-1S+

Specifications

Product code	CCR1016-12S-1S+
CPU	Tilera Tile-Gx16 CPU, 16 cores, 1.2 GHz per core
Size of RAM	2 GB
Storage	128 MB NAND
1G SFP ports	12
10G SFP+ ports	1
Supported input voltage	AC power supply 100 - 240 V
Redundant supply	Yes
USB port	USB type A
Serial port	RJ45
Dimensions	443 x 197 x 44 mm
Operating temperature	-20°C .. +60°C
Operating system	RouterOS, License level 6
Max power consumption	48 W

Included parts

2 IEC cords

RJ45 SFP coper module

Screw kit

Rack ears

Figura 55. Datasheet CCR1016-12S-1S+

MikroTik CCR2004-1G-12S+2XS

Specifications

Product code	CCR2004-1G-12S+2XS
CPU	AL32400 1700 MHz
CPU core count	4
Size of RAM	RouterOS v7 4GB ECC
RAM type	DDR4
Storage	128 MB, NAND
Number of 1G Ethernet ports	1
Number of 10G SFP+ ports	12
Number of 25G SFP28 ports	2
Operating system	RouterOS v7
Router license level	6
Supported input voltage	AC power supply 100 - 240 V
Number of AC inputs	2
Dimensions	443 x 224 x 44 mm
Operating temperature	-20°C to +60°C tested
Max power consumption	49 W

Included parts

2 IEC cords

Rackmount bracket white

Fastening set for rackmount case

Figura 56. Datasheet CCR2004-1G-12S+2XS

Cloud Core Router

CCR1009

The CCR1009 is a powerful Ethernet router based on the cutting edge TILERA 9 core CPU.

Two models are available:

- low-cost model CCR1009-8G-1S with with 1GB of RAM, eight Gigabit Ethernet ports, and one SFP cage (SFP module not included).
- full feature model CCR1009-8G-1S-1S+ with 2GB of RAM, eight Gigabit Ethernet ports, one SFP port and one SFP+ port with 10G support (SFP module not included). CCR1009-8G-1S-1S+ model also have dual power supplies built in for redundancy (if one power line fails, the other one will take over automatically). Also, CCR1009-8G-1S-1S+ supports a Smart card, to store your private key for use in all features that support Certificate based authentication.

Model	CCR1009-8G-1S	CCR1009-8G-1S-1S+
CPU	Tilera TILE-Gx8009 CPU (9-cores, 1.2Ghz per core)	
Memory	RAM: 1GB DDR3 800 MHz	RAM: 2GB DDR3 800 MHz
Network interfaces	Eight 10/100/1000 Mbit/s Gigabit Ethernet with Auto-MDI/X (Ports 1-4 can be configured for Switch mode)	
SFP	1x SFP cage	1x SFP cage, 1x SFP+ cage
Expansion	microUSB port	microUSB port, SmartCard slot, MicroSD slot
Storage	128MB Onboard NAND	
Serial port	One DB9 RS232C asynchronous serial port	
Extras	Reset switch; beeper; voltage, current and temperature monitoring; speed controlled fan	Reset switch; beeper; voltage, current and temperature monitoring; speed controlled fan, LCD
Power options	1x IEC C14 power jack AC 110/220V, PoE in 12-58V	2x IEC C14 power jacks AC 110/220V, PoE in 12-58V
Max power consumption	34W (with loaded SFP)	35W (with loaded SFP)
Unit dimensions	444x175x47mm	
Temperature	-20C .. +60C	
OS	MikroTik RouterOS v6 (64bit), Level 6 license	
Included	router in a 1U case, IEC power cable, USB cable, rackmount ears	router in a 1U case with LCD, 2x IEC power cables, USB cable, rackmount ears

Figura 57. Datasheet CCR1009

Specifications

Product code	CCR2004-16G-2S+PC
CPU	AL32400 1.2 GHz
CPU architecture	ARM 64bit
CPU core count	4
Size of RAM	4 GB
RAM type	DDR4
Storage	128 MB, NAND
Number of 1G Ethernet ports	16
Number of 10G SFP+ ports	2
Operating system	RouterOS v7, License level 6
Switch chip model	88E6191X
Number of Gbit ports per switch (there are two switch-chips)	8
Dimensions	272 x 195 x 44 mm
Operating temperature	-20°C to +60°C

Powering

Number of DC inputs	2
Supported input voltage	36-57 V (DC jack) 36-57 (2-pin terminal)
Power adapter nominal voltage	48 V
Power adapter nominal current	0.9 A
Max power consumption (without attachments)	30 W
Max power consumption	36 W

Certification & Approvals

Certification	CE, FCC, IC

Included parts

48 V 0.95 A power adapter

Rackmount bracket

Fastening set

Figura 58. Datasheet CCR2004-16G-2S+PC

Specifications

Product code	CCR2004-16G-2S+
CPU	AL32400 1.7 GHz
CPU architecture	ARM 64bit
CPU core count	4
Size of RAM	4 GB
RAM type	DDR4
Storage	128 MB, NAND
Number of 1G Ethernet ports	16
Number of 10G SFP+ ports	2
Operating system	RouterOS v7 only
Switch chip model	88E6191X, 88E619X
Dimensions	443 x 210 x 44 mm
Operating temperature	-20°C to +60°C

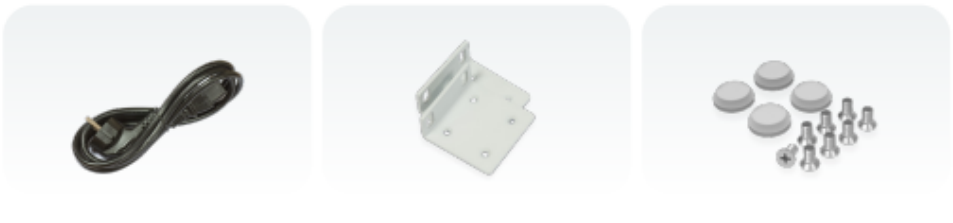
Powering

Number of AC inputs	2
AC input range	100-240 V
Max power consumption (without attachments)	35 W
Max power consumption	48 W

Certification & Approvals

Certification	CE, FCC, IC

Included parts



2 Power cords

Rackmount bracket white

Fastening set

Figura 59. Datasheet CCR2004-16G-2S+

Anexo 5. Configuración de Correo y Telegram

1. Configuración de Media type para correo electrónico

Para configurar los ajustes para correo electrónico se selecciona **Administration →Media types → Email**, como se observa en la figura 60.

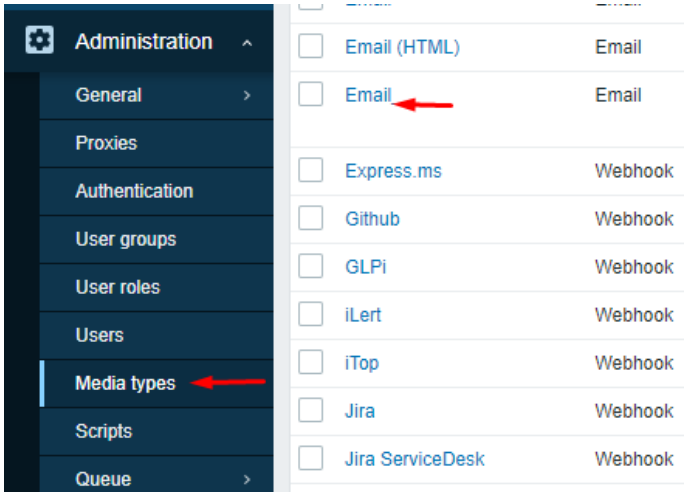


Figura 60. Media Type Email

Luego de escoger el Media type de Email se configuro el SNMP server, SNMP server port, SMNP helo, SNMP email, y el usuario y contraseña del correo que se utilizó para él envió de las alertas, ver figura 61.

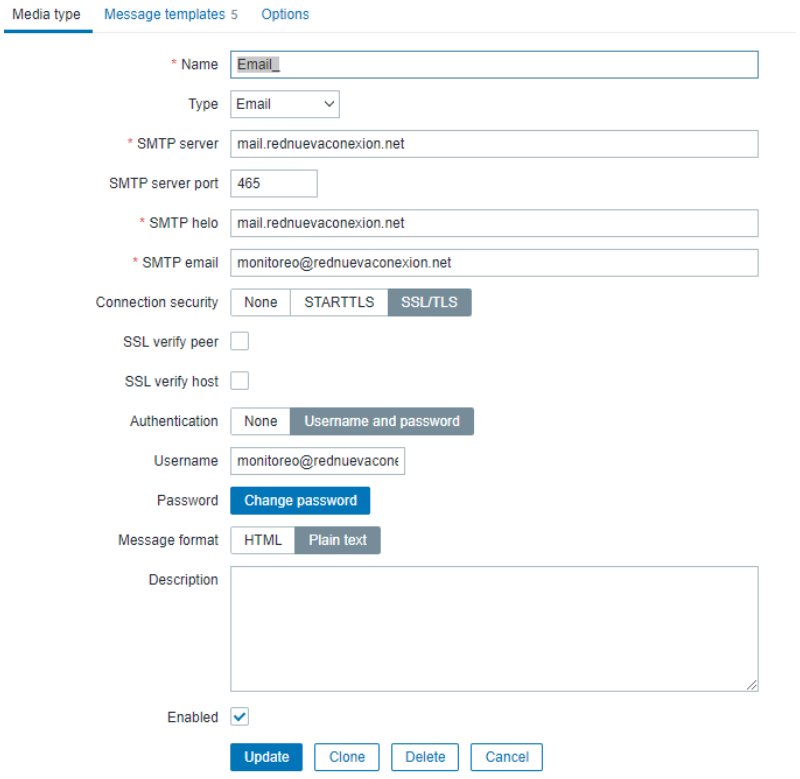


Figura 61. Configuración de Media type Email

En la pestaña **Message templates**, se configura el mensaje que será enviado, según el tipo de evento a alertar. Y finalmente clic en **update** para actualizar el Media type.

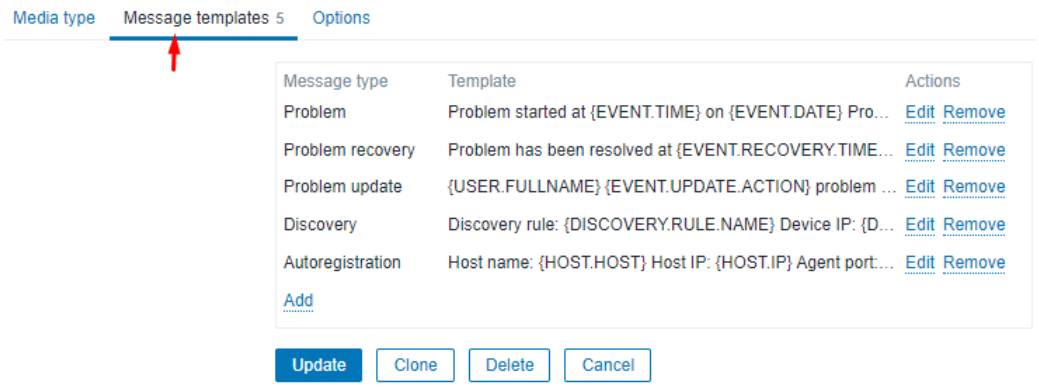


Figura 62. Configuración de la plantilla para mensajes de alerta por Email

Se agregó un medio a los usuarios para definir la dirección de correo en la pestaña **Administration** → **Users** y se asignó un **usuario,** después en “Media” se añadió el medio por el cual recibirá las notificaciones, ver figura 63.

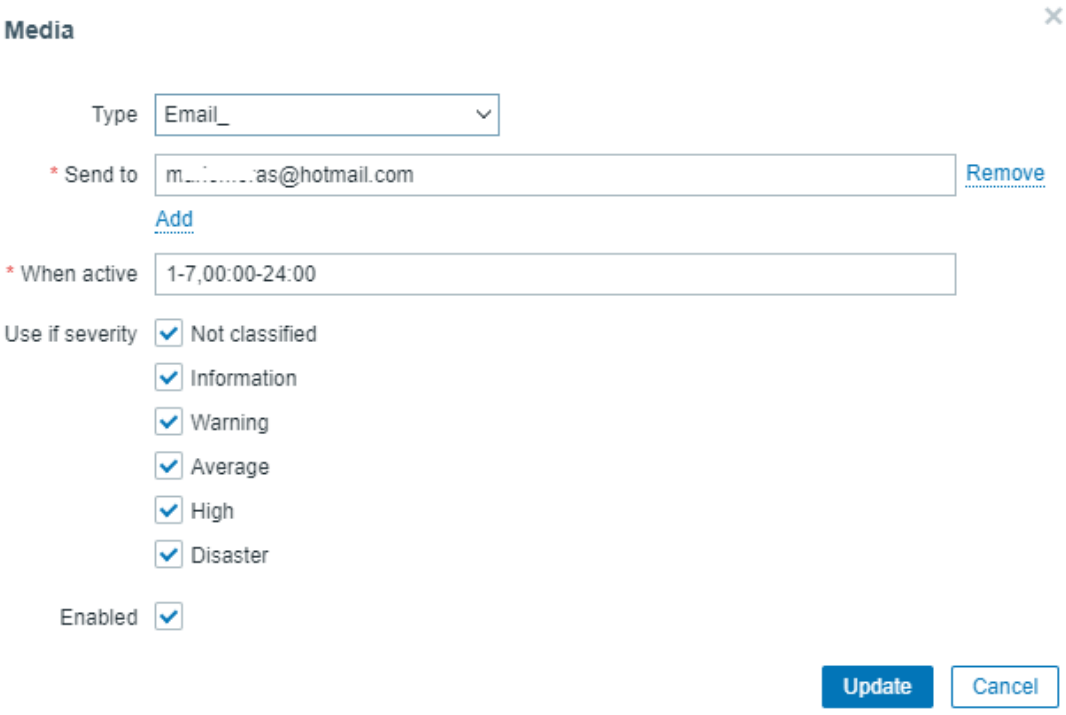


Figura 63. Configuración de media type en el usuario

En la Figura 64, se muestra la alerta “No SNMP data collection” que se envió por correo electrónico, indicando que no se está recolectando datos a través de SNMP en el equipo del ISP Yaneznet. Esta representación visual proporciona una clara evidencia de cómo se lleva a cabo el proceso de notificación de eventos críticos.

Figura 64. Alerta de correo enviado

2. Configuración de media type para Telegram

Previo a la configuración de las notificaciones usando Telegram en Zabbix, es necesario crear un bot de Telegram, para ello, en la aplicación Telegram y se buscó **@BotFather** para crear el bot que fue usado para enviar las notificaciones de Telegram.

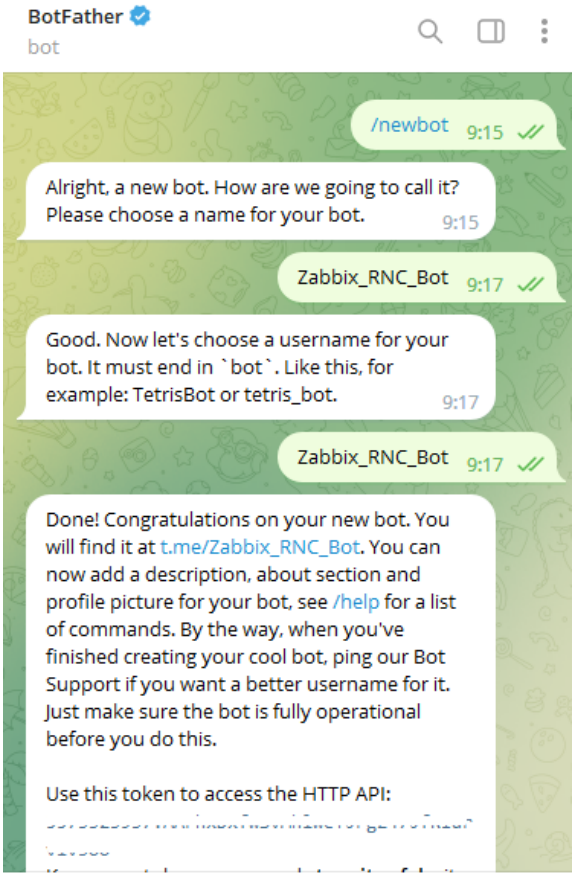


Figura 65. Creación del Bot en Telegram

Posterior a la creación del Bot se lo buscó en Telegram y se escribió /**start** para inicializar el Bot, como indica la figura 66.

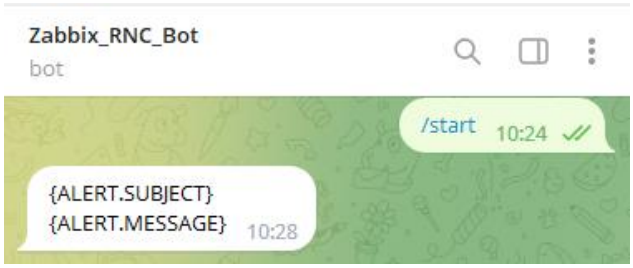


Figura 66. Inicializar el Bot

Para configurar los ajustes para notificaciones mediante Telegram se selecciona **Administration →Media types → Telegram**, como se observa en la figura 67.

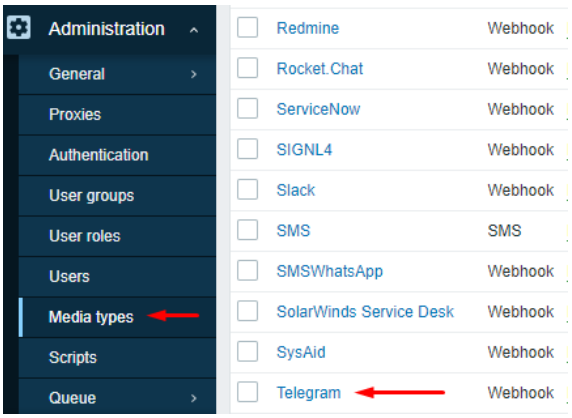


Figura 67. Media type para Telegram

Luego se selecciona el Media type Telegram se configura los parámetros adicionales para el Media type Telegram, ver figura 61.

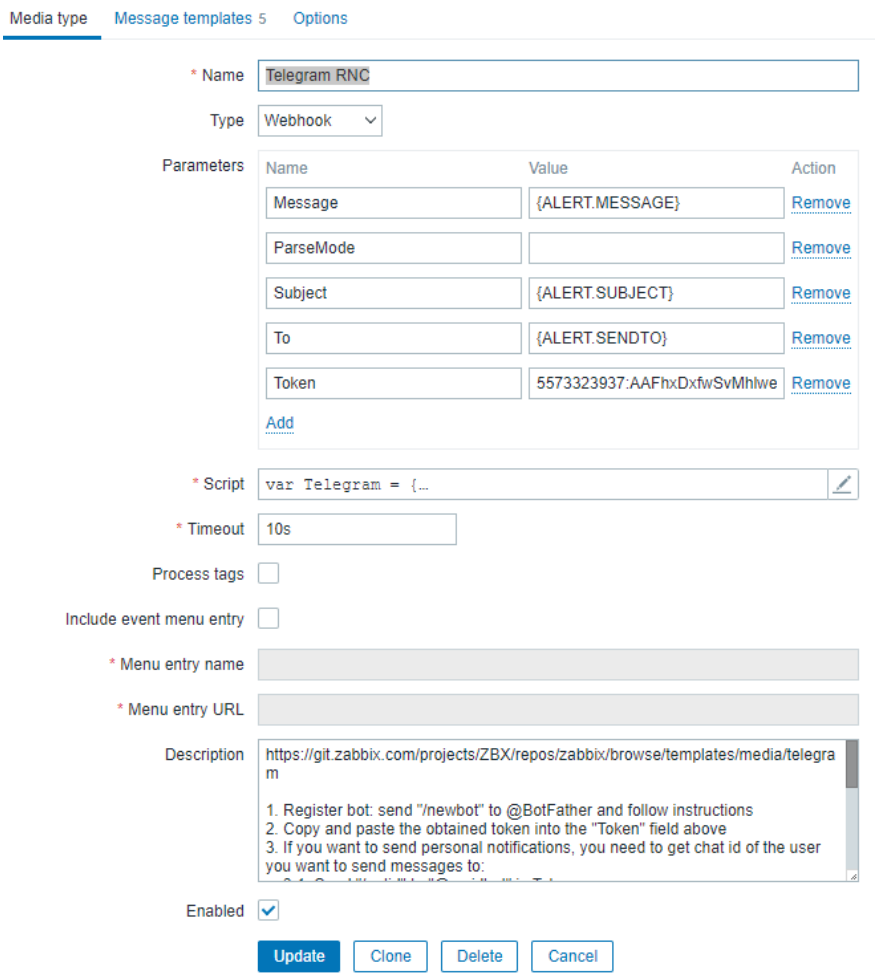


Figura 68. Configuración del Media type Telegram

Se agregar un medio a los usuarios para definir las direcciones de entrega. Para ello se dirige a la pestaña **Administration** → **Users** y se selecciona un **usuario** al que va a configurar el envío por Telegram. Después en “Media” se agrega el medio de envío.

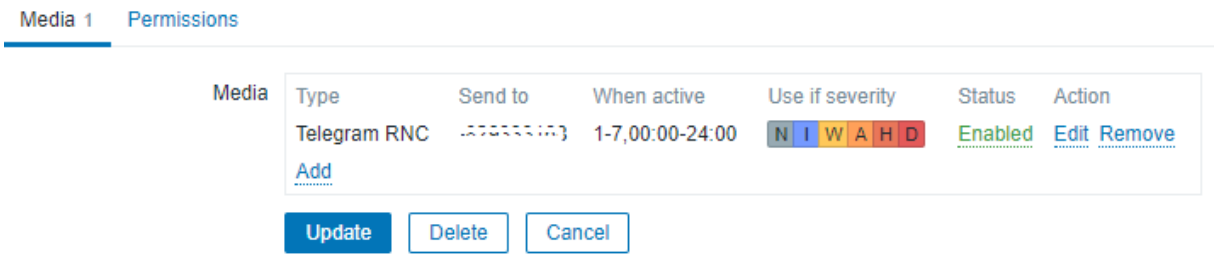


Figura 69. Configuración del id de Telegram en el usuario

En la Figura 70, se indica la alerta con severidad “warning” que indica que “el Equipo HCNET-Chongon ha sido reiniciado”

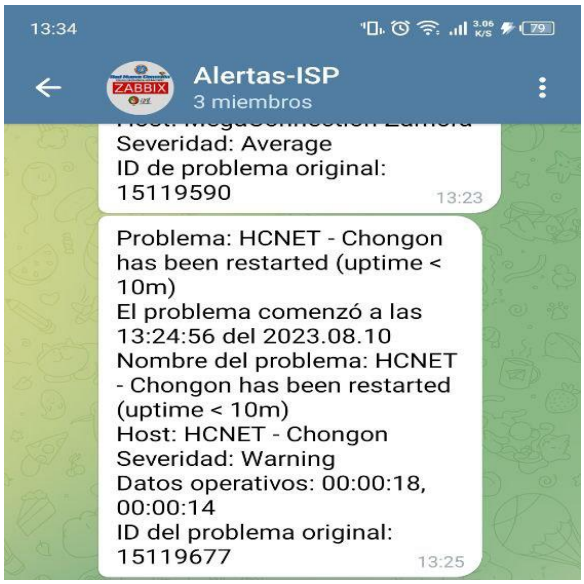


Figura 70. Notificaciones de los eventos de los ISP en el grupo de Telegram

Anexo 6. Grupos de Telegram para Administradores de red e ISP

Este anexo indica los 35 grupos de Telegram creados respectivamente para cada ISP, a los que el bot de Telegram envía las notificaciones de los eventos detectados por Zabbix.

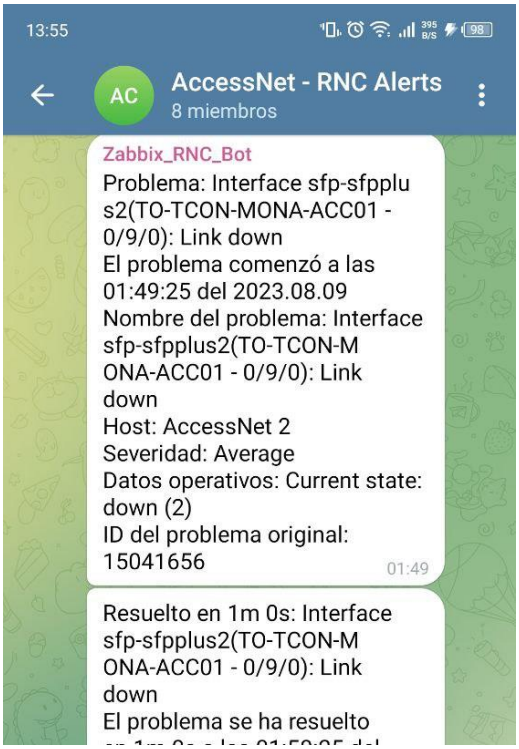


Figura 71. Telegram ISP 1

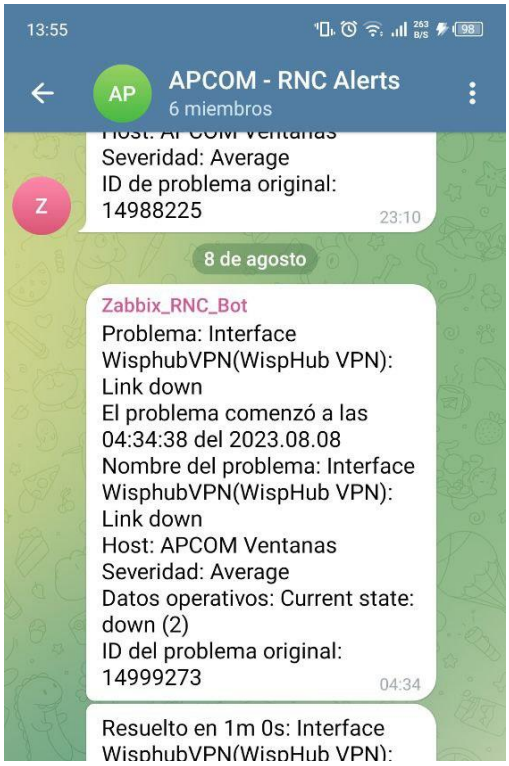


Figura 72. Telegram ISP 2

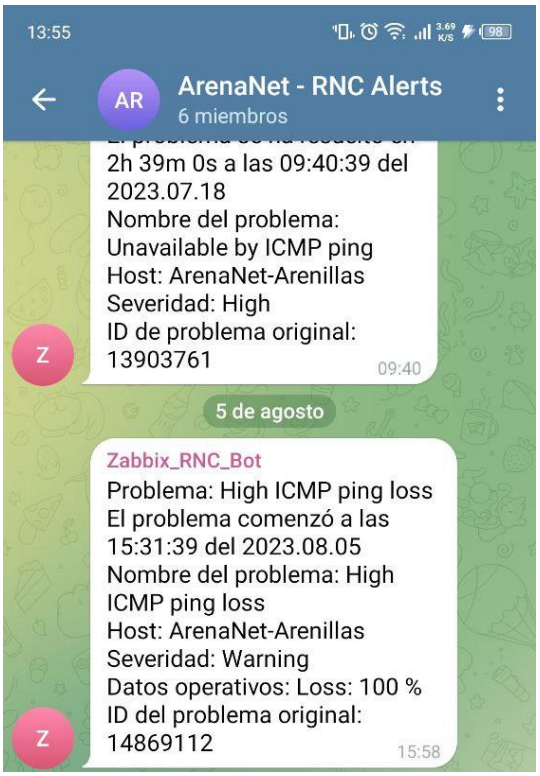


Figura 73. Telegram ISP 3

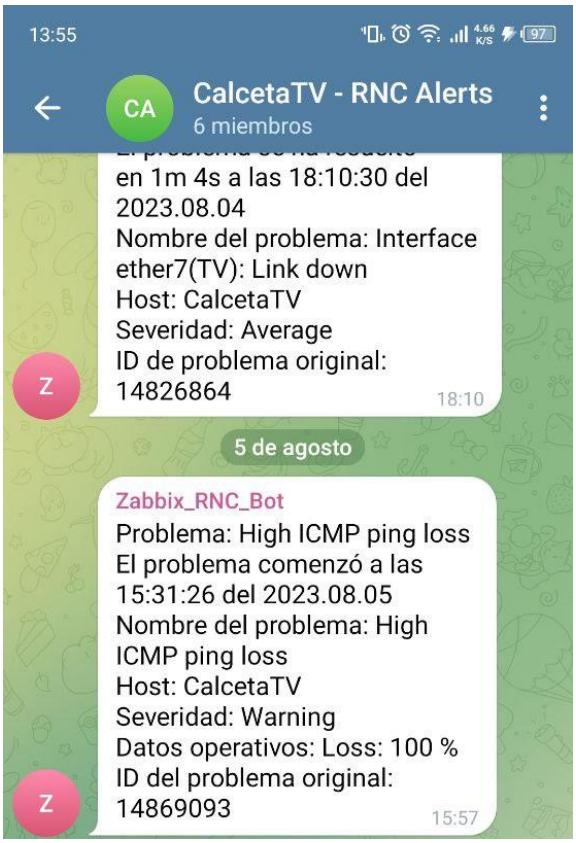


Figura 74. Telegram ISP 4

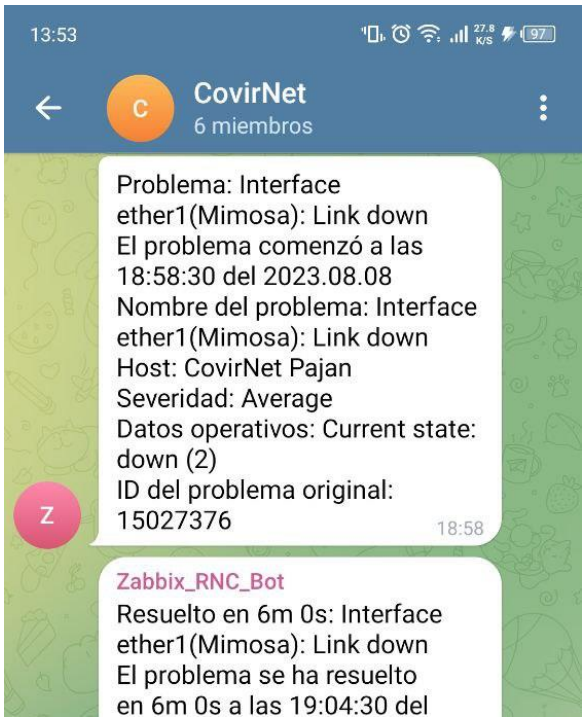


Figura 75. Telegram ISP 5

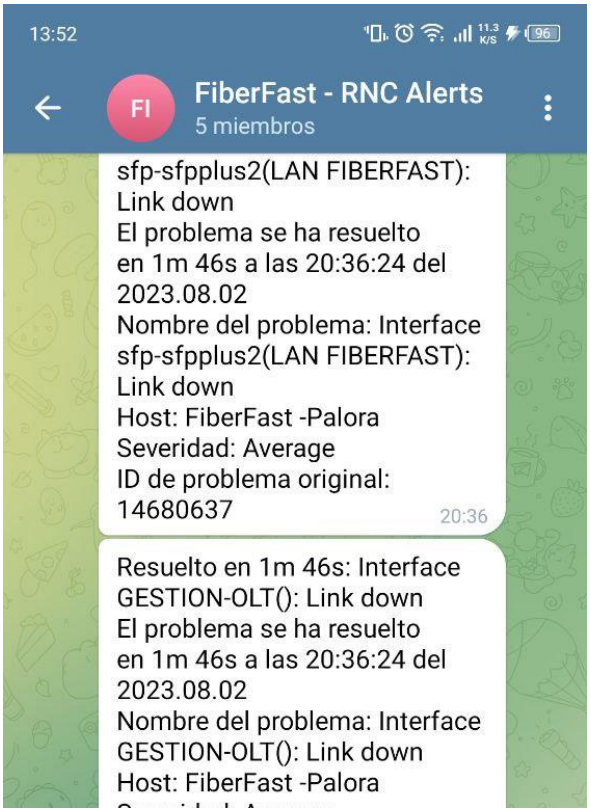


Figura 76. Telegram ISP 6

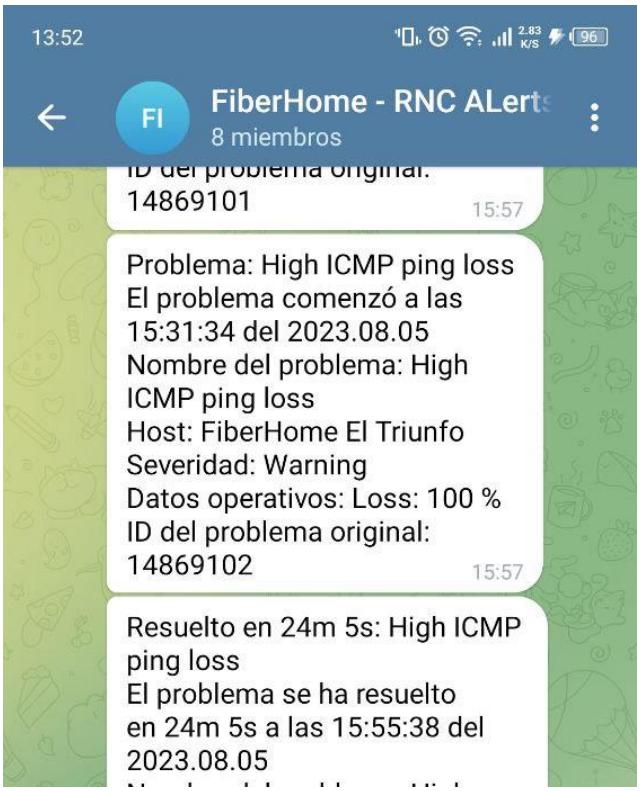


Figura 77. Telegram ISP 7

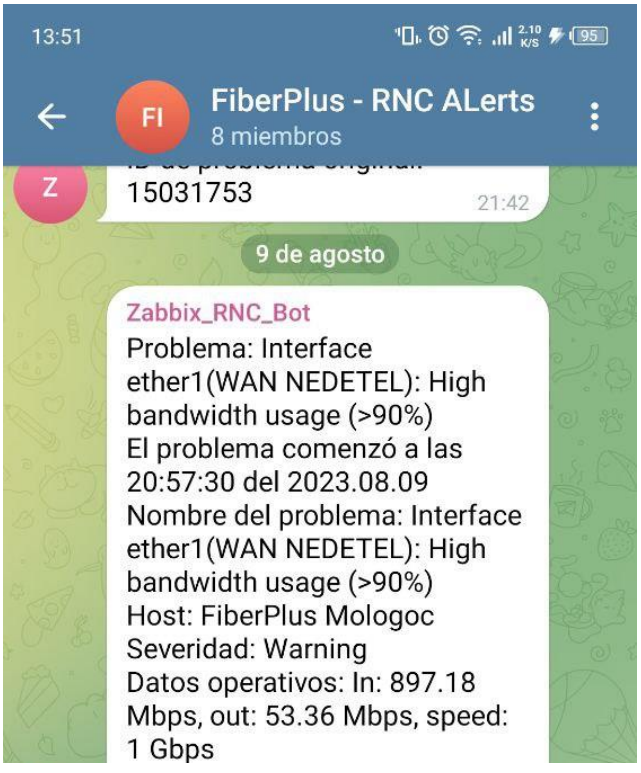


Figura 78. Telegram ISP 8

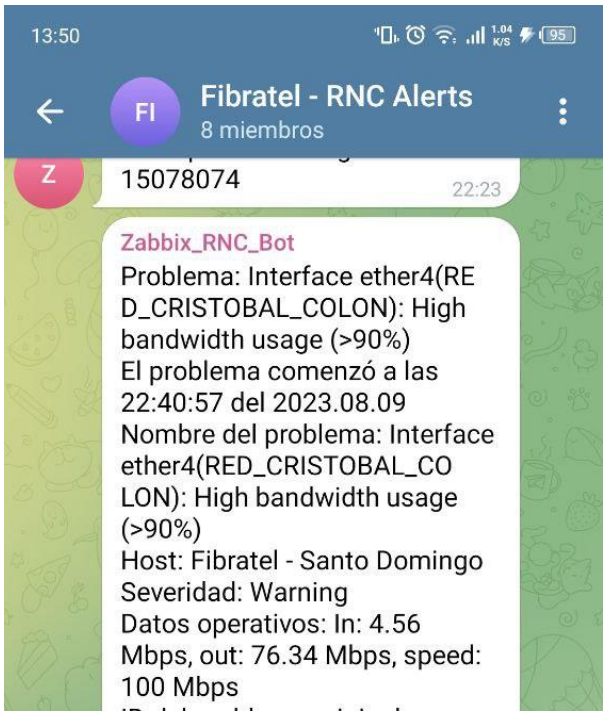


Figura 79. Telegram ISP 9

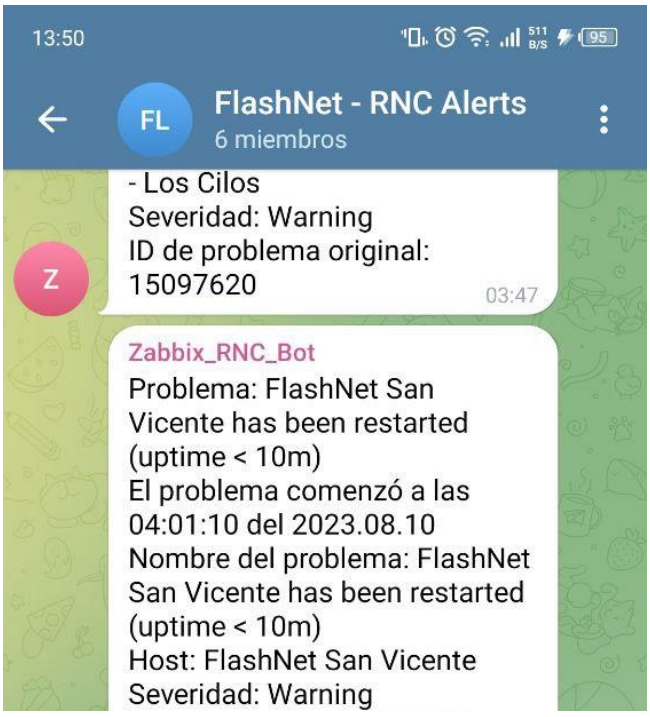


Figura 80. Telegram ISP 10

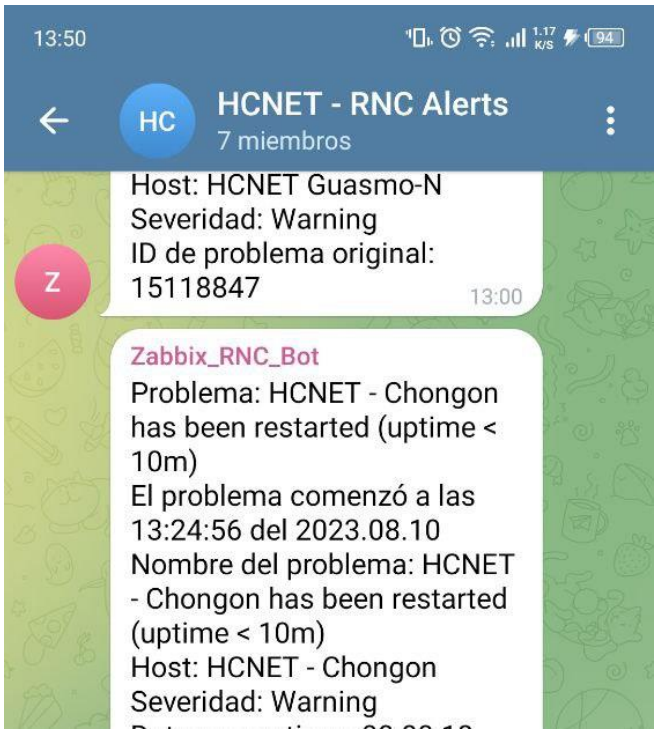


Figura 81. Telegram ISP 11

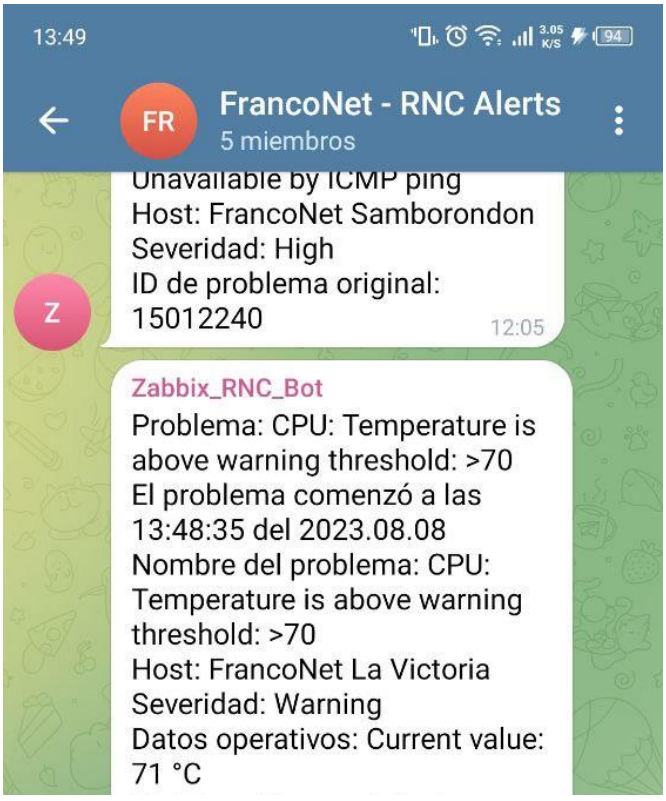


Figura 82. Telegram ISP 12

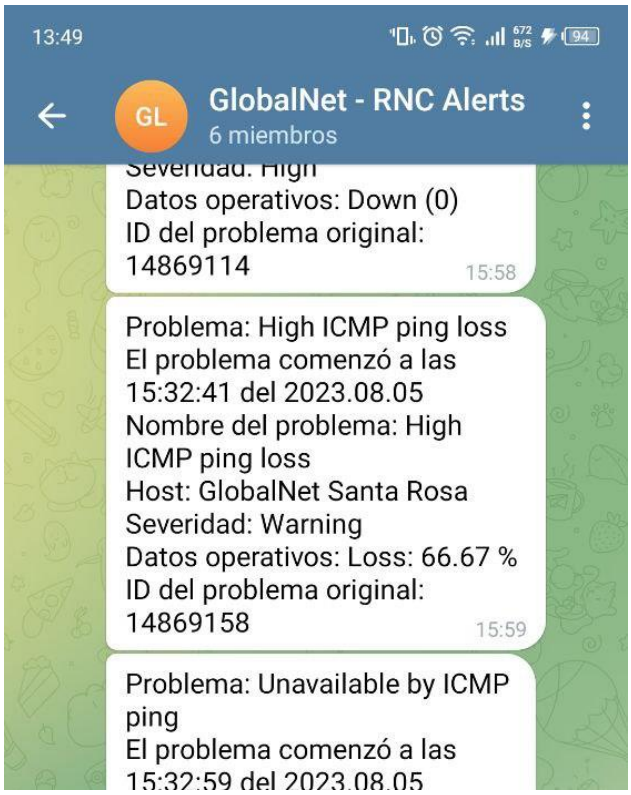


Figura 83. Telegram ISP 13

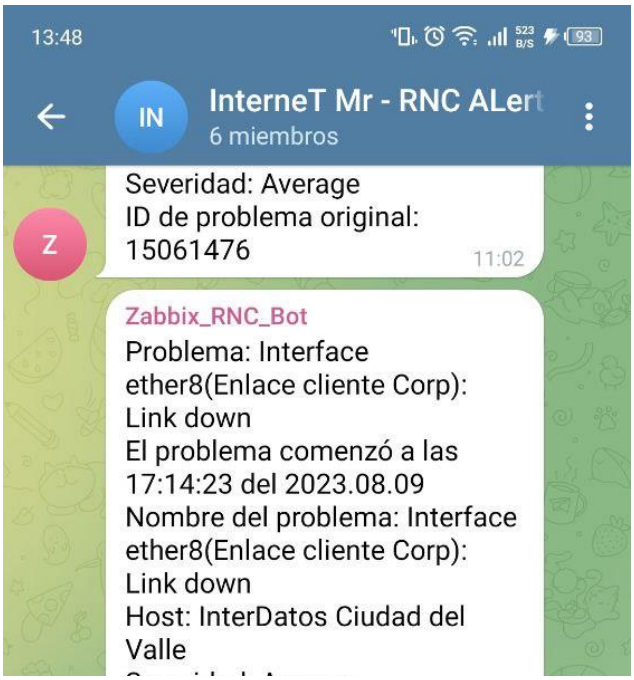


Figura 84. Telegram ISP 14

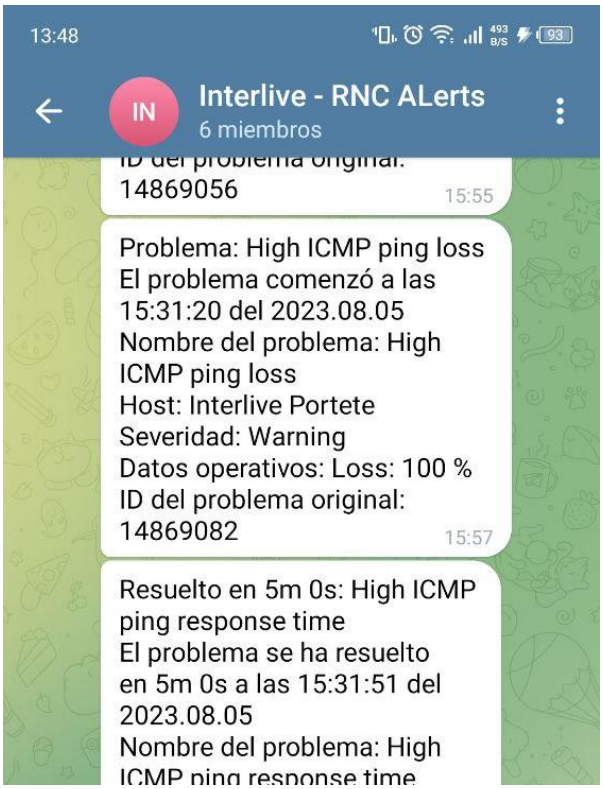


Figura 85. Telegram ISP 15

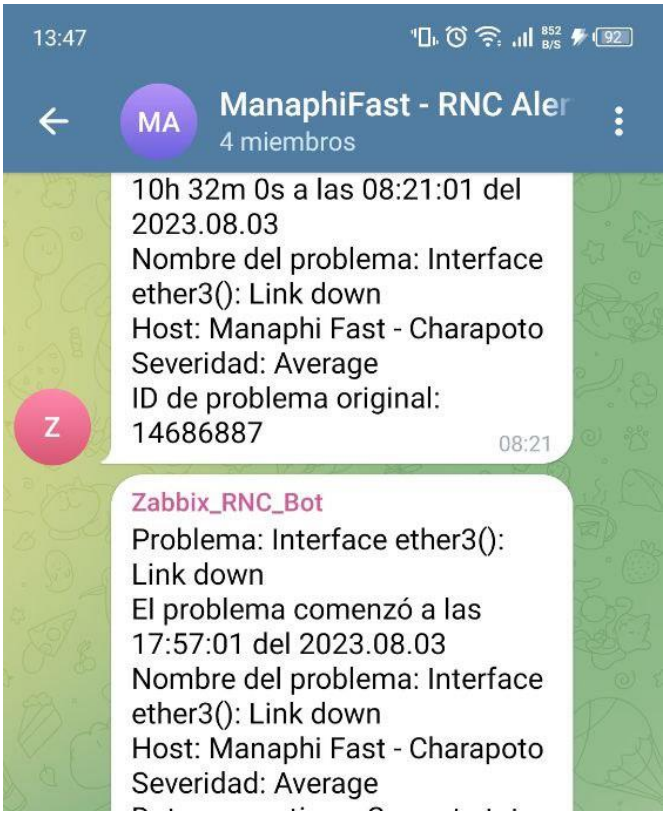


Figura 86. Telegram ISP 16

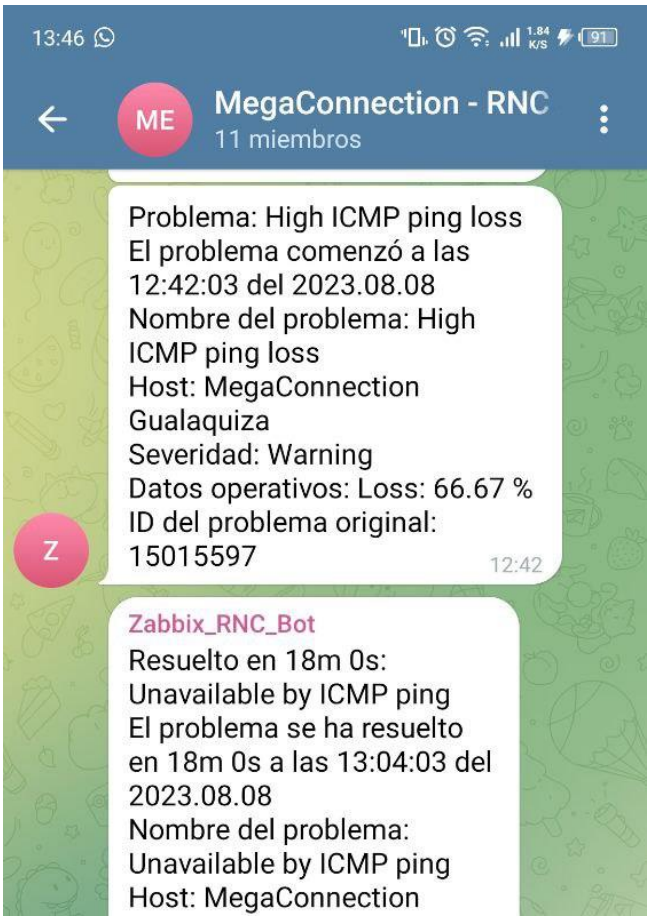


Figura 87. Telegram ISP 17

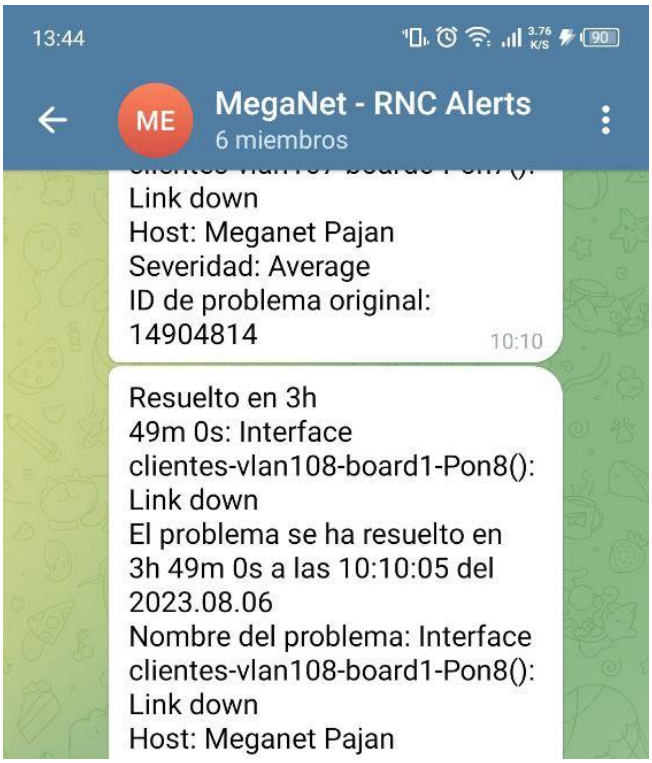


Figura 88. Telegram ISP 18

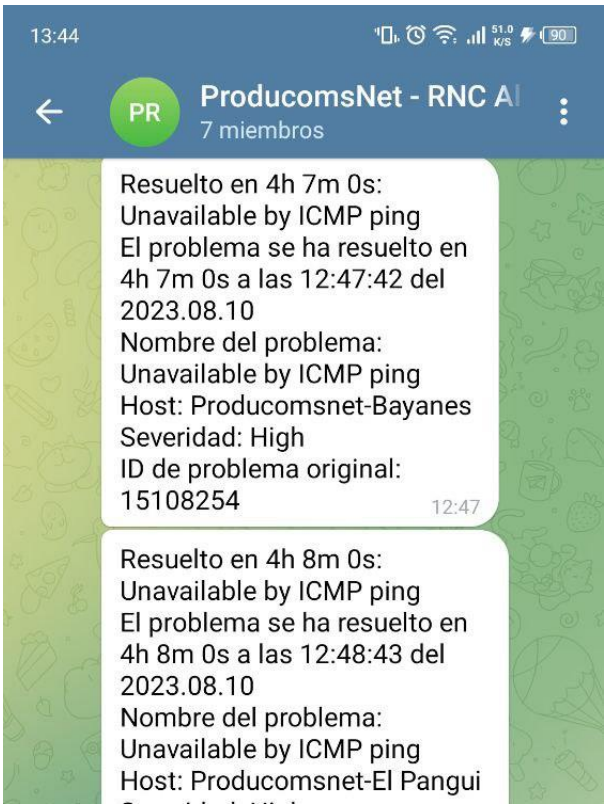


Figura 89. Telegram ISP 19

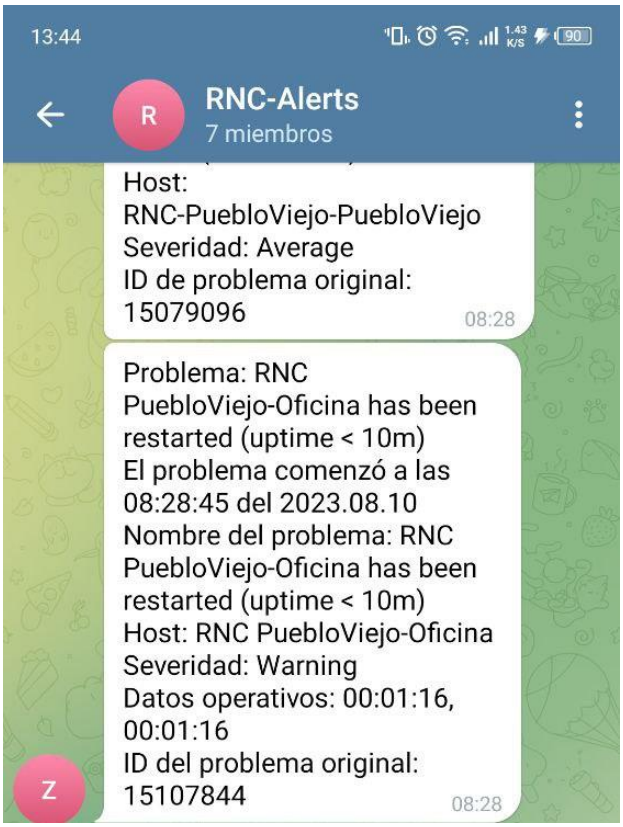


Figura 90. Telegram ISP 20

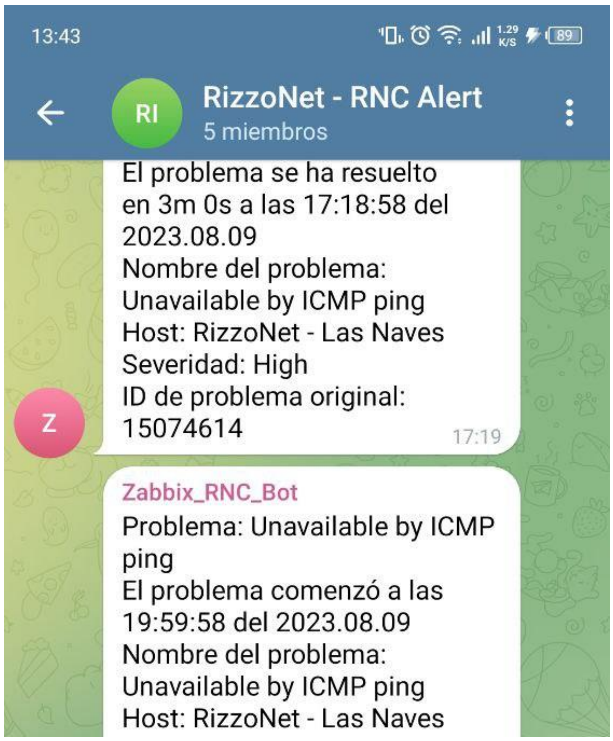


Figura 91. Telegram ISP 21

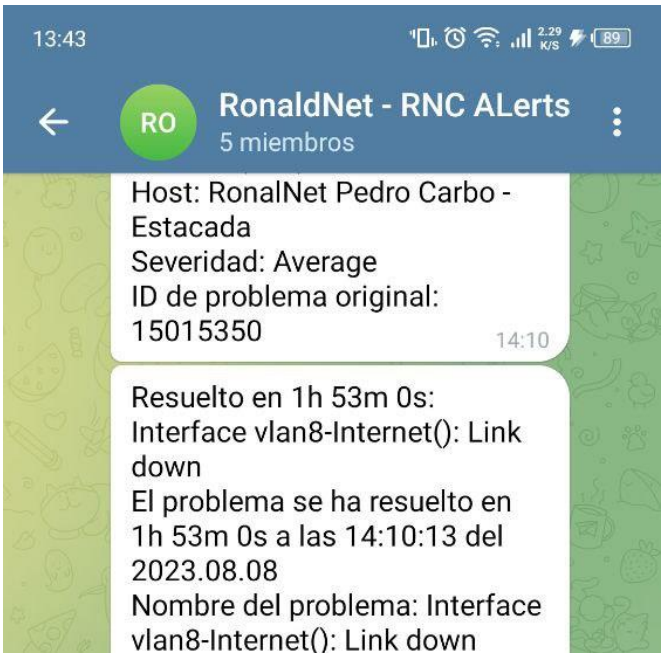


Figura 92. Telegram ISP 22

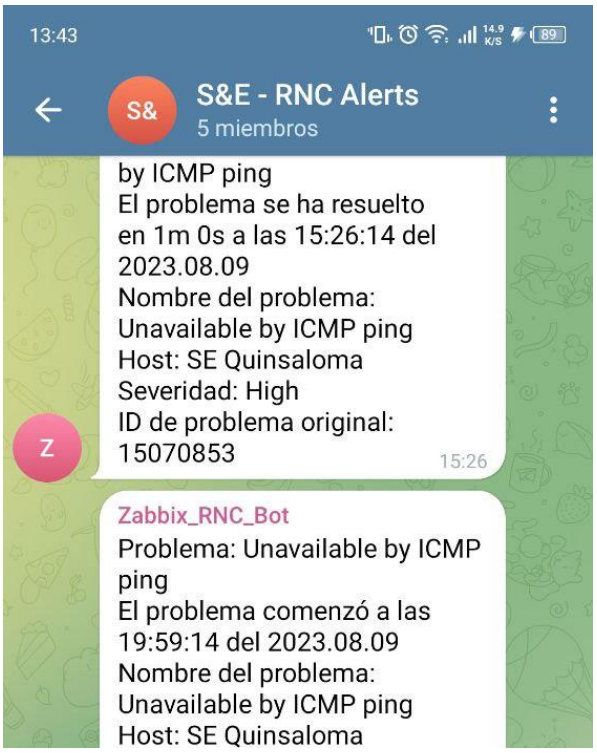


Figura 93. Telegram ISP 23

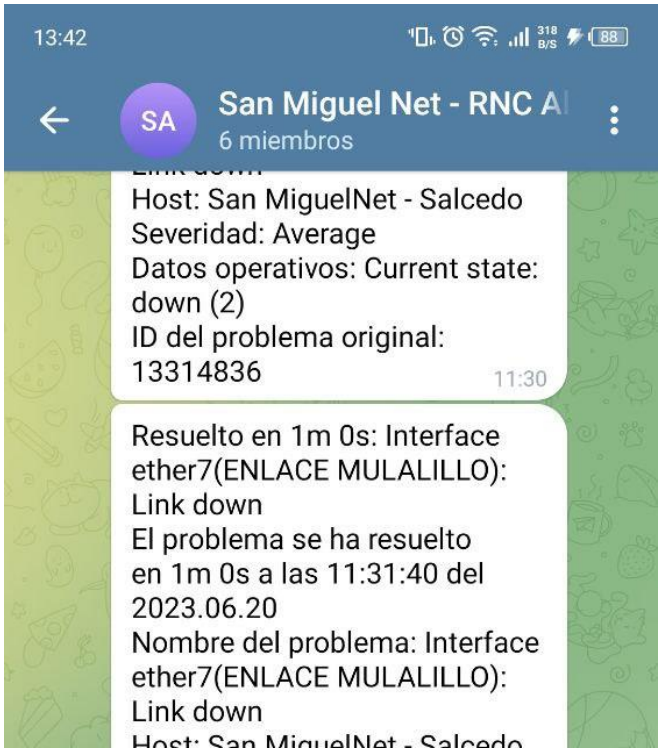


Figura 94. Telegram ISP 24

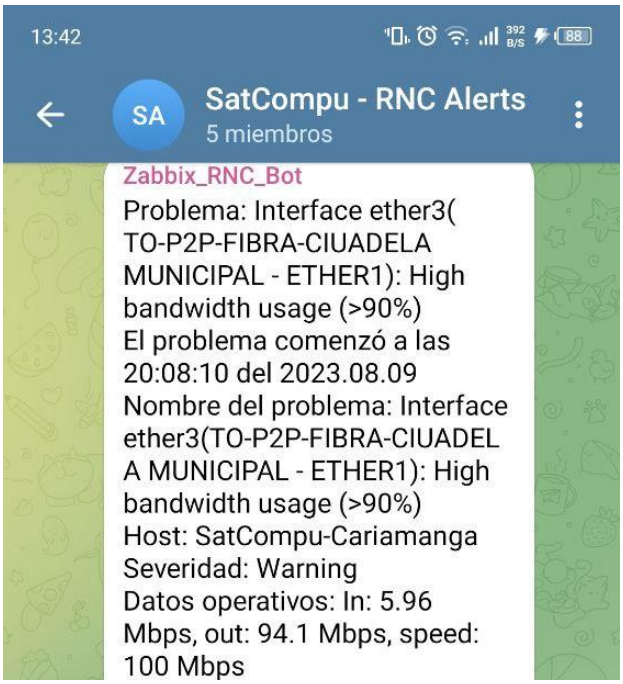


Figura 95. Telegram ISP 25

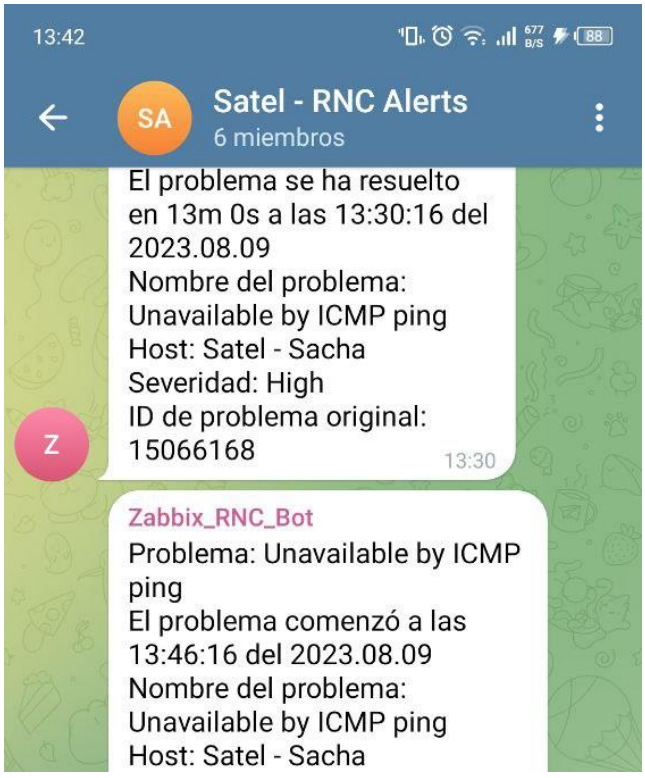


Figura 96. Telegram ISP 26

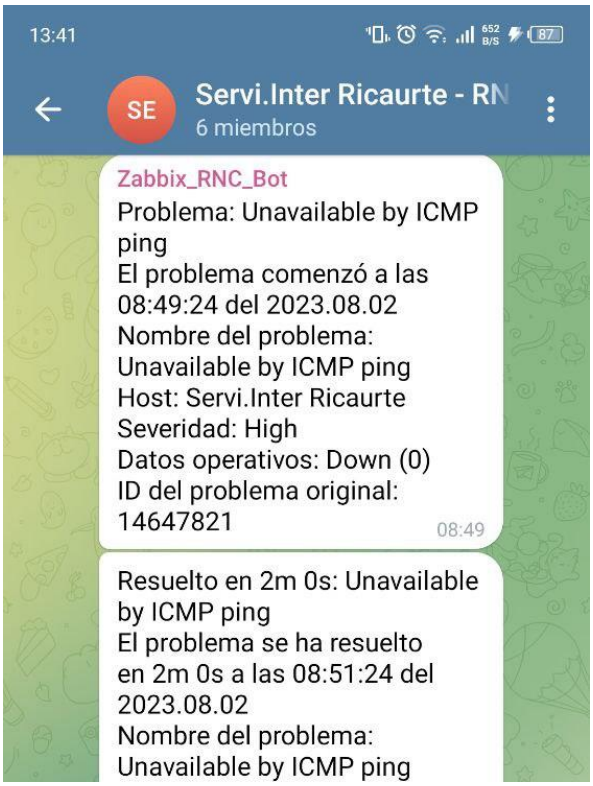


Figura 97. Telegram ISP 27

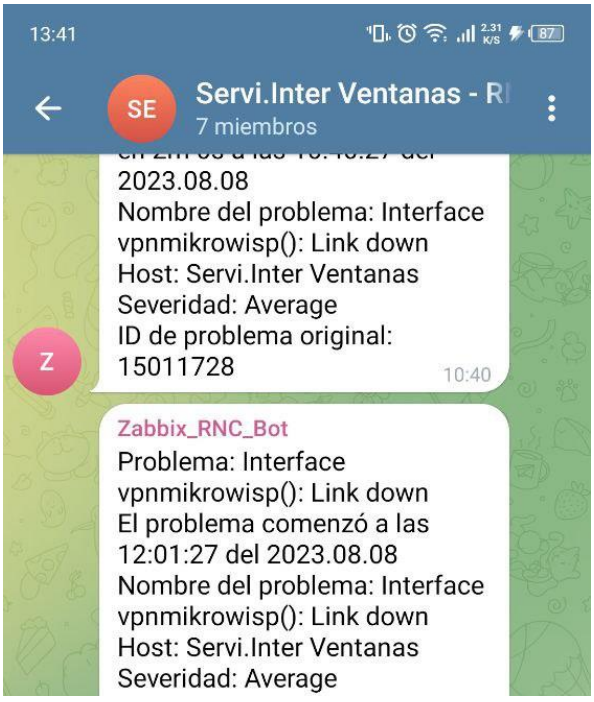


Figura 98. Telegram ISP 28

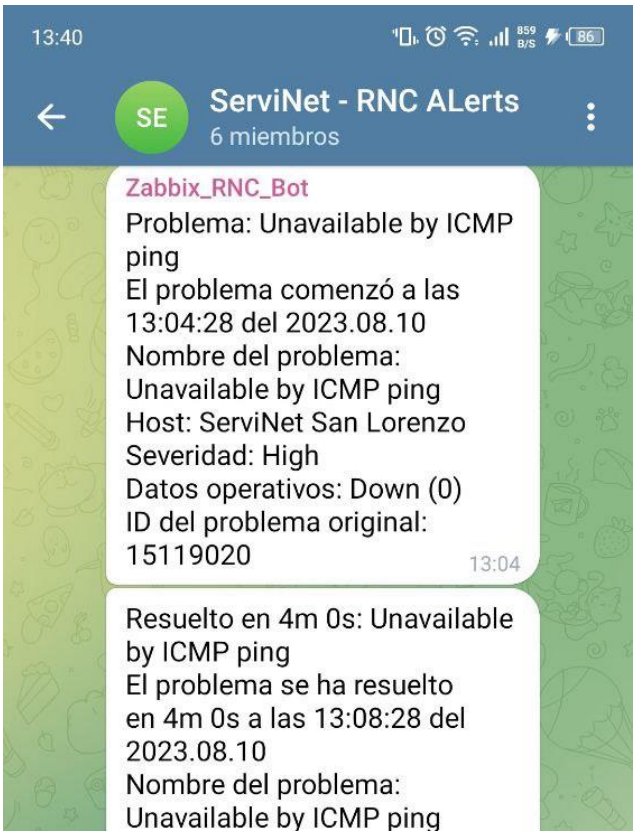


Figura 99. Telegram ISP 29

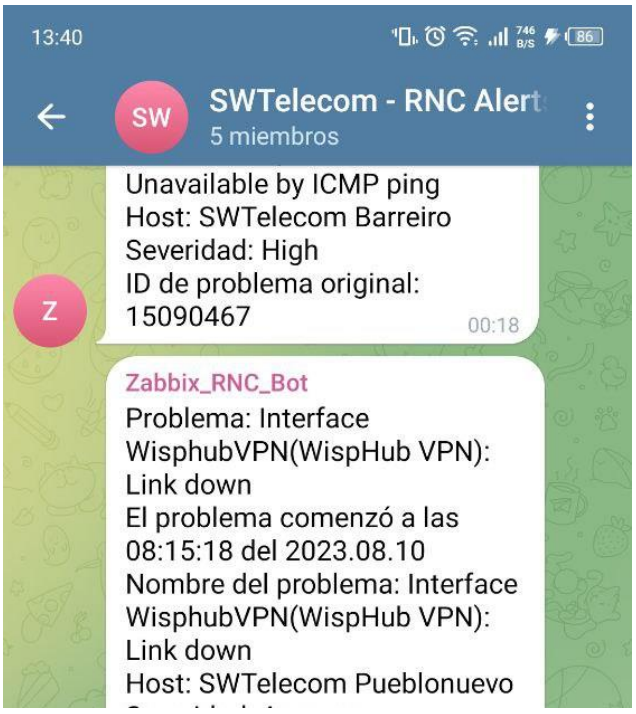


Figura 100. Telegram ISP 30

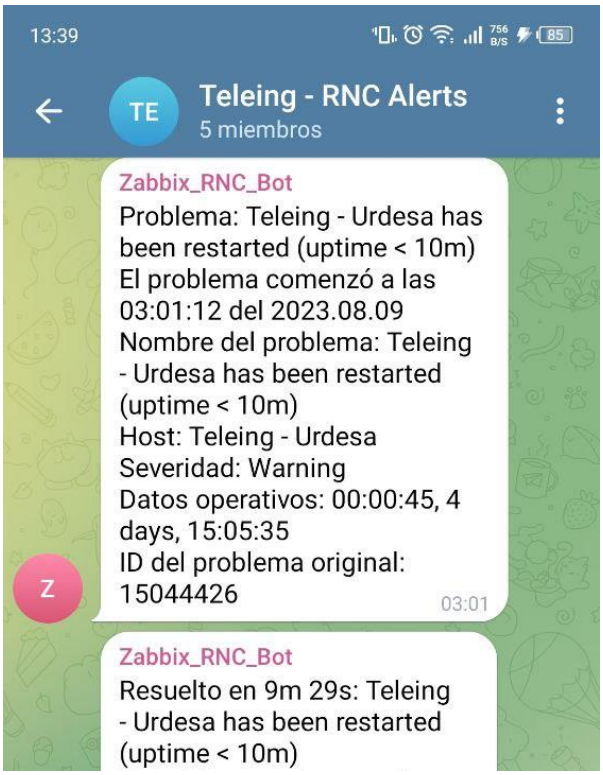


Figura 101. Telegram ISP 31

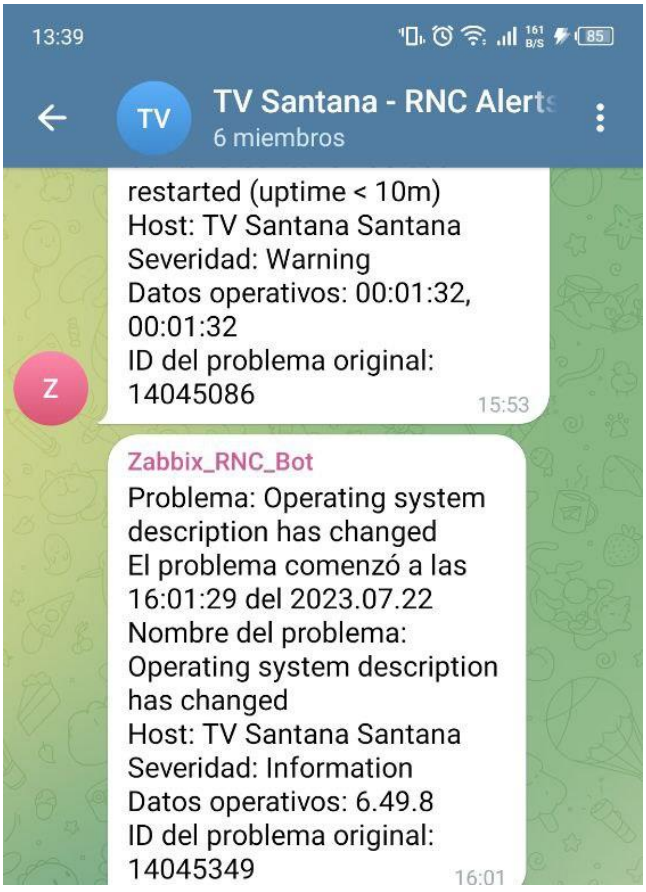


Figura 102. Telegram ISP 32

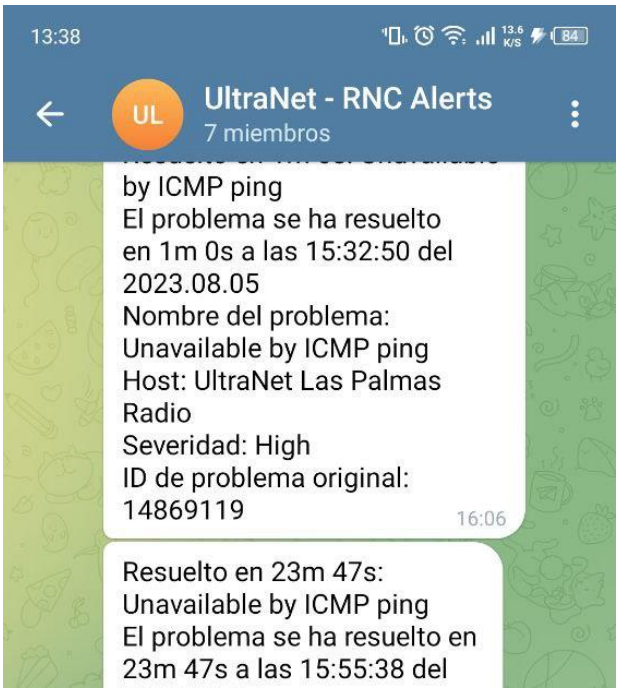


Figura 103. Telegram ISP 33

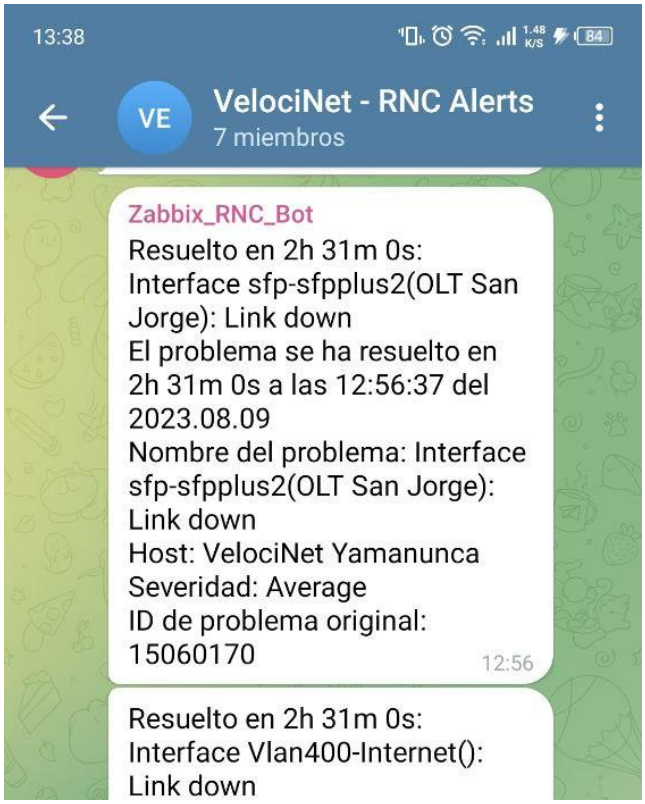


Figura 104. Telegram ISP 34

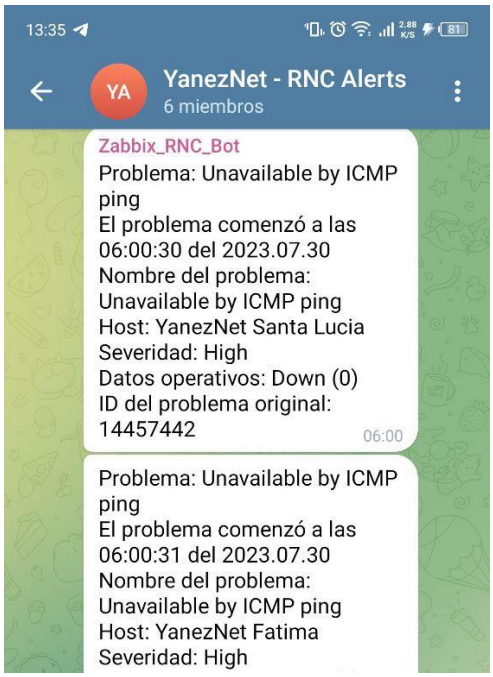


Figura 105. Telegram ISP 35

Anexo 7. Manual de Usuario de Zabbix

Manual de usuario del NMS Zabbix

Implementación de un Sistema de Administración de Red (NMS) para los clientes ISP de la empresa Red Nueva Conexión.

1. Generalidades

1.1. Introducción

El propósito de este documento es facilitar información comprensiva y descriptiva de las funciones del NMS Zabbix para la administración de los ISP que gestiona la empresa Red Nueva Conexión.

1.2. Objetivo

Realizar una guía para el administrador de red pueda realizar cada proceso necesario para la administración de los equipos gestionados por el NMS Zabbix.

1.3. Alcance

El presente manual de usuario está dirigido para el administrador de red de la empresa Red Nueva Conexión, con la finalidad de que pueda realizar los procesos y funciones que posee el NMS.

1.4. Requisitos Previos

Los requisitos necesarios son los siguientes:

- Conexión a internet
- Un navegador Web (Google Chrome, Mozilla Firefox, Microsoft Edge u Opera).

2. Funcionalidades

2.1. Inicio de sesión

Para iniciar sesión en el NMS se abre la siguiente dirección **https://direccion-IP/zabbix/** en el formulario se ingresa las credenciales de acceso (ver Figura 106), luego de ingresar las credenciales, hacer clic en el botón **Sign in** para iniciar sesión.

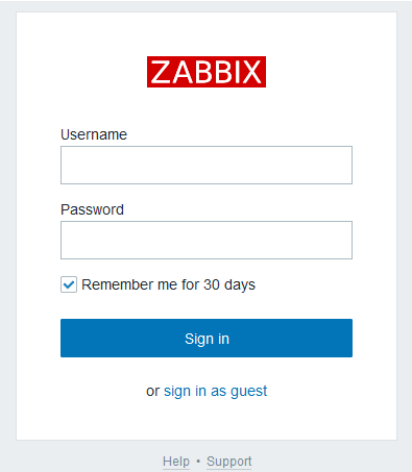


Figura 106. Inicio de sesión

Posteriormente se muestra la pantalla principal de Zabbix, en la barra lateral se muestra el menú con las siguientes funciones: Monitoring, Services, Inventory, Reports, ConFiguration y administration.

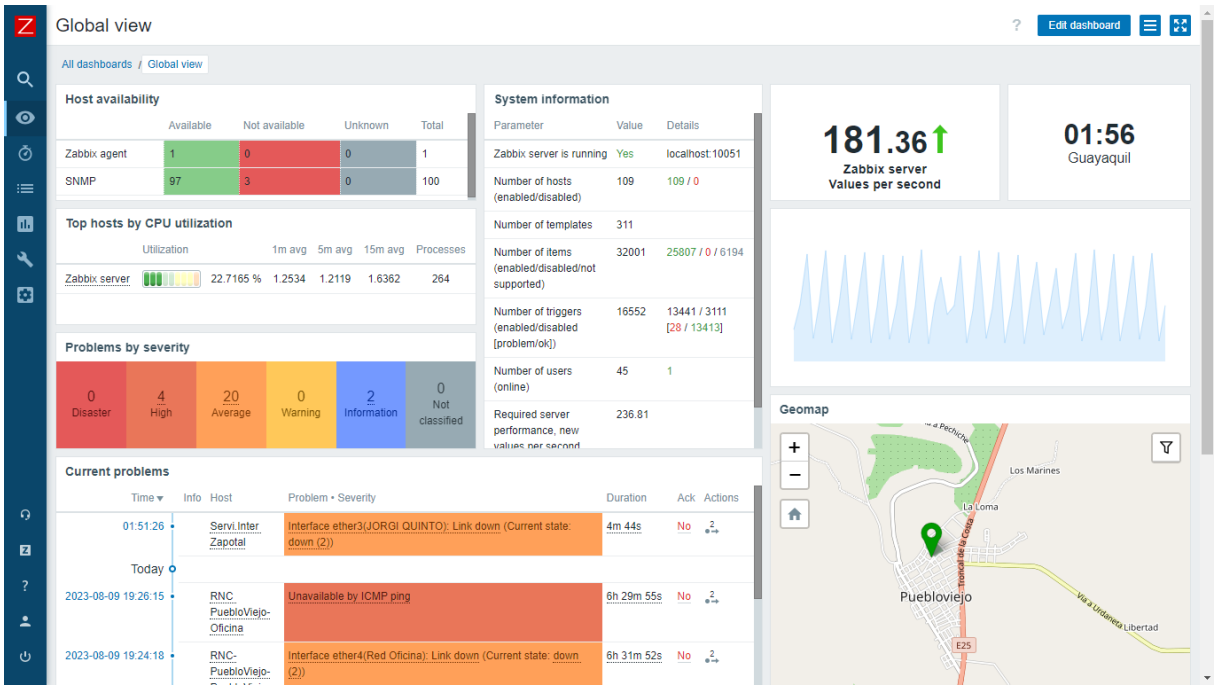


Figura 107. Página principal de Zabbix

2.2. Configuración de host

Para configurar un host en Zabbix se hace clic en **ConFiguration → Host** se ingresa la información correspondiente al host, como indica la Figura 108.

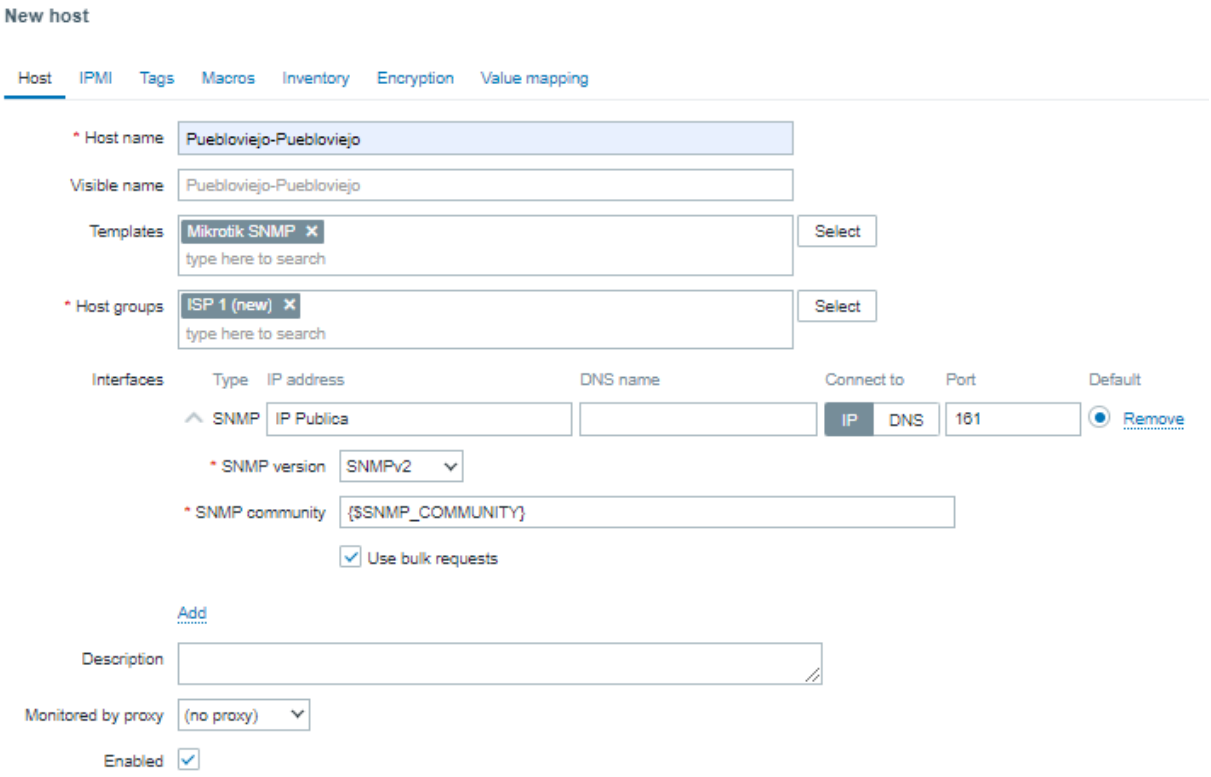


Figura 108. Crear nuevo Host

2.3. Configuración de grupo de host

Para crear un grupo de host se hace clic en **Configuration → Host Groups →Create host group**

En esta ventana se escribe el nombre del grupo de host a crear y finalmente se hace clic en **Add** para añadir el grupo de host, como se muestra en la Figura 109.

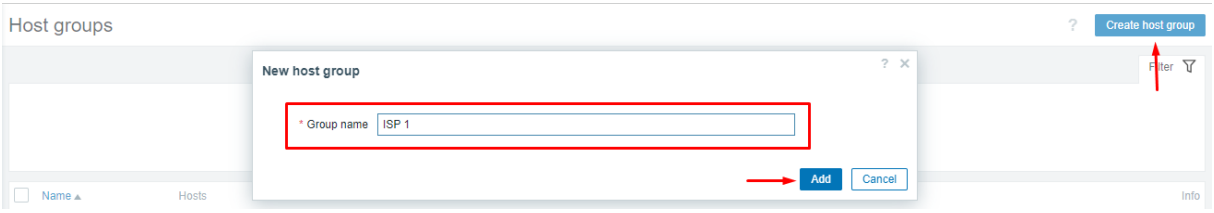


Figura 109. Creación de Host Groups

Nota: Cada Host Group es un ISP al que pueden pertenecer muchos hosts.

También se puede editar el nombre del host Group haciendo clic sobre el grupo creado, editar la información y hacer clic en **update**, como se muestra en la Figura 110.

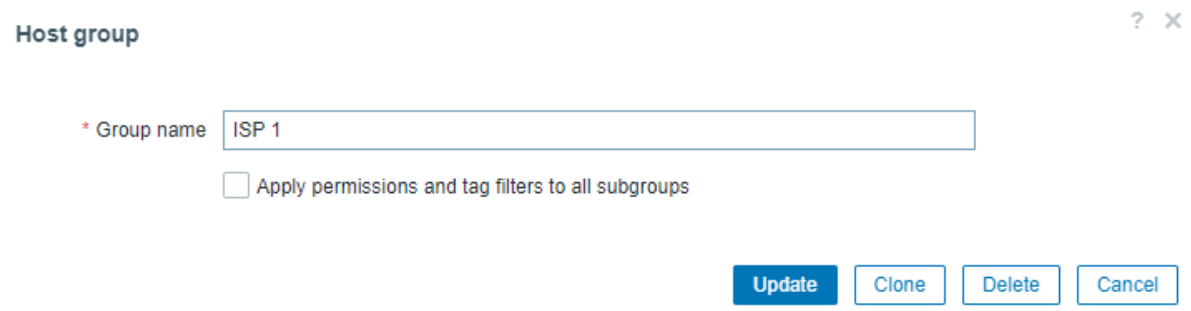


Figura 110. Editar Host Groups

2.4. Configuración de Notificaciones

Para activar las notificaciones se hace clic en **Configuration → Actions → Trigger actions,** como se muestra en la Figura 111.

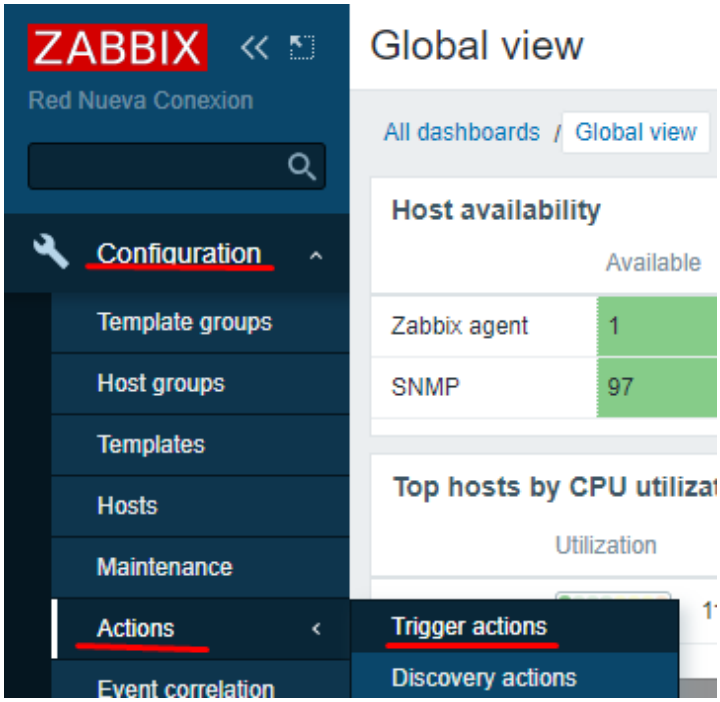


Figura 111. Trigger actions-para el envío de notificaciones

Luego se crea una regla para el envío de notificaciones haciendo clic en **Create action,** como se muestra en la Figura 112.

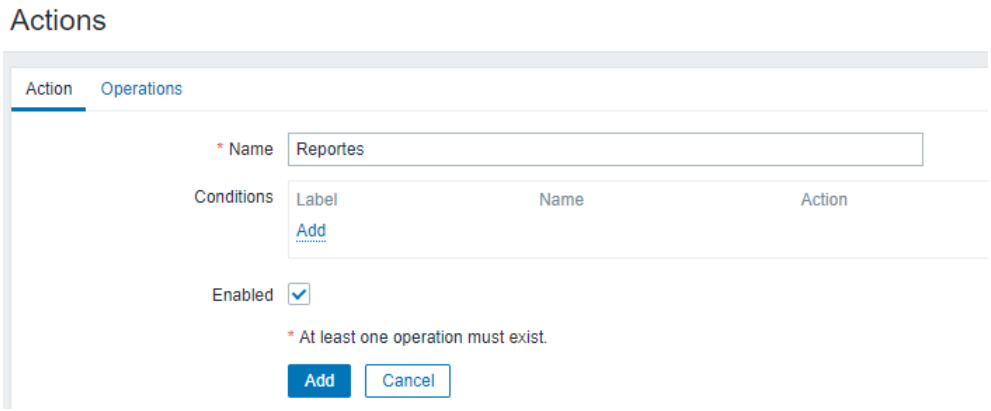


Figura 112. Crear Trigger para envío de notificaciones

Y se finaliza creando una operación, para ello se hace clic en **Operations** y dentro de esta ventana se selecciona el tipo de notificación, en este caso **Email y Telegram**, además de seleccionar a los usuarios que serán notificados, como se muestra en la Figura 113.

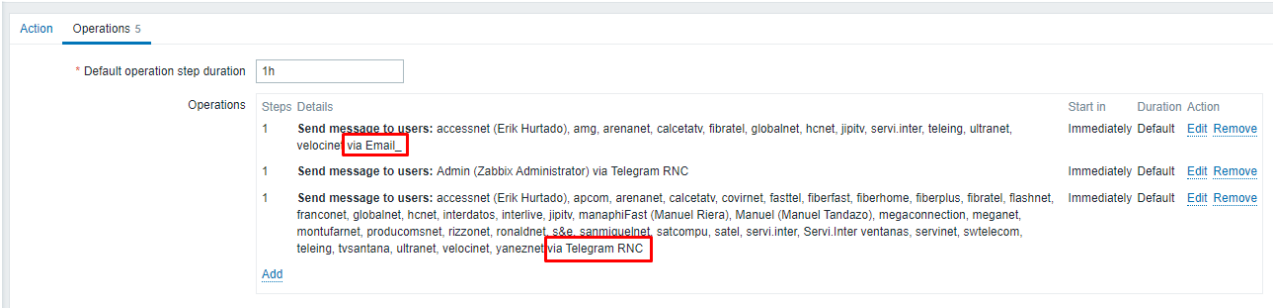


Figura 113. Activación de usuarios para envío de notificación

Crear Ítem

Los ítems dependen de los hosts

Configuration → **Hosts** y se busca el host y se hace clic en **Items** →**Create Item, c**omo se muestra en la Figura 114.

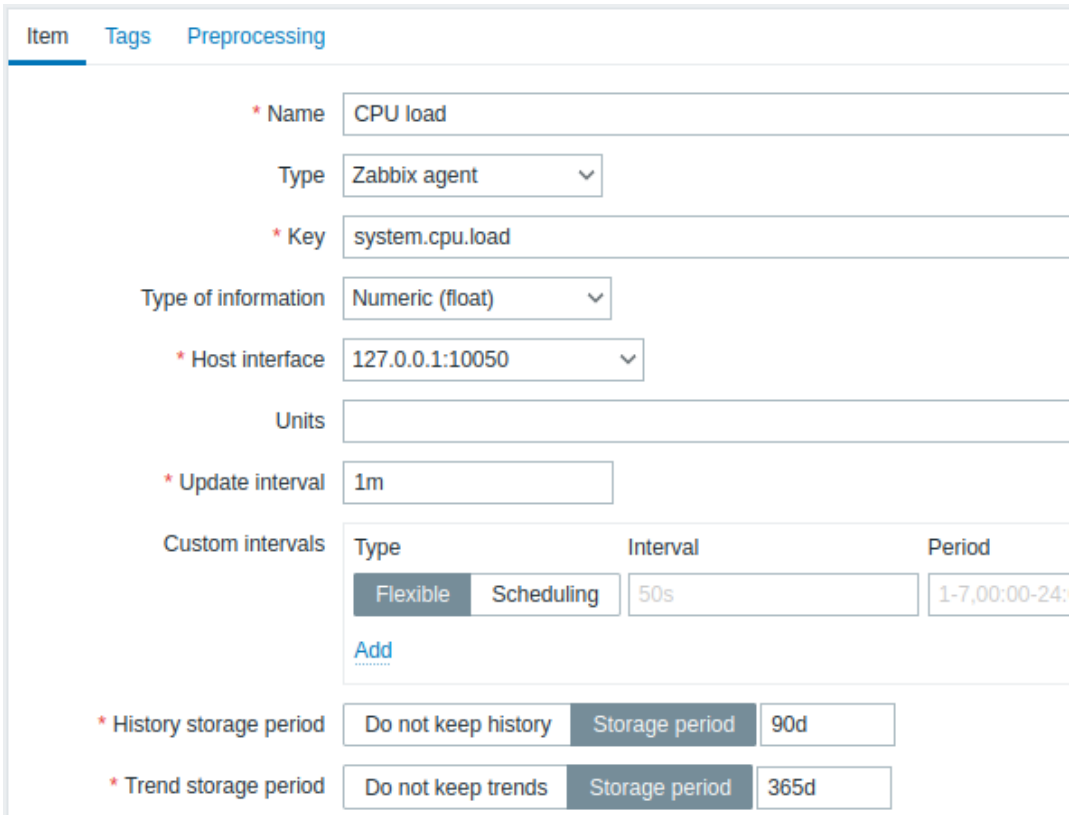


Figura 114. Crear Item

Crear Trigger

El trigger se debe agregar a un Item:

Configuration → **Hosts** y se busca el host y se hace clic **en Triggers →Create Trigger,** como se muestra en la figura 115.

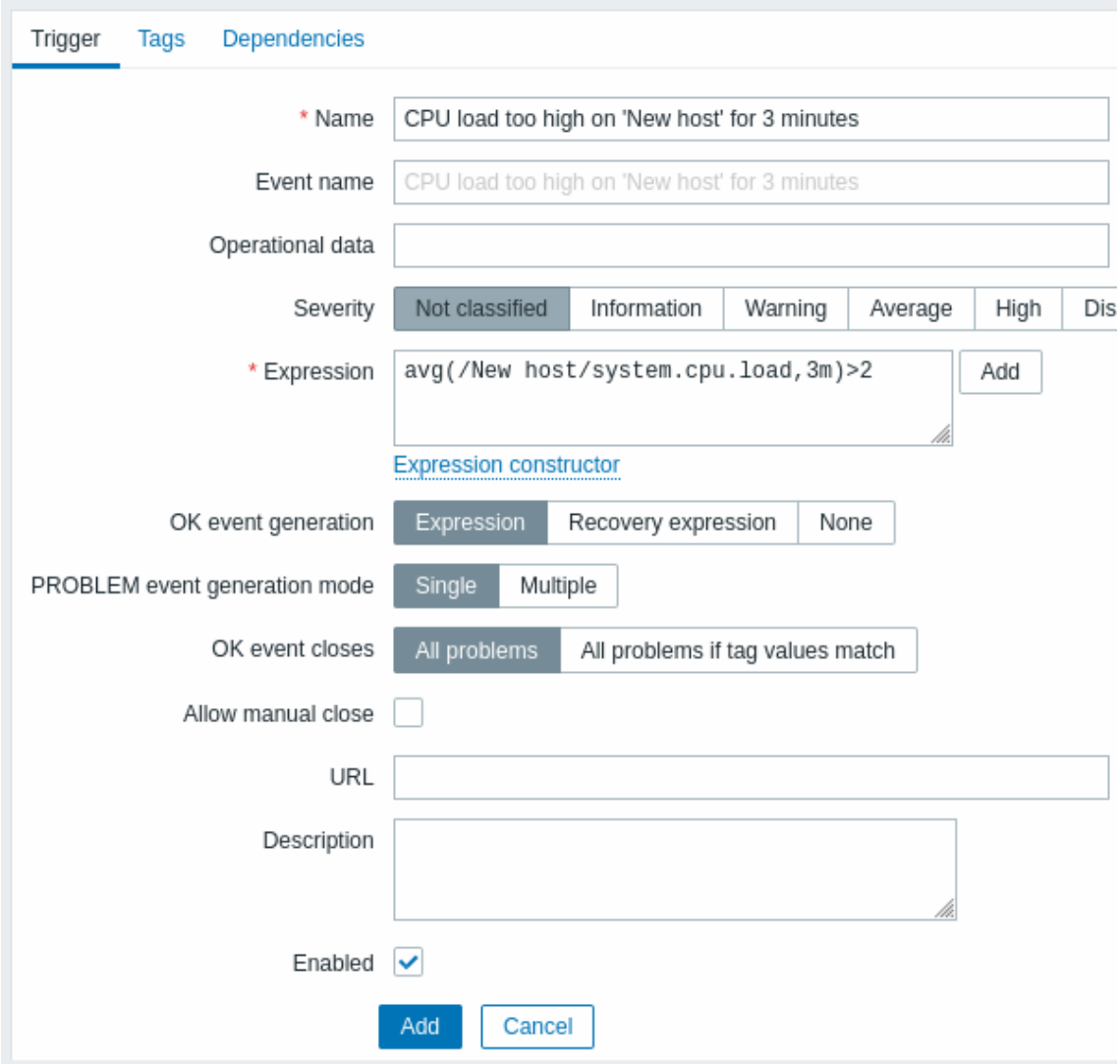


Figura 115. Crear Trigger

Creación de usuarios

Se selecciona **Administration →User→Create user** y se ingresa la información del usuario, como se muestra en la Figura 116.

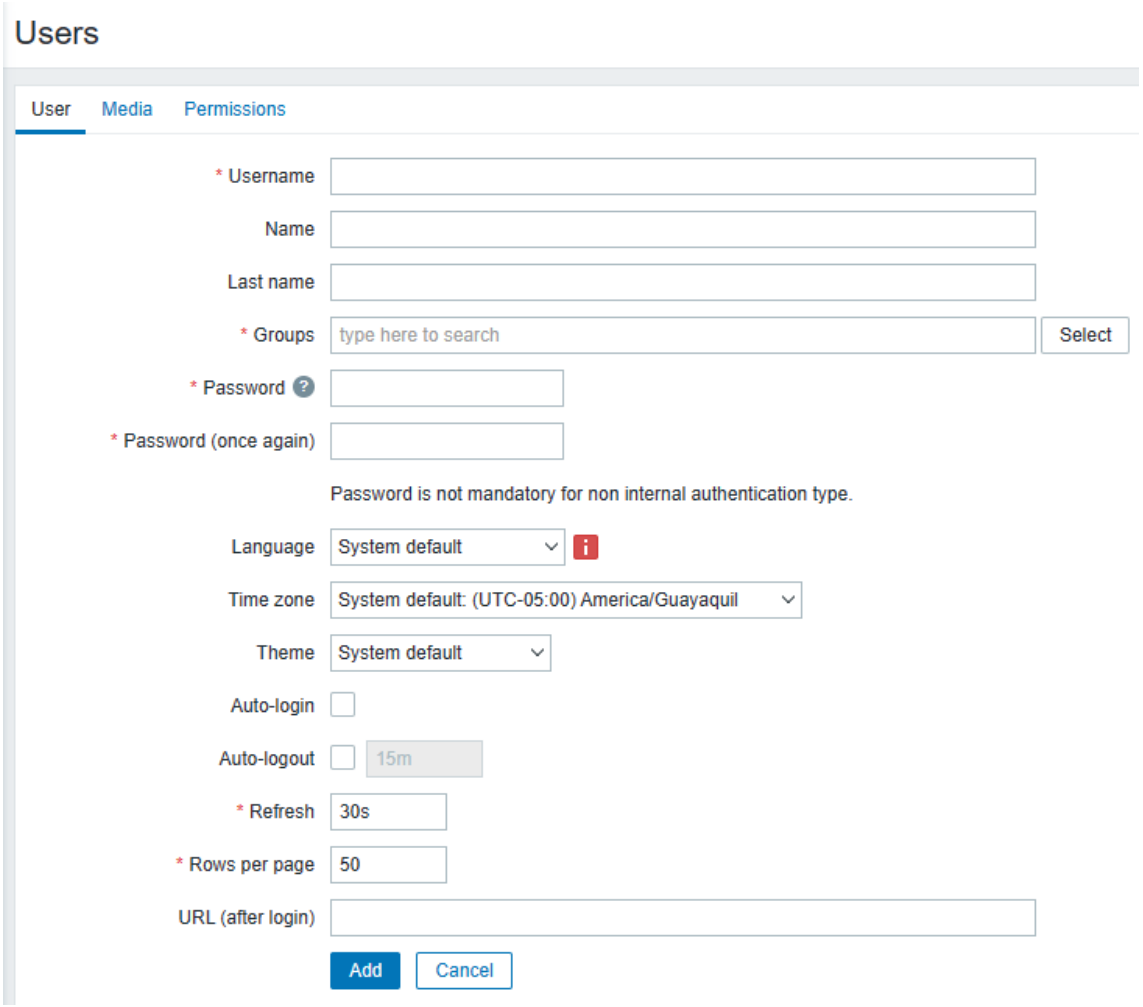


Figura 116. Crear usuario

En la pestaña **Permissions**, se selecciona el tipo de rol del usuario a crear, luego se hace clic en **Add** para finalizar la creación del usuario, como se muestra en la Figura 117.

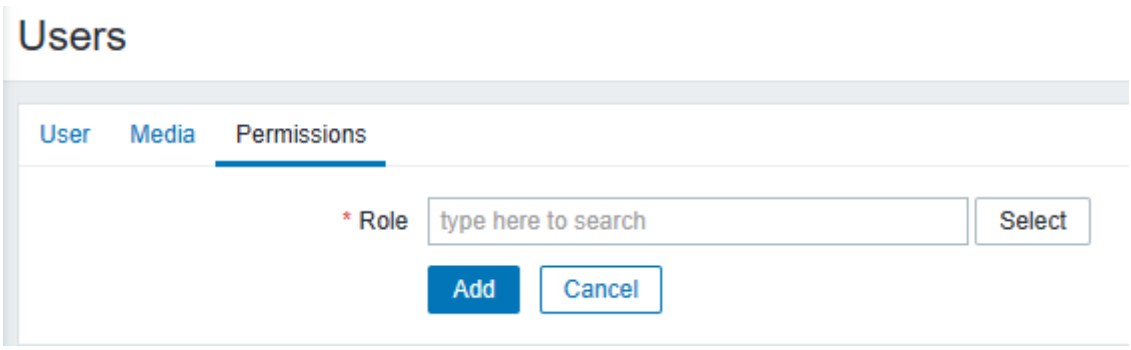


Figura 117. Selección de Rol del usuario

Crear roles de usuario

Se selecciona **Administration→User roles→create user role** y se ingresa el nombre del rol a crear, como se muestra en la Figura 118.

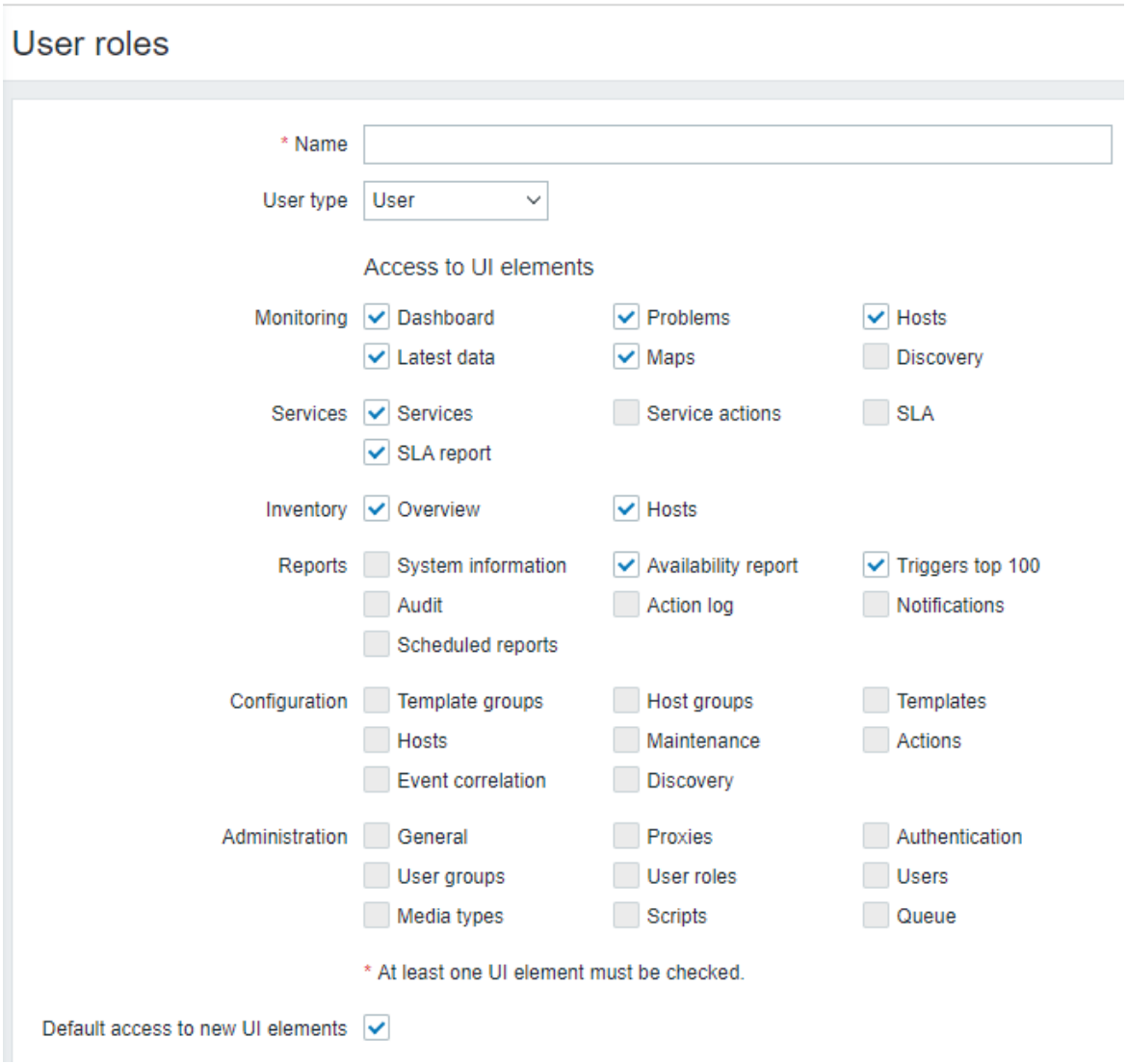


Figura 118. Crear rol de usuario

Crear de grupos de usuario

Se selecciona **Administration→User groups→create user group** y se ingresa la información del grupo a crear (nombre del ISP) y se agrega los usuarios que pertenecen al grupo, como se muestra en la Figura 119.

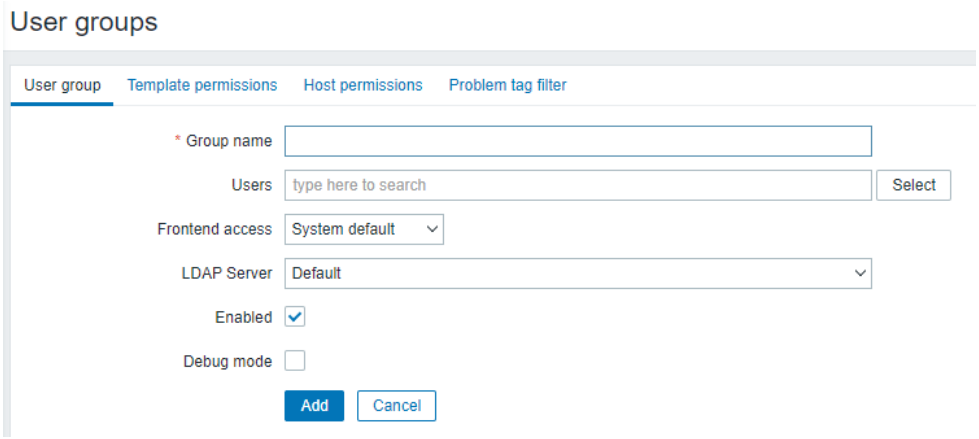


Figura 119. Crear grupo de usuarios

Nueva Plantilla

Configuration → **Templates**, luego clic en **Create Template**.

Esto presenta un formulario de configuración de plantilla. Se configura la plantilla y se finaliza haciendo clic en **Add**, como se muestra en la Figura 120.

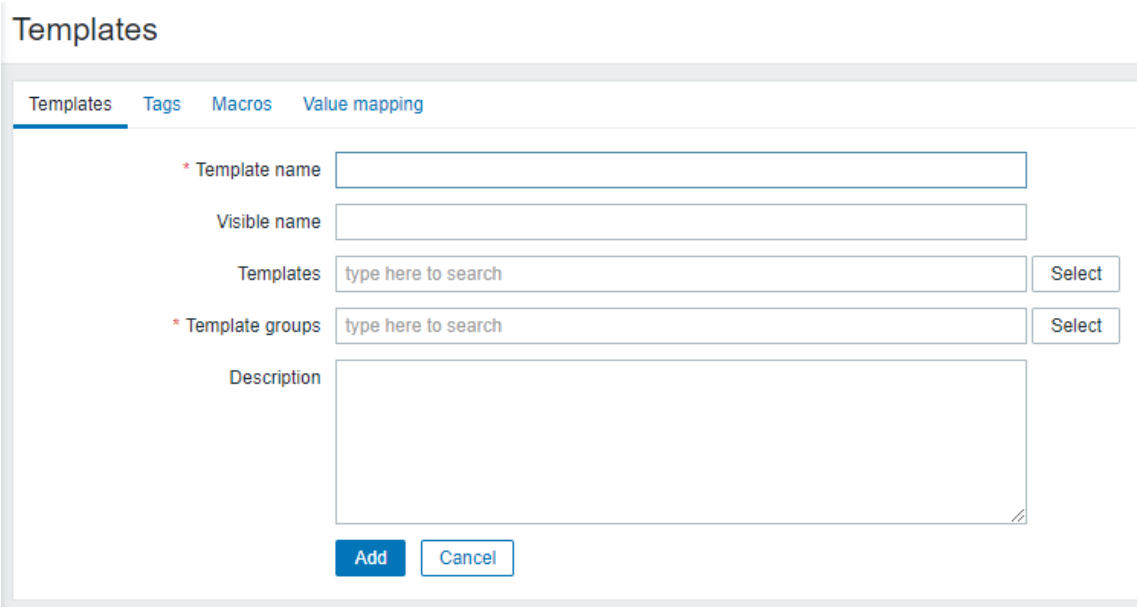


Figura 120. Crear plantilla

Importar Plantilla

Para importar una plantilla se hace clic en el botón **import** se agrega la plantilla y se finaliza haciendo clic en **import,** como se muestra en la Figura 121.

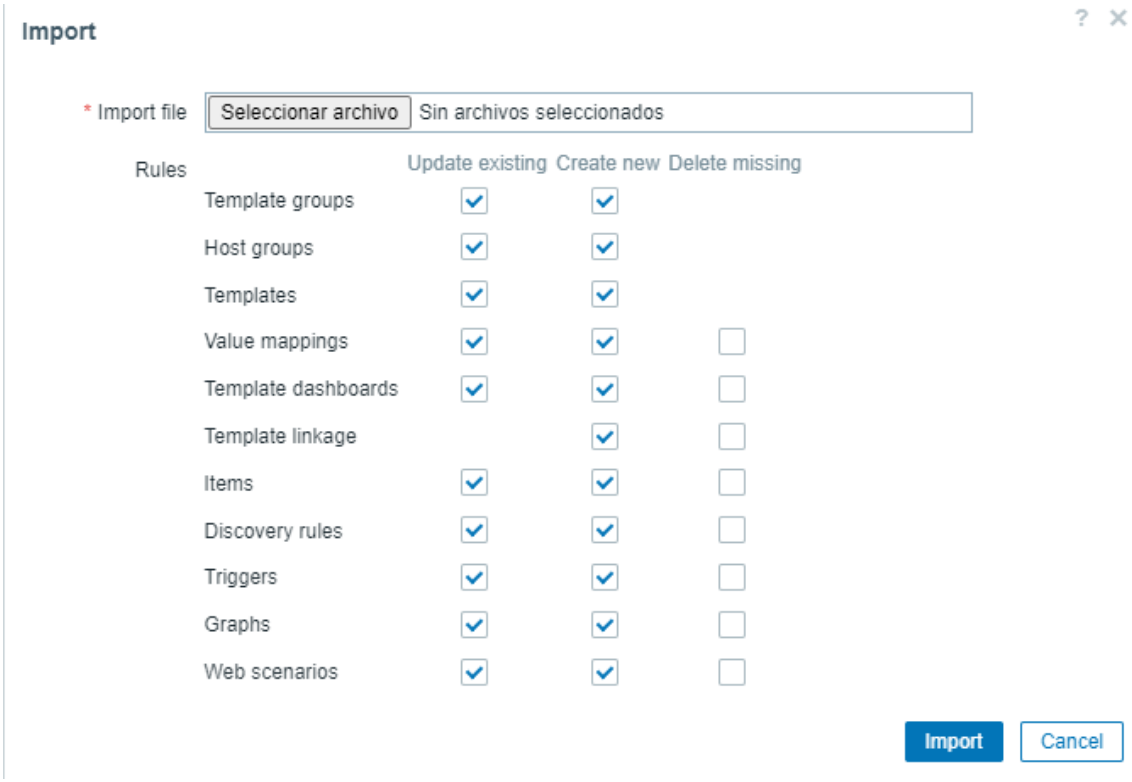


Figura 121. Importar plantilla

Sección monitoring

Monitoring→Dashboard

En la Figura 122, se observar el dashboard predeterminado para el inicio de sesión.

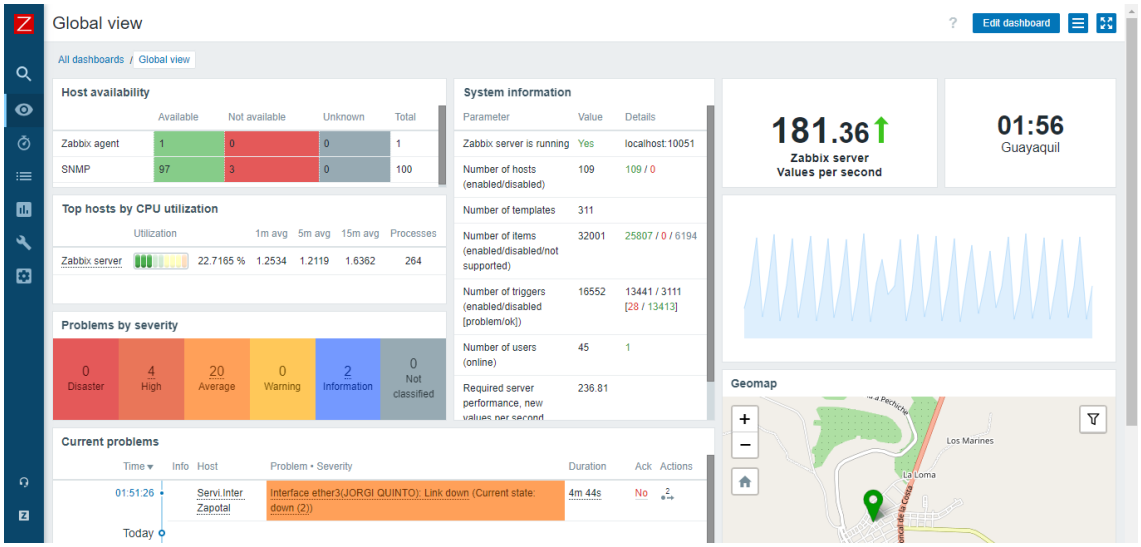


Figura 122. Dashboard Global

Monitoring→Dashboard→All dashboard

La Figura 123, permite observar todos los dashboard disponibles y creados.

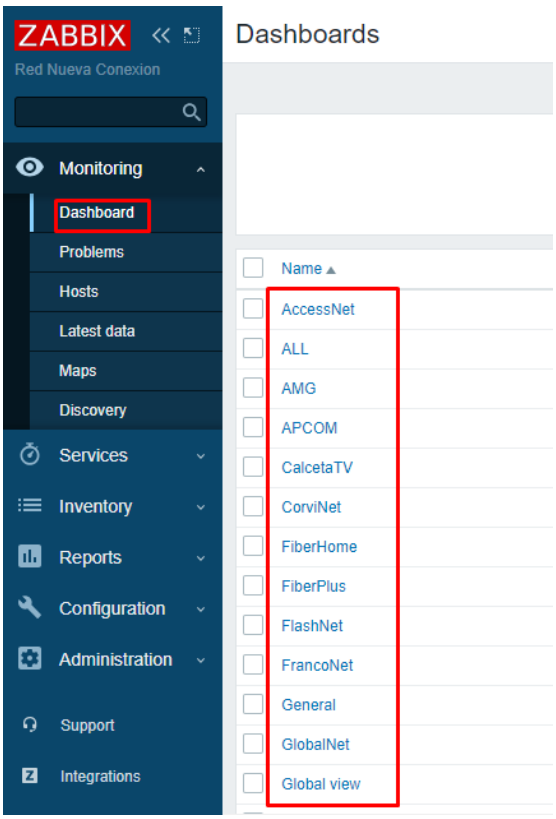


Figura 123. Lista de Dashboard

Monitoring→Problems

Esta opción permite revisar los problemas reportados, también se puede hacer uso del filtro para ver un problema en específico.

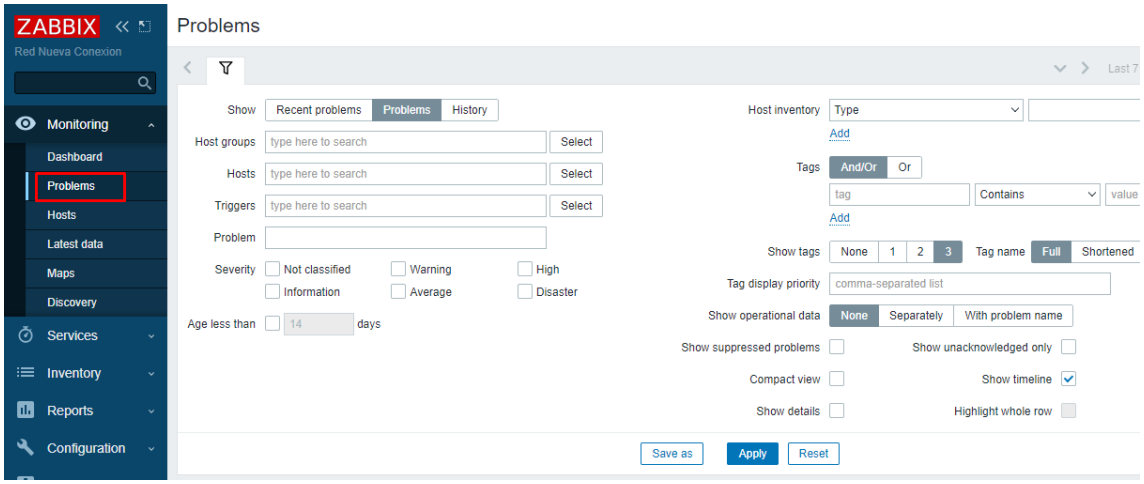


Figura 124. Problems

Monitoring →Hosts

Esta pestaña permite ver los hosts agregados y el servicio habilitado. Como se indica en la Figura 125, esta pestaña también permite crear host directamente.

Figura 125. Hosts

Monitoring →Latest data

Permite observar los últimos valores obtenidos por Zabbix, también tiene una opción de filtro para seleccionar el host a revisar, como se muestra en la Figura 126.

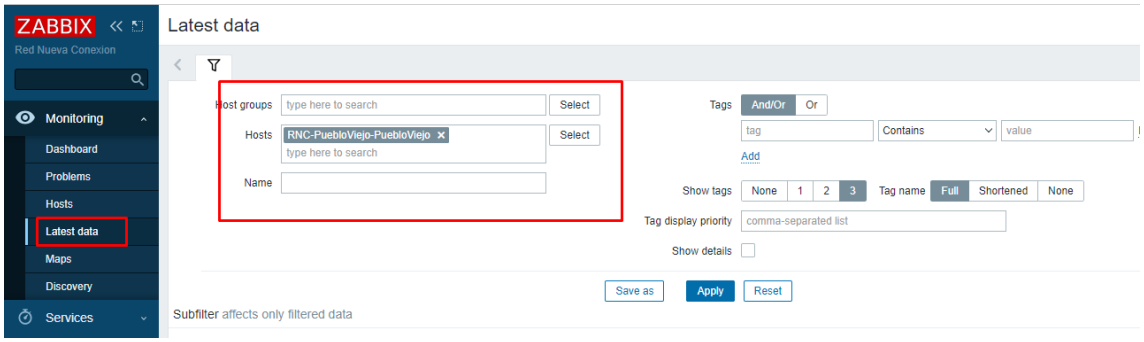


Figura 126. Latest date

Monitoring →Maps

Permite crear y observar los mapas disponibles en Zabbix.

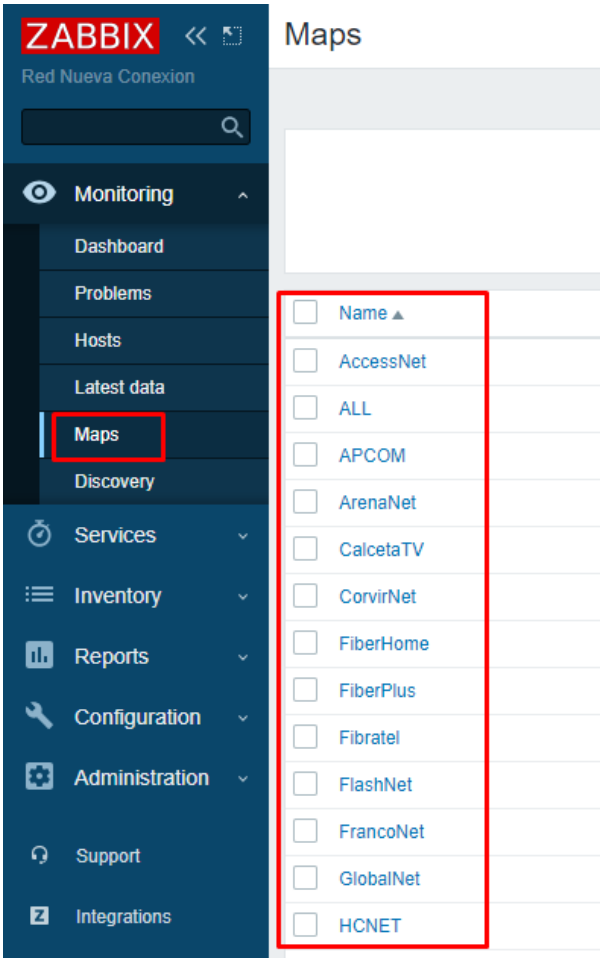


Figura 127. Maps

Sección Reports

Reports→System information

Permite obtener la información general del sistema, como se indica en la Figura 128.

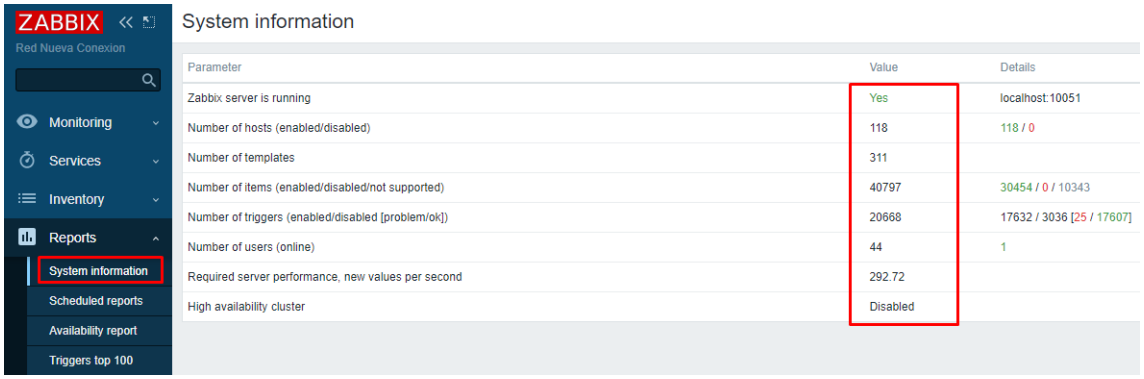


Figura 128. System information

Reports→Trigger top 100

Esta estaña permite visualizar el 100 de los triggers(disparadores)enviados, también se puede hacer uso del filtro para seleccionar los triggers por el grado de severidad, como se indica en la Figura 129.

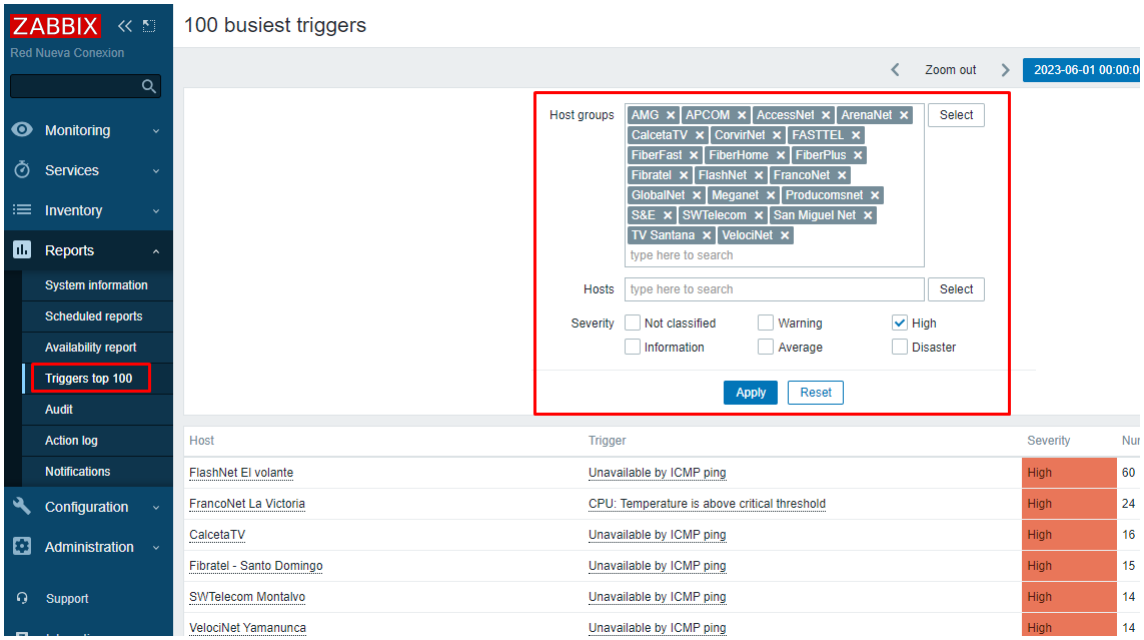


Figura 129. Triggers top 100

Reports→Audit log

Esta pestaña permite revisar el log de forma detallada, se puede filtra por usuario y por tipo de acción como: login. Add, Execute, Configutation refresh, deletre logout, como se indica en la Figura 130.

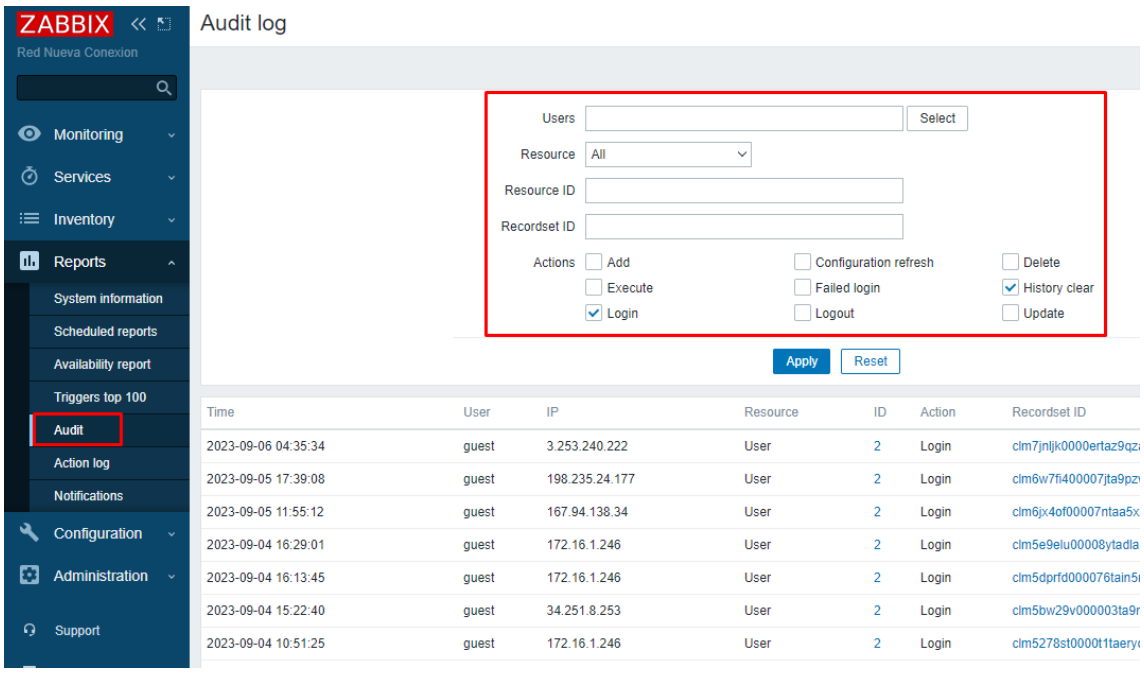


Figura 130. Audit

Reports→Action Logs

Esta pestaña permite observar las acciones programadas por un usuario en el servidor. Como se indica en la Figura 131.

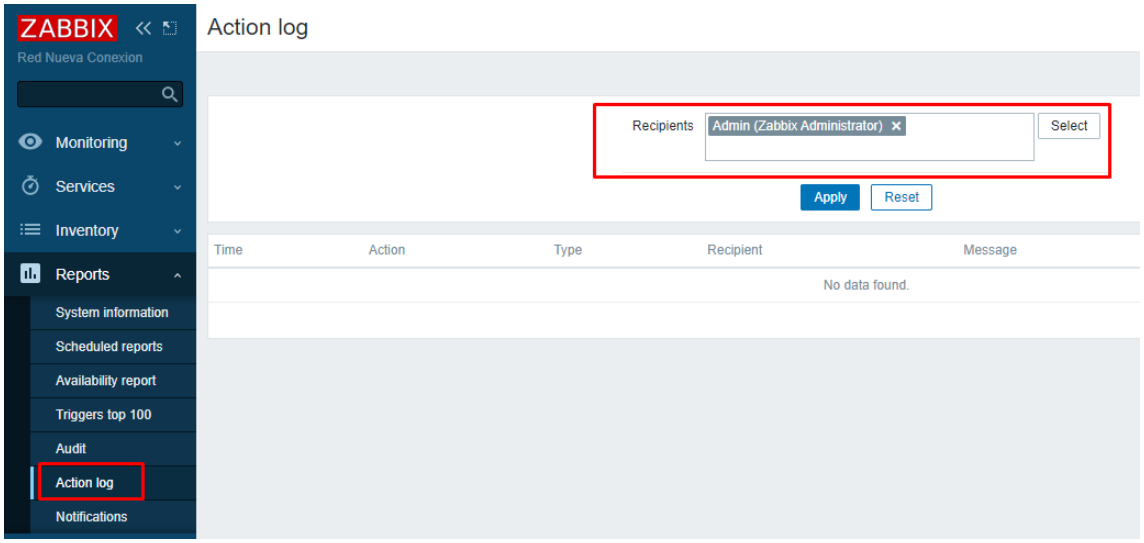


Figura 131. Action log

Configuration→Template groups

Permite crear grupos de plantillas para identificar los tipos de servicios monitoreados como indica la Figura 132.

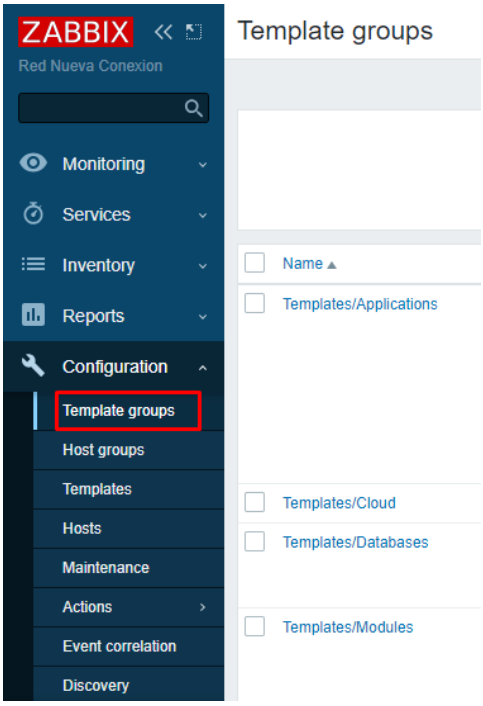


Figura 132. Template Groups

Configuration→Host groups

Permite crear grupos de host con el objetivo de diferenciar la organización que pertenecen, como indica la Figura 133.

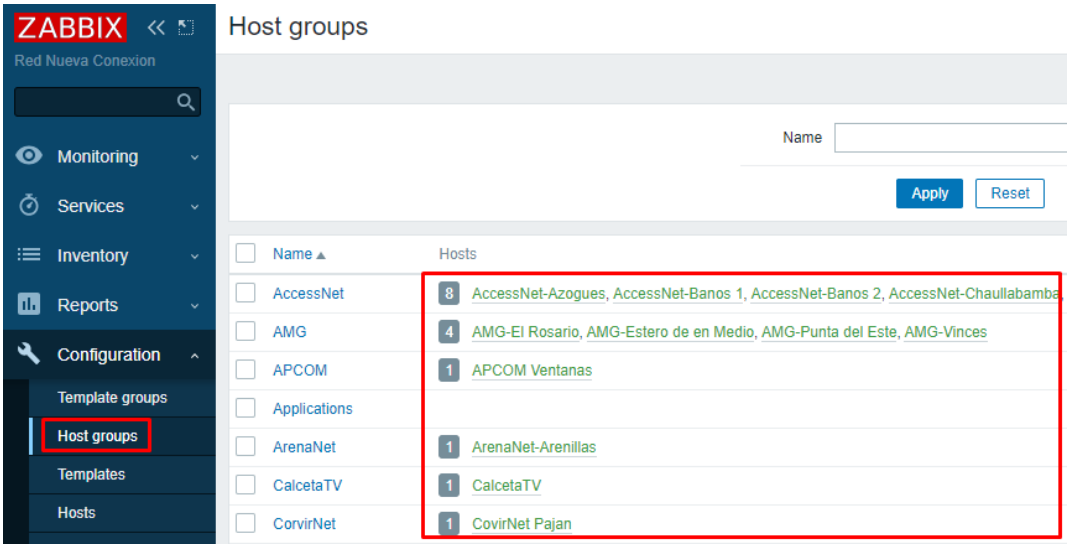


Figura 133. Host Group

Configuration→Templates

Permite editar y crear plantillas para administrar los hosts de los distintos vendors (Fabricantes) como indica la Figura 134.

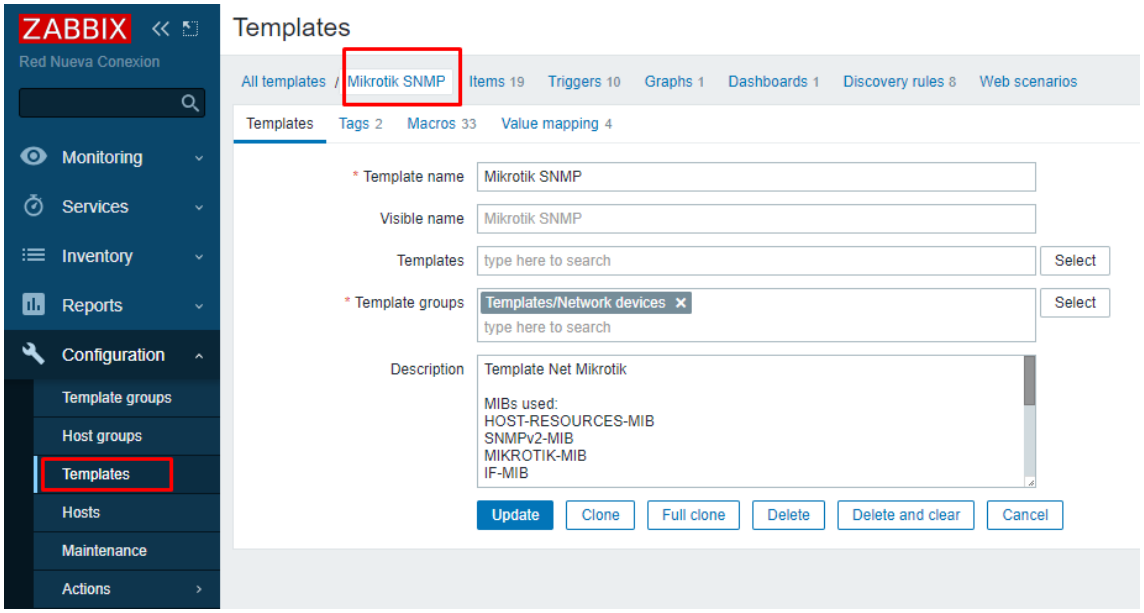


Figura 134. Templates

Configuration→Maintenance

Permite crear periodos de mantenimiento programados, como indica la Figura 135.

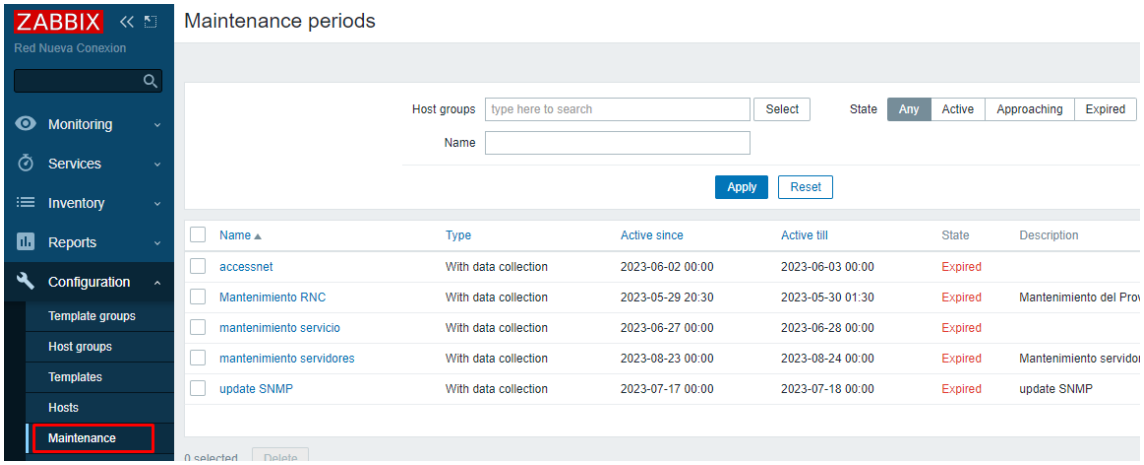


Figura 135. Maintenance

Anexo 8. Oficio de entrega del Manual de usuario

Pueblo viejo, 06 de septiembre de 2023

Ing. Manuel Ignacio Tandazo Mera
Gerente de Red Nueva Conexión

Asunto: Entrega del Manual de usuario para el administrador, como parte de la Tesis "Implementación de un sistema de Administración de red (NMS) para los clientes ISP de la empresa Red Nueva Conexión".

Como parte de mi tesis titulada "**Implementación de un sistema de Administración de red (NMS) para los clientes ISP de la empresa Red Nueva Conexión**" en la **Universidad Nacional de Loja**, me complace compartir con usted el Manual de Usuario de Zabbix, el cual he desarrollado como parte de mi investigación. El manual proporciona una guía detallada sobre cómo configurar y administrar Zabbix para el monitoreo y la gestión de la infraestructura de red. He trabajado en estrecha colaboración con el equipo de Red Nueva Conexión para garantizar que este recurso sea relevante y útil para su organización.

Quiero agradecer a Red Nueva Conexión por brindarme la oportunidad de realizar esta tesis, y por su apoyo continuo en este proceso.

Por favor, encuentre adjunta la carta de aceptación de este manual, firmada por el representante autorizado de Red nueva Conexión.

Atentamente,

RUBEN DARIO LOZANO LOZANO

Ruben Dario Lozano Lozano
C.I. 1900826569
Email: rdlozanol@unl.edu.ec
Celular: +593 989055780

Aceptación de la entrega del Manual de Usuario de Zabbix

Por la presente, Manuel Tandazo, en calidad de gerente de Red Nueva Conexión, acepta la entrega del Manual de Usuario de Zabbix como parte de la tesis titulada "**Implementación de un sistema de Administración de red (NMS) para los clientes ISP de la empresa Red Nueva Conexión**" presentada por **Ruben Dario Lozano Lozano** de la **Universidad Nacional de Loja**.

MANUEL IGNACIO TANDAZO MERA
Firmado digitalmente por MANUEL IGNACIO TANDAZO MERA
Fecha: 2023.09.07 11:13:32 -05'00'

Ing. Manuel Tandazo Mera
C.I. 1206535450
Gerente - Red Nueva Conexión

Anexo 9. Certificado de la implementación del NMS

Red Nueva Conexión

Puebloviejo, 06 de septiembre de 2023

Ing. Manuel Ignacio Tandazo Mera
Gerente de Red Nueva Conexión

Asunto: Certificación de la Implementación de un sistema de Administración de red (NMS) para los clientes ISP de la empresa Red Nueva Conexión.

A quien corresponda,

Por la presente, certifico que el NMS Zabbix ha sido implementado con éxito en la empresa Red Nueva Conexión, como parte de la tesis titulada" **Implementación de un sistema de Administración de red (NMS) para los clientes ISP de la empresa Red Nueva Conexión**" por el tesista **Ruben Dario Lozano Lozano**. La implementación del NMS se realizó siguiendo las especificaciones acordadas y los requisitos de Red Nueva Conexión, y se ha completado satisfactoriamente. El NMS Zabbix ha sido configurado y personalizado para adaptarse a las necesidades específicas de monitoreo y gestión de la infraestructura de los ISP que monitorea Red nueva Conexión.

Las características y funcionalidades del NMS Zabbix, que han sido implementadas y verificadas, incluyen:

- Monitoreo en tiempo real de los routers de borde.
- Configuración de alertas y notificaciones personalizadas.
- Generación de paneles de control intuitivos.

El tesista Ruben Dario lozano Lozano ha trabajado estrechamente con el personal de la Red nueva Conexión, para garantizar una transición sin problemas y un funcionamiento óptimo del sistema.

Atentamente,

MANUEL IGNACIO TANDAZO MERA
Firmado digitalmente por MANUEL IGNACIO TANDAZO MERA
Fecha: 2023.09.07 11:14:50 -05'00'

Ing. Manuel Tandazo Mera
C.I. 1206535450
Gerente - Red Nueva Conexión

Anexo 10. Certificado Zabbix Starter Week

Figura 136. Certificado Zabbix Starter Week

Anexo 11. Certificado de traducción del resumen

English Speak Up Center

Nosotros "English Speak Up Center"

CERTIFICAMOS que

La traducción del resumen de Trabajo de Titulación titulado "IMPLEMENTACIÓN DE UN SISTEMA DE ADMINISTRACIÓN DE RED (NMS) PARA LOS CLIENTES ISP DE LA EMPRESA RED NUEVA CONEXIÓN." documento adjunto solicitado por el señor Ruben Dario Lozano Lozano con cédula de ciudadanía número 1900826569 ha sido realizada por el Centro Particular de Enseñanza de Idiomas "English Speak Up Center"

Esta es una traducción textual del documento adjunto. El traductor es competente y autorizado para realizar traducciones.

Loja, 19 de septiembre de 2023

Elizabeth Sánchez de Vélez

Mg. Sc. Elizabeth Sánchez Burneo
DIRECTORA ACADÉMICA

DIRECCION: SUCRE 207-16 ENTRE AZUAY Y MIGUEL RIOFRIO | TELÉFONO: 099 5263 264