ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

CARRERA TELECOMUNICACIONES

"IMPLEMENTACION DE UN SISTEMA INTEGRAL DE MONITOREO EN TIEMPO REAL EN LA RED CORE CON SNMPv3 UTILIZANDO EL SOFTWARE ZABBIX, PARA LA EMPRESA MAXXNET"

Trabajo de Integración Curricular

Tipo: Propuesta Tecnológica

Presentado para optar al grado académico de:

INGENIERO EN ELECTRÓNICA, TELECOMUNICACIONES Y REDES.

AUTOR:

ÁNGEL SANTIAGO TOAPANTA CARVAJAL

Riobamba – Ecuador

2023

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

CARRERA TELECOMUNICACIONES

"IMPLEMENTACION DE UN SISTEMA INTEGRAL DE MONITOREO EN TIEMPO REAL EN LA RED CORE CON SNMPv3 UTILIZANDO EL SOFTWARE ZABBIX, PARA LA EMPRESA MAXXNET"

Trabajo de Integración Curricular

Tipo: Propuesta Tecnológica

Presentado para optar al grado académico de:

INGENIERO EN ELECTRÓNICA, TELECOMUNICACIONES Y REDES.

AUTOR: ÁNGEL SANTIAGO TOAPANTA CARVAJAL

DIRECTOR: ING. OSWALDO GEOVANNY MARTÍNEZ GUASHIMA MSc.

Riobamba – Ecuador

2023

Yo, **ÁNGEL SANTIAGO TOAPANTA CARVAJAL**, declaro que el presente Trabajo de Integración Curricular es de mi autoría y los resultados del mismo son auténticos. Los textos en el documento que provienen de otras fuentes están debidamente citados y referenciados.

Como autor asumo la responsabilidad legal y académica de los contenidos de este trabajo de integración curricular; el patrimonio intelectual pertenece a la Escuela Superior Politécnica de Chimborazo.

Riobamba, 05 de abril del 2023

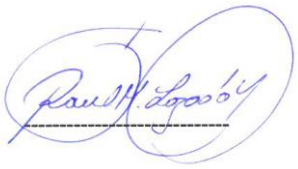
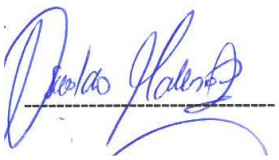
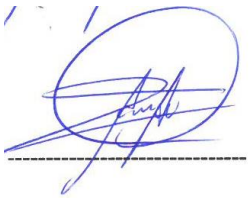
Ángel Santiago Toapanta Carvajal
060462184-7

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

CARRERA TELECOMUNICACIONES

El Tribunal del Trabajo de Integración Curricular certifica que: El Trabajo de Integración Curricular; tipo: Propuesta Tecnológica, **"IMPLEMENTACION DE UN SISTEMA INTEGRAL DE MONITOREO EN TIEMPO REAL EN LA RED CORE CON SNMPv3 UTILIZANDO EL SOFTWARE ZABBIX, PARA LA EMPRESA MAXXNET"**, realizado por el señor: ÁNGEL SANTIAGO TOAPANTA CARVAJAL, ha sido minuciosamente revisado por los Miembros del Tribunal del Trabajo de Integración Curricular, el mismo que cumple con los requisitos científicos, técnicos, legales, en tal virtud el Tribunal Autoriza su presentación.

	FIRMA	**FECHA**
Ing. Raúl Marcelo Lozada Yanez. MSc. **PRESIDENTE DEL TRIBUNAL**		2023-04-05
Ing. Oswaldo Geovanny Martinez Guashima. MSc. **DIRECTOR DEL TRABAJO** **DE INTEGRACIÓN CURRICULAR**		2023-04-05
Ing. Alberto Leopoldo Arellano Aucancela. MSc. **ASESOR DEL TRABAJO** **DE INTEGRACIÓN CURRICULAR**		2023-04-05

DEDICATORIA

Dedico a Dios por las enseñanzas a lo largo de mi vida académica y personal, a mi familia por haber estado siempre cuando necesitaba para no rendirme hasta conseguir al objetivo previsto, a mis profesores que estuvieron la paciencia para despejar las dudas que se presentaban a lo largo de la carrera con sus enseñanzas y experiencia. Especialmente dedico este trabajo de titulación a mis padres que fueron el motor de mi vida que es un ejemplo a seguir por su lucha y perseverancia de sacar a mi familia adelante sin importar las adversidades de la vida. Este trabajo también quiero dedicar a todo el profesorado de la FIE que gracias a su experiencia me han inculcado sus conocimientos para desarrollar este documento.

Ángel

AGRADECIMIENTO

Agradezco infinitamente a mis queridos padres que con su lucha, perseverancia me inculcaron valores éticos y morales que han estado presentes en cada minuto de mi vida, los mismos que me ayudaron en toda mi trayectoria estudiantil. De la misma manera quiero agradecer a la ilustre Escuela Superior Politécnica de Chimborazo por la oportunidad de formarme como profesional de principios.

Ángel

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

RESUMEN

La empresa “Maxxnet” realiza continuamente el monitoreo de algunos puntos críticos dentro de su gestión, para medir la clase de servicio que ofrece a los clientes, actualmente el software que utiliza es compatible solo con ciertos equipos, además la empresa trabaja 24/7 con equipos como; router, switch, Terminal de Línea Óptica (OLT), etc., de diferentes marcas, cualquier incidente puede ocasionar la caída del servicio, afectando a muchos usuarios y provocando cuantiosas pérdidas, por lo tanto, el objetivo del presente trabajo de integración curricular fue implementar un sistema integral de monitoreo en tiempo real del núcleo de la empresa (CORE) con el protocolo simple de administración de red versión 3 (SNMPv3) utilizando el software de monitoreo ZABBIX, para administrar la red interna de manera óptima, elevando la seguridad en el tráfico de datos en procesos de comunicación, con algoritmos de autentificación y privacidad. Se empleó un enfoque investigativo y aplicativo, se utilizó el software Open Source Zabbix para realizar las pruebas de control. Mediante esta metodología se garantizó que la información de gestión recibida no sufra alguna alteración durante el viaje por la red, permitiendo que solo dispositivos autorizados que utilicen las mismas claves de encriptación y autentificación se comuniquen hacia el ente de control que en este caso es servidor Zabbix. Se logró tener una encriptación robusta de la información durante la transmisión de datos, gracias a la interfaz web, se puede ingresar en cualquier navegador a través de la dirección IP del servidor y utilizar las diferentes herramientas que proporciona. En ese contexto se concluye que el protocolo SNMPv3 posibilita manejar la información de una forma modular, garantizando un control restringido de acceso mediante las políticas que maneja la empresa, evitando la suplantación de identidades o modificación de los mensajes que puedan alterar el funcionamiento de la red Core.

Palabras clave: < SNMPv3>, <HOST>, <ZABBIX>, <OPEN SOURCE>, <IP>, <ROUTER>, <SWITCH>, <OLT>.

SUMMARY

The company "Maxxnet" continuously monitors some critical points within its management, to measure the kind of service it offers to customers, currently the software it uses is compatible only with certain equipment, in addition the company works 24/7 with teams like; router, switch, Optical Line Terminal (OLT), etc., of different brands, any incident can cause the service to fall, affecting many users and causing large losses, therefore, the objective of this curricular integration work was to implement a comprehensive real-time monitoring system of the core of the company (CORE) with the simple network management protocol version 3 (SNMPv3) using the ZABBIX monitoring software, to optimally manage the internal network, increasing security in data traffic in communication processes, with authentication and privacy algorithms. An investigative and application approach was used, the Open Source Zabbix software was used to carry out the control tests. Through this methodology, it was guaranteed that the management information received does not undergo any alteration during the journey through the network, allowing only authorized devices that use the same encryption and authentication keys to communicate with the control entity, which in this case is the Zabbix server. It was possible to have a robust encryption of the information during the transmission of data, thanks to the web interface, it can be entered in any browser through the IP address of the server and use the different tools it provides. In this context, it is concluded that the SNMPv3 protocol makes it possible to manage information in a modular way, guaranteeing restricted access control through the policies managed by the company, avoiding identity theft or modification of messages that may alter the operation of the network Core.

Palabras clave: < SNMPv3>, <HOST>, <ZABBIX>, <OPEN SOURCE>, <IP>, <ROUTER>, <SWITCH>, <OLT>.

MSc. Wilson G. Rojas

C.I 0602361842

INTRODUCCIÓN

Las telecomunicaciones hoy en día cumplen un papel muy importante para la sociedad, uno de ellos es el acceso al internet, que fue fundamental en la temporada de la pandemia que la gente buscaba estar conectado.

Los ISP pequeños y grandes tendieron sus propios anillos de fibra por todo el territorio ecuatoriano, por consecuencia sus redes crecieron y su administración se vuelve más compleja tanto en la parte de control y seguimiento que se vuelven grandes retos para los administradores.

La seguridad y la disponibilidad de la red para un proveedor de internet son los puntos claves para su óptimo funcionamiento, ya que la información que se utiliza para la gestión de monitoreo a los dispositivos de forma remota debe ser confiable y segura para resguardar su integridad en el camino para evitar que conozca cómo está estructurado la red.

Para este trabajo de integración curricular se propone trabajar con protocolo de SNMPv3 para la gestión de la red, cabe mencionar que el protocolo garantiza diferentes formas de encriptación por ejemplo AES, DES, etc que garantiza la seguridad en la información que se utiliza para la administración de la red.

En el mercado hay diferentes aplicaciones para el monitoreo de la red que son Open Source, y Zabbix es uno de ellos que se utilizara como herramienta de monitoreo ya que procesara la información generada por SNMPv3. Zabbix se escogió por tener características amigables al momento de programar, tener plantillas para diferentes equipos que existen en el mercado, es compatibles en todas las versiones SNMP, graficas en tiempo real, chequeos de disponibilidad y desempeño, tiene una interfaz web, controla cualquier dispositivo que sea compatible los protocolo, etc.

CAPÍTULO I

1. DIAGNÓSTICO DEL PROBLEMA

1.1 Planteamiento del problema

¿Es factible la implementación de un sistema integral de monitoreo en tiempo real de la red Core de la Empresa Maxxnet, utilizando SNMPv3 con el software Zabbix?

1.2 Sistematización del problema

¿Qué ventajas ofrece SNMPv3 respecto a las versiones anteriores?

¿Zabbix permite la implementación de un sistema integral de monitoreo utilizando SNMPv3, que ventajas y desventajas tiene respecto a otras soluciones open source?

¿Qué diseño y configuración se pueden aplicar para medir en tiempo real el consumo de ancho de banda, uptime, downtime de los enlaces de la red de Core, implementado con Zabbix y SNMPv3 para cumplir los niveles de servicio pactados con los clientes corporativos de la empresa Maxxnet que son reportados a la entidad de control?

¿El diseño propuesto cumple con los niveles de servicio de la empresa Maxxnet, y permite el monitoreo efectivo?

1.3 Justificación del proyecto

1.3.1 Justificación teórica

Un sistema integral de monitoreo como proyecto de investigación, constituye un aporte de academia que servirá como referente técnico para mejorar de la seguridad de la red entre servidor-agente. El desarrollo del proyecto permitirá implementar el monitoreo del estado de la red en tiempo real, atención, resolución y análisis de incidentes que afecten la operatividad y disponibilidad del servicio.

1.3.2 Justificación aplicativa

El monitoreo es una parte primordial de un proveedor de internet (ISP) porque actuado a tiempo se puede prevenir daños grandes en las redes, el monitoreo en tiempo real de las redes es un proceso de control, supervisión, toma medidas preventivas y correctivas para el óptimo funcionamiento de la red, mediante el uso de herramientas de gestión.

En el caso de estudio se podrá implementar y evaluar el ancho de banda, uptime, downtime en el diseño del sistema integral de monitoreo que conforman con algunos equipos en la red Core entre router de Mikrotik, switch Cisco, OLT de la marca Huawei, también se va a tomar una muestra significativa de usuarios corporativos para determinar la seguridad que existe entre el servidor y el agente.

Los niveles de los servicios de la empresa Maxxnet son regidos por el ente de control que es el Arcotel ya que dice claramente que deben tener: (León Vasquez, 2011)

- Porcentaje de averías o Interrupción del servicio.- Qué tiempo estuvo caído el servicio.
- Tiempo medio de reparación de averías.- Porcentaje de averías con tiempo de reparación mayor a 8 horas.
- Porcentaje de disponibilidad del servicio.- qué tiempo está activo el servicio y en qué velocidad estaba trabajando.

Que son puntos críticos para un proveedor de internet para medir la clase de servicio que ofrece a los clientes, actualmente la empresa Maxxnet trabaja con DUDE que es un software de monitoreo compatible solo con equipos mikrotik versión 6.41.2 y como la empresa Maxxnet necesita monitorear equipos de otras marcas comerciales busca nuevas soluciones también utiliza el protocolo SNMPv2.

En vista que la calidad del internet, es muy importante para el consumidor se pretende mejorar el servicio que se tiene con los clientes corporativos y se opta en actualizar el sistema de monitoreo con un protocolo que nos brinda seguridad y los resultados nos den en tiempo real. En este proyecto la estructura principal es el SNMPv3 por la seguridad que ofrece al momento de monitorear ya que la información de la empresa es muy importante mantenerla en secreto, refuerza las prestaciones de seguridad, incluyendo autentificación, privacidad y control de acceso; y de administración de protocolo, con una mayor modularidad y la posibilidad de configuración remota.

Zabbix un open source hace factible cumplir algunos parámetros para el monitoreo de la red en este caso la red Core que son, el monitoreo hardware y software, genera alertas en situaciones inusuales, el monitoreo sin agente propio, detectar interfaces caídas, enviar mensajes al correo, Telegram, etc., informando cuando falle algún sistema esencial para la empresa, generar alertas cuando se sobrepasen umbrales definidos, monitorear corta fuegos, proxis, routers, switches y controlar el acceso de los usuarios a ciertas áreas de la aplicación. (A Crespata, 2012)

1.4 Objetivos

1.4.1 Objetivo general

Implementar un sistema integral de monitoreo en tiempo real en la red Core con SNMPv3 utilizando el software Zabbix, para la empresa MAXXNET.

1.4.2 Objetivos específicos

- Determinar las ventajas que ofrece SNMPv3 para cumplir los requerimientos técnicos para la gestión y tráfico de datos de la empresa Maxxnet.
- Analizar el software Zabbix para la implementación de un sistema integral de monitoreo utilizando SNMPv3.
- Realizar el diseño y la configuración que se pueden aplicar para medir en tiempo real el consumo de ancho de banda, uptime, downtime de los enlaces de la red de Core, implementado con Zabbix y snmp v3 para cumplir los niveles admitidos en la entidad de control.
- Evaluar el diseño propuesto para el cumplimiento de los niveles de servicio requerimientos por la empresa Maxxnet para el monitoreo efectivo

CAPÍTULO II

2. MARCO TEÓRICO

2.1 Elementos de la red CORE

2.1.1 La red core

La red CORE podemos decir que es el cerebro de cualquier ISP donde converge todos los enlaces físicos o virtuales que son encargados de llevar toda la información, su buen funcionalidad y disponibilidad de servicio es de un grado muy alto de prioridad para la empresa ya que el mal funcionamiento del mismo puede ocasionar que el internet tenga intermitencias por ende baja la calidad y perdida de abonados.

La funcionabilidad de la red CORE es de proporcionar la conectividad entre los distintos puntos de accesos como en los router, switch, OLT, etc. También la red CORE se encarga de enlazar diferentes servicios no solo el internet si no redes privadas, redes LAN, túneles, entre otros. Algo importante es que al tener una red CORE para diferentes servicios, se mejora el rendimiento y nos hace posible crecimiento escalable de la red. (Codifícame, 2012)

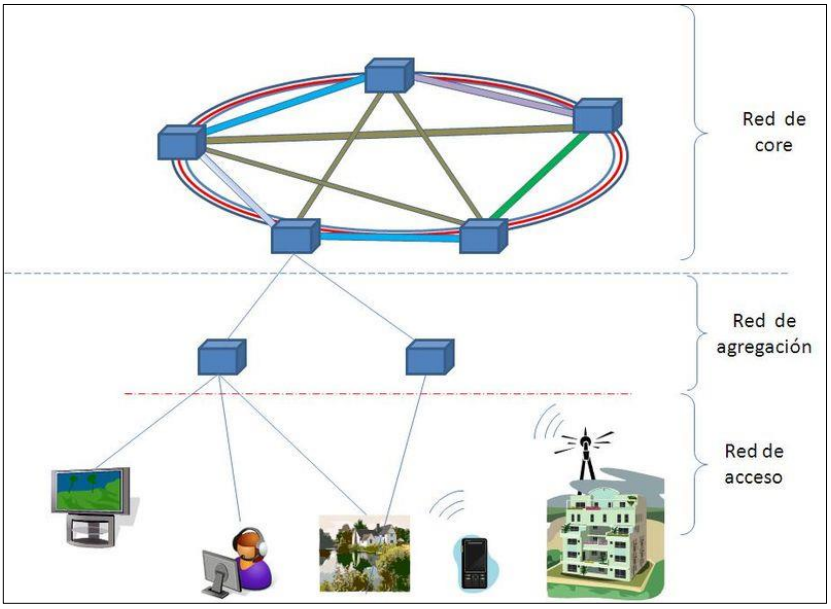


Ilustración 1-2: Esquema general de una red de telecomunicaciones

Fuente: Muñoz Mesa, José Luis, 2009

2.1.2 Router

Un router es un dispositivo que enruta por diferentes caminos la información respetando las políticas, protocolos, seguridad, etc. Para fabricar amplias redes que faciliten la comunicación entre el emisor y receptor.

En la estructura de las telecomunicaciones los routers llegan confundirse con los concentradores de red, los módems o los switch de red. Pero los routers por su capacidad procesamiento de datos pueden combinar las funciones de estos dispositivos y conectarse con los mismos para mejorar el acceso a Internet o ayudar a crear redes empresariales. Estos routers están capacitados para hacer un label swapping (intercambio de etiquetas), label push y label pop.

El funcionamiento es dirigir los datos de la red mediante paquetes que contienen varios tipos de datos, archivos, comunicaciones y transmisiones simples como interacciones web. Los paquetes de datos tienen varias capas, una capa por ejemplo es la que transporta la información de identificación, como emisor, tipo de datos, tamaño y, aún más importante, la dirección IP que es protocolo de Internet. El router es capaz de leer esta capa, prioriza los datos y elige la mejor ruta para cada transmisión de datos. (Cisco Networking Academy, 2021)

2.1.3 Switch

Los switches son dispositivos importantes para cualquier red. Su función se basa en conectar varios dispositivos, como computadoras, access points inalámbricos, impresoras y servidores, en la misma red. Un switch permite a los dispositivos conectados compartir información y comunicarse entre sí.

2.1.4 OLT

OLT es un terminal de línea óptica, que se utiliza para conectar la fibra óptica y transferir señales en forma de luz. Hace una diferencia significativa en PON (red óptica pasiva).

OLT es uno de los dispositivos que conforman en los nodos de servicio en la red de acceso. El acceso al servicio a través de la conexión con los dispositivos de los nodos de servicio correspondientes a través del puerto SNI. La OLT se coordina con diferentes tipos de ONU que existen en el mercado para lograr todo tipo de redes de acceso como FTTC, FTTH, FTTO, FTTM , etc.

2.2 Monitoreo

El monitoreo de red, el gran objetivo es proporcionar la información adecuada a los administradores de las redes, en tiempo real, para diagnosticar si la red está funcionando de manera óptima y según los estándares de cada empresa. Con ayuda de herramientas como el software de monitoreo de redes que puede ser de Open Source con el fin de detectar fallas en la red y en los nodos.

La Monitorización involucra dos factores primordiales, el tiempo de duración del monitoreo y el uso de recursos de la red. Mayor sea el tiempo de monitoreo más efectiva será la detección de problemas. (Junco Romero, G., & Rabelo Padua, 2018)

2.2.1 Monitoreo activo

El monitoreo activo se realiza insertando paquetes de prueba en la red, o en otras palabras enviando paquetes a determinadas aplicaciones midiendo los tiempos de respuesta, la técnica tiene la particularidad de agregar tráfico a la red y que será utilizado para medir el rendimiento de la misma red. (Junco Romero, G., & Rabelo Padua, 2018)

2.2.1.1 Técnicas de Monitoreo

Basado en ICMP

- Diagnosticar Problemas en la red.
- Detectar retardo, perdidas de paquetes.
- Disponibilidad de host de host y redes.

Basado en TCP

- Tasa de transferencia
- Diagnosticar problemas a nivel de aplicación.

Basado en UDP

- Perdidas de paquete en un sentido (one-way)
- RTT (trace route)

2.2.2 Monitoreo pasivo

Este método principalmente se basa en la obtención de datos a partir de recolectar en una base de datos y analizar el tráfico que circula por la red, empleando diversos dispositivos que soporte snmp (1, 2,3),rmon y netflow. Este enfoque no agrega tráfico a la red.

El uso de SNMP para el monitoreo pasivo es una técnica que utilizada estadísticas sobre la utilización de ancho de banda en los dispositivos de red, con el respectivo acceso a dichos dispositivos. Este protocolo genera paquetes llamados traps que indican que un evento inusual se ha producido. (Junco Romero, G., & Rabelo Padua, 2018)

2.3 Simple Network Management Protocol (SNMP)

Es un protocolo Simple Network Management Protocol (SNMP) que se traduce en un Protocolo Simple de Manejo de Red que trabaja en la capa de aplicación basado en IP que intercambia información entre una solución de administración de red y cualquier dispositivo que soporta SNMP.

La administración de la red es un punto muy crucial en los proveedores de internet como la eficiente en la gestión del rendimiento de la red, la búsqueda de problemas y la gestión del crecimiento de la red. SNMP se considera el lenguaje de administración de red, por los componentes de la red que deben tener capacidad de integrar SNMP, y con un software de monitoreo de red que en este caso es OpenSource.

SNMP podemos decir que es un protocolo de nivel de aplicación diseñado para la supervisión de toda la infraestructura de la red que tenga un proveedor y además proporciona al administrador visibilidad del equipo que está monitoreando, como SNMP no es exclusivo para una sola marca de dispositivos, la integración de diferentes dispositivos de varias marcas que existen en el mercado se hace fácil simultáneamente utilizando el mismo software.

El SNMP trabaja recogiendo la información a través de un sondeo. El software de monitoreo de la red actúe como cliente para enviar paquetes de sondeo al servidor SNMP o agente, una parte del código que se va a ejecutar en el propio dispositivo. El agente debe responder a la encuesta y envía un paquete SNMP con las respectivas configuraciones de las métricas predefinidas al cliente. El software de monitoreo de la red procesa, recopilar, revisa y analiza estadísticamente la información de diferentes dispositivos. (ManageEngine, 2023)

2.3.1 Componentes básicos de SNMP

En un sistema SNMP para su funcionamiento óptimo debe constar con:

- Sistemas administradores de red NMS(Network Management Systems)
- Dispositivos administrados
- Agente SNMP
- Base de datos de información de administración denominada de otro modo Base de información de administración (MIB)

2.3.2 Sistemas administradores de red NMS

El administrador o un sistema administrador de red (NMS) es responsable de comunicarse con los dispositivos que están implementados en la red por los agentes SNMP con el objetivo de ejecutar aplicaciones que supervisan y controlan a los dispositivos administrados. Por lo general es un grupo de trabajo que está a cargo de administrar la red para que proporcionen el volumen de recursos de procesamiento y memoria requeridos. (ManageEngine, 2023)

2.3.2.1 Funciones principales del administrador SNMP

- Agentes de consultas
- Obtiene respuestas de agentes
- Establece variables en agentes
- Reconoce eventos asincrónicos de agentes

2.3.3 Dispositivo administrado

El dispositivo administrado o elemento es el cual debe contener un agente de SNMP y reside en la red, que debe estar en una parte de la red que requiera algún tipo de monitorización y administración. La información que recoja y almacena estarán a disposición de los NMS. Los dispositivos o elementos por ejemplo son: enrutadores, conmutadores, servidores, estaciones de trabajo, impresoras, UPS, etc.

2.3.4 Agente SNMP

El agente es un programa o un módulo de software de administración de red que está dentro del dispositivo al cual va estar administrado. En si el agente SNMP permite la recopilación local de información de administración en la base de datos cuando el administrador SNMP lo solicite, en una forma organizada en jerarquías.

2.3.4.1 Funciones principales del agente SNMP

- Recopila información de administración sobre su entorno local, esto puede ser memoria libre, número de paquetes IP recibidos, rutas, caídas de la red, trafico, velocidad, ancho de banda, temperatura, etc.
- Recupera y almacena información de gestión de la MIB.
- Señala eventos inusuales de la red al administrador.
- Actúa como proxy a los nodos de red que no son administrables con SNMP.

2.3.4.2 Diagrama de comunicación de SNMP

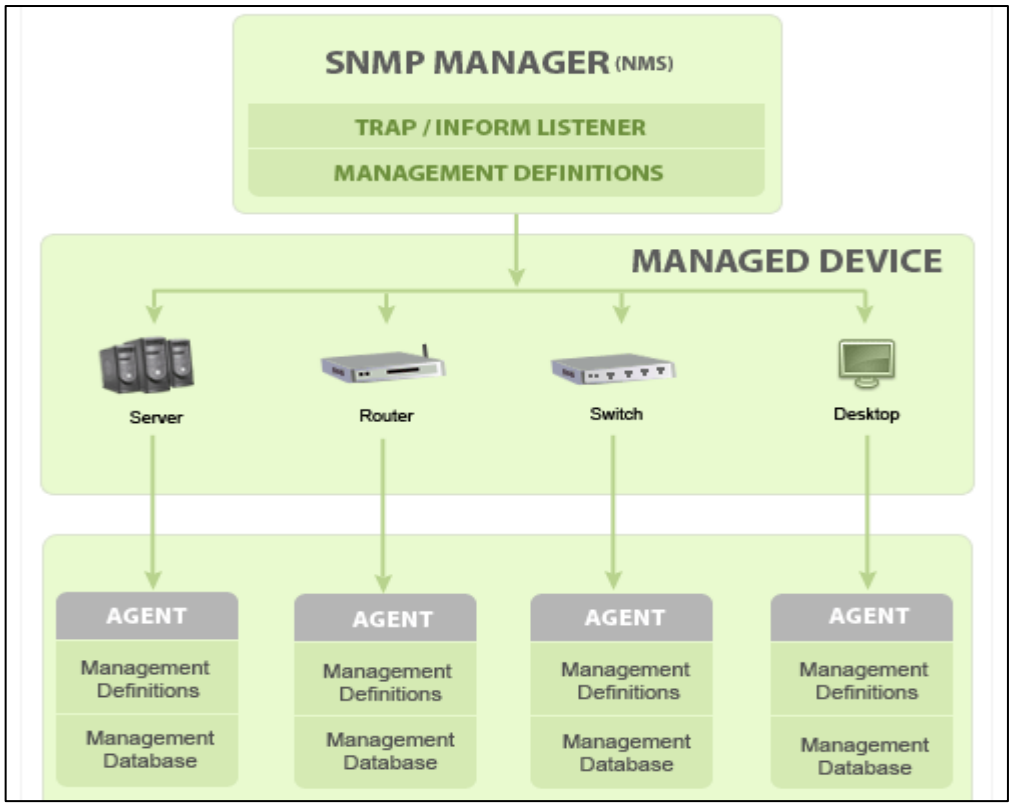


Ilustración 2-2: Diagrama básico de la comunicación SNMP

Fuente: ZOHO Corporation, 2022

2.4 Estructura MIB

2.4.1 Base de información de administración SNMP (MIB)

Management Information Base (MIB) es una base de información de Administración que consiste en la colección de información de los parámetros del dispositivo administrado que está organizada jerárquicamente. El acceso a la MIB el administrador utiliza el protocolo de administración que en este caso es SNMP con el objetivo de solicitar al agente información específica del dispositivo administrado según sea necesario para el Sistema de administración de red (NMS). MIB en su base de datos maneja valores estadísticos y de control que están configurados para nodos de hardware.

El protocolo SNMP va a permitir la extensión de los valores estándar con valores específicos, a través de un agente y que use MIB privadas. El agente recolecta datos localmente y los almacena, como se define en la MIB.

2.4.2 Identificador de objeto (object ID)

Conocidos como objeto MIB, es un número cualquiera de características específicas del dispositivo administrado, cada identificador es único, los objetos administrados por lo general van a estar compuestas de una o más instancias de objeto, que son esencialmente variables. El camino de retorno el valor de cada identificador podría ser diferente, por ejemplo, Texto, Número, Contador, etc. (Steward, 2015)

Objetos administrados escalares: Estos objetos escalares se defines una sola instancia de objeto.

Objetos administrados tabulares: Estos objetos tubulares se definen por poseer múltiples instancias de objetos relacionados que están agrupados en la tabla MIB.

El objeto ID está organizado jerárquicamente en MIB a un objeto administrado, la jerarquía MIB puede representarse por una estructura de árbol con un identificador de variables individuales y los niveles que son asignados por diferentes organizaciones. La identificación de objeto será una secuencia de números enteros que permitirá identificar el objeto.

2.4.3 El árbol MIB

La estructura que está formado el árbol de MIB viene dado en jerarquías, forma de cascada donde sus ramificaciones son objetos a ser gestionados con una función específica de la red, donde están definidas por la SMI que están en el estándar para referir y caracterizar la información de gestión.

Cada nodo contiene un determinado número de objeto que se relaciona entre sí en forma jerárquica según la función que está en el dispositivo a ser gestionado.

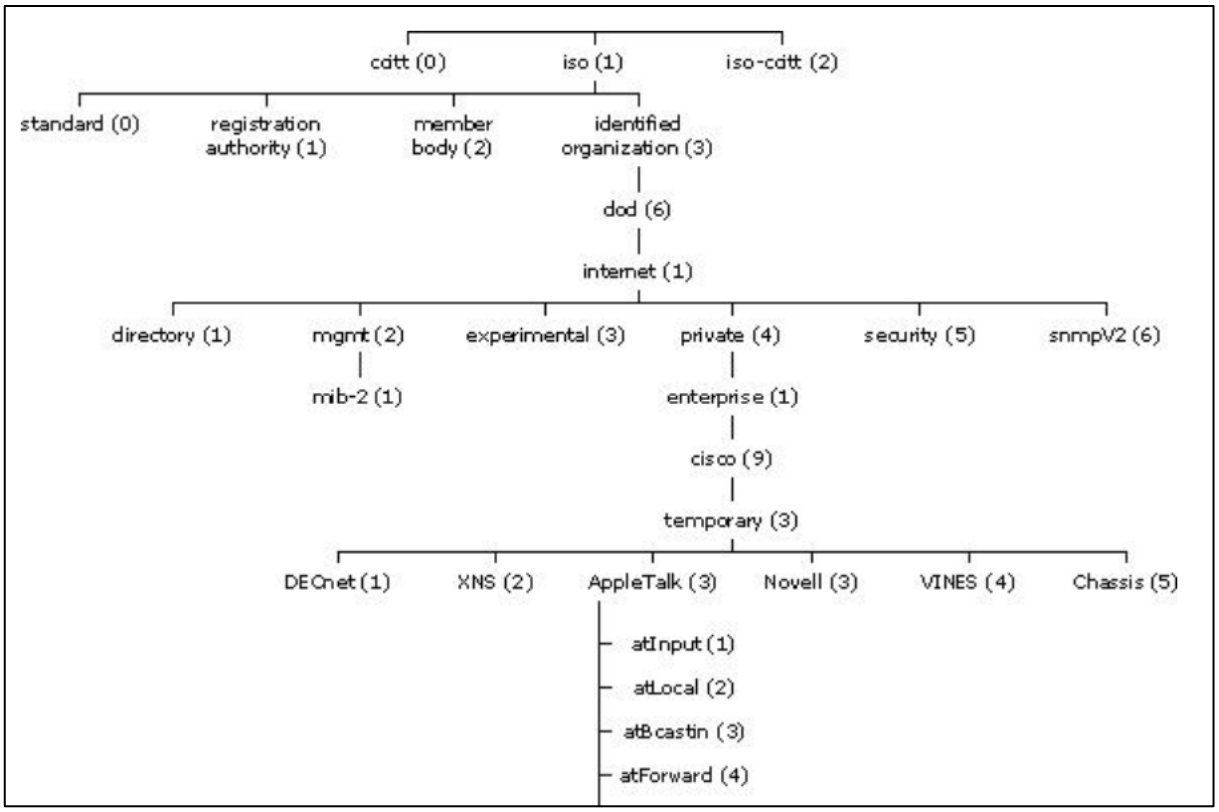


Ilustración 3-2: Estructura de Árbol MIB

Fuente: Muñoz Mesa, José Luis, 2009

En la parte superior del árbol vamos a encontrar objetos que pertenecen a varias organizaciones de estándares, mientras en la parte inferior son objetos que representan a las organizaciones asociadas,

El nudo que nos interesa nace desde la ISO que es la rama principal de la gestión de la red donde están los apartados que definen su propio uso ahí se encuentra la rama de la comunidad de internet que vamos a ocupar para este trabajo. (RFC, 2002)

El nodo de internet hay subcapas principales que se muestran en la Tabla 1-2:

Tabla 1-2: Nodo principal de Internet

NODOS	ESPECIFICACIÓN
Directory	Nodo de reserva para las discusiones futuras sobre la estructura de la ISO que se usa en el internet.
Mgmt	Nodo donde se identifica el objeto que está definida el documento en la junta de arquitectura de internet (IAB) Anexo B, en este lugar se encuentran almacenadas las MIBs estandarizadas.
Experimental	Este nodo es donde se encuentran la MIBs en están en modo de prueba.
Private	Este nodo se almacena MIBs definidas de forma unilateral es decir cada fabricante reconocido dispone de su propio espacio de almacenamiento de las MIBs de los dispositivos gestionados.

Fuente: RFC, 2002

Realizado por: Toapanta, Ángel, 2023

2.4.4 Sintaxis MIB

Abstract Syntax Notation One (ASN.1)

Es una norma que esta estandarizada muy flexible que proporciona un conjunto de normas, tipos constructores, para definir una estructura de codificación, decodificación y transmisión de datos de forma independientes del dispositivo gestionado y sus formas de representación interna es decir que este protocolo va a servir para definir la forma en que los datos del dispositivo gestionado van hacer almacenados en los nodos. Este protocolo se usa de forma restringida para mantener la simplicidad de los agentes. Cabe mencionar que fue desarrollada por la capa de representación del modelo OSI que esta notación proporciona un nivel de abstracción datos similar a los lenguajes de alto nivel.

Los tipos de datos ASN.1 se divide en tres partes que son:

A) Tipo primitivo

Estos datos son escalares, se conoce también como registros escalares, almacenan un solo valor como una cadena de texto o un entero. En la Tabla 2-2 se describen los más importantes. (Completo, 2019)

Tabla 2-2: Tipos de datos primitivos escalares

TIPO	CARACTERÍSTICAS
INTEGER	Se utiliza para la representación de números enteros.
OCTET STRING	Almacena una secuencia de bytes. De este tipo de deriva. • DisplayString se usa para cadenas de caracteres ASCII • OctetBitString se usa para cadenas de bits mayores de 32 • PhysAddress se usa para representar direcciones del nivel de enlace
OBJECT IDENTIFIER	Se utiliza para la representación de los identificadores de los objetos.
BOOLEAN	Se utiliza para los valores que solo pueden ser verdaderos o falso.
NULL	Se utiliza para la representación de la ausencia de valor.

Fuente: Completo, 2019

Realizado por: Toapanta, Ángel, 2023

B) Tipo constructores

Esta clase datos son registros vectoriales, que se utiliza para definir arrays y tablas, construidos a partir de otros tipos primitivos o compuestos. Los más importantes están en la Tabla 3-2. (Completo, 2019)

Tabla 3-2: Tipos de datos constructores

TIPO	CARACTERÍSTICA
SEQUENCE	Se utiliza para el almacenamiento de una fila de una tabla de forma ordenada con datos diferentes, se construye por datos primitivos.
SEQUENCE OF	Es una lista ordenada de varias filas iguales. Sirve para generar una tabla que contenga todas las filas. Se construyen con tipos compuestos.
SET	Es equivalente a SEQUENCE pero los datos no están ordenados, cabe mencionar que los datos que componen a las listas deben ser diferentes.
SET OF	Equivalente a SEQUENCE OF pero los datos no están ordenados.
CHOICE	Es el dato que se debe escoger de una lista predefinida.

Fuente: Completo, 2019

Realizado por: Toapanta, Ángel, 2023

C) Tipos Definidos

Son tipos derivados de los anteriores primitivos y compuestos con la particularidad de tener un nombre más descriptivo, se usa para distinguir los tipos datos dentro de la aplicación. Los importantes están detallados en la Tabla 4-2. (Completo, 2019)

Tabla 4-2: Tipos de datos definidos

TIPO	CARACTERÍSTICA
IpAddress	Almacena una dirección IP.
Counter	Contador que incrementa hasta un valor máximo (2^{32-1}) y vuelve a cero, solo puede tomar números enteros positivos.
Gauge	Es un indicador de nivel, el valor puede aumentar o decremento, está definido como un entero de 32 bits.
Time Ticks	Tipos de datos que se usan para medir tiempo transcurrido de eventos temporales en centésimas de segundo.
Opaque	Datos arbitrarios codificados. Representa un Octect String.
NetworkAddress	Representa una dirección de la red, con alguna familia de protocolos.

Fuente: Completo, 2019

Realizado por: Toapanta, Ángel, 2023

2.4.5 Tipos MIB

En la gestión de red en internet las bases de información de gestión (MIB) podemos subdividir en tres grupos que son:

a) Estándares:

MIB-I y MIB-II

b) Experimentales:

Que están en fase de desarrollo.

c) Privadas:

Es la información que incorpora los fabricantes de los equipos.

2.4.5.1 Bases de información de gestión I (MIB I)

Este tipo de base de datos fue la primera en normalizarse y estandarizarse, que estaba compuesta con objetos de la torre de protocolos TCP/IP. Los grupos que la conforman esta en la Tabla 5-2. (CYPRESS, 2010)

Tabla 5-2: Grupos de la base de información de gestión MIB I

GRUPO	NÚMERO	FINALIDAD
System	3	El propio sistema.
Interfaces	22	Interfaces de red.
At (Adress translation)	3	Correspondencia de dirección IP
IP	33	Protocolo Internet
ICMP	26	Protocolo de mensajes de control intenet.
TCP	17	Protocolo de control de transmisión.
UDP	4	Protocolo de datagrama de usuario
EGP	6	Protocolo de Gateway exterior.
	114	

Fuente: UJAEN, 2020

Realizado por: Toapanta, Ángel, 2023

2.4.5.2 Bases de información de gestión II (MIB II)

La MIB- II es la base de gestión común para los equipos de internet, tiene modificaciones respecto a la anterior MIB-I con la aparición de SNMPv2 y SNMPv3, nuevo grupo para cada tipo de interfaz, que se apoya en el modelo de información estructurado para definir las bases de MIB, indicar además los objetos que se puedan usar y define el uso de ASN.1. [9]

El detalle del grupo con las modificaciones se observa en la Tabla 6-2.

Tabla 6-2: Grupos de la base de información de gestión MIB II

GRUPO	NÚMERO	OBSERVACIONES
System	7	Antes eran 3
Interfaces	23	Antes eran 22
At (Adress translation)	3	Sin cambios
IP	38	Antes eran 33
ICMP	26	Sin cambios
TCP	19	Antes eran 17
UDP	7	Nueva tabla
EGP	18	Se expansión de tabla
Transmisión	0	Nuevo
SNMP	30	Nuevo

Fuente: UJAEN, 2020

Realizado por: Toapanta, Ángel, 2023

2.4.5.3 MIB experimentales

Estas bases de datos están en desarrollo por grupos de trabajos organizados de internet. Actualmente existen MIB que son:

a. IEEE 802.4 Token Bus (RFC 1230).
b. IEEE 802.5 Token Ring (RFC 1231).
c. IEEE 802.3 Repeater Devices (RFC 1368).
d. Ethernet (RFC 1398). (ya estándar).
e. FDDI (RFC 1285).
f. RMON (RFC 1271).
g. Bridges (RFC 1286).

2.4.5.4 MIBs privadas

Son bases de datos con productos específicos que añaden funciones de MIB estandarizadas, fueron desarrollados por los propios fabricantes de dispositivos encargados de dar comunicación en la red y la hacen públicas a través de internet.

- Cabletron.
- Synoptics.
- Proteon.
- ATT.
- Cisco.

2.4.6 Descripción e identificación de los objetos MIB-II

Para la MIB-II se definieron anteriormente 10 grupos con funciones específicas que son: (RFC, 2002)

2.4.6.1 Grupo System

El grupo provee información de manera general el funcionamiento del sistema gestionado, tiene 7 objetos escalares que se detallan en la Tabla 7-2.

Tabla 7-2: Detalles de los objetos del Grupos System MIB II

NOMBRE	VALOR	DESCRIPCIÓN
Sysdescr	1	Descripción de la entidad hardware.
SysObjectID	2	Identificación del sistema Operativo
SysUptime	3	Tiempo transcurrido desde que fue reiniciado el dispositivo.
SysContact	4	Nombre del contacto de la persona que está a cargo el nodo de gestión.
Sysname	5	Nombre del dispositivo gestionado
SysLocation	6	Locación física del nodo de gestión.
SysServices	7	Numero entero 0 – 127 que indica de los servicios que ofrece el dispositivo

Fuente: RFC, 2002

Realizado por: Toapanta, Ángel, 2023

2.4.6.2 Grupo Interfaces

El grupo va a contener información sobre las interfaces físicas del dispositivo gestionado, este grupo es obligatorio la implementación ya que puede dar información de fallos sobre uptime y downtime (up (1), down (2), testing (3)). (RFC, 2002)

El detalle de los objetos está en la Tabla 8-2.

Tabla 8-2: Detalles de los objetos del Grupos interface MIB II

NOMBRE	VALOR	DESCRIPCIÓN
IfIndex	1	Detalla número de una interfaz
IfDescr	2	Describe una interfaz
ItType	3	Describe el tipo de interfaz
IfMTU	4	Máximo de octetos en un Datagrama
IfSpeed	5	Ancho de banda en bps
IfPhysAddress	6	Dirección física
IfAdminStatus	7	Detalle del cambio del estado de la interfaz
IfOperStatus	8	Detalle del estado actual de la interfaz
IfLastChange	9	El valor de Sysuptime sobre la interfaz
IfInOctects	10	Octetos recibidos en su totalidad en una interfaz
IfInUcastPkts	11	Número de paquetes unicast de subred de entrada
IflnNucastPkts	12	Número de paquetes no unicast de subred de entrada
IfInDiscard	13	Paquetes entrantes descartados
IfInErrors	14	Paquetes descartados por error en la entrada
IfInUnKnownProtocols	15	Paquetes con error de protocolo en la entrada
IfOutOctets	16	Total de octetos transmitidos por una interfaz
IfOutUcastPkts	17	Numero de paquetes unicast de subred de salida
IfOutNUcastPkts	18	Número de paquetes no unicast de subred de salida
IfOutDiscard	19	Número de paquetes de salida descartados
IfOutErrors	20	Paquetes descartados por error en la salida
IfOutQlen	21	Longitud de la cola de paquetes de salida

Fuente: RFC, 2002

Realizado por: Toapanta, Ángel, 2023

2.4.6.3 Grupo At

El grupo address translation, hace un mapeo de las direcciones de la red a direcciones físicas, es decir de la dirección IP a direcciones físicas MAC. Este grupo está en el estado deprecated y se mantiene por la compatibilidad de MIB-I hasta la MIB-II. (RFC 1156, 1990)

Tabla 9-2: Detalles de los objetos del Grupos At MIB II

NOMBRE	VALOR	DESCRIPCIÓN
AtIfIndex	1	Indica la interfaz a la fila que hace referencia.
AtPhysAddress	2	Dirección física del medio del mapeo
AtNetAddress	3	Dirección de red del mapeo

Fuente: RFC 1156, 1990

Realizado por: Toapanta, Ángel, 2023

2.4.6.4 Grupo IP

Encargado de la información más relevante de las operaciones e implementaciones del protocolo IP de cada nodo que se esté gestionando, lleva un registro de los aspectos de IP. No todos los objetos son relevantes para el sistema por tal razón llevan un valor nulo, este grupo cuenta con 24 objetos escalares que son utilices para el gestiona miento de la red (monitoreo). (RFC 1156, 1990)

Tabla 10-2: Detalles de los objetos del Grupos IP MIB II

NOMBRE	VALOR	DESCRIPCIÓN
ipForwarding	1	Indica si la entidad está actuando como enrutador IP.
ipDefaultTTL	2	Número predeterminado del encabezado IP de los datagramas.
ipInReceives	3	Número total de datagramas recibidos en la interfaz de entrada.
ipInHdrErrs	4	Número de datagramas descartados en la entrada por errores en su cabecera IP.
ipInAddrErrors	5	Número de datagramas descartados en la entrada por errores en su cabecera no era una dirección valida.
ipForwDatagrams	6	Número de datagramas de entrada para el cual la entidad no era su destino IP final.
ipInUnknownProtos	7	Número de datagramas direccionados localmente recibidos con éxito.
ipInDiscards	8	Número de datagramas de entrada sin problemas
ipInDelivers	9	Número de datagramas de entrada entregados
ipOutRequests	10	Número de datagramas IP de solicitudes de transmisión.
ipOutDiscards	11	Número de datagramas IP de salida sin problemas.
ipOutNoRoutes	12	Número de datagramas IP descartados por no encontrar su destino para la transmisión.
ipReasmTimeout	13	Número máximo de segundos que se retiene los fragmentos.
ipReasmReqds	14	Número de fragmento de IP recibidos.
ipReasmOKs	15	Número de fragmento de IP reensamblados.
ipRsasmFails	16	Número de fallas detectadas por el algoritmo.
ipFragOKs	17	Número de datagramas IP que se han fragmentado.
ipFragFails	18	Número de datagramas IP que se han descartado.
ipFragCreates	19	Número de datagramas IP que se han creado.
ipAddrTable	20	Tabla de información de direccionamiento
ipRoutingTable	21	Tabla de enrutamiento IP
ipNetToMediaTable	22	Tabla de traducción de direcciones IP
ipRoutingDiscards	23	Número de entradas de enrutamiento
ipForward	24	Visualizador de rutas IP múltiples CIDR.

Fuente: RFC 1156, 1990

Realizado por: Toapanta, Ángel, 2023

2.4.6.5 Grupo ICMP

Este grupo integra los protocolos TCP/IP, por lo tanto todos los sistemas IP deben implementar ICMP. Provee información de los problemas en el entorno de las comunicaciones en el nodo que se está gestionando, es decir lleva estadísticas del tráfico ICMP. En este grupo consta de 26 objetos que contabilizan los mensajes ICMP enviados y recibidos, se detallan en la Tabla 11-2.

Tabla 11-2: Detalles de los objetos del Grupos ICMP MIB II

NOMBRE	VALOR	DESCRIPCIÓN
IcmpInMsgs	1	Mensajes recibidos totales
IcmpInErrors	2	Mensajes recibidos con errores
IcmpInDestUnrecheable	3	Mensajes recibidos con destino inalcanzable.
IcmpInTimeExcds	4	Mensajes recibidos con tiempo extendido.
IcmpInParmProbs	5	Mensajes recibidos con problemas de parámetros icmp.
IcmpInSrcQuenchs	6	Mensajes recibidos de fuentes apagadas
IcmpInRedirects	7	Mensajes recibidos redireccionados.
IcmpInEchos	8	Mensajes icmp Echo recibidos.
IcmpInEchosRep	9	Mensajes recibidos con respuesta de eco.
IcmpInTimestamps	10	Mensajes recibidos de marcas de tiempo (solicitudes)
IcmpInTimestampReps	11	Mensajes recibidos de respuestas de marcas de tiempo
IcmpInAddrMasks	12	Mensajes recibidos de solicitud de mascara de direccion
IcmpInAddrMaskResp	13	Mensajes recibidos de respuestas de mascara de subred
IcmpOutMsg	14	Mensajes enviados incluyendo con los de error
IcmpOutErrors	15	Mensajes no enviados por problemas icmp
IcmpOutDestUnrecheable	16	Mensajes enviados con destino inalcanzable.
IcmpOutTimeExcs	17	Mensajes enviados con tiempo extendido.
IcmpOutParmProbs	18	Mensajes enviados con problemas de parámetros icmp.
IcmpOutSrcQuenchs	19	Mensajes enviados con fuente apagada
IcmpOutRedirects	20	Mensajes enviados redireccionados.
IcmpOutEchos	21	Mensajes icmp Echo enviados.
IcmpOutEchosResp	22	Mensajes enviados con respuesta de eco
IcmpOutTimestamp	23	Mensajes enviados con solicitud de marcas de tiempo
IcmpOutTimestampResp	24	Mensajes enviados con respuestas de marcas de Tiempo.
IcmpOutAddrsMasks	25	Mensajes enviados con solicitud de mascara de subred
IcmpOutAddrsMaskResp	26	Mensajes enviados con respuesta de mascara de subred

Fuente: RFC 1156, 1990

Realizado por: Toapanta, Ángel, 2023

2.4.6.6 Grupo TCP

Este grupo provee información sobre la operación e implementación del protocolo TCP del nodo donde se está gestionando, se conforma de objetos escalares donde se detalla los segmentos recibidos, enviados, segmentos erróneos recibidos, retransmitidos, número máximo de conexiones TCP que soporta el dispositivo, máximo timeout de retransmisión, etc. Los objetos se detallan en la Tabla 12-2. (RFC 1156, 1990)

Tabla 12-2: Detalles de los objetos del Grupos TCP MIB II

NOMBRE	VALOR	DESCRIPCIÓN
TcpRtoAlgorithm	1	Algoritmo utilizado para la retransmisión.
TcpRtoMin	2	Tiempo de espera de retransmisión minimo.
TcpRtoMax	3	Tiempo de espera de retransmisión máximo.
TcpMAxconn	4	Total de conexiones TCP que soporta.
TCpActiveOpens	5	Cambio de estadso a SYN-SENT del estado closed
TcpPassivesOpens	6	Cambio de estado a SYN-RCVD del estado Listen
TcpAttemptFAil	7	Cambio de estado closed del estado SYN-SENT.
TcpEstabResets	8	Cambio de estado closed al estado established.
TcpCurrEstab	9	Número de conexiones con el estado established o closed
TcpInSegs	10	Número de segmentos recibidos, incluyendo con error
TcpOutSegs	11	Números Segmentos enviados, incluyendo con error
TcpRetransSegs	12	Número de segmentos retransmitidos.
TcpConnTable	13	Tabla que contiene información específica Tcp.
TcpConnState	1	Estado de la conexión Tcp
TcpConnLocalAddress	2	Dirección IP local para esta conexión Tcp
TcpConnLocalPort	3	Número de puerto para esta conexión Tcp
TcpConnRmAddress	4	Dirección IP remota para esta conexión Tcp
TcpConnremPort	5	Número de puerto Remoto para conexión Tcp

Fuente: RFC 1156, 1990

Realizado por: Toapanta, Ángel, 2023

2.4.6.7 Grupo UDP

Este grupo provee información sobre la operación e implementación del protocolo UDP del nodo donde se está gestionando, controla las estadísticas de los datagramas enviados y recibidos y una tabla udpTable. Los objetos se detallan en la Tabla 13-2. (RFC 1156, 1990)

Tabla 13-2: Detalles de los objetos del Grupos UDP MIB II

NOMBRE	VALOR	DESCRIPCIÓN
UdpInDatagrams	1	Datagramas enviados a los usuarios Udp
UdpNoPorts	2	Datagramas recibidos a puertos desconocidos
UdpInErrors	3	Datagramas no enviados por error de los formatos.
UdpOutDatagrams	4	Datagramas enviados desde la entidad
Udptable	5	Tabla con contenido de información Udp
UdpLocalAddress	1	Dirección IP para esta aplicación Udp
UdpLocalPort	2	Número de puerto local para esta aplicación UDP

Fuente: RFC 1156, 1990

Realizado por: Toapanta, Ángel, 2023

2.4.6.8 Grupo EGP

Este grupo va a tener información sobre la operación e implementación del protocolo External Gateway Protocol EGP en el nodo que está gestionado, almacena información sobre los mensajes EGP enviaos y recibidos. Está formado por 5 objetos escalares que se detalla en la Tabla 14-2. (RFC 1156, 1990)

Tabla 14-2: Detalles de los objetos del Grupos EGP MIB II

NOMBRE	VALOR	DESCRIPCIÓN
egpInMsgs	1	Mensajes EGP recibidos sin error
egpInErrors	2	Mensajes EGP recibidos con error
egpOutMsgs	3	Mensajes EGP generados localmente
egpOutErrors	4	Mensajes EGP no enviados por falta de recursos.

Fuente: RFC 1156, 1990

Realizado por: Toapanta, Ángel, 2023

2.4.6.9 Grupo transmisión

Este grupo provee detalles sobre el medio de transmisión subyacente para cada interfaz, no es un grupo sino se define como una jerarquía de MIB-II, pero no ha sido implementada.

2.4.6.10 Grupo SNMP

Este grupo almacena información importante del rendimiento de la implementación y operación del protocolo SNMP en el dispositivo gestionado para el control de paquetes enviados y recibidos. Podemos observar en la Tabla 15-2. (RFC, 2002)

Tabla 15-2: Detalles de los objetos del Grupos SNMP MIB II

NOMBRE	VALOR	DESCRIPCIÓN
SnmpInpKTS	1	Mensajes recibidos del servicio de transporte
SnmpInOutPkts	2	Mensajes pasados al servicio de transporte
SnmpInBadVersions	3	Mensajes recibidos error en la versión.
SnmpInBadConmmunityNames	4	Mensajes basados en la comunidad.
SnmpInBadConmmunityUses	5	Mensajes basados con errores en la comunidad
SnmpInASNParseErrs	6	Mensajes con errores ASN.1 o VER.
SnmpOutPkts	7	Mensajes que pasaron al servicio de transporte
SnmpInTooBigs	8	Msm PDU entrantes con errores de tipoTooBlg
SnmpInNoSuchNames	9	PDU entrante con errores de tipo NosuchName
SnmpInBadValues	10	Msm PDU entrante con errores de tipo BadValue
SnmpInReadOnly	11	Msm PDU entrante con errores de tipo ReadOnly
SnmpInGenErrs	12	Msm PDU entrante con errores de tipo GenErrs
SnmpInTotalReqVars	13	Msm como resultado de solicitudes.
SnmpInTotalSetVars	14	Objetos alterados como resultado PDU
SnmpInGetRequest	15	Get-request aceptados y procesados por snmp
SnmpInGetNexts	16	Get-next aceptados y procesados por snmp
snmpInSetRequests	17	Msm de solicitudes de configuración recibidos.
SnmplnGetResponse	18	Get-Response aceptados y procesados por snmp
SnmplnTraps	19	Traps procesados y aceptados por SNMP
SnmpOutTooBig	20	Msm PDUs generados con error Too-Big
SnmpOutNosuchNames	21	Msm PDU generado con error tipo suchname
snmpOutBadValues	22	Msm PDU enviados con errores de tipo BadValue
snmpOutGenErrs	24	Msm PDU enviados con errores de tipo GenErrs
snmpOutGetRequests	25	Get-request aceptados y procesados por snmp
snmpOutGetNexts	26	Get-next aceptados y procesados por snmp
snmpOutSetRequests	27	Msm de solicitudes de configuración enviados.
snmpOutGetResponses	28	Get-Response aceptados y procesados por snmp
snmpOutTraps	29	Traps procesados y aceptados por SNMP

Fuente: RFC, 2002

Realizado por: Toapanta, Ángel, 2023

2.5 The Simple Network Management Protocol (SNMP) versión 3

SNMPv3 nace de la evolución de SNMP en el año 1998, que refuerza las prestaciones de seguridad como autentificación, privacidad y control de accesos para un manejo mayor en modulación y la posibilidad de configuración remota. No hay que olvidar que SNMPv3 no trata de reemplazar a las versiones anteriores sino que tiene mejores prestaciones como una serie de capacidades adicionales de seguridad y administración.

SNMPv3 proporciona el acceso seguro a los dispositivos gestionados por las prestaciones de seguridad como la autentificación y encriptación de los paquetes a través de la red, es decir cuando los paquetes sean transportados no sufra en el camino ninguna alteración. (Omalie, Vicksai y Wilson, 2018)

2.5.1 Modelos y niveles de seguridad

Los modelos y niveles que tiene toda la estructura de SNMP se detalla en la Tabla 16-2.

Tabla 16-2: Descripción de las versiones, modelos y niveles de SNMPv3

VERSIONES	NIVEL	AUTENTIFICACIÓN	ENCRIPTACIÓN
V1	noAuthNopriv	Comunidad	No
V2	noAuthNopriv	Comunidad	No
V3	noAuthNopriv	usuario	No
V3	AuthNopriv	MD5 o SHA	Si
V3	AuthPriv	MD5 o SHA	Si

Fuente: Completo, 2019

Realizado por: Toapanta, Ángel, 2023

2.5.2 Características SNMPv3 en seguridad

- Seguridad del mensaje: el mensaje no sufra ninguna alteración mientras este en tránsito.
- Autenticación: el mensaje tenga las llaves de encriptación para verificar que provenga de una fuente valida.
- Encriptado: encripta un paquete con diferentes técnicas para evitar que el contenido sea visto por una fuente no autorizada.

2.5.3 Arquitectura SNMPv3

La arquitectura de SNMP viene dado principalmente de entidades que están formadas por un único motor SNMP y una o varias aplicaciones, cabe mencionar que el motor SNMP como las aplicaciones están conformadas por modelos.

Los subsistemas interactúan o se comunican entre sí a través de primitivas y parámetros abstractos con el objetivo de proveer un servicio determinado. Las entidades pueden actuar como agente, gestor o una combinación entre los dos dependiendo del tipo de módulos. (De Redfort, 2008)

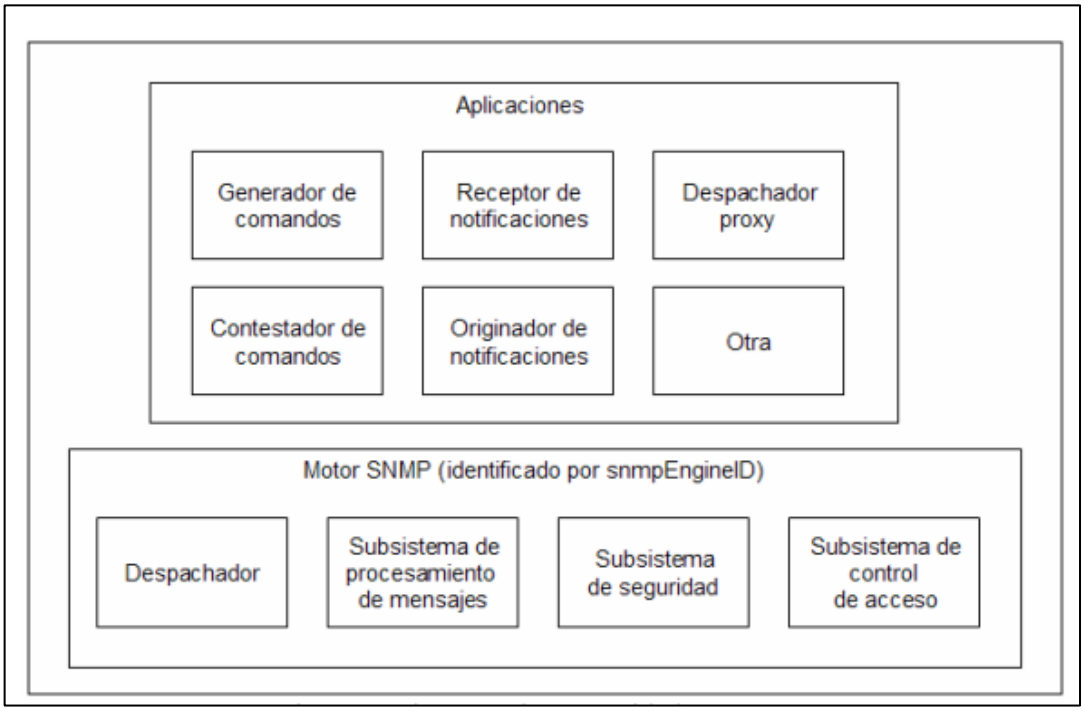


Ilustración 4-2: Diagrama de una entidad SNMP

Fuente: Tinajero, Baldomero, 2014

En la Ilustración 4-2 muestra la estructura en un diagrama de bloques que tiene SNMPv3, que es un conjunto de módulos que interactúan entre sí. Cada entidad incluye un motor que implementa las funciones de recibir y enviar mensajes con el objetivo de autentificar y encriptar mensajes y controlar el acceso.

2.5.3.1 Descripción del motor SNMP

Esta entidad esta es encargada en implementar funciones que son: (De Redfort, 2008)

- enviar/recibir
- autenticar
- cifrar/descifrar los mensajes SNMP.
- Control de Acceso a los objetos administrados.

2.5.3.2 Despachador

La función de este módulo son los siguientes:

- Recibe y envía mensajes SNMP de la red.
- Maneja diferentes mensajes de las diferentes versiones de SNMP.
- Se encarga de enviar las PDU que provienen de las aplicaciones hacia la entidad remota y viceversa, para un procesamiento adecuado.
- Interactúa con un subsistema de procesamiento de mensajes para determinar la versión para extraer el mensaje entrante y formar el mensaje de salida.

2.5.3.3 Subsistema de proceso de mensajes

- Se comunica con el despachador para los manejos de los mensajes concretos con una versión específica.
- Prepara mensajes para enviar y extraer los datos del mensaje recibido.
- Puede estar conformado por uno o varios modelos de proceso de mensajes.

2.5.3.4 Subsistema de seguridad

- Proporciona los servicios de seguridad de autentificación y encriptación para los mensajes que lo necesitan.
- Contiene múltiples modelos de seguridad (USM para SNMPv3 y nombres de comunidades para SNMP v1 o v2)

2.5.3.5 Subsistema de control de acceso

- Administra niveles de accesos para los objetos gestionados.
- Implementa el modelo de control de accesos basado en vistas (VACM).

2.5.4 Aplicaciones SNMP

Son subsistemas que usas los servicios de un motor SNMP para llevar a ejecución operaciones específicas para el procesamiento de la información de control. No existen restricciones en aplicaciones que se pueda tener en la entidad.

2.5.4.1 Generadores de comandos

- Genera específicamente PDUs por solicitudes de tipo de lectura GetRequest, GetNextRequest, GetBulkRequest) o escritura (SetRequest) y procesa respuesta (GetResponse).
- Monitorea y modifica los datos de administradores remotos de las entidades.

2.5.4.2 Respondedor de comandos

- Recibe PDUs GetRequest, GetNextRequest, GetBulkRequest o SetRequest, para conformar mensajes de respuesta GetResponse a las solicitudes de una NMS.
- Es encargada de ejecutar el comando.
- Permite el acceso a los datos informativos.

2.5.4.3 Receptor de Notificaciones

- Esta continuamente monitoreando el sistema por fallas o eventos particulares que genera una operación de Trap.
- Monitorea por el puerto 162.
- Genera la respuesta GetResponse al recibir un InformRequest generada por una entidad gestora.

2.5.4.4 Originador de notificaciones

- Genera notificaciones por la constante monitorización del sistema en caso de detectar alguna irregularidad del sistema.
- Genera las Traps para eventos suscriptos donde fueron programados.
- Consta con parámetros de seguridad, versiones SNMP y destino del mensaje.

2.5.4.5 Reenviador Proxy

- Son funcionalidad es de direccionar los mensajes a través de las entidades
- La implementación de esta aplicación es opcional.

2.5.5 Estructura del Gestor y del Agente

2.5.5.1 Gestor SNMP

Debe contener dos módulos, el primer debe contener una o varias aplicaciones por ejemplo: originador de notificaciones, receptor de notificaciones y generador de comandos junto a un motor de SNMP , se llama Gestor de SNMP, el segundo módulo debe contener un motor SNMP, donde se recibe los mensajes de la capa de transporte UDP, para realizar los procedimientos de autentificación y descifrado con el objetivo de extraer las PDUs que luego serán entregadas a las aplicaciones pertinentes es decir los mensajes entraran primero al motor de SNMP, se procesan con los protocolos de seguridad para luego entregarles al módulos de aplicaciones.

Para visualizar mejor en la Ilustración 5-2 se muestra el camino como recorre el mensaje.

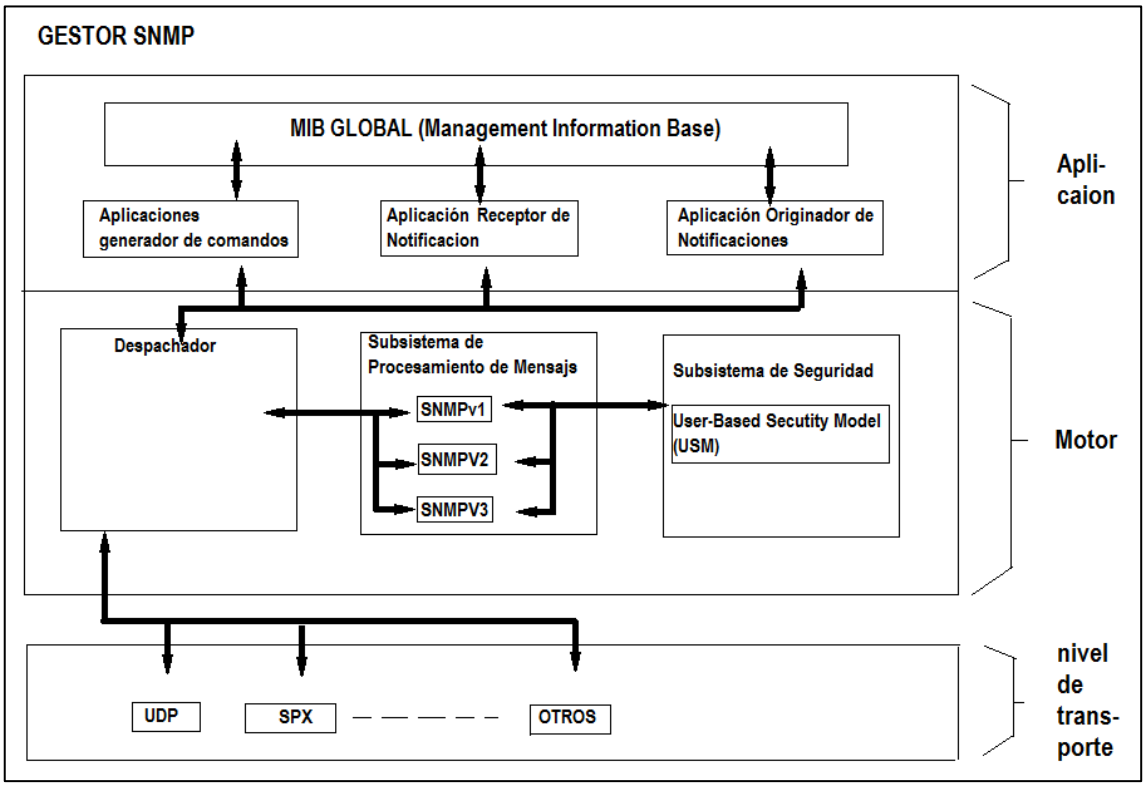


Ilustración 5-2: Modelo de referencia de administrador SNMP

Fuente: Rosales Briceño, Cariuly, 2012

2.5.5.2 Agente SNMP

Esta entidad contiene nace del módulo de aplicaciones que puede tener una o varias, pueden ser la contestadoras de comandos, originadora de notificaciones y un reenviador Proxy, se llama agente SNMP. El segundo módulo contiene un motor SNMP de un agente contiene un subsistema de control de acceso, subsistemas de seguridad para la encriptación de las PDUs para luego ser enviadas a la capa de transporte UDP. En el diagrama de bloque de la Ilustración 6-2 se muestra el agente tradicional.

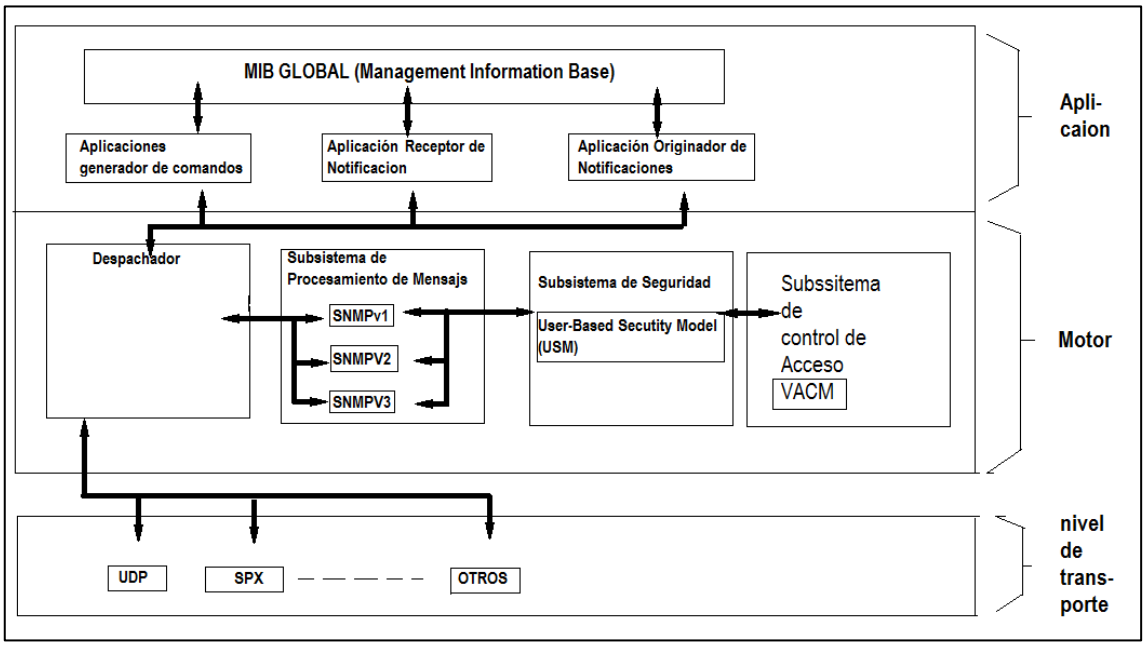


Ilustración 6-2: Modelo de referencia de Agente SNMP

Fuente: Watson, Joseph, 2008

2.5.5.3 Formato mensaje SNMPv3

El formato de mensaje se ha definido como las versiones anteriores, que va hacer diferente porque va a introducir parámetros de autentificación y encriptación. Cada mensaje va tener un encabezado y un PDU. Se puede observar mejor en la Ilustración 7-2.

El formato se puede dividir en tres partes:

a. Parte superior considerada como la cabecera del mensaje
b. En la mitad parámetros de seguridad.
c. Parte inferior como datos propiamente dichos.

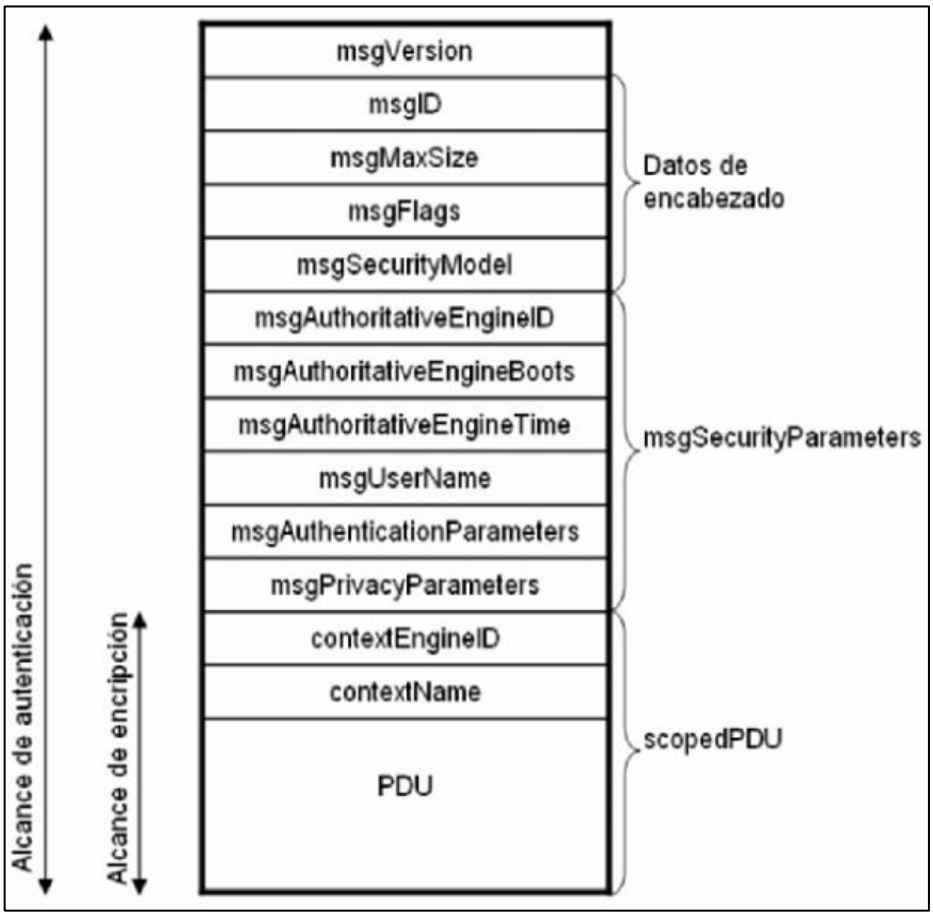


Ilustración 7-2: Formato del mensaje SNMP v3

Fuente: Muñoz Mesa, José Luis, 2009

2.5.5.4 Detalle de la cabecera SNMPv3 del mensaje

- msgVersion.- Identifica la versión SNMP que se utilizó. Es seteado con 3 por la versión (SNMPv3)
- msgID.- Identifica la relación entre los mensajes de solicitudes con los de respuesta entre dos entidades.
- msgMaxSize.- Tamaño el máximo del mensaje que puede transmitir y pueda ser soportado por el remitente del mensaje, cuando genera un mensaje SNMP este campo es provisto por el motor que genera el mensaje y en la parte de recepción el motor SNMP se utiliza para determinar el mensaje máximo que puede acomodar.
- msgFlags.- este campo contiene en el mensaje (un octeto) varios bits que controla el procesamiento del mensaje, los tres últimos bits que se conocen como bits significativos son usados para la identificación de las tres banderas como muestra la Ilustración 8-2.

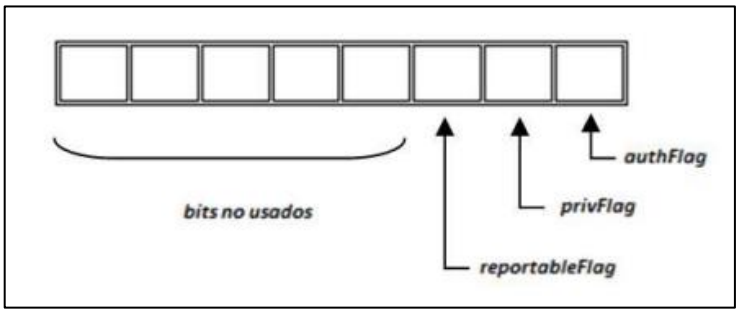


Ilustración 8-2: Campos de msgFlag del mensaje SNMP v3

Fuente: Calderón, Luis, 2006

- La bandera reportableFlag.- existen dos estados cuando esta seteada en 1 se manda una PDU report a la entidad emisora del mensaje y seteada en 0 no debe mandar PDU.
- authFlag y privFlag.- estas banderas sirven esencialmente para indicar el nivel de seguridad aplicado al mensaje. Cuando la bandera authFlag esta seteada en 1, deber estar autentificado el mensaje y cuando privFlag esta seteada en 1 el mensaje debe estar encriptado por ende debe también estar seteada la bandera authFlag.
    - Combinación de los estados de las banderas:

Tabla 17-2: Combinación de banderas auth y pri

NIVEL DE SEGURIDAD	AUTHFLAG	PRIVFLAG
noAuthNoPriv	0	0
Combinación inválida	0	1
authNoPriv	1	0
authPriv	1	1

Realizado por: Toapanta, Ángel, 2023

- mgsSecurityModel.- identifica el modelo de seguridad que uso el remitente del mensaje para así procesar el mensaje en el receptor. Puede tomar los valores de SNMPv1 (1), SNMPv2 (2) y USM de SNMPv3 (3).

2.5.5.5 Parámetros de seguridad del mensaje SNMPv3

- msgAuthoritativeEngineID.- Es un identificador que es asignado a un motor autorizado de un entidad SNMP ya sea esta un agente o gestor de la red con el objetivo de responder las peticiones o que reciba las notificaciones. Que va a servir como referencia para el motor autorizado AutoritatveEngine.

- msgAuthoritativeEngineBoots.- detalla el número de ocasiones que el motor SNMP se reinician desde su configuración original.
- msgAutoritativeEngineTime.- representa el tiempo en segundos cuando el msgAuthoritativeEngineBoots se inició por última vez.
- msgUserName.- va especificar el nombre del principal de la entidad que intervienen en el intercambio de mensajes.
- msgAuthenticationParameters.- va estar definido por los protocolos de autentificación como el uso del algoritmo HMAC, caso contrario va a ser nulo.
- msgPrivacyParameters.- va estar definido por los protocolos de cifrado como es el algoritmo DES. (Omalie, Vicksai en Wilson, 2018)

2.5.5.6 Datos del mensaje SNMPv3

- ContextEngineID.- Identifica únicamente una entidad SNMP, para los mensajes provenientes y determinar a qué aplicación del scopedPDU va a ser enviado, es decir es el identificador de una entidad SNMP asociado con un contexto.
- ContextName.- es el nombre que es asigna a un contexto que tiene relación con la información de administración contenida en la PDU del mensaje.
- PDU.- datos (OID o instancias) que están asociadas a una petición o respuesta SNMP.

2.5.5.7 Seguridad de SNMPv3

En SNMPv3 el mecanismo de seguridad está formado por niveles y modelos, siendo la accesibilidad unos del parámetro importantes en tener en cuenta ya que se le da a un usuario dentro del modelo de seguridad, también, las estrategias de autentificación que se les da a los usuarios o miembros de la organización.

Un logro con este protocolo es que tiene mejoras respectos a sus antecesoras que incluyen varios modelos incluyendo subsistemas de seguridad que pueden obstaculizar amenazas cibernéticas como modificación de los mensajes de gestión, contraseñas vulneradas y el descubrimiento de los mensajes no autorizados, pero todavía tiene una falencias que son a los ataque DoS.

SNMPv3 con los logros de encriptación de mensajes y autentificación de los mismos, va a incrementar la seguridad en los entornos gestión durante el flujo de datos de la red y reducir al máximo los riesgos de que la información de gestión.

Se hace importante el uso de un modelo de seguridad basado en usuario (USM) y un control de acceso basado en vistas (VACM), los cuales tienen una buena combinación y aseguran el transito seguro de la información de gestión atreves de la red.

2.5.6 Modelo de seguridad basado en usuario (USM)

Se representa con las siglas (USM) es un subsistema de seguridad que proporciona a la entidad SNMPv3 los servicios de autentificación y privacidad.

- Un mayor porcentaje de seguridad para el monitoreo y la configuración de los dispositivos que están siendo gestionados.
- El cifrado es aplicado para los mensajes de configuración de los dispositivos.
- En el camino que recorre el mensaje se asegura que no sufra ninguna modificación por parte de los atacantes.
- Certifica el mensaje de donde fue enviado.

USM tiene en uso un mecanismo de usuario y contraseña que funciona conjuntamente con el grupo VACM que consiste en una serie de vistas configuradas con privilegios de acceso.

En el modelo USM contamos con tres módulos con funciones específicas que corresponde con la seguridad:

Tabla 18-2: Módulos del modelo USM

MÓDULOS DEL MODELO USM		
Módulo de autenticación: Este módulo tiene el objetivo de verificar si el mensaje que se recibe viene de la fuente que fue generada y que no haya sufrido ningún cambio en el camino, para que se establezca la comunicación las dos partes deben tener las llaves de autentificación.	**Módulo timelines**: Este módulo tiene el objetivo de proporcionar la protección contra el retraso y retransmisión de mensajes maliciosos. Para el control el agente administrador va a copiar los parámetros para sincronización (snmpEngineBoots y snmpEngineTime). Con estos parámetros tiene un estimado del tiempo que los mensajes llegan hacia el agente, si se retarda mucho el mensaje queda descartado, un mensaje dependiendo si existe una diferencia alrededor de 150 segundos, este tiempo estimado queda guardado en la memoria no volátil del agente.	**Módulo de privacidad**: Este módulo tiene el objetivo de proporcionar el cifrado y descifrado del contenido de un mensaje.

Realizado por: Toapanta, Ángel, 2023

2.5.6.1 Elementos necesarios del motor SNMP para USM

El motor SNMP va a tener tres elementos fundamentales para la implementación USM.

Tabla 19-2: Elementos de seguridad para el modelo USM

ELEMENTOS	DESCRIPCIÓN
snmpEngineID	Identifica de forma del motor SNMP dentro del dominio de gestión.
snmpEngineBoots	Consiste en un contador que lleva la suma del número de cuantas veces que el motor snmp ha sido reiniciado desde que se definió su snmEngineID.
snmpEngineTime	Es el número en segundos que han pasado desde la última reiniciación del motor.

Realizado por: Toapanta, Ángel, 2023

2.5.6.2 Motor SNMP autoritativo

En una transmisión de un mensaje, este proceso van involucrar dos entidades sea en el receptor o emisor deben tener designado un motor autoritativo que se encarga de gestionar la seguridad.
Hay unas reglas que se deben tomar en cuenta.

- Un mensaje SNMP que contiene un payload va a espera una respuesta (puede ser Get, GetNext o Set) el receptor de los mensajes es autoritativo.
- Un mensaje SNMP que contiene un payload el cual no se espera una respuesta (como un Trap, Response) entonces el remitente del mensaje es autoritativo.

Tareas fundamentales del motor autoritativo.

A. Claves localizadas: son claves que se crean para compartir un usuario con un motor SNMP determinado. Cabe destacar cuando un usuario utiliza las mismas claves para todos los motores, la clave seleccionada va hacer diferente y se llama clave localizada, para mejor entendimiento la clave original pasa por una serie de procesos como la función de hash y envolviendo el parámetro snmpEngineID del motor, que va dar un resultado, para que luego volver aplicar la función de hash y obtener la clave localizada que es diferente a la original para comunicarse con cada motor SNMP.
B. Guía temporal: al momento de enviar un mensaje el motor autoritativo añade integra una serie de marcadores con tiempos temporales con el objetivo que al ser analizadas por parte del receptor el motor de esa entidad determina que el mensaje este dentro de la ventana temporal correcta para que sea aceptado.

2.5.6.3 Descubrimiento de motores SNMP

Para tener una noción clara se debe requerir un proceso de descubrimiento para extraer la información de otros motores SNMP y así establecer la comunicación. Se necesita conocer primero el snmpEngineID, cuando el motor no es autoritativo, va a manda un mensaje de Request al motor que quiere conocer datos. La solicitud va contener en el campo securityLevel en noAuthnoPriv, el msgUserName con valor 1 y el msgAuthoritativeEngineID como 0. El motor autoritativo va a responder con un mensaje Report, con snmpEngineID en el campo 0.

En una comunicación debe ser autenticada, el motor SNMP no autoritativo debe establecer una etapa de sincronización con el motor autoritativo. Se lograrlo, cuando el motor no autoritativo manda un mensaje de Request, con msgAuthoritativeEngineID pero con el valor del snmpEngineID y msgAuthoritativeEngineBoots y msgAuthoritativeEngineTime con el valor de 0. La respuesta del mensaje va hacer Report del motor autoritativo, con los valores de 0 a snmpEngineBoots y snmpEngineTime. El motor no autoritativo puede crear y mantener una ventana temporal que permitirá la comunicación al motor autoritativo para validar los mensajes que lleguen al mismo.

2.5.7 Formato del bloque msgSecurityParameters

Como estamos hablando de la seguridad el bloque msgSecurityParameters del mensaje SNMPv3, está construido por varios campo está compuesto por los siguientes campos que se describe en la Tabla 20-2:

Tabla 20-2: Campos que contiene msgSecurityParameter

MSGSECURITYPARAMETERS	
CAMPOS	**DESCRIPCIÓN**
msgAuthoritativeEngineID	Es el snmpEngineID del motor SNMP autorizado
msgAuthoritativeEngineBoots	Es el snmpEngineBoots del motor SNMP autorizado.
msgAuthoritativeEngineTime	Es el snmpEngineTime del motor SNMP autorizado
msgUserName	Describe el usuario principal
msgAuthenticationParameters	Parámetros definidos por el protocolo de autenticación que se esta
msgPrivacyParameters	Parámetros definidos por el protocolo de privacidad que se está usando.

Realizado por: Toapanta, Ángel, 2023

2.5.7.1 Autenticación

Este paso se basa el trabajo de titulación ya que al momento de proteger la información con varios modelos de autentificación garantizamos la integridad de los datos para que en el camino no sea alterado o modificado y garanticemos que los mensajes recibidos sean del dispositivo que debe ser. La autenticación es cuando se usa criptografía que busca cifrar el mensaje del cual va a requerir de una clave inicial (authKey) que por seguridad se recomienda que sea de al menos de 8 caracteres y es administrada por el administrador, por el cual también va a brindar la autenticación a las entidades SNMP involucradas en el proceso de gestión con nombre de usuario (securityName).

El usuario local o remoto en el motor SNMP va almacenar una authkey. El usuario local va a tener permisos de operaciones de administrador de red mientras el usuario remoto va a tener permisos para comunicarse e intercambiar la información.

Los protocolos que se usan para autenticación y que son soportadas para SNMPv3:

- HMAC-MD5-96 y
- HMAC-SHA-96.

2.5.7.2 Protocolo HMAC-MD5-96

El protocolo va a trabajar utilizando el código de autentificación HMAC (Código de autenticación de mensajes basado en hash) y la función de hsh33 MD5.
HMAC es una construcción de un código para autenticar mensajes, en base del uso de una llave secreta y funciones hash. La llave secreta se usa para el cálculo y la verificación de los valores de autenticación de los mensajes. HMAC entre las dos entidades SNMP usan una misma llave con el objetivo de validar la información intercambiada entre ellas.

La función hash MD5 (Message Digest Algorithm v5) el proceso de autenticación de un mensaje saliente, comienza una llave se originan de la llave secreta authKey de 16 octetos es decir sirve para convertir un dato de longitud cualquiera a un dato de longitud pequeña fija de 128 bits (16 octetos).

2.5.7.3 Protocolo HMAC-SHA-96

Este protocolo tiene características parecidas al anterior con la diferencia de que usa funciones SHA-1 (Algoritmo de Hash Seguro) que es un algoritmo de autentificación con una longitud de 160 bits (20 bytes) que luego se trunca a 12 octetos.

SHA-1 es más lento, todo va a referir de la seguridad que van a implementar en la gestión de monitoreo, pero con un algoritmo más robusto podemos evitar ataques de fuerza bruta. Los dos algoritmos son no reversibles porque no es posible encontrar el mensaje original a partir del resumen y llave secreta.

2.5.7.4 Privacidad

Los protocolos usados por SNMPv3 para realizar cifrado del campo scopedPDU del mensaje son DES o AES para los cual usa llaves de 128 bits. El algoritmo DES tiene una clave un poco liviana que no es muy fuerte para el cifrado por lo cual ha sido reemplazado por AES que mantiene un algoritmo muy seguro y que ha resistido a los diferentes ataques.

El algoritmo de cifrado que requiere de una clave privada (privkey), el motor SNMP almacena para cada usuario (local o remoto) una privKey.

2.5.7.5 Protocolo DES

DES se describe (Data Encryption Standard - Cifrado Estándar de Datos) es un algoritmo de encriptación simétrico que usa la misma llave para:

- Encriptar
- Desencriptar.

El algoritmo va a generar una llave secreta de 16 bytes (128 bits). El modo CBC requiere de unos 8 bytes iniciales que se denomina vector de inicialización (IV), para comenzar a ejecutar el algoritmo de cifrado. Para la creación de la llave secreta y el vector de inicialización en el modelo USM se considera dos valores que ya fueron obtenidos (un valor secreto (privKey) y un valor timelines (snmpEngineBoots)) y el valor secreto se comparte tanto para un usuario (Principal) y un motor SNMP autorizado.

Los primeros 8 octetos (64 bits) de privKey se va a utilizan como llave secreta para DES, cabe mencionar que DES funciona con 56 bits para que no haya ningún error el bit menos significativo de cada octeto es ignorado. El vector de inicialización se genera partiendo:

- De la clave privKey se utilizan los últimos 8 bytes para usarlos como un pre-IV.
- Para que no se genere dos IV distintos para diferentes entradas de texto cifrados bajo la misma clave, se crea un octeto llamado salt value. Salt value se crea a con la concatenación de snmpEngineBoots y un valor entero de 64 bits que está dado por el protocolo de encriptación.
- En el algoritmo de encriptación se realiza una operación XOR bit a bit entre el pre-IV y el octeto salt value, el resultado es el vector de inicialización.
- El octeto salt value se coloca en el campo msgPrivacyParameters del mensaje SNMPv3.

2.5.7.6 Protocolo AES

AES se describe (Advanced Encryption Standard – Cifrado Estándar Avanzado) que es un algoritmo de encriptación robusto simétrico que fue diseñado para la resistencia mejorada contra ataques, fácil implementación, eficiencia y diseño escalable. En el modelo USM, AES se define bajo la norma RFC 3826 para su funcionamiento.

- El modo que se utiliza es CFM (Cipher Feedback Mode – Modo de Cifrado Retroalimentado) que soporta algoritmos con longitudes de llave de 128, 192 y 256 bits, pero la de 128 bits se utiliza para USM.
- Para la generación de las llaves secretas y el IV utilizan formas similares que DES.
- Para formar la llave secreta se toman los primeros 128 bits de clave privKey y para formar el vector de inicialización de 128 bits se realiza una concatenación de snmpEngineBoots, snmpEngineTime que pertenecen motor SNMP autorizado y de un entero local de 64 bits.
- El entero local es inicializado a un valor aleatorio al reiniciarse el motor SNMP. Este entero local es colocado en el campo msgPrivacyParameters.

2.5.7.7 Puntualidad (Timelines)

Protege contra la recepción de mensajes que lleguen tarde, el reenvío y redireccionamiento no autorizados de mensajes. Antes de usar este módulo Timelines es indispensable haber aplicado antes un servicio de autenticación al mensaje. Los mecanismos de puntualidad son:

- Administración de relojes autorizado.
- Los motores autorizados SNMP deben administrar los objetos snmpEngineBoots y snmpEngineTime, los cuales indican su tiempo local.

La gestión de los relojes consiste en:

- Cuando snmpEngineTime alcanza su máximo valor, se efectúa un incremento en el valor del snmpEngineBoots y comienza desde 0 nuevamente.
- Cuando el motor autorizado no logra identificar su último valor del snmpEngineBoots, lo setea al valor umbral, que es $(2^{31} - 1)$.
- Cuando snmpEngineBoots alcanza su máximo valor, el campo se bloquea y se produce un error de autenticación, por lo cual requiere una reconfiguración manual del sistema que consiste en cambiar el snmpEngineID o las claves de los protocolos de autenticación y privacidad de todos los usuarios conocidos por este motor.

Sincronización: Un motor no autorizado para que pueda sincronizarse con los motores autorizados, debe almacenar copias de las variables que pertenecen a cada motor autorizado como: snmpEngineBoots, snmpEngineTime y latestrecivedEngineTime. La variable latestReceivedEngineTime representa el valor más alto de msgAuthoritativeEngineTime del motor autorizado.

Un motor no autorizado para que reciba por primera vez las variables de sincronización se sigue un mecanismo de descubrimiento de motores autorizados. Para después de cada mensaje SNMP recibido, el motor no autorizado lee los valores y actualice las variables. Para la actualización de las variables se utiliza, previamente las comparaciones entre variables guardadas localmente (snmpEngineBoots, snmpEngineTime, y latestReceivedEngineTime) contra las variables recibidas en los mensajes SNMP (msgAuthoritativeEngineBoots, msgAuthoritativeEngineTime, y msgAuthoritativeengineTime), respectivamente, pero cuando el valor de la variable recibida es mayor o igual al almacenado, entonces se realiza la actualización; caso contrario no.

Verificación de puntualidad: la verificación de un mensaje se utiliza el concepto de ventana de tiempo, que consiste en un intervalo de tiempo por el cual si un mensaje llega dentro de dicho intervalo, el mensaje es auténtico.

Cuando el receptor del mensaje en un motor autorizado, se considera que el mensaje llegó fuera de la ventana de tiempo siempre cuando cumpla con alguna de las siguientes condiciones:

- El campo snmpEngineBoots está trabado en su máximo valor que es $(2^{31} - 1)$.
- Cuando msgAuthoritativeEngineBoots y snmpEngineBoots no tienen los mismos valores.
- El valor del campo difiere de msgAuthoritativeEngineTime con respecto snmpEngineTime por más de 150 segundos.

Cuando receptor del mensaje en un motor no autorizado, se considera que el mensaje llegó fuera de la ventana de tiempo siempre cuando se cumple con alguna de las siguientes condiciones:

- El campo snmpEngineBoots está trabado en su máximo valor.
- EL msgAuthoritativeEngineBoots tiene un valor menor que snmpEngineBoots.
- El valor del campo difiere de msgAuthoritativeEngineTime con respecto al snmpEngineTime por más de 150 segundos.

2.5.7.8 Gestión de claves

Se define como los procedimientos de generar, localizar y actualizar las claves. El gestor SNMP (principal) su función es de gestionar las claves. Cada principal debe mantener una clave de autenticación y una de privacidad únicas.

- Generación de claves: La generación de claves se basa con el algoritmo Password-Key, del cual requiere de uno o dos passwords, que son dados desde el sistema de gestión, para crear dos claves de 16 o 20 octetos. Pero para mayor seguridad se recomienda que las dos claves sean diferentes tanto para generar las claves de autenticación y encriptación.

- El procedimiento se genera con:

    - ✓ La formación de una cadena de texto de longitud 2^{20} si se repitiendo el password, la cadena de texto se denomina digest0.
    - ✓ Mientras para la creación de la llave de 16 octetos se aplica la función MD5 al digest0 y se obtiene la clave de usuario que denomina digest1.
    - ✓ En cambio, para crear una llave de 20 octetos se aplica la función SHA-1.

Localización de claves: Es el proceso de generación de varias claves diferentes a partir de la clave del usuario digest1. Cada clave producida se denomina clave localizada. Cabe recalcar que la clave localizada es la que se comparte entre un principal en un motor no autorizado y un motor autorizado (agente), también, la clave localizada puede ser authKey (autenticación) o privKey (privacidad). El procedimiento para la localización de claves es:

Cuando se forma una cadena de texto con digest1, el snmpEngineID del motor autorizado y nuevamente digest1, la cadena de texto se va a denominar digest2. Después se aplica funciones como MD5 o SHA-1 sobre digest2 y el resultado de toda la operación es la clave localizada.

Actualización de claves: Se realiza la actualización de claves para mantener la seguridad y confiabilidad del sistema y el cambio de claves se realiza desde el sistema de gestión.

2.5.8 Modelo de control de acceso basado en vistas (VACM)

Este modelo se basa en el RFC 3415 que se refiere a los mecanismos que permiten o restringe el acceso a ciertos objetos administrados según las políticas de acceso que tiene los mismo es decir controlar el acceso hacia un objeto MIB a un principal remoto, también qué tipos de operaciones se puede hacer sobre una entidad local a través de una entidad remota.

Este modelo utiliza los campos de msgFlags, msgSecurityModel y scopedPdu del mensaje SNMPv3 para saber el tipo de acceso que tiene el mensaje. Si el acceso no es permitido a dicho tipo de solicitud, entonces de envía una notificación de error al principal.

El modelo VACM tiene dos características importantes:

- El VACM determina si el acceso a un objeto administrado en una MIB local, por un gestor SNMP es permitido o no.
- El VACM poseen su propia MIB que permite controlar las políticas de control de acceso para el agente y habilita la configuración remota.

Dentro del modelo de acceso basado en vistas encontramos 5 elementos que son:

2.5.8.1 Grupos

Se definen como un conjunto de cero o más tuplas (Modelo de Seguridad, Nombre de seguridad) que definen los Objetos que pueden ser administrados por ese Nombre, por lo cual un administrador de objetos SNMP tiene acceso.

- El securityName a un principal y los derechos de acceso para todos los principales en un grupo, para que todos los que pertenezcan al grupo tienen los mismo accesos.
- Cada grupo tiene un nombre único (groupName) para definir los derechos de acceso.

2.5.8.2 El nivel de seguridad

Los derechos de acceso para un grupo pueden definirse según el nivel de seguridad del mensaje en la solicitud (noAuthNoPriv, authNoPriv y uthPriv). Un ejemplo, se puede permitir la lectura para un mensaje no autorizado, pero necesitar autenticación para escribir. El securityLevel, identifica el nivel de seguridad, para que pueda ser asumido cuando se chequea los derechos de acceso.

2.5.8.3 Los contextos

Un contexto MIB es un subconjunto de las instancias de los objetos de la MIB local, es decir es una colección de información de administración accesible por una entidad SNMP. Permite que a una colección de objetos tengan una colección diferente de políticas de acceso.

- El contexto se refiere a control de acceso.

La solicitud SNMP, se identifica únicamente por un contextEngineID que puede mantener más de un contexto. Un objeto o una instancia de un objeto contener uno o más contextos. Pero cuando existen múltiples contextos, la instancia para poderle identificarle la instancia de un objeto, se deben identificar su contextName y contextEngineID.

2.5.8.4 Las vistas MIB

Por seguridad, este valor específicamente es usado para restringir el acceso a algunos grupos o un subgrupo de la información de administración en el dominio de administración. Para realizar esto, el acceso al contexto se hace mediante la definición de vistas MIB. Una ventaja es que los objetos están organizados en forma jerarquía de árbol. Por esto está asociado a cada 36 entradas en la tabla vacmAccessTable, tiene tres vistas:

- Lectura
- Escritura
- Notificación de acceso (que representa el conjunto de instancias de objetos autorizados).

2.5.8.5 Las políticas de acceso

El modelo de control de acceso basado en vistas define los derechos de acceso de un grupo, es decir, que el motor SNMP sea configurado para impartir ciertos derechos de acceso.
La determinación de acceso va a depender de:

- El gestor SNMP (principal) que hace la solicitud de acceso.
- El VACM permite que un agente pueda acceder a diferentes privilegios de acceso a diferentes usuarios.
- El nivel de seguridad del mensaje de solicitado.
- El modelo de seguridad usado para procesamiento el mensaje de solicitud.
- El contexto de la MIB para la solicitud del mensaje pedidi.
- El tipo de acceso solicitado.

2.5.8.6 Beneficios SNMPv3

- Los datos pueden ser colectados en forma segura por equipos SNMP sin el temor que hayan sido forzados o corrompidos.
- Manejo de la información confidencial. Por ejemplo un conjunto de comandos SNMP que cambian la configuración de un equipo, pueden ser configurado para prevenir la exposición de su contenido en la red.
- Acceso selectivo hacia cada uno de los objetos de la MIB.
- Identificación del origen de los mensajes
- Robustos algoritmos para la autenticación y la encriptación

Cabe mencionar que SNMPv3 basada en RFC 2574, fue diseñada para evitar ataques cibernéticos mediante el uso de algoritmos de autentificación y de encriptación que son:

- ✓ Modificación de la información: si el atacante tiene éxito en vulnerar la seguridad podría alterar un mensaje y así lograr que haya una acción no autorizada en la entidad que recibe el mensaje.
- ✓ Enmascaramiento (masquerade): consiste en operaciones no autorizadas del ente de control, el usuario puede estar asumiendo la identidad de otro usuario que tenga todos los permisos de autorización para la operación deseada.
- ✓ Reenvío de mensajes: SNMP opera en un protocolo de transporte sin conexión, existe el riesgo que el mensaje sea interceptado y almacenado por algún tercero para luego el mensaje sea reenviado o duplicado, para operaciones de administración no autorizadas.
- ✓ Poca privacidad (disclosure): un atacante puede observar el intercambio de mensajes entre un agente y una consola de administración.(23)

2.6 Ventajas SNMPv3 que se adaptaron a los requerimientos para la gestión y tráfico de datos de la empresa Maxxnet

Tabla 21-2: Ventajas del protocolo para la empresa Maxxnet

VENTAJAS	
FUNCIONAMIENTO	Funciona de forma modular
CONTROL DE ACCESO	Restringe el acceso de la información a los objetos gestionados, mediante las políticas de acceso que tienen los mismos, a través vistas de la MIB que restringen la visión completa de la misma.
AUTENTICACIÒN	Utiliza mecanismos de encriptación , como los protocolo DES y AES para dar privacidad a los mensajes y robustez
PRIVACIDAD	Utiliza mecanismos de autenticación que verifican el mensaje SNMP , a través de claves de autenticación (authkey) y soporta protocolos HMAC-MD5-96 yHMAC-SHA-96
SUPLANTACIÒN DE IDENTIDAD	Utiliza la autenticación para verificar los mensajes SNMP si viene donde dice venir.
MODIFICACIÒN DE LA INFORMACIÓN	Se defiende con los algoritmos de encriptación.
MODIFICACIÒN DEL FLUJO DE MENSAJES	Utiliza etapas de sincronización y ventanas temporales de llegadas de mensajes,
GESTIÓN DE RED CENTRALIZADA	Permite.
TRAFICO DE DATOS	El intercambio de mensajes SNMP son más seguros.

DIVULGACIÓN	Evita las escuchas ilegales de los analizadores de protocolos, etc, mediante el uso de cifrado.
AMENAZAS DE TRAFICO	Se protege a través de Modelo de seguridad basado en el usuario
TRANSPORTE DEL TRÁFICO	Tráfico SNMP se cifra durante el tránsito
GESTIÓN DE RED DISTRIBUIDA	Hereda las operaciones del protocolo SNMPv2 por lo tanto permite una gestión distribuida, es decir permitiendo la existencia de dos o más estaciones que hagan de máquinas gestoras, dependiendo de la complejidad de la red
GESTIÓN DE RED JERARQUICA	Como Hereda las operaciones de SNMPv2 lo que permite una gestión jerárquica

Realizado por: Toapanta, Ángel, 2023

2.7 Software Zabbix

La creación de Zabbix fue realizado por Alexei Vladishev y actualmente está desarrollado por Zabbix SIA. El objetivo de Zabbix es dar una solución al monitoreo de redes, equipos, máquinas virtuales, servidores, bases de datos, sitios web, la nube, aplicaciones, etc., que nos van a permitir conocer y registrar el estado en tiempo real e historial de los mismos, cabe destacar que es un software de código abierto (open source) de clase empresarial esto quiere decir que su código fuente se distribuye gratuitamente y está disponible para el público en general.

Además utiliza un mecanismo de notificación flexible que a los usuarios permitirá la configuración de alertas basadas en correo electrónico y mensajes de telagram o WhatsApp para prácticamente cualquier evento que este fuera de lo normal que permitirá reacción rápidamente a los problemas del servidor o los equipos que este monitoreando.

Con una instalación y configuración correcta, Zabbix va desempeñar un papel importante para cualquier organización ISP grandes o pequeñas como la Empresa Maxxnet, sabiendo que es un software libre se puede ahorrar en licencias teniendo un producto bueno como cualquier sistema licenciado. (Server Zeo, 2021)

2.7.1 Funcionamiento del software Zabbix

Para el funcionamiento de Zabbix para este proyecto se instaló en un servidor Alma Linux 8.5, donde se encargará de recolectar y monitorear la información pertenecientes de la red Core con la ayuda del protocolo SNMPv3, además facilita una interfaz Web la cual se presenta de forma gráfica toda la información que va ir recolectando y almacenando de todos los dispositivos que vayan a ser administrados por Zabbix.

Zabbix cuenta con agentes para sistemas operativo de Linux, Mac y Windows en los cuales se instalan en los servidores o puestos de trabajo que vayan a ser monitorizados. También permite observar el estado en tiempo real de las impresoras, routers, switches, sensores de temperatura y humedad entre otros. Algunas funciones de Zabbix que son: (Córdova, 2019)

- Alertas configurables.
- Gráficos en tiempo real.
- Capacidad de monitoreo
- Almacenamiento de datos históricos.
- Una configuración dinámica.
- Recopilación de datos.

En la Ilustración 9-2 podemos visualizar de mejor manera el funcionamiento de Zabbix.

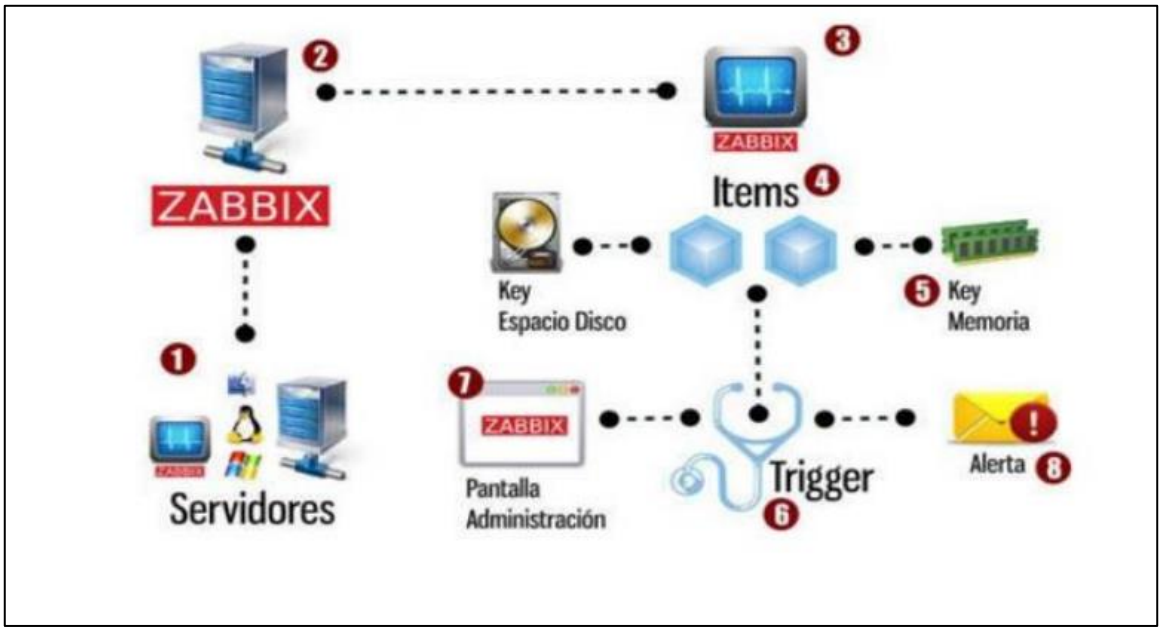


Ilustración 9-2: Funcionamiento del software Zabbix

Fuente: Hernández, Juan, 2010

2.7.2 Ventajas de Zabbix

Algunas ventajas que utilizar Zabbix dentro del monitoreo de red son:

- Tiene a solución de código abierto que ofrece el uso sin bloque y la seguridad a través de la disponibilidad del código fuente. A la vez también incluye no solo al software Zabbix sino también los componentes necesarios como Linux, Apache, MySQL / PostgreSQL, PHP.

- Contiene un sistema de administración centralizado es decir que utiliza un monitor web donde se encuentran todo los dispositivos de la red en una misma interfaz.
- Sistema de manejo de usuarios con autenticación mediante contraseñas y usuarios.
- Manera de alertar un evento, las más utilizadas son a través de correo electrónico y mensajes SMS, que automáticamente son enviados algún dispositivo cuando surjan algún problema.
- Capacidad de encontrar diferentes dispositivos de red como router, switch, servidores, impresoras y periféricos a través de varios protocolos como SNMP (1, 2,3).
- Capacidades integradas de visualización que van a facilitar el trabajar con sus datos más rápido e inteligente.
- Incorpora un sistema de limpieza que permite mantener los datos bien actualizados y con un nivel de organizado. (Córdova, 2019)

2.7.3 Características de monitorización del software ZABBIX

Monitorización

- Una configuración centralizada.
- Acceso centralizado de la información.
- Soporta hasta 1000 nodos Zabbix.
- Un número ilimitado de proxis en el sistema.

Escalabilidad

- Estudios han probado hasta 100000 dispositivos y servidores monitorizados.
- Probado por la organización Zabbix con 1000000 chequeos de rendimiento y disponibilidad
- Capacidad de procesar en segundo miles de chequeo de rendimiento y disponibilidad del sistema.

Monitorización en tiempo Real

- Monitorea el rendimiento y disponibilidad
- Condiciones de notificaciones flexibles.
- Alertas para los usuarios (SMS, email)
- Registros de log

Auto detección

- Detección por SNMP (1,2,3), rangos IP y servicios.
- Monitorea automáticamente de los dispositivos auto detectado.
- Flexibilidad.
- Soporte tanto IPv4 como IPv6
- Agentes nativos.

Monitorización proactiva

- Monitorea sin agente
- Monitorea los servicios remotos (FTP, SSH, HTTP, entre otros)
- Soporte para el protocolo SNMP v1, 2, 3
- Traps SNMP v3

Seguridad

- Permisos flexibles por cada usuario
- Autenticación por IP.
- Protección contra los ataques de fuerza bruta

Funciones de administración

- Ping
- Trace route a un host

2.7.4 Arquitectura de Zabbix

Zabbix para la arquitectura utiliza varios elementos para el funcionamiento del monitoreo en la red, en la Ilustración 10-2 representa los elementos de Zabbix.

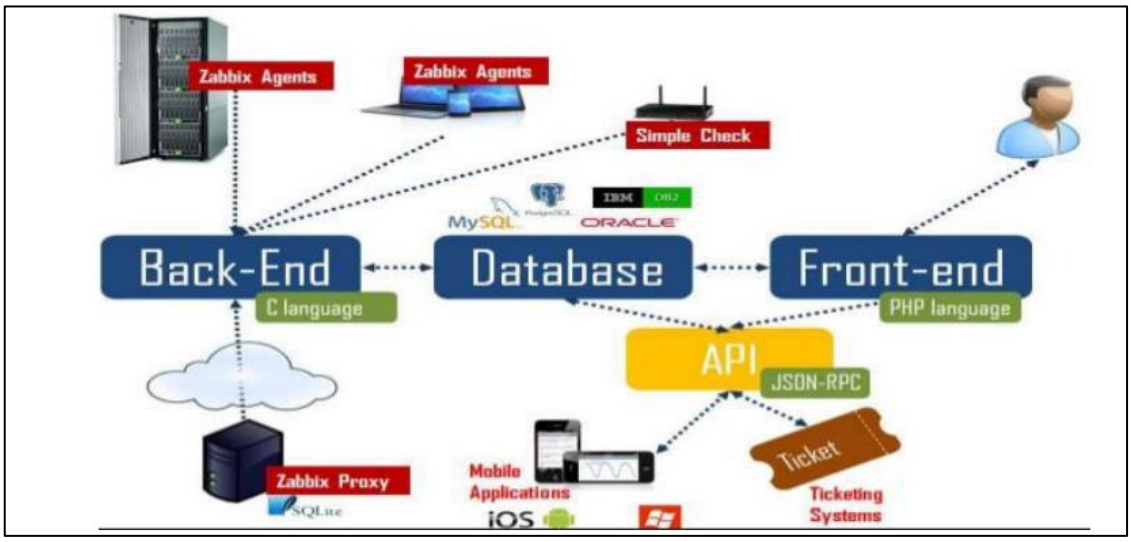


Ilustración 10-2: Arquitectura de Zabbix

Fuente: Hernández, Juan, 2009

2.7.5 Elementos que constituye Zabbix

2.7.5.1 Servidor Zabbix

Es el componente más importante de Zabbix porque se puede comprobar de forma remota los servidores en la red mediante comprobaciones de servicio sencillas, también los agentes informan toda la información, las estadísticas de disponibilidad e integridad al servidor lo cual esto nos hace que el servidor de Zabbix sea un componente central ya que almacena todos los datos tanto de configuración, estadístico y operarios para que sean organizados por el servidor.

Otra función del servidor de Zabbix es que alertara activamente a los administradores, todos los problemas que cuando se produzca los sistemas monitoreados que son enviados desde los agentes. También el servidor es donde se encuentra instalada la consola de administración y la base de datos central de Zabbix, donde se va a recopilar la información de los dispositivos gestionados por Zabbix. (Pozo, 1995)

2.7.5.2 Zabbix Agente

Componente de Zabbix importante basado en el protocolo SNMP que permite monitorear los recursos de la red en tiempo real. Un agente nativo de Zabbix, está desarrollado en lenguaje C que se puede ejecutarse en varias plataformas compatibles como Linux, UNIX y Windows. Recopilar datos como el uso de la CPU, la memoria del disco, la interfaz de red de un dispositivo, la velocidad de datos, etc.

2.7.5.3 Host y group host

Los host son todos los dispositivos que se van a monitorear como servidores, estaciones de trabajo, conmutadores, router, switch, etc. Otro caso es la creación de grupos de dispositivos (group host) sirve para la organización de los host que pertenecen a un grupo determinado. Los equipos se organizan en grupos de equipos.

2.7.5.4 Triggers

Los disparadores son módulos creados por el administrador de red que son expresiones lógicas que evalúan los datos recopilados por los elementos (ítems) lo cual representan el estado actual del sistema.

2.7.5.5 Ítems

Los elementos son módulos que se encargan recopilar los datos de un host.
Cuando se crea un host, debemos agregar algunos elementos para el monitoreo para comenzar la recopilación datos reales.

2.7.5.6 Templates

En Zabbix el uso de plantillas (templates) es una excelente forma de reducir la carga de trabajo y por ende optimizar la configuración de Zabbix. Una plantilla se puede definir como un conjunto de entidades que pueden aplicar convenientemente a múltiples hosts.

Las entidades que pueden estar:

- Ítems (Elementos)
- Triggers (disparadores)
- Graphs (gráficos)
- dashboards
- low-level discovery rules
- web scenarios

En el mercado hay muchos dispositivos que son idénticos o bastante similares, se escoge un conjunto de entidades (elementos, disparadores, gráficos,...) que ha creado para un dispositivo y puede ser útil para muchos.

Cuando la plantilla está vinculada a un host o dispositivo, todas las entidades se agregan al host para utilizarlo al monitoreo.

2.7.5.7 Discovery

Zabbix tiene la función de descubrimiento automático de redes que es flexible y efectiva, con el objetivo de acelerar la implementación de Zabbix y simplificar la administración.

El descubrimiento de red en Zabbix se basa:

- Rangos de IP.
- Disponibilidad de servicios externos.
- Información recibida del agente de Zabbix.
- Información recibida del agente SNMP.

2.7.5.8 Interfaz web

Zabbix para fácil acceso a los datos de monitoreo y las configuraciones podemos utilizar cualquier plataforma que proporcionen la interfaz basada en web.

2.7.5.9 Macros

Las macros son variables, identificadas por una sintaxis {MACRO}, también las macros se resuelven en un valor específico según el contexto que se utiliza. Los requerimientos del protocolo SNMPv3 en Zabbix son los siguientes:

Tabla 22-2: Parámetros de SNMPv3 en Zabbix

PARÁMETRO PARA SNMPV3	DESCRIPCIÓN
Context name	Es un nombre de contexto para identificar el elemento SNMP en la subred.
Security name	Es un nombre de la seguridad que se va a ocupar.
Security level	Elección del tipo de seguridad. • noAuthNoPriv • AuthNoPriv • AuthPriv
Authentication protocol	Selección del protocolo de autenticación: MD5, SHA1, SHA224, SHA256, SHA384 o SHA512.
Authentication passphrase	Contraseña de autenticación o llaves que sirve para verificar el acceso al usuario.
Privacy protocol	Selección del protocolo de privacidad: DES , AES128 , AES192 , AES256 , AES192C (Cisco) o AES256C (Cisco)
Privacy passphrase	Contraseña o llaves que sirve para encriptar la información.

Fuente: Pozo, J, 1995

Realizado por: Toapanta, Ángel, 2023

2.7.6 Ventajas y desventajas de Zabbix respecto a otros open source

A continuación se presenta una tabla comparativa que Zabbix ofrece frente a otros open source que soporte el protocolo SNMPv3 para nuestro proyecto.

Dentro de la tabla de comparación la búsqueda se centró en los sistemas de monitoreo más conocidas y usadas que son: (Isaias, D., & Barona, 2016)

- Zabbix.
- Cacti.
- Nagios.
- Munin.

Tabla 23-2: Comparación de Zabbix con los demás open source

CARACTERÍSTICAS.	ZABBIX	NAGIOS	CACTI	MUNIN.
Interfaz Web	✓	✓	✓	✓
Graficas.	✓	✓	✓	✓
reportes	✓	✓		
Envíos de notificaciones email,msm de texto	✓	✓		
Open Source	✓	✓	✓	✓
Soporte SNMP (1,2,3)	✓	Si pero con plugins	✓	Si pero con plugins
autodescubrimiento	✓	Si pero con plugins	Si pero con plugins	
Monitoreo de servidores Linux,unix y Windows	✓	✓	✓	✓
Monitoreo de firewalls, proxis, router, etc.	✓	✓	✓	✓
Detección de caídas de red	✓	✓	✓	✓
Mapas	✓	desconocido	Si pero con plugins	Desconocido
Seguridad	✓	desconocido	Roles personalizados	Desconocido
Licencia	GPL	GPL	GPL	GPL
Alertas	✓	✓	✓	
Estadística	✓	✓	✓	✓

Realizado por: Toapanta, Ángel, 2023

CAPÍTULO III

3. MARCO METODOLÓGICO

3.1 Tipo de proyecto

Este proyecto es de tipo aplicativo, ya que con Zabbix actualizamos el sistema de monitoreo que existe actualmente en empresa Maxxnet Internet porque al utilizar una interfaz web lo vuelve más versátil con lo cual nos va a brindar portabilidad del software en toda la red local en un dispositivo que tenga un navegador web.

Además Zabbix va a tener un control acceso ya que las personas autorizadas por el administrador van a poder ingresar a la interfaz web donde se puede observar el estado del equipo con los parámetros de configuración asignadas.

Teniendo en cuenta que el proyecto es aplicativo en un ambiente real los resultados que se muestra son de los equipos que están en funcionamiento 24/7 ubicados en el Core de la empresa.

3.2 Diseño

Para la ejecución del diseño de este proyecto se logró teniendo en cuenta una investigación previa del software Zabbix, se consideró experimental porque en la transición del estudio se planteó el montaje de Zabbix en dos ambientes controlados antes de entrar en la fase de implementación lo cual se llevó al análisis de conceptos, posibles fallas de programación y configuración SNMPv3 de prueba.

El diseño va encaminada a solucionar la problemática de seguridad que no cuenta la empresa con el protocolo SNMPv3, la portabilidad y tener graficas que representen el tráfico en tiempo real de todas las interfaces que contengan el router al ser monitoreado.

Las contraseñas que se utilizaron son propiedad de la empresa y en este proyecto se van a encontrar restringidas por motivos de seguridad.

Además el diseño propuesto va a tener dos fases que se dividen en:

- Fase de implementación del software Zabbix que consiste en levantar el servidor, configuración del software, configuraciones de los host, creación de mapas, creación de notificaciones.
- Fase de análisis de resultados por nodos donde se implementó el sistema de monitoreo con SNMPv3

3.3 Implementación del sistema integral de monitoreo

En esta fase del proyecto la herramienta Zabbix nos ayuda con el monitoreo de uptime, downtime y el ancho de banda, que son los puntos clave del proyecto. Una vez adquirido previamente los conocimientos del protocolo SNMPv3, a ver experimentado en una máquina virtual las configuraciones de Zabbix para tener un mejor manejo, procedemos a la implementación en el servidor local de la empresa con todas las medidas de seguridad.

En este capítulo serán descritas los pasos de instalación del servidor Zabbix, incorporación de host (router del Core), aviso de alertas por vía Telegram y la obtención de reportes de Zabbix que se involucradas en el proyecto de tesis.

Se describe a detalle la implementación del sistema de monitoreo y las consideraciones que se debe tener en cuenta durante el proceso.

3.3.1 Instalación del software zabbix

La empresa Maxxnet Internet para este trabajo de tesis nos provee de un espacio en el servidor local donde instalamos el sistema operativo Alma Linux con la versión 8.5 que se utiliza en ambientes empresariales.

Ya que es un sistema operativo robusto, que es una distribución Linux gratuita y de código abierto que utiliza el código fuente del sistema operativo Red Hat Enterprise Linux que son algunas características del sistema operativo y los más importante que va hacer compatible con Zabbix 6.0.

Zabbix para su correcto funcionamiento debe tener unos prerrequisitos previamente instalados en el servidor alma Linux estos deben ser:

- Instalación de Apache.
- Instalación de la base de datos MySQL.
- Instalación de PHP.

3.3.2 Instalación de apache 2.0

La instalación del servidor HTTP Apache es un punto importante en la instalación de Zabbix ya que es un servidor HTTP de código abierto, los cuales son ocupados en sistemas operativos moderno, incluido UNIX y Windows.

El objetivo de instalar HTTP APACHE es proporcionar un servidor eficiente y extensible que proporcione servicios HTTP con sincronía de los estándares actuales de HTTP.

Los comandos que se usaron la instalar HTTP APACHE son los siguientes:

- sudo yum update
- sudo yum install -y httpd
- sudo systemctl start httpd
- sudo systemctl enable httpd
- sudo systemctl status httpd

Una vez actualizado el repositorio e instalado el paquete de httpd el siguiente paso es mandarle a comenzar y habilitar para su funcionamiento como se muestra la Ilustración 1-3. Debe estar de color verde active (running) donde nos demuestra que el sistema está corriendo correctamente.

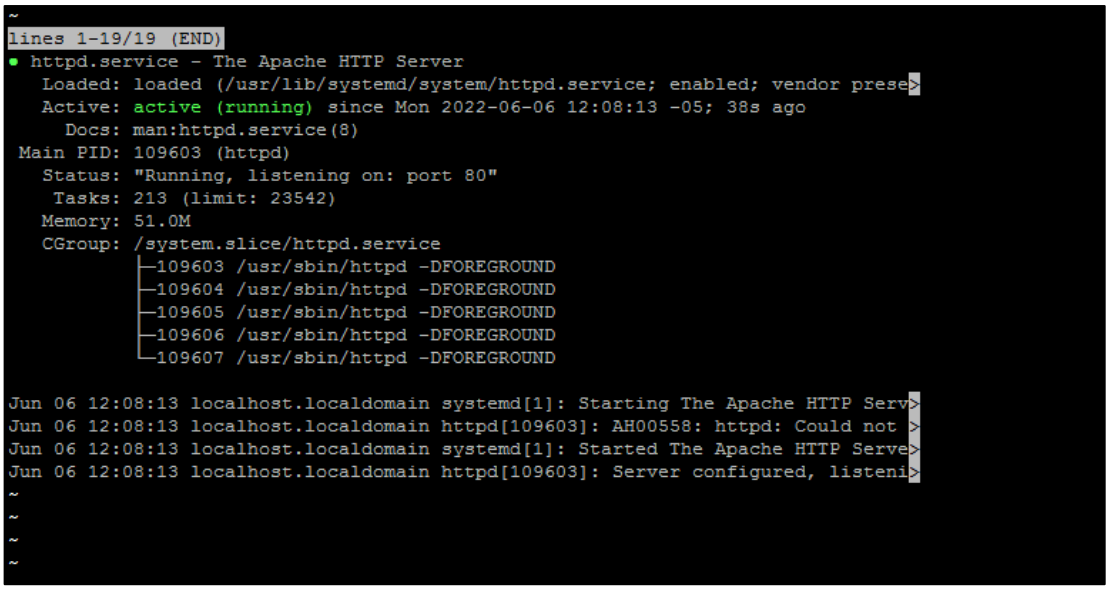


Ilustración 1-3: Estado de activación de Apache HTTP server

Realizado por: Toapanta, Ángel, 2023

Después es necesario habilitar los puertos http y https que por defecto son el 80 y 443, en el firewall con el objetivo de conectar sin ningún bloqueo los comandos son:

- sudo firewall-cmd --permanent --add-service={http,https}
- sudo firewall-cmd –reload

Para que los cambios sean ejecutados debemos reiniciar el firewall, si los pasos son correctos se deben mostrar los datos de la Ilustración 2-3.

```
[1]+  Stopped                 sudo systemctl status httpd
[dpusay@localhost ~]$ sudo firewall-cmd --permanent --add-service={http,https}
success
[dpusay@localhost ~]$ sudo firewall-cmd --reload
success
[dpusay@localhost ~]$
```

Ilustración 2-3: Activación de puertos y reiniciación del firewall

Realizado por: Toapanta, Ángel, 2023

Si seguimos todos los pasos lo último es probar desde cualquier navegador de su agrado, si nuestra instalación es correcta, buscamos con la IP del servidor http://172. . .7, la página de inicio de Apache lo cual nos indica que tenemos comunicación con el servidor a través de una interfaz web.

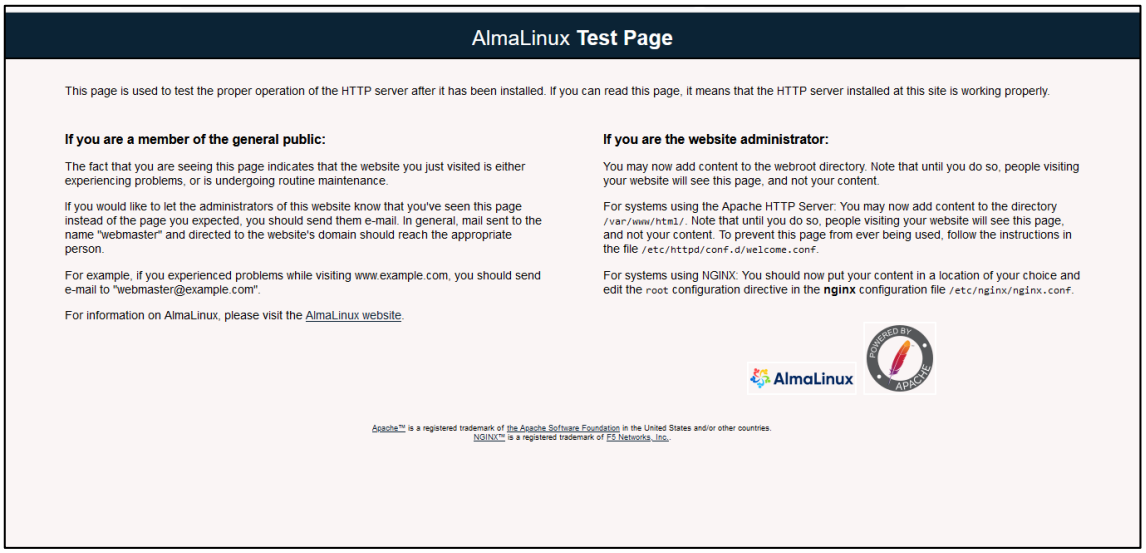


Ilustración 3-3: Página inicial de APACHE en alma Linux

Realizado por: Toapanta, Ángel, 2023

3.3.3 Instalación de la base de datos MySQL

Para poder usar el software Zabbix, se debe instalar una base datos relacionados de código abierto para almacenamiento los datos de monitoreo que recogerá el servidor a través de los agentes de Zabbix.

Los comandos que se ocuparon fueron:

- sudo yum install -y mysql-server
- sudo systemctl enable --now mysqld

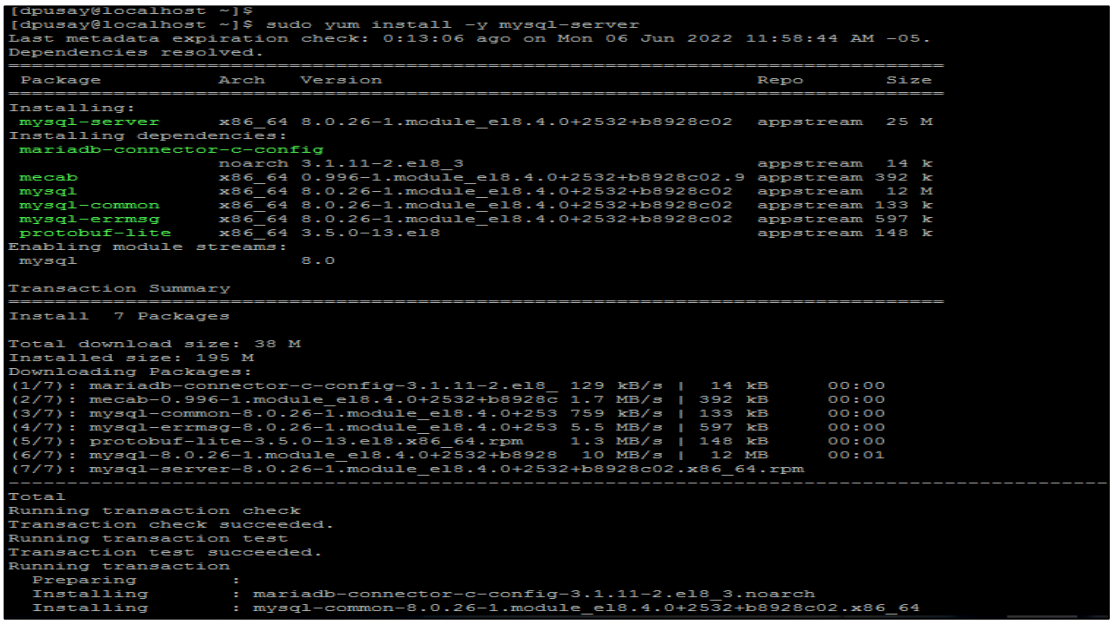


Ilustración 4-3: Representación de la instalación de MySQL

Realizado por: Toapanta, Ángel, 2023

La instalación de MySQL se crea una cuenta de root que viene sin contraseña para acceder a la base de datos, el problema radica en el ámbito de seguridad, por lo cual para solucionar este inconveniente debemos ejecutar un comando:

- mysql_secure_installation

Que nos permitirá crear una contraseña para root, borrar base de datos de pruebas, remover usuarios anónimos y eliminar el acceso remoto a la base de datos usando root.

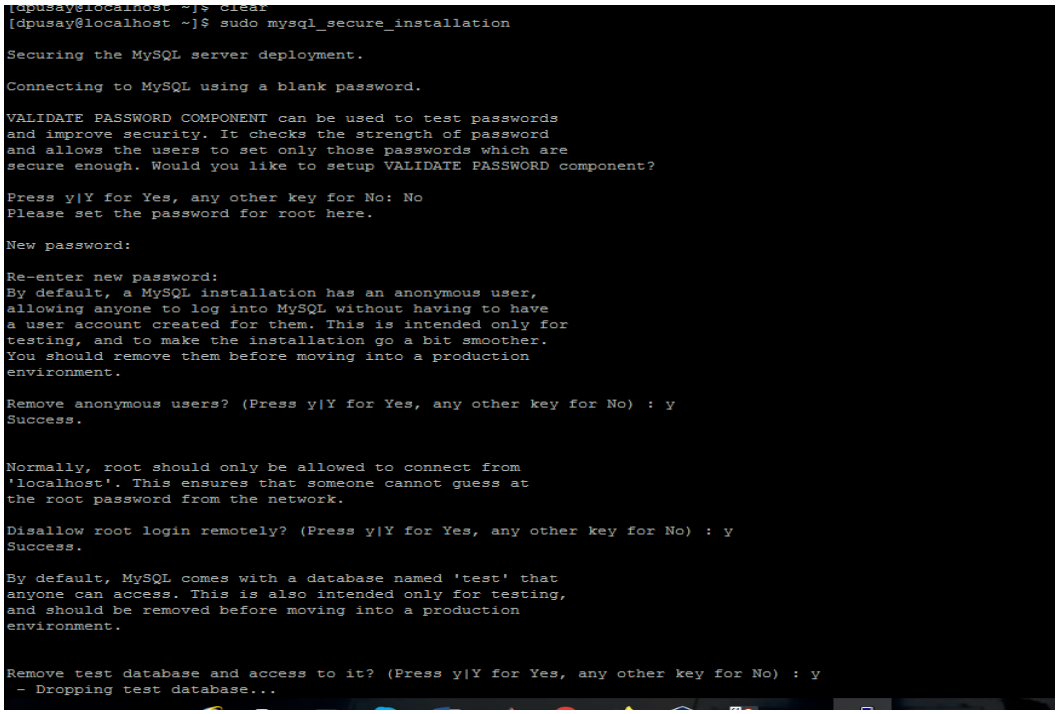


Ilustración 5-3: Instalación de los paquetes de seguridad MySQL

Realizado por: Toapanta, Ángel, 2023

Para podernos conectar al motor de MySQL debemos ejecutar el comando

- mysql -u root -p

Que posteriormente vamos a utilizar en la instalación de Zabbix.

3.3.4 Instalación de PHP

Esta instancia es de mucha utilidad porque el front end de Zabbix está escrito en PHP, por lo cual requiere que el servidor web soporte PHP obligatoriamente. Sabiendo que PHP es un lenguaje de comunicación de secuencias de comandos que en general es utilizado para el desarrollo web.

Los comandos que se usaron:

- sudo yum install -y https://rpms.remirepo.net/enterprise/remi-release-8.rpm

```
Complete!
[root@localhost dpusay]# sudo yum install -y https://rpms.remirepo.net/enterpris
e/remi-release-8.rpm
Last metadata expiration check: 1:46:17 ago on Thu 09 Jun 2022 08:44:04 AM -05.
remi-release-8.rpm                              20 kB/s |  29 kB     00:01
Dependencies resolved.
================================================================================
 Package            Architecture Version              Repository          Size
================================================================================
Installing:
 remi-release       noarch       8.6-1.el8.remi       @commandline        29 k
Installing dependencies:
 epel-release       noarch       8-10.el8             extras              22 k

Transaction Summary
================================================================================
Install  2 Packages

Total size: 51 k
Total download size: 22 k
Installed size: 56 k
Downloading Packages:
epel-release-8-10.el8.noarch.rpm               158 kB/s |  22 kB     00:00
--------------------------------------------------------------------------------
Total                                           18 kB/s |  22 kB     00:01
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :                                                        1/1
  Installing       : epel-release-8-10.el8.noarch                           1/2
  Installing       : remi-release-8.6-1.el8.remi.noarch                     2/2
  Running scriptlet: remi-release-8.6-1.el8.remi.noarch                     2/2
  Verifying        : epel-release-8-10.el8.noarch                           1/2
  Verifying        : remi-release-8.6-1.el8.remi.noarch                     2/2

Installed:
  epel-release-8-10.el8.noarch        remi-release-8.6-1.el8.remi.noarch

Complete!
[root@localhost dpusay]#
```

Ilustración 6-3: Instalación de PHP del repositorio Remi

Realizado por: Toapanta, Ángel, 2023

Debemos desactivar la versión de PHP que viene por defecto ya que Zabbix 6.0 requiere la PHP 7.4 por ser más rápida y confiable.

- sudo yum module disable -y php

```
Complete!
[root@localhost dpusay]# sudo yum module disable -y php
Last metadata expiration check: 0:00:15 ago on Thu 09 Jun 2022 10:32:08 AM -05.
Problems in request:
Modular dependency problems with Defaults:

 Problem: module composer:2:20220609143258:00000000.x86_64 requires module(php),
 but none of the providers can be installed
  - conflicting requests
  - module php:7.2:8030020210119114311:2c7ca891.x86_64 is disabled
  - module php:7.3:8030020210119114205:ceb1cf90.x86_64 is disabled
  - module php:7.4:8060020220419142549:a4870ff1.x86_64 is disabled
  - module php:8.0:8060020220406185241:a4870ff1.x86_64 is disabled
  - module php:remi-7.2:20220609143250:00000000.x86_64 is disabled
  - module php:remi-7.3:20220609143253:00000000.x86_64 is disabled
  - module php:remi-7.4:20220609143255:00000000.x86_64 is disabled
  - module php:remi-8.0:20220609143257:00000000.x86_64 is disabled
  - module php:remi-8.1:20220609143257:00000000.x86_64 is disabled
Dependencies resolved.
================================================================================
 Package          Architecture     Version            Repository         Size
================================================================================
Disabling modules:
 php

Transaction Summary
================================================================================

Complete!
[root@localhost dpusay]#
```

Ilustración 7-3: Desactivación de PHP que viene por defecto

Realizado por: Toapanta, Ángel, 2023

Ahora activamos la versión PHP 7.4 que nos interesa en este proyecto.

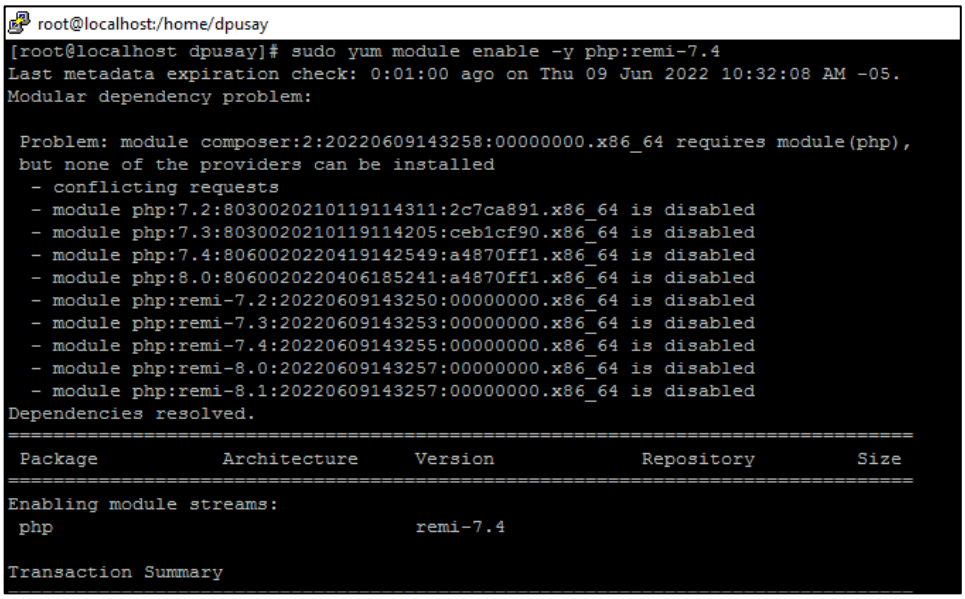


Ilustración 8-3: Activación de la versión PHP 7.4

Realizado por: Toapanta, Ángel, 2023

Ahora instalamos el lenguaje de comunicación PHP y la extensión PHP para la conexión de la base de datos, también debemos habilitar PHP y reiniciarlo para que comience de una forma normal, los comandos que se utilizaron fueron:

- sudo yum install -y php php-MySQL
- sudo systemctl enable --now php-fpm
- sudo systemctl restart httpd

Si la estación es correcta nos muestra de color verde el estado running.

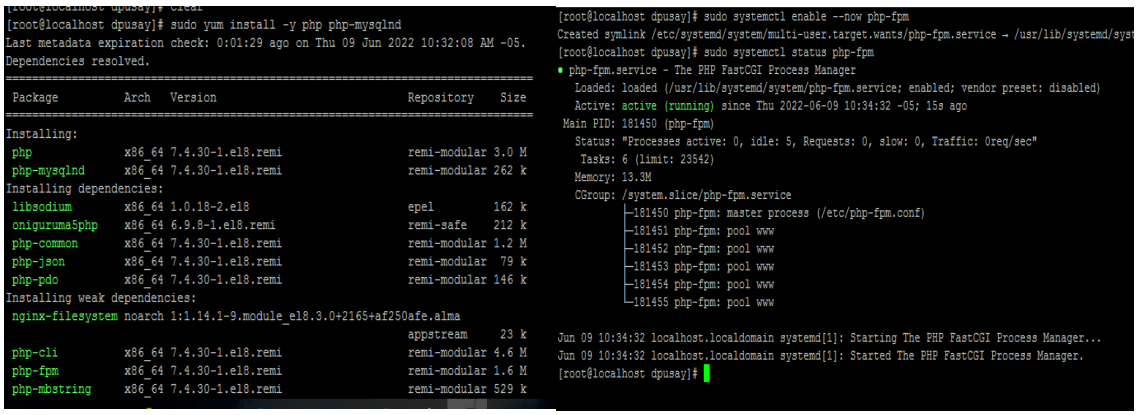
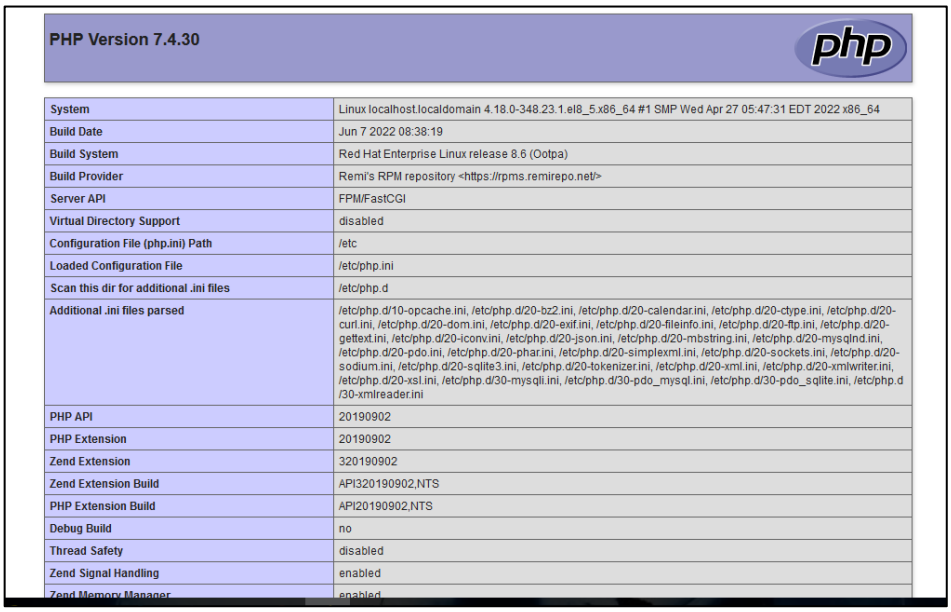


Ilustración 9-3: Conexión PHP con la base de datos y el estado de PHP

Realizado por: Toapanta, Ángel, 2023

El último paso es verificar si PHP se instaló adecuadamente, crearemos un script de prueba en este lenguaje llamado info.php y lo guardaremos en la ruta por defecto de Apache. En el cual se usa **sudo vi /var/www/html/info.php** y dentro de ese archivo colocamos <?php phpinfo();

Para terminar verificamos en un navegador con la siguiente url: http://ip/ info o hostname/info.php



PHP Version 7.4.30

System	Linux localhost.localdomain 4.18.0-348.23.1.el8_5.x86_64 #1 SMP Wed Apr 27 05:47:31 EDT 2022 x86_64
Build Date	Jun 7 2022 08:38:19
Build System	Red Hat Enterprise Linux release 8.6 (Ootpa)
Build Provider	Remi's RPM repository <https://rpms.remirepo.net/>
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini
Scan this dir for additional .ini files	/etc/php.d
Additional .ini files parsed	/etc/php.d/10-opcache.ini, /etc/php.d/20-bz2.ini, /etc/php.d/20-calendar.ini, /etc/php.d/20-ctype.ini, /etc/php.d/20-curl.ini, /etc/php.d/20-dom.ini, /etc/php.d/20-exif.ini, /etc/php.d/20-fileinfo.ini, /etc/php.d/20-ftp.ini, /etc/php.d/20-gettext.ini, /etc/php.d/20-iconv.ini, /etc/php.d/20-json.ini, /etc/php.d/20-mbstring.ini, /etc/php.d/20-mysqlnd.ini, /etc/php.d/20-pdo.ini, /etc/php.d/20-phar.ini, /etc/php.d/20-simplexml.ini, /etc/php.d/20-sockets.ini, /etc/php.d/20-sodium.ini, /etc/php.d/20-sqlite3.ini, /etc/php.d/20-tokenizer.ini, /etc/php.d/20-xml.ini, /etc/php.d/20-xmlwriter.ini, /etc/php.d/20-xsl.ini, /etc/php.d/30-mysqli.ini, /etc/php.d/30-pdo_mysql.ini, /etc/php.d/30-pdo_sqlite.ini, /etc/php.d/30-xmlreader.ini
PHP API	20190902
PHP Extension	20190902
Zend Extension	320190902
Zend Extension Build	API320190902,NTS
PHP Extension Build	API20190902,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled

Ilustración 10-3: Instalación correcta de PHP

Realizado por: Toapanta, Ángel, 2023

3.3.5 Instalación de Zabbix 6.0

Zabbix para el funcionamiento va a requerir una memoria física mínima de 128 MB y 256 MB de espacio libre en disco y disponer de un sistema operativo Linux en este caso es el Alma Linux 8.5, la cantidad de memoria tomar mucho en cuenta que esto va a depender de la cantidad de hosts y parámetros que se van a monitorizar, si se plantea mantener un largo historial de los seguimiento de los parámetros, debemos pensar en por lo menos un par de gigabytes para su funcionamiento para tener suficiente espacio para almacenar la historia en la base de datos.

Para comenzar la instalación luego de cubrir los prerrequisitos debemos Seleccionar la versión de Zabbix en la página oficial y en la sección de descargas seleccionar la versión de Zabbix 6.0.

3.3.5.1 Instalación de zabbix del repositorio oficial

Lo primero que debemos hacer es instalar el repositorio oficial de Zabbix, lo cual necesitamos ejecutar lo siguiente el siguiente comando:

- rpm -Uvh https://repo.zabbix.com/zabbix/6.0/rhel/8/x86_64/zabbix-release-6.0-2.el8.noarch.rpm
- dnf clean all

Ilustración 11-3: Instalación del repositorio de Zabbix de la página oficial

Realizado por: Toapanta, Ángel, 2023

La segunda línea de comando sirve principalmente en eliminar del sistema los archivos cache que son generados a partir de los metadatos del repositorio.

3.3.5.2 Instalación del servidor, de la interfaz y el agente de Zabbix

Este paso es para la instalación del servidor, la interfaz, el agente de Zabbix y el front end web pero con el soporte de la base de datos MySQL, también el agente de Zabbix permitirá recoger datos sobre el estado del servidor.

El comando es:

- dnf install zabbix-server-mysql zabbix-web-mysql zabbix-apache-conf zabbix-sql-scripts zabbix-selinux-policy zabbix-agent

Cuando se esté ejecutando este comando en una parte va preguntara si quiere continuar, presionamos yes o y para continuar.

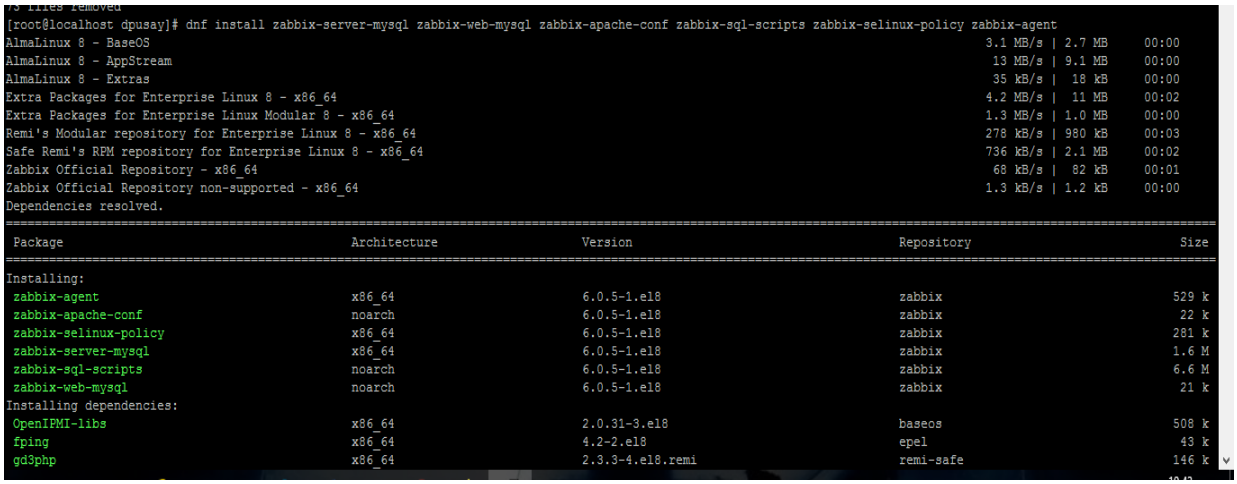


Ilustración 12-3: Instalación de Zabbix server, la interfaz y agent de zabbix

Realizado por: Toapanta, Ángel, 2023

3.3.5.3 Instalación de la Base de Datos

Una de partes importantes para usar Zabbix, es tener una disponibilidad de instalar una base de datos para el almacenamiento de datos que el servidor recogerá de los agentes.

- Debemos preparar la base de datos, para lo cual nos conectamos a la base de datos con la ejecución root.
    - mysql -u root –p ; con la contraseña “password” que se definió en la instalación de MySQL
- Luego creamos una base de datos para el monitoreo Zabbix. El nombre es " zabbix " como nombre de la base de datos. Puedes poner cualquier nombre de preferencia.
    - create database zabbix character set utf8mb4 collate utf8mb4_bin;
- después toca configurar el usuario y la contraseña de Zabbix, puede reemplazar el nombre de usuario y la contraseña según sus preferencias, en este caso son localhost y password
    - create user zabbix@localhost identified by 'password';
- Por último debemos dar permisos de acceso a la base de daros al usuario recién creado.
    - grant all privileges on zabbix.* to zabbix@localhost;
    - quit;

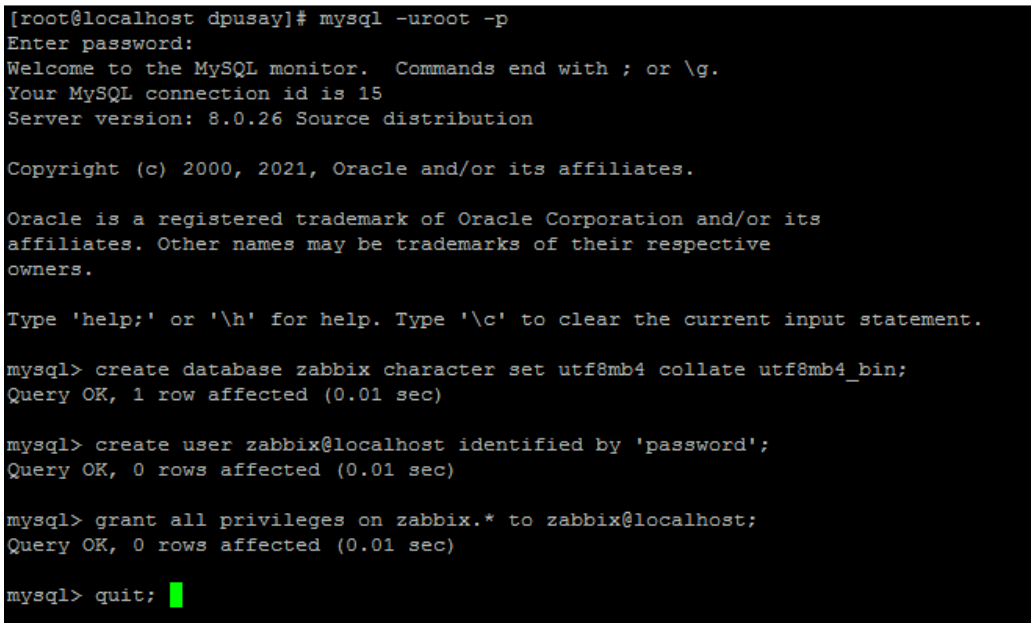


Ilustración 13-2: Creación de la base de datos inicial

Realizado por: Toapanta, Ángel, 2023

3.3.5.4 Importar el esquema y los datos iniciales a la base de datos

En este paso debemos importar el esquema y los datos iniciales a la base de datos, en este paso la instancia nos pedirá que ingreses la contraseña que recién creamos para ejecutar y se utiliza zcat porque los datos en el archivo están comprimidos.

- zcat /usr/share/doc/zabbix-sql-scripts/mysql/server.sql.gz | mysql -uzabbix -p zabbix

Después configuraremos SELinux en modo permisivo para Zabbix

- sudo semanage permissive -a zabbix_t

También debemos permitir que la aplicación Zabbix Front end, pueda realizar conexiones de la red a través del servicio web.

- sudo setsebool -P httpd_can_network_connect on

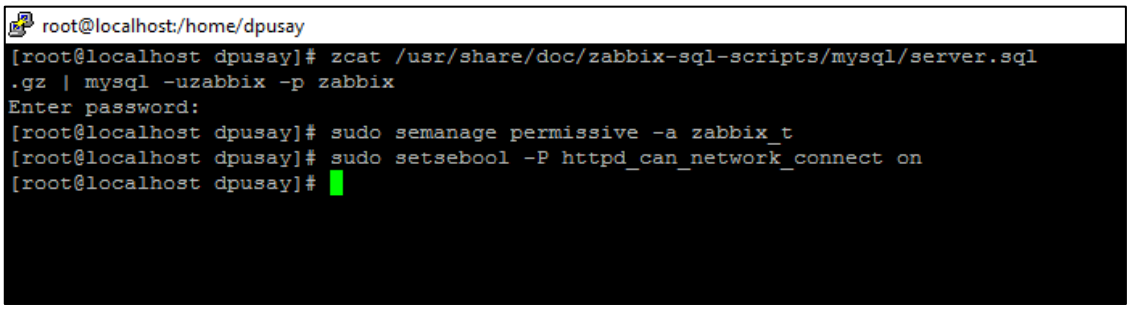


Ilustración 14-3: Datos iniciales con la configuración realizada en la base de datos

Realizado por: Toapanta, Ángel, 2023

3.3.5.5 Configuración de la base de datos para el servidor Zabbix

Para poder usar la base de datos del servidor Zabbix se debe establecer una contraseña a la base de datos con el comando de configuración del servidor:

- sudo vi /etc/zabbix/zabbix_server.conf

Cuando estemos dentro de la instancia de configuración, buscamos el parámetro DBPassword=password, posteriormente guardar los cambios realizados.
Cabe recalcar que se debe elimine "#" en el valor buscado y también elimine el espacio en blanco, si existe. Caso contrario, las variables no serán aplicable y se tratarán como comentarios.

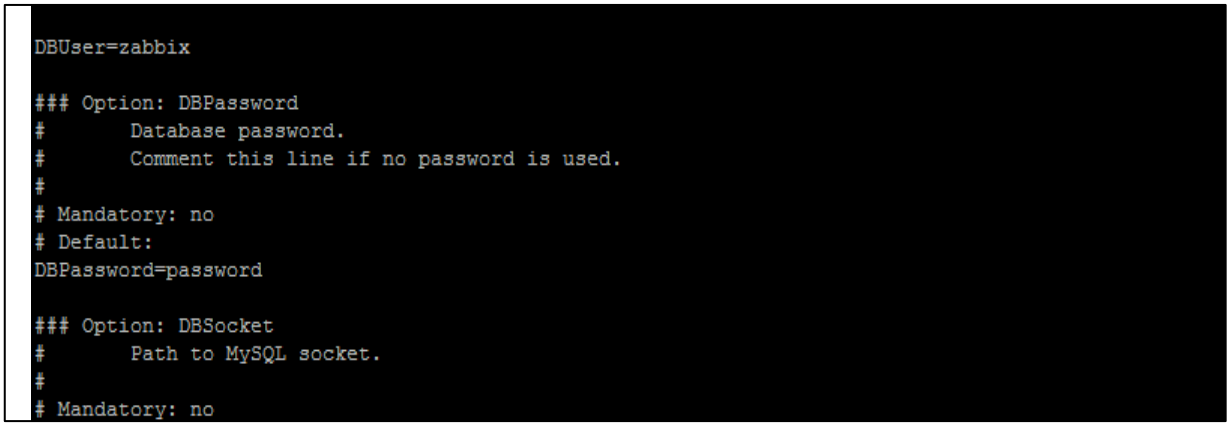


Ilustración 15-3: Configuración de la base de datos para el servidor Zabbix

Realizado por: Toapanta, Ángel, 2023

3.3.5.6 Iniciación de los procesos y restauración del agente y del servidor Zabbix

En este paso vamos a ocupar el comando restart para reiniciar el servidor de Zabbix y los procesos de agent, para que comience recopilar las nueva configuración realizadas anteriormente y con el comando enable sirve para habilitar el sistema para su inicialización.

- systemctl restart zabbix-server zabbix-agent httpd php-fpm
- systemctl enable zabbix-server zabbix-agent httpd php-fpm

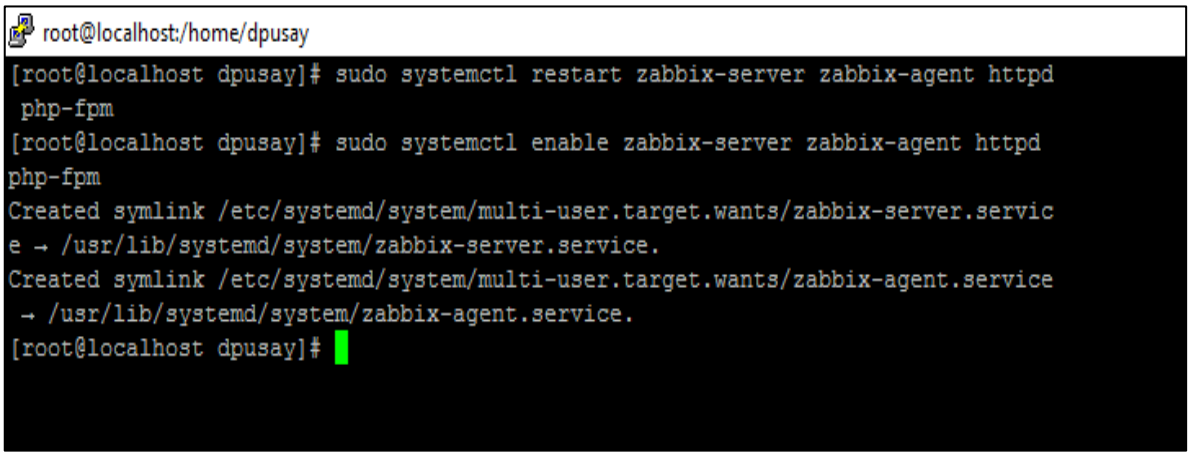


Ilustración 16-3: Inicialización del sistema

Realizado por: Toapanta, Ángel, 2023

3.3.5.7 Verificación del estado del agente y del servidor Zabbix

Una vez reiniciado tanto el agente y el servidor debemos verificar el estado con el objetivo que las instancias estén en el estado en modo activo caso contrario una modificación en la configuración se ejecutó en error y Zabbix no se ejecutara con normalidad.

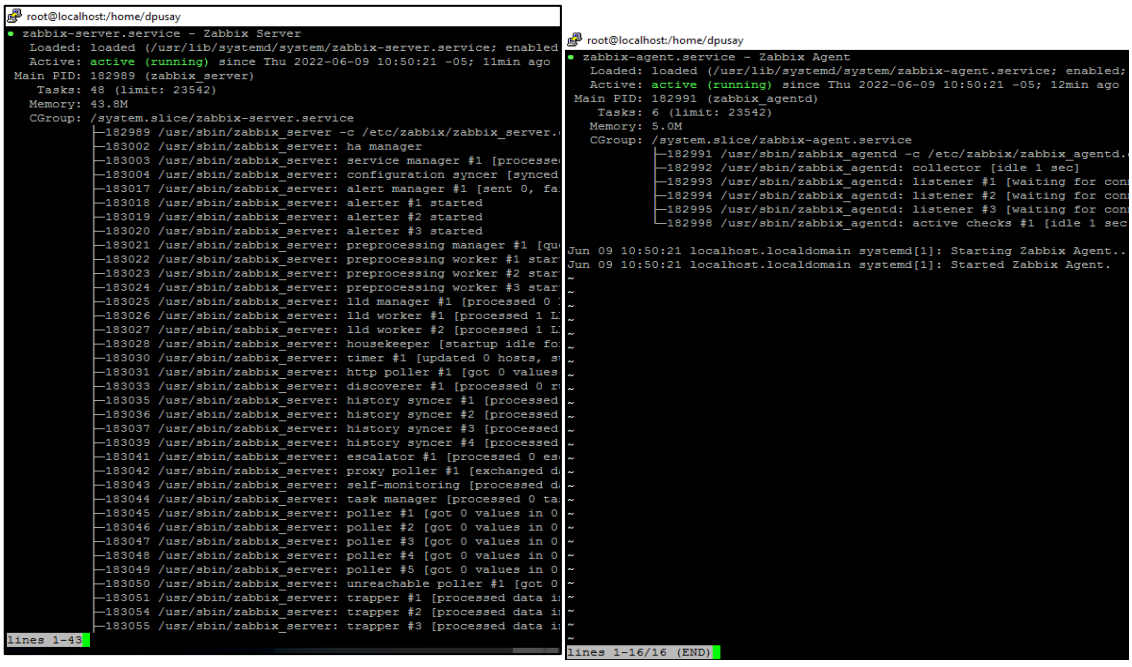


Ilustración 17-3: Estado modo activo del servidor y el agente de Zabbix

Realizado por: Toapanta, Ángel, 2023

3.3.6 Configuración de la interfaz web del servidor zabbix

En este punto ya podemos instalar la interfaz web de zabbix (front end) ingresando a la URL con la dirección IP y con el nombre del servidor como 172.16.255.7/zabbix en cualquier navegador.

Ilustración 18-3: Interfaz de bienvenida a Zabbix

Realizado por: Toapanta, Ángel, 2023

3.3.6.1 Verificación de los prerrequisitos

En la segunda instancia de la interfaz verificamos los requisitos previos del servidor web Zabbix, cabe recalcar que todos los componentes estén en OK para proceder con el proceso de instalación.

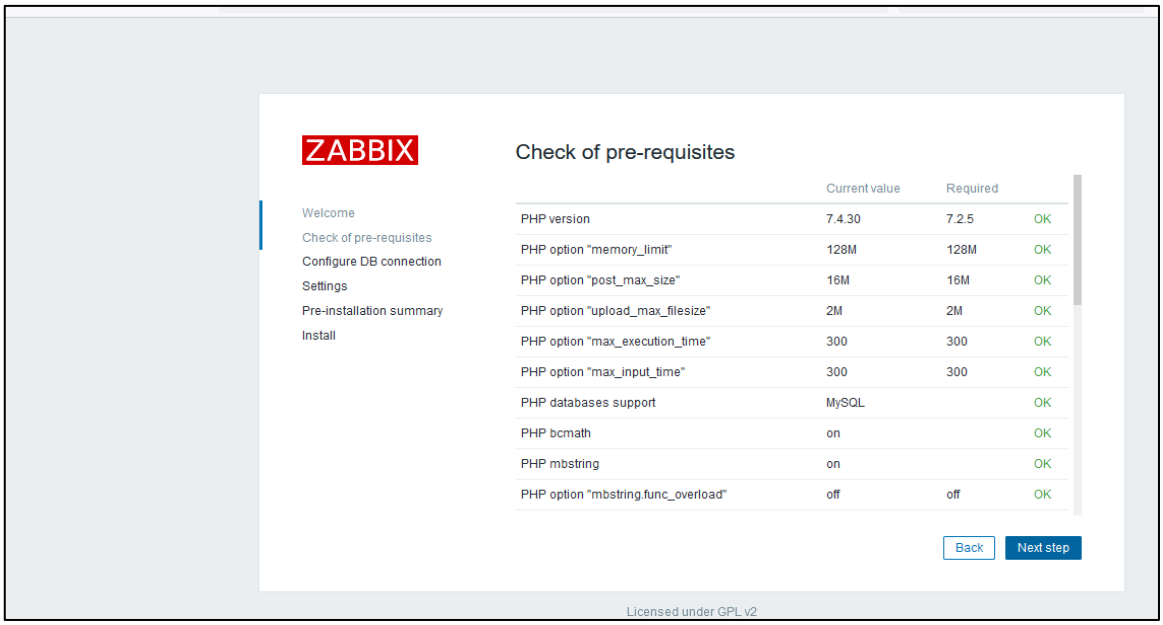


Ilustración 19-3: Chequeo de prerrequisitos en la instalación de Zabbix

Realizado por: Toapanta, Ángel, 2023

3.3.6.2 Configuración de la conexión de la base de datos

En esta instancia de la interfaz debemos configurar la conexión de la base de datos, por lo cual debemos tener en cuenta las configuraciones que hicimos anterior mente en la parte de la instalación de la base de datos, donde se introdujo los siguientes datos:

- Nombre de la base de datos = zabbix
- User zabbix = localhost.
- Password = password.

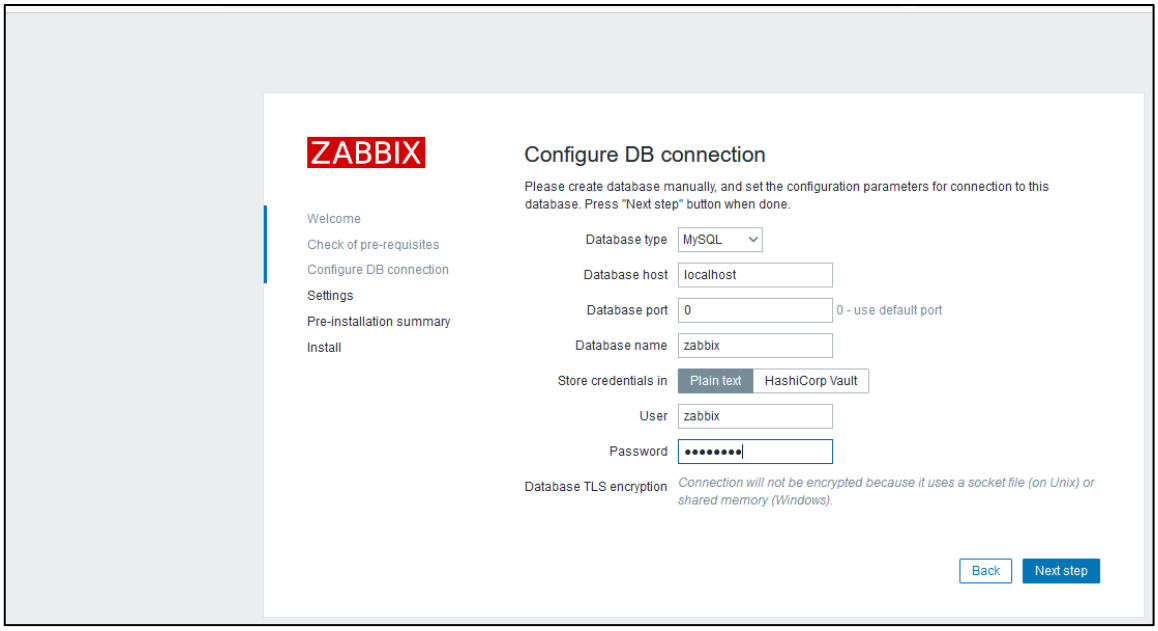


Ilustración 20-3: Configuración de conexión de la base de datos predeterminada

Realizado por: Toapanta, Ángel, 2023

3.3.6.3 Ajustes de Zabbix

En los ajustes al servidor Zabbix se puede dejar los valores predeterminado o se puede crear un nombre para el servidor, ya que con el nombre se puede distinguir un servidor de otro en caso de tener varios servidores de monitorización, en este caso se optó el nombre de la empresa Maxxnet, también se selecciona la zona horaria y el tema de la interfaz gráfica.

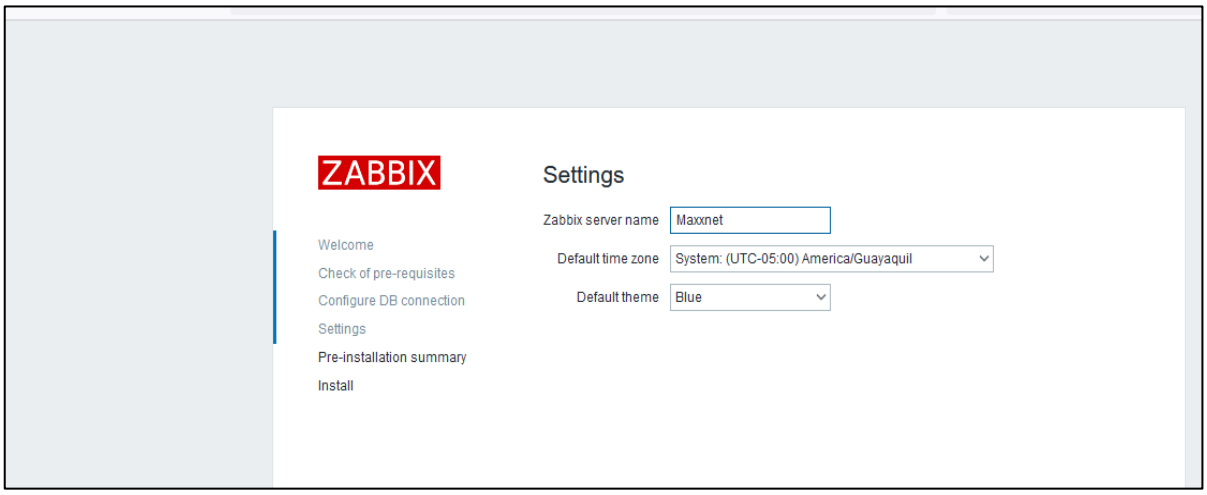


Ilustración 21-3: Configuración del nombre del servidor

Realizado por: Toapanta, Ángel, 2023

3.3.6.4 Resumen de la preinstalación

En este paso nos mostrara un resumen la preinstalación que se va a proceder a realizar, donde se verificara lo todo los parámetros que se configuraron anteriormente como el nombre de la base de datos, contraseña, usuario, etc para poder continuar con la instalación. Y a veces en este punto sale errores que tuvimos en la instalación

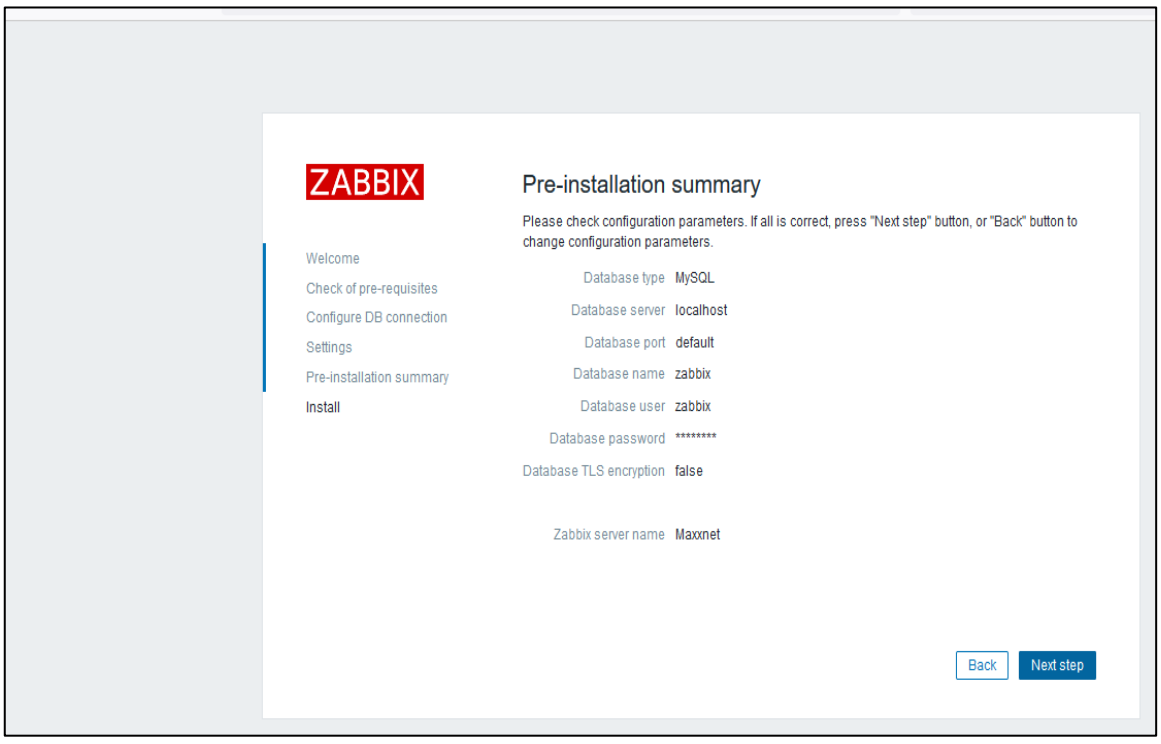


Ilustración 22-3: Resumen de la preinstalación de Zabbix

Realizado por: Toapanta, Ángel, 2023

3.3.6.5 Configuración exitosa de Zabbix

Siguiendo con la instalación para finalizar nos debe aparecer un mensaje donde nos explicas que la instalación fue exitosa, por lo cual procedemos a dar clic en finalizar y comenzar a las respectivas configuraciones de los host.

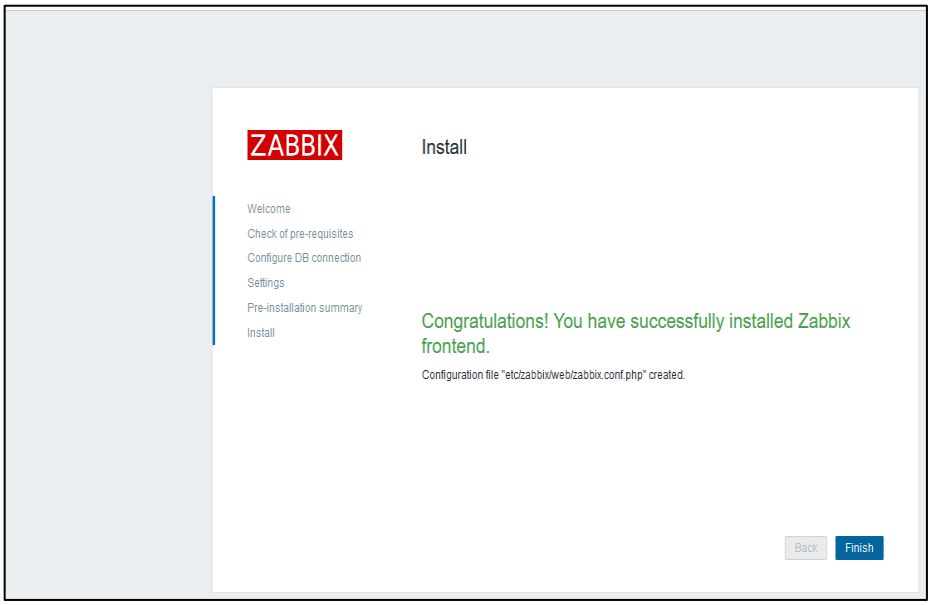


Ilustración 23-3: Instalación exitosa de la interfaz web de zabbix

Realizado por: Toapanta, Ángel, 2023

3.3.6.6 Inicio de sesión

Una vez finalizado la instalación nos redirigía a la página de logueo donde se abrirá automáticamente la interfaz de inicio de sesión para acceder a la interfaz web del servidor con nombre de usuario administrador Admin y la contraseña zabbix que viene por defecto.

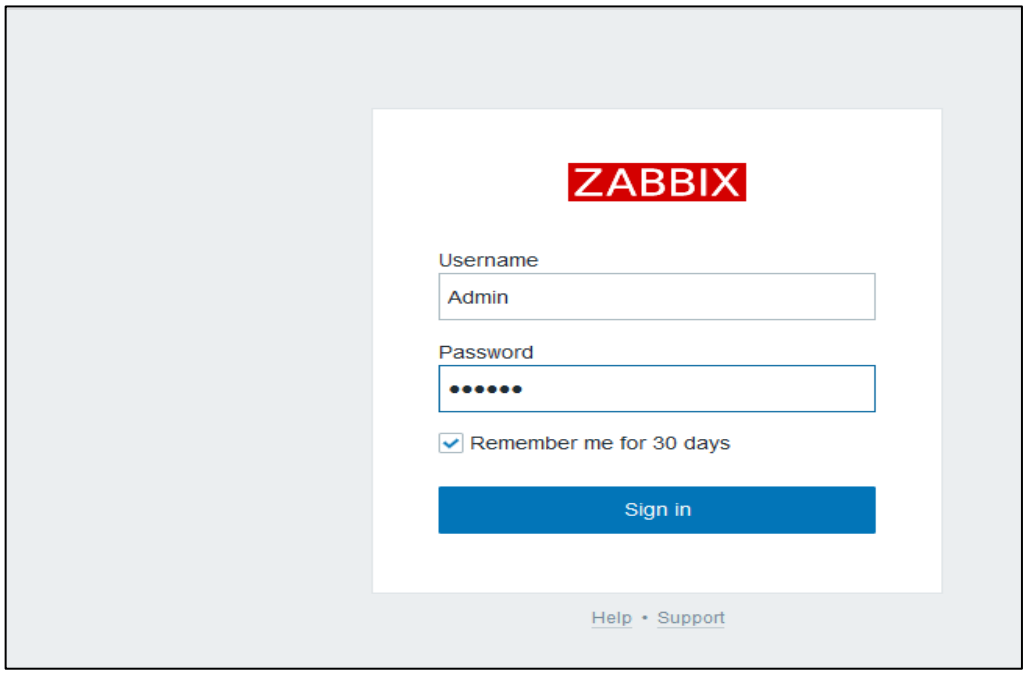


Ilustración 24-3: Interfaz de inicio de sesión

Realizado por: Toapanta, Ángel, 2023

3.3.6.7 Interfaz web del panel de control de Zabbix

Cuando ya nos identificamos para iniciar sesión mostrará la página principal de Zabbix, donde veremos varios parámetros como el sistema de información donde nos la información como Zabbix Server está funcionando correctamente (yes) con el puerto de conexión (10051), los host que están activado, los problemas y el panel de control donde nos muestra los componentes para el monitoreo de red.

Ilustración 25-3: El sistema de información de los parámetros y el panel de control

Realizado por: Toapanta, Ángel, 2023

3.3.7 Creación y configuración de un Host con SNMPv3

La creación de un Host nos permitirá a la integración de un equipo a zabbix para su eventual monitorización, pero importante con el protocolo SNMPv3 que está en este proyecto de tesis.

3.3.7.1 Creación host groups

En los pasos que se deben realizar es dirigirse al panel de control de Zabbix escoger la opción configuration, luego a host groups, en la parte derecha está la opción de créate groups damos clic y nos llevara a la interfaz donde nos va a pedir un nombre distintivo en este caso se nombró Prueba 1 para los router del Core y Clientes corporativos para los clientes que tiene un convenio más privilegiado en la empresa. Cabe recalcar que se hace grupos para tener una mejor administración al momento de las búsquedas de un dispositivo particular.

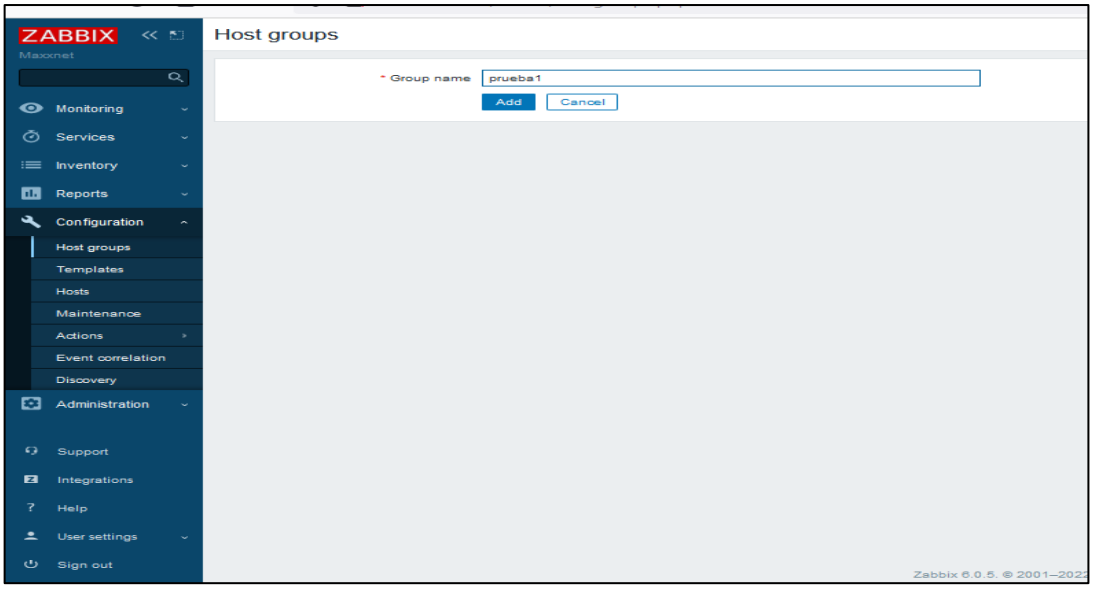


Ilustración 26-3: Creación del grupo prueba 1 para los equipos del Core

Realizado por: Toapanta, Ángel, 2023

3.3.7.2 Configuración del host

En esta parte nos dirigimos de nuevo a configuration donde escogeremos la opción de Host donde nos llevara a la interfaz donde se van a encontrar todos los host creados, en la parte superior derecha está la opción créate host donde daremos clic.

Mikrotik

Parte 1

La configuración del nuevo host debemos llenar los parámetros que nos pide:

- Host name: N Cacha; el nombre del router del cual se va a monitorear.
- Templates: En español se trata de planillas, para los requerimientos de la tesis hay dos formas la primera es usar este elemento que son utilizando Generic SNMP e Interfaces SNMP (a). El segundo de utilizar la plantilla exclusiva de Mikrotik.(b)
- Groups: escoger el grupo donde se va encontrar el dispositivo a monitorear.

Opción (a) donde se ocupa los templates Generic SNMP e Interface SNMP

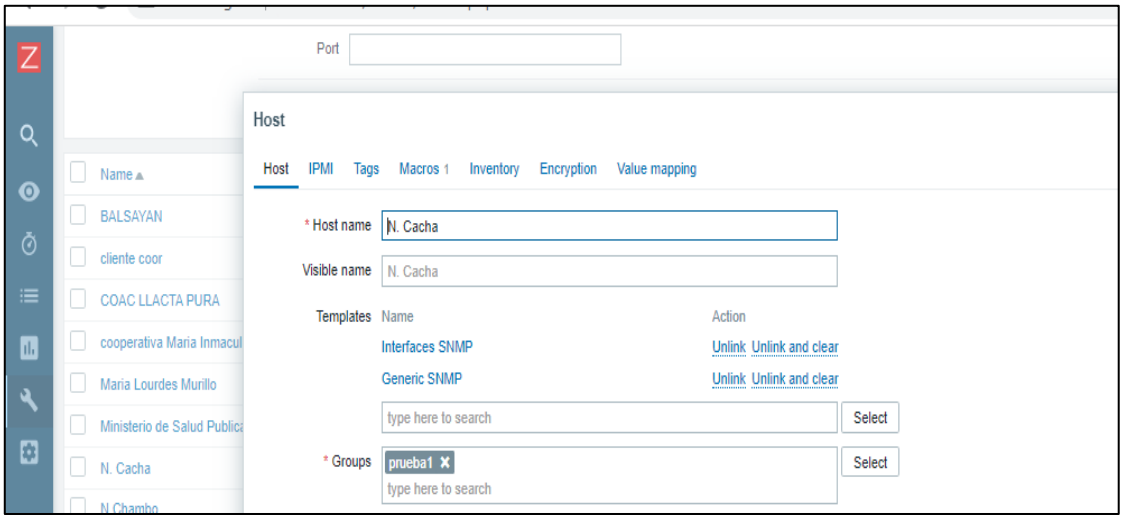


Ilustración 27-3: Configuración del nombre, Templates y grupos. (a)

Realizado por: Toapanta, Ángel, 2023

Opción (b) donde se ocupa los templates de Mikrotik.

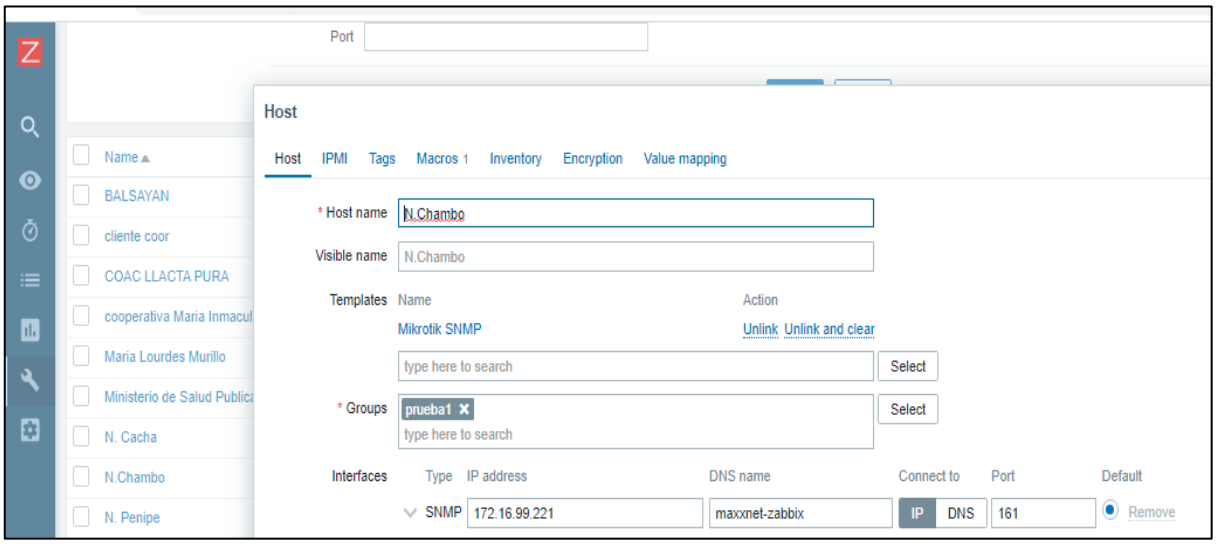


Ilustración 28-3: Configuración del nombre, Templates y grupos. (b)

Realizado por: Toapanta, Ángel, 2023

Cisco

Como vimos anterior debemos seguir los mismos pasos sugeridos, cabe mencionar que para zabbix versión 6.0 la plantilla anterior mente utilizada Generic SNMP no va a servir para los equipos Cisco Nexus 9000 en nuestro caso el equipo utilizado es un Cisco switch Nexus N9K-C93180YC-EX, lo cual incorporar la plantilla para que reconozca Zabbix, caso contrario no hay recolección de datos.

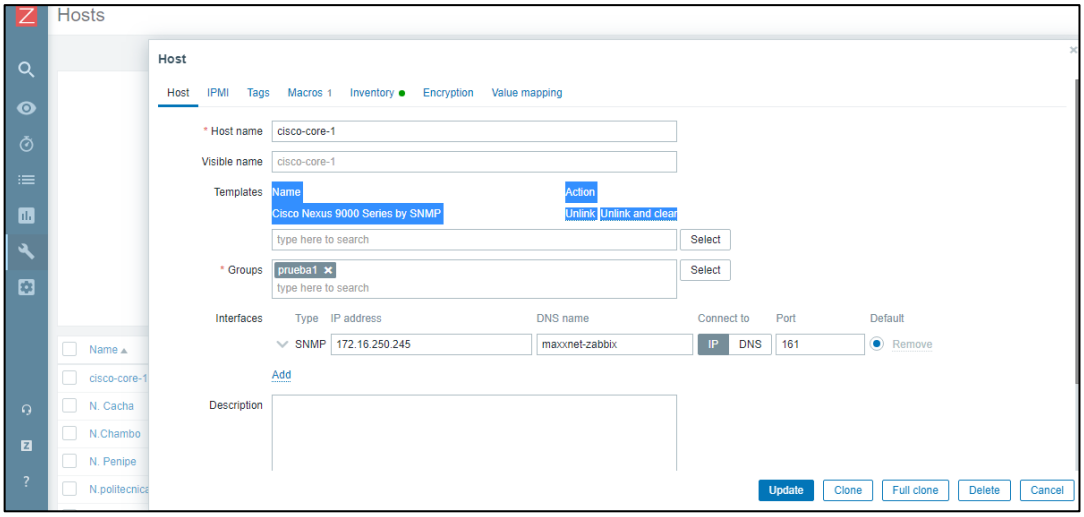


Ilustración 29-3: Configuración del nombre, Templates y grupos del N9K-C93180YC-EX

Realizado por: Toapanta, Ángel, 2023

Parte 2

En esta parte debemos conocer la IP del router a monitorear para empezar con la configuración, sabiendo que zabbix soporta SNMP(1,2,3) escogemos la 3 la cual nos va a desplegar una serie de campos que debemos llenar que son:

- Context name: Podemos utilizar el nombre de la Macro, que corresponde a la comunidad de SNMP
- Security name: de igual manera utilizaremos el nombre de la macro.
- Security level: este parámetro se puede escoger tres niveles de seguridad pero la que nos interesa es authPriv, donde nos garantiza tener una clave de autentificación y otra clave de encriptación.
- Authentication passphrase y Privacy passphrase: son claves que nos garantiza la conexión con el dispositivo con el protocolo SNMPv3 la cual mantendremos en secreto. Se recomienda que las contraseñas sean diferentes para mayor seguridad.

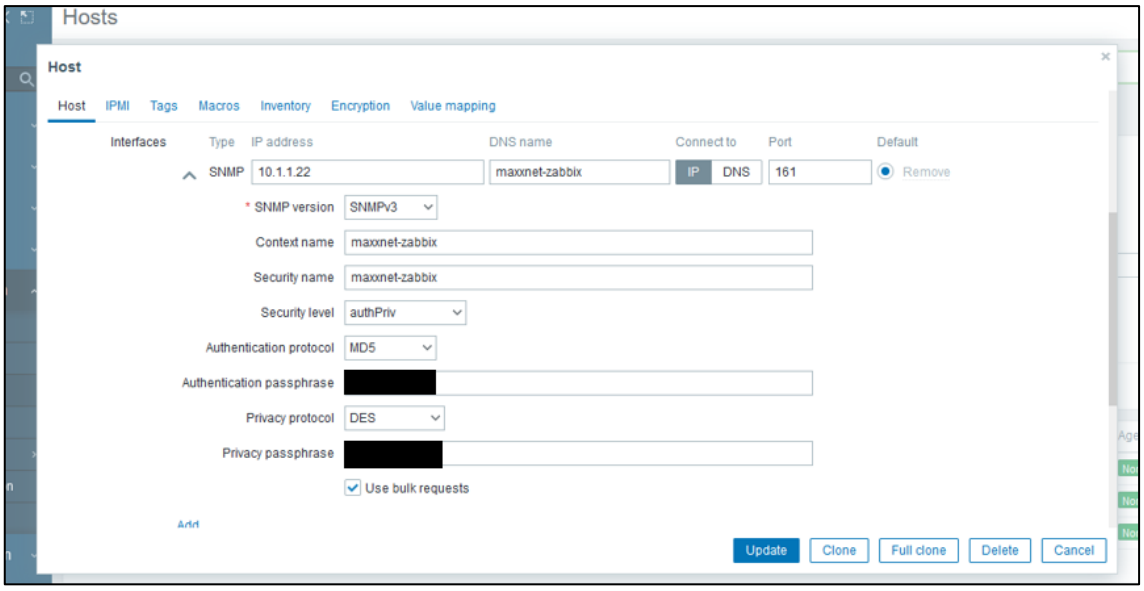


Ilustración 30-3: Configuración de la interfaz SNMPv3 del host

Realizado por: Toapanta, Ángel, 2023

Parte 3

Al momento de llenar los parámetros anteriores vamos en la parte superior donde está la opción Macros, para configurar el SNMP_COMMUNITY que fue creado en la herramienta de Winbox de mikrotik en el espacio de value agregamos el nombre creado que es Maxxnet-zabbix por conveniencia de la empresa, por último actualizamos para comenzar a monitorear.

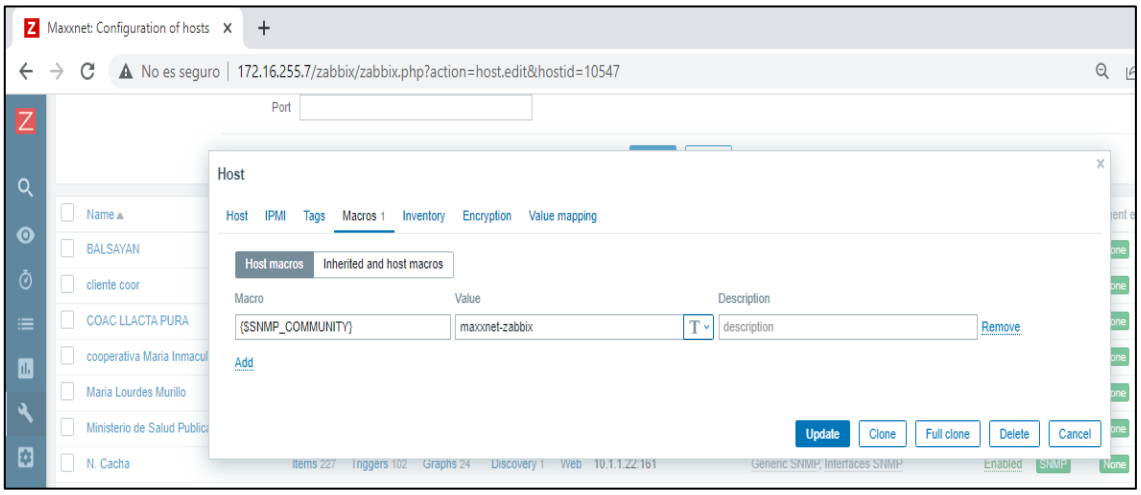


Ilustración 31-3: Configuración de la Macro SNMP COMMUNITY

Realizado por: Toapanta, Ángel, 2023

Para verificar que la configuración fue exitosa en la parte donde se encuentran los host hay un apartado en un recuadro con las letras SNMP que se deben poner de color verde lo cual nos indica que el sistema ya está monitoreando.

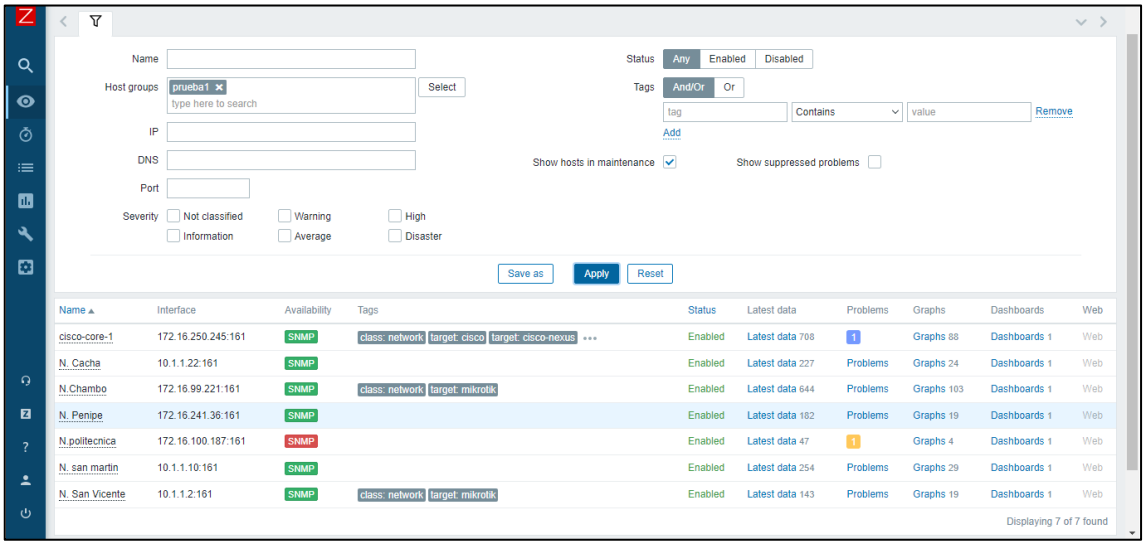


Ilustración 32-3: Dispositivos enganchados con SNMPv3

Realizado por: Toapanta, Ángel, 2023

3.3.8 Configuración SNMPv3 del router Mikrotik con Winbox

Una característica de los router Mikrotik es un ambiente amigable para el administrador para su configuración porque podemos utilizar la herramienta Winbox, que es una pequeña aplicación

que nos permite la administración de Mikrotik RouterOS usando una interfaz gráfica. Para acceder al router debemos tener tres importantes partes.

- La IP.
- Login, que es un nombre distintivo del equipo.
- Password, clave de seguridad.

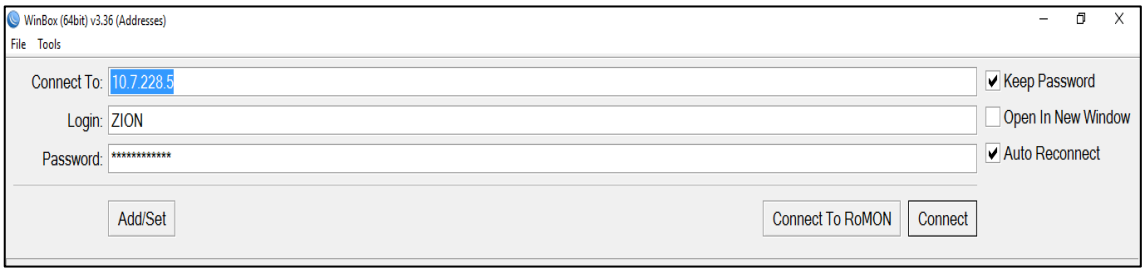


Ilustración 33-3: Credenciales del router mikrotik propiedad de Maxxnet

Realizado por: Toapanta, Ángel, 2023

Una vez inicializado winbox procedemos la configuración del protocolo SNMPv3 él nos dirigimos a la opción IP que está a la derecha, se va desplegar un serie de opciones pero la cual nos interesa es el apartado SNMP. Procedemos a habilítale el protocolo, lo primordial es crear la comunidad que es un parámetro importante en zabbix, en la comunidad definimos un nombre distintivo, una IP y el nivel de seguridad el cual nos exige poner la clave de autentificación y encriptación cabe recalcar que estas credenciales deben ser las misma que tiene zabbix para la conexión se exitosa. Después nos dirigimos en la parte de SNMP sittings donde debemos llenar los parámetros contact info, location que son opcionales.

El engine ID es un parámetro importante dependiendo de la situación si tiene uno solo con un nombre será suficiente para identificarse pero si son más de dos equipos de la misma marca el nombre debe ser diferente para cada router para evitar que el servidor se confunda en la recolección de datos.

Por último debemos escoger la versión SNMP, las trap generators y que interfaz nos interesa que nos comparta la información. En la Ilustración 34-3 siguiente muestra los parámetros que se configuraron.

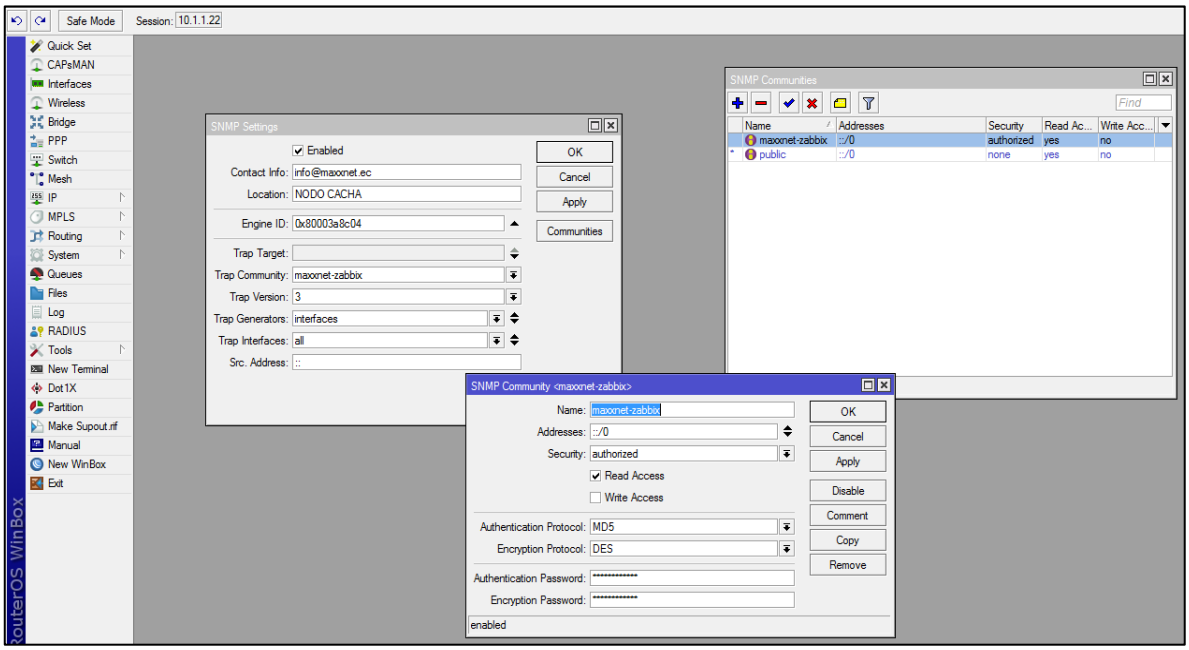


Ilustración 34-3: Configuración del router mikrotik con el protocolo SNMPv3.

Realizado por: Toapanta, Ángel, 2023

3.3.8 Configuración SNMPv3 del switch cisco Nexus N9K-C93180YC-EX

En el switch cisco es el corazón de toda la empresa Maxxnet Internet, el objetivo de administrar este equipo es para darle un monitoreo y tomar medidas necesarias para el funcionamiento correcto.

Ya que es el equipo Core las medidas de seguridad son importantes. Cisco da la ventaja de adminístrale por SNMPv3 el equipo es robustos y sus interfaces manejan grandes cantidades de datos por ende soporta con tráfico considerado.

La configuración del switch se hiso atreves de SSH, una vez inicializada la sección a través de comandos de cisco Nexus se crea la comunidad, el usuario y las respectivos accesos de control de autentificación como las de encriptación.

Los comandos que se utilizaron son:

- configure terminal
- snmp-server community public ro
- snmp-server user maxxnet-zabbix

- snmp-server user Maxxnet-zabbix auth sha (clave por defecto) priv aes-128 (clave por defecto)
- snmp-server host (ip del servidor) informs version 3 priv Maxxnet-zabbix
- snmp-server enable traps
- exit
- copy running-config startup-config

Y con estas credenciales podemos conectarnos con éxito al servidor zabbix para comenzar con el monitoreo.
Por defecto el equipo cisco va a mostrar la contraseña encriptada para mayor seguridad.

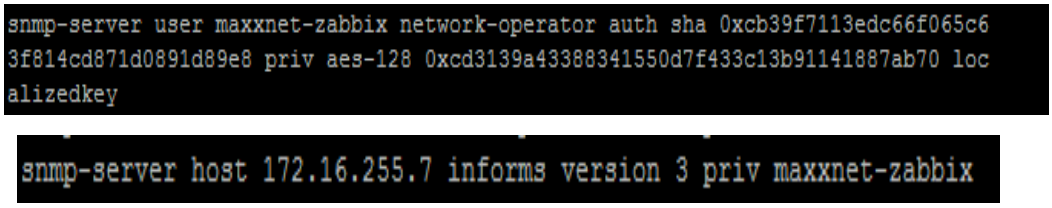


Ilustración 35-3: Configuración del switch cisco Nexus con el protocolo SNMPv3.
Realizado por: Toapanta, Ángel, 2023

3.3.9 Creación de notificaciones por telegram

Telegram es un servicio de mensajería instantánea y voz sobre IP basado principalmente nube. Zabbix 6.0 es posible integrar Telegram para un sistema de alarma de notificaciones sobre una plataforma de comunicación más sencilla. Esta aplicación nos ayudara a dar solución rápida sin estar en la estación de monitoreo, se divide en dos partes:

Parte 1: Interfaz de telegram

En esta parte buscamos el usuario BotFather, en Telegram, el propósito de BotFather es controlar a otros bots y crearlos por cuenta propia. Los comandos que debemos utilizar:

- /newbot: Creación de un nuevo bot
- Maxxnet__bot: Nombre del bot.
- Maxxnettesis_bot: Nombre de usuario.

Cuando ingresemos estos datos nos aparecerá el token que nos servirá para la programación de zabbix.

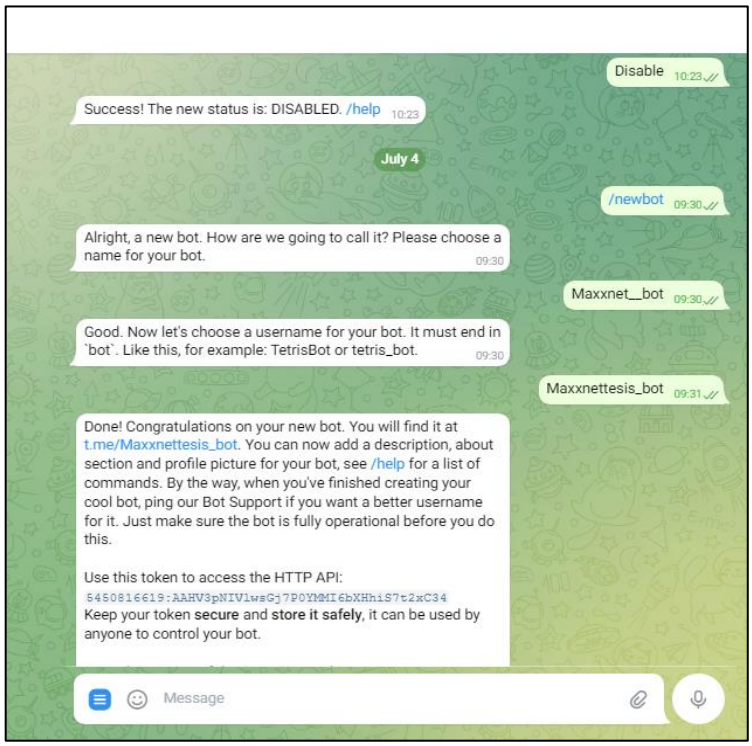


Ilustración 36-3: Generación del token para usar en zabbix.

Realizado por: Toapanta, Ángel, 2023

A continuación vamos a obtener el Your own ID que es el ID de chat del usuario el cual nos proporciona telegram con lo cual nos va ayudar que los mensajes generados de zabbix se envíen a telegram cuando se presente algún inconveniente.

Buscamos el usuario IDBot en telegram e ingresamos el comando:

- /getid

Ilustración 37-3: Obtención de your own ID

Realizado por: Toapanta, Ángel, 2023

Parte 2: Configuración de telegram en zabbix

Teniendo las credenciales de telegram vamos a la interfaz de zabbix, en la opción administración que ubicado en la parte izquierda de la pantalla, luego a la opción de Tipos de Medios nos cual nos dirigirá a una serie de plantillas donde estará Telegram.

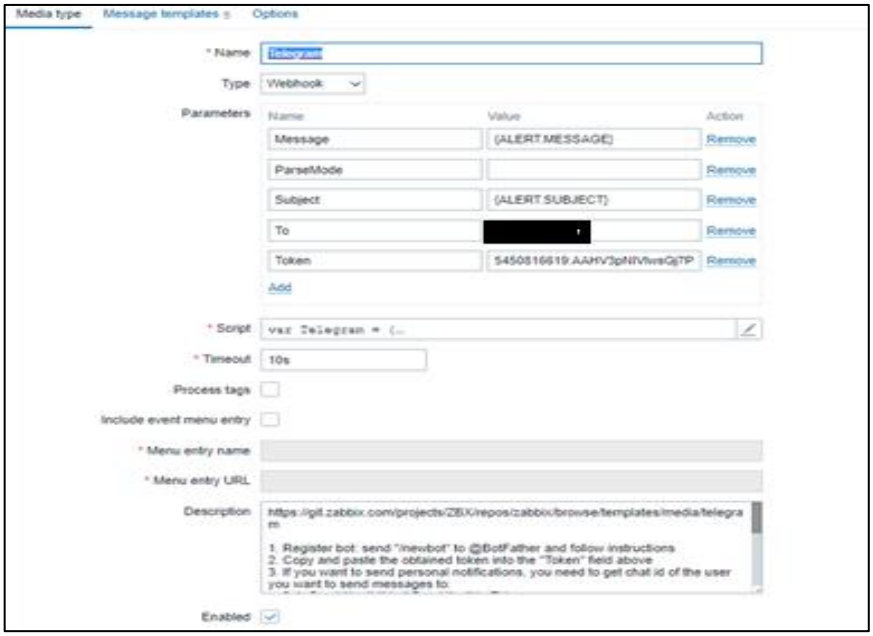


Ilustración 38-3: Configuración de Telegram para el sistema de alarma

Realizado por: Toapanta, Ángel, 2023

En esta parte nos vamos a enfocar en la parte del token el cual copiamos desde Telegram, para ubicarle en el aparatado de zabbix y también donde dice To en zabbix ubicamos el ID que nos proporcionó telegram anteriormente para que nos mande al mensaje y actualizamos para que se guarde los cambios.

Una rápida comprobación que el sistema funciona exitosamente es realizar un test el cual consiste en mandar un mensaje desde zabbix hacia telegram el cual solo debemos proporcionar el ID y el token.

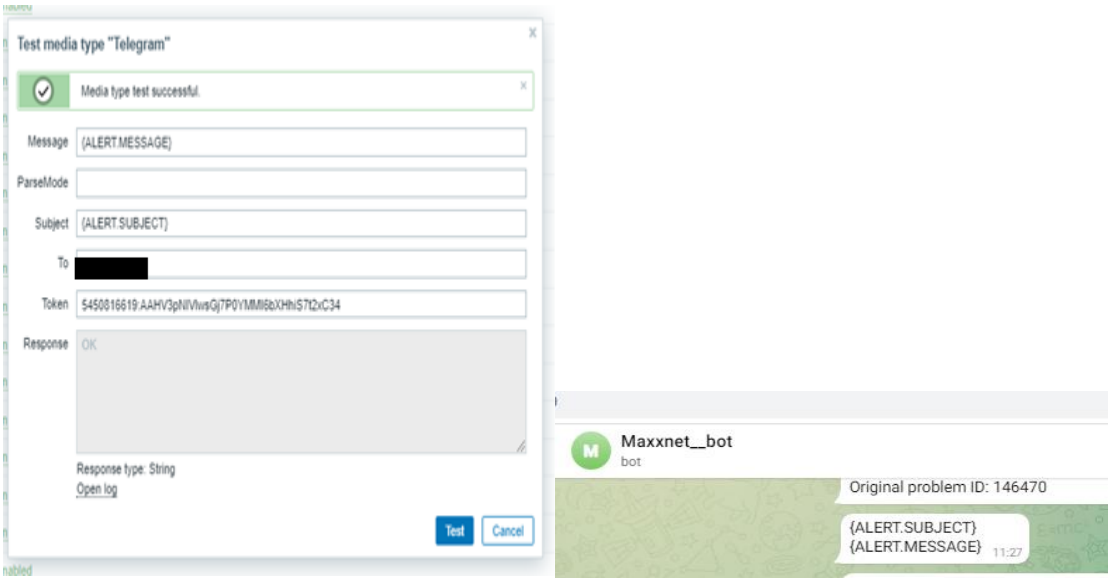


Ilustración 39-3: Prueba de conexión exitosa de zabbix hacia telegram.

Realizado por: Toapanta, Ángel, 2023

Por último configuraremos el usuario de Admin porque administra todos los host y el servidor para escoger la información que necesita las notificaciones. Por consiguiente vamos al apartado administración en la parte de User donde se abrirá una interfaz donde debemos aparecerá Admin como usuario damos clic.

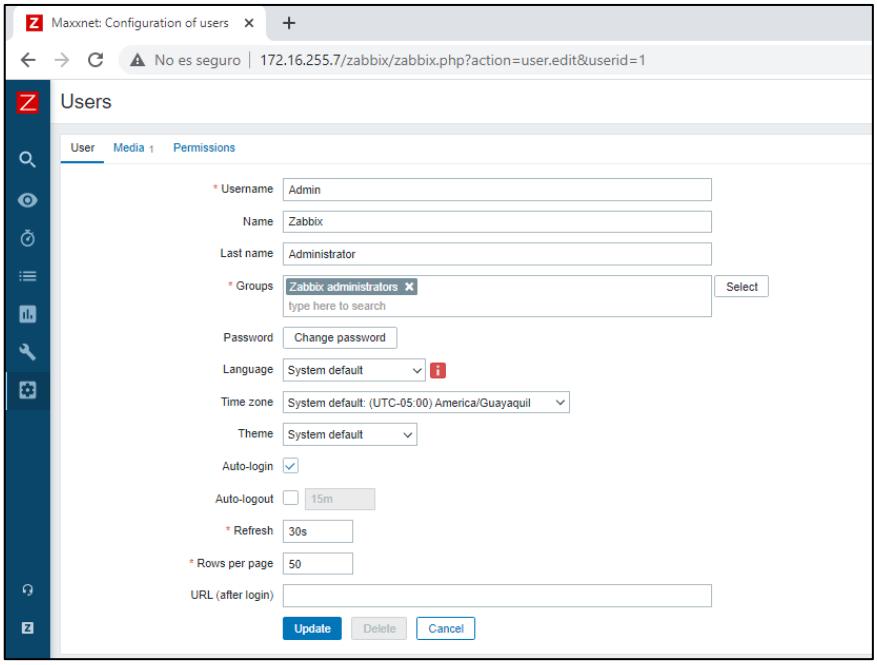


Ilustración 40-3: Configuración de User para las notificaciones de Telegram

Realizado por: Toapanta, Ángel, 2023

En esta página nos ubicaremos en la parte de Media donde debemos escoger la opción de Telegram para que se establezca la comunicación, debe tener ID para que nos pueda enviar los mensajes y estar habilitado. Actualizamos las configuraciones y zabbix nos comenzara el envió de las notificaciones.

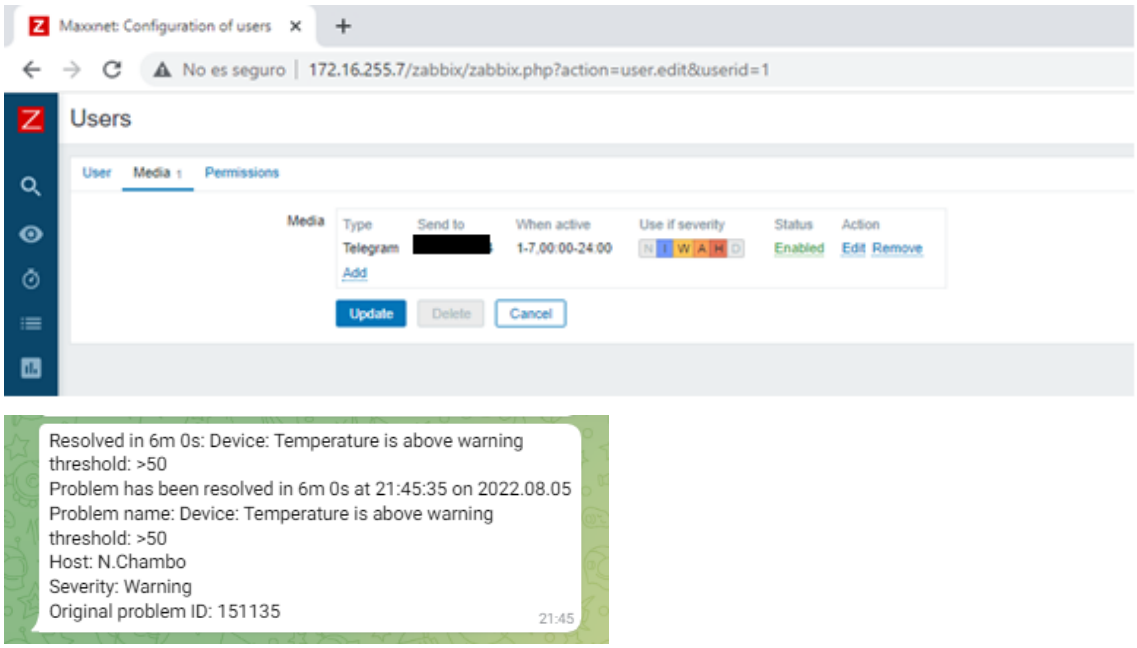


Ilustración 41-3: Comunicación exitosa entre Zabbix y Telegram para control en el sistema

Realizado por: Toapanta, Ángel, 2023

3.3.8 Creación de mapas

Una ventaja de zabbix es que tenemos la capacidad de creación de mapas para el mejor manejo de los router porque desde esa interfaz podemos dirigirnos a las configuraciones y gráficas rápidamente para un ahorro de tiempo.

En la parte del panel de control en el apartado monitory seleccionamos la opción Map que nos llevará a la interfaz donde nos aparecerá créate map en el cual se llena los datos necesarios como nombre map y aplicar cambios si requiere o puede dejar por defecto.

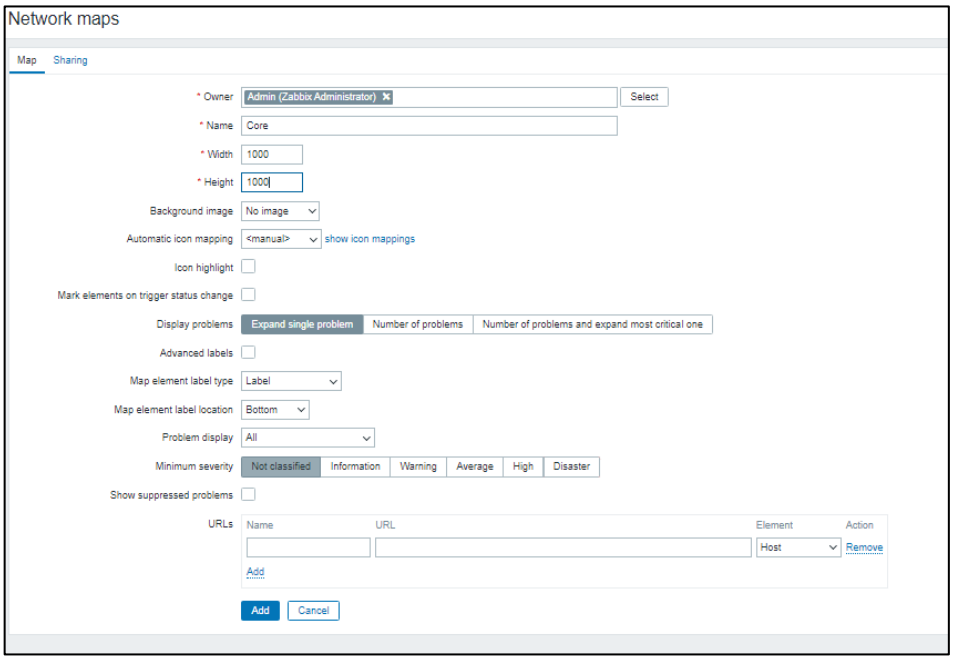


Ilustración 42-3: Creación de un nuevo mapa

Realizado por: Toapanta, Ángel, 2023

3.3.8.1 Creación de elementos

Después debemos ingresar al mapa recién creado en este caso se llama Core, vamos a la parte de edit map en el cual nos llevara a una interfaz vacía donde está lista para agregar elementos.
Nos dirigimos a apartado element add el cual nos permite agregar una gráfica que nos representara a un host y se arrastra hasta donde nosotros queremos colocar para que sea más rápido el trabajo de editar podemos copiar y pegar la gráfica.

Para unir los host a través de una línea debemos seleccionar a los host se debe seleccionar 2 a la vez y escogemos el aparatado link add, para dibujar la línea que simula la conexión.

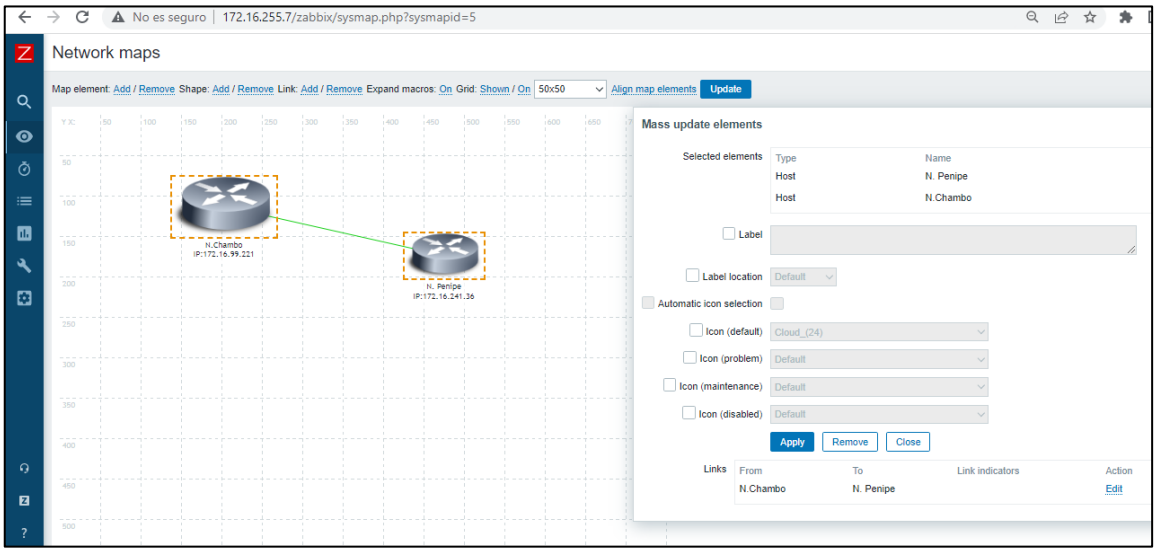


Ilustración 43-3: Conexión entre los router

Realizado por: Toapanta, Ángel, 2023

Configuración de equipos del mapa.

En la configuración del equipo debemos llenar varios parámetros:

- Type = host.
- Label= Nombre del equipo y IP.
- Host = Al equipo que queremos integrar al mapa.
- Icons= podemos seleccionar la gráfica que nos represente al equipo como un router.

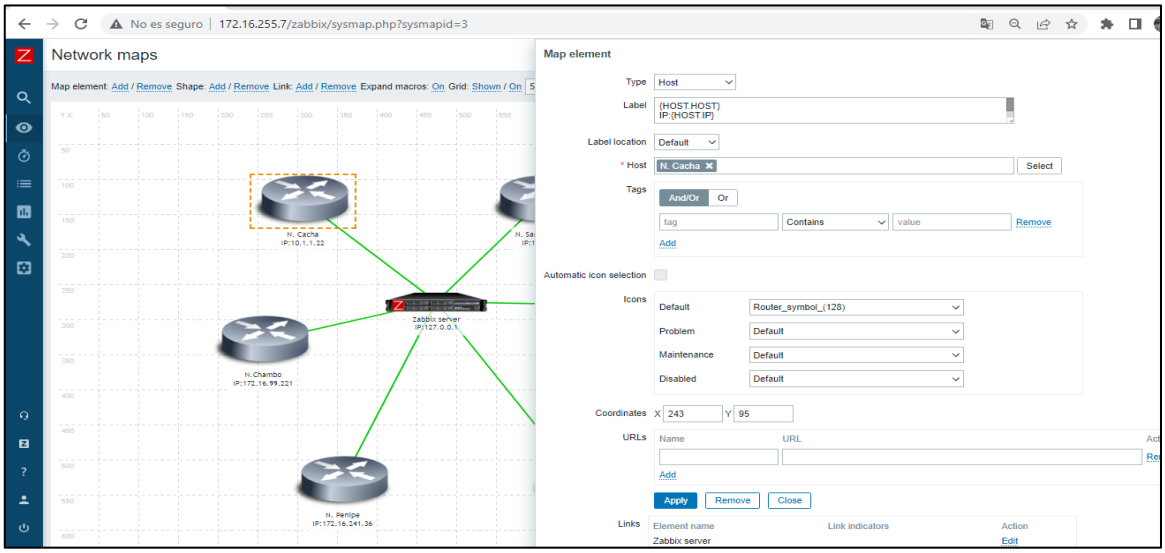


Ilustración 44-3: Configuraciones del router en el mapa

Realizado por: Toapanta, Ángel, 2023

3.3.8.2 Topología del mapa

Una vez configurado todos los Router y establecido la conexión, debemos guardar ante de salir, en cada router en la parte inferior mostraran la información que se les programo con un adicional que es un OK que significa que el equipo está trabajando con normalidad.

Ya que los router se encuentra en una parte centralizada la mejor representación es la topología en estrella donde el centro de acogida de los datos es el servidor de zabbix y en la periferia se encuentra los router del Core.

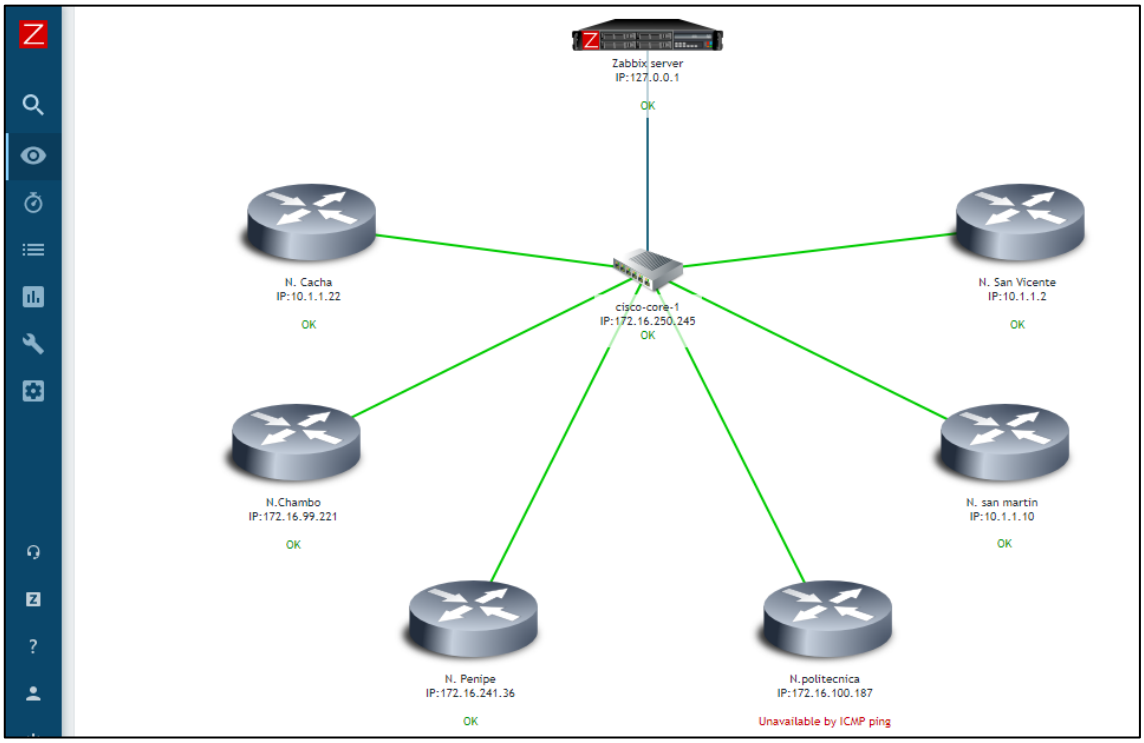


Ilustración 45-3: Representación de la topología del Core

Realizado por: Toapanta, Ángel, 2023

En este caso también el router que esta con un gran aporte es el equipo cisco que es el corazón de la empresa y debe tener enlazado los router de la periferia que son la gran mayoría mikrotik, ya que este equipo es muy versátil y económico a comparación de cisco.

Al momento de escoger un equipo zabbix le dirige a otra interfaz de su interés ya pueda ser los gráfico, configuraciones, historial y datos estadísticos.

3.4 Métodos que se implementaron en el desarrollo del proyecto

Se utilizará para este proyecto los siguientes métodos de investigación:

- **Método Deductivo**: como el proyecto se basa en una fase de investigación la comprensión de los conceptos, principios de funcionamiento, uso de tecnologías que son necesarios para la realización del proyecto.
- **Método Inductivo**: para un mejor entendimiento del protocolo SNMPv3 se debe investigar cómo funcionan las versiones anteriores y tener una mejor idea del comportamiento de la seguridad que ofrece el protocolo SNMPv3.
- **Método de Análisis**: Ya que para llegar a una solución, el sistema de monitoreo debe ser instalada correctamente y tener un historial donde conste el almacenado de datos para el desarrollo de graficas en zabbix.
- **Método estadístico**: En este proyecto se va a tomar la muestra del tiempo que ha estado activo el equipo, con el análisis determinar cualitativamente del porcentaje de efectividad y también se va a analizar las gráficas para un nivel de comparación.

3.5 Aspectos éticos

Los resultados de este trabajo de titulación son totalmente verídicos, Maxxnet Internet es una empresa seria que está laborando activamente en la ciudad de Riobamba y los datos que manejan son de gran utilidad para el servicio de internet que la empresa maneja.

CAPITULO IV

4. PROPUESTA TECNOLÓGICA

Este capítulo hablaremos de los resultados estadísticos del tiempo de disponibilidad que tienen los equipos desde que se inició hasta la última toma de datos utilizando variables arbitrarias para demostrar el tiempo de funcionamiento y así comparar con lo permitido por el ente de control ARCOTEL.

Otro parámetro importante es el uso de ancho de banda que tiene los equipos desde el inicio de operaciones hasta la última toma de datos gracias a Zabbix obtenemos graficas que nos muestre el estado real de uso por interfaces.

4.1 Equipos del CORE analizados

En la siguiente tabla representa algunos equipos que se trabajó del CORE de la empresa Maxxnet-Internet con el cual se basó este proyecto.

Tabla 1-4: Direcciones IP de los equipos administrados

NODO	**IP ADDRESS**
CHAMBO	172.--.--.221
CACHA	10. --.--.22
PENIPE	172. --.--.36
SAN VICENTE	10. --.--.2
POLITECNICA	172. --.--.167
SAN MARTIN	10. --.--.10
Cisco-Core-1	172. --.--.245

Realizado por: Toapanta, Ángel, 2023

Estos equipos que la empresa Maxxnet dio apertura para el estudio que están en operación y trabajando las 24 horas, los 7 días de la semana, por ende los resultados a continuación muestran el estado real del sistema.

4.2 Uptime and downtime

Para un proveedor de internet el tema de la disponibilidad es un punto muy crucial para su funcionamiento, zabbix ofrece gráficas y porcentajes para controlar este parámetro de cada router que esté conectado a su interfaz.

En esta fase del proyecto analizaremos cada nodo que corresponde a un router partiendo de tres graficas que nos muestra cuanto tiempo estaba disponible el servicio y un pequeño análisis matemático para comparar los datos obtenidos a través de zabbix.

4.2.1 Nodo Cacha

El router que se monitorea para el porcentaje de tiempo de disponibilidad de servicio (PDS), cuando el equipo está funcionando correctamente, utilizaremos un informe de disponibilidad (availability report) que nos ofrece zabbix para controlar este parámetro.

Primero es encontrar el host el cual queremos visualizar, con el disparador (trigger) UPTIME donde es un enlace a los últimos eventos ocurridos durante todo el tiempo que paso monitoreado el equipo, este enlace nos va a dar los datos como el tiempo estaba disponible y caído el sistema por algún problema.

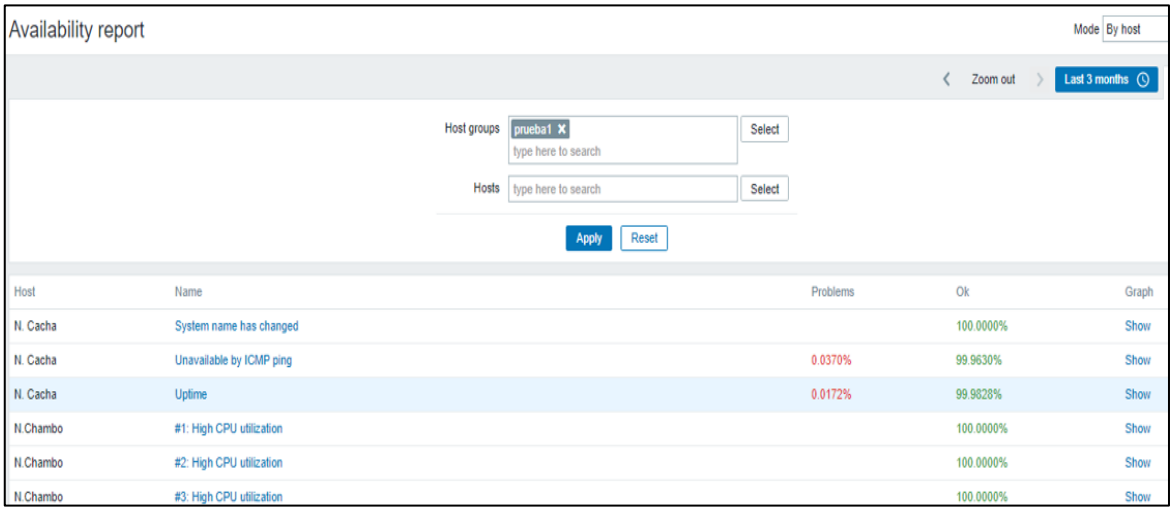


Ilustración 1-4: Disponibilidad y caída en porcentaje del equipo en el nodo Cacha

Realizado por: Toapanta, Ángel, 2023

Nos dirigimos a la opción show que esta opción se encuentra en la parte derecha donde nos representa un gráfico con la información de disponibilidad en formato de barra donde casa barra representa un periodo de 7 días.

En esta grafica se puede presentar con dos colores donde el tiempo de correcto esta de color verde y el color rojo es el tiempo donde tuvo problemas, en nuestro caso la caída del sistema (downtime) es muy pequeño el cual no se puede apreciar a simple vista.

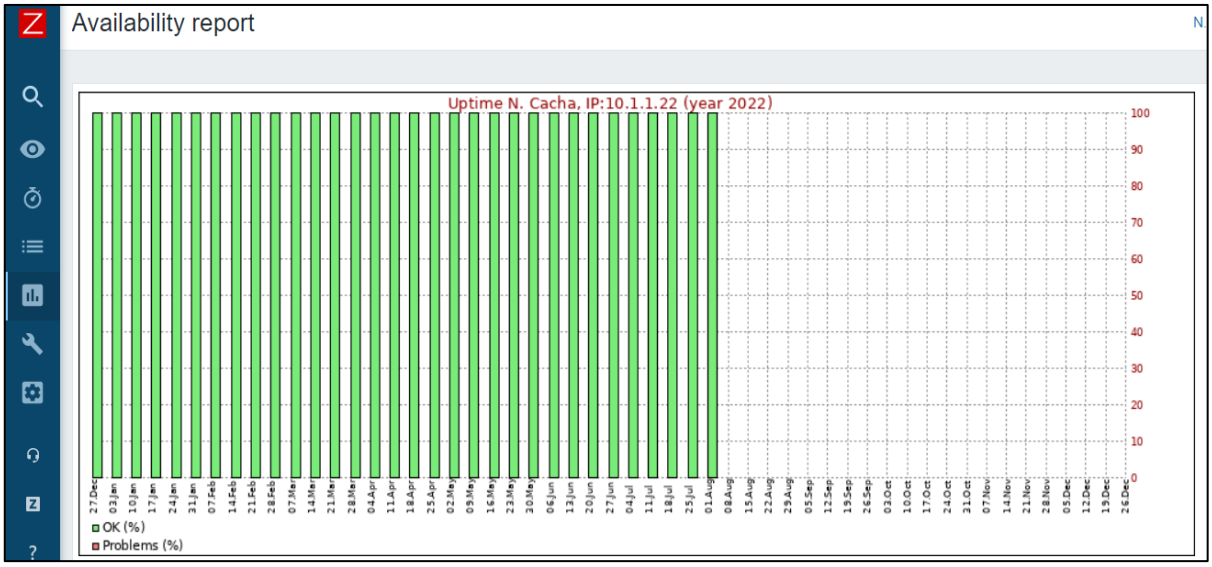


Ilustración 2-4: Disponibilidad del equipo representado en barras nodo Cacha

Realizado por: Toapanta, Ángel, 2023

Por último tenemos el grafico en forma lineal donde podemos visualizar el momento específico donde el sistema se cayó y el cuanto tiempo estuvo caído. En lo cual nos da una idea que el equipo monitoreado algo está pasando y que debe necesitar una inspección lo más pronto posible ya si se cae el servicio a varios usuarios poden quedar sin servicio de internet, o a sus ves estar más pendiente.

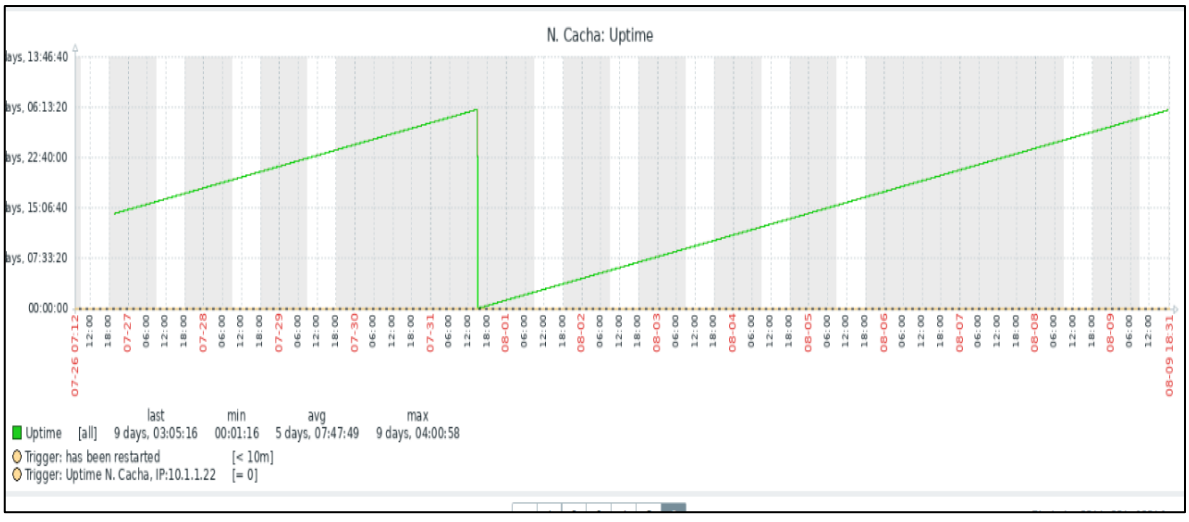


Ilustración 3-4: Disponibilidad del equipo en forma lineal nodo Cacha

Realizado por: Toapanta, Ángel, 2023

Comprobación matemática: Una forma de comprobar si el sistema está dando el porcentaje correcto es evaluar el tiempo (en segundos para mayor facilidad) el cual estuvo con problemas y restar con el tiempo que estuvo trabajando correctamente para sacar el porcentaje que se debe estar parecido a zabbix. [19]

TP= tiempo que tuvo problemas.
TTD= tiempo total de disponibilidad
PDS= porcentaje de disponibilidad del servicio.

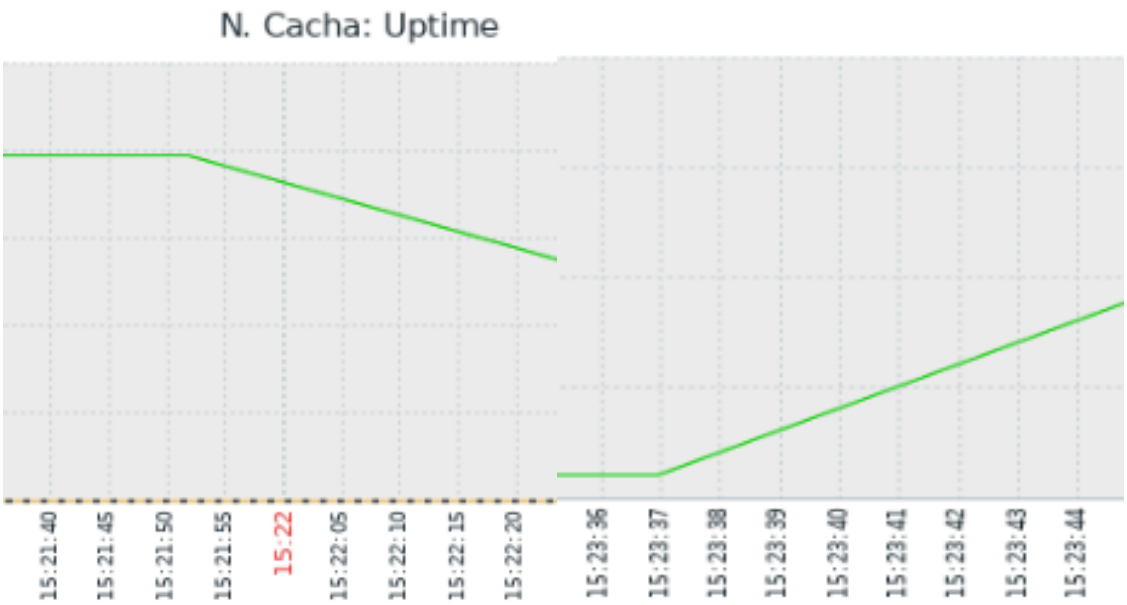


Ilustración 4-4: Tiempo exacto de caída/levantamiento del sistema
Realizado por: Toapanta, Ángel, 2023

Ti= 15:21:52 & Tf= 15:23:38 donde Ti=tiempo inicial, Tf= tiempo final.

$TP \approx Tf - Ti$ Ecuación 1

$$TP \approx 00:01:47 \text{ Anexo B}$$

$$TP \approx 108\ segundos$$

Para el tiempo total de disponibilidad de servicio se tomó la consideración cuando el sistema se levantó y hasta el último momento de la toma de datos que nos proporciona la Ilustración 4-4.

$$TTD \approx 13 dias, 14\ horas\ y\ 31 minutos$$

$$TTD \approx (13 * 24 * 3600)s + (14 * 3600)s + (31 * 60)s \text{ Ecuación 2}$$
$$TTD \approx 1175460\ segundos$$

El porcentaje de disponibilidad se realizaría con una regla de 3 donde TTD es el 100%

$$PDS = \frac{100\% * TP}{TTD}$$

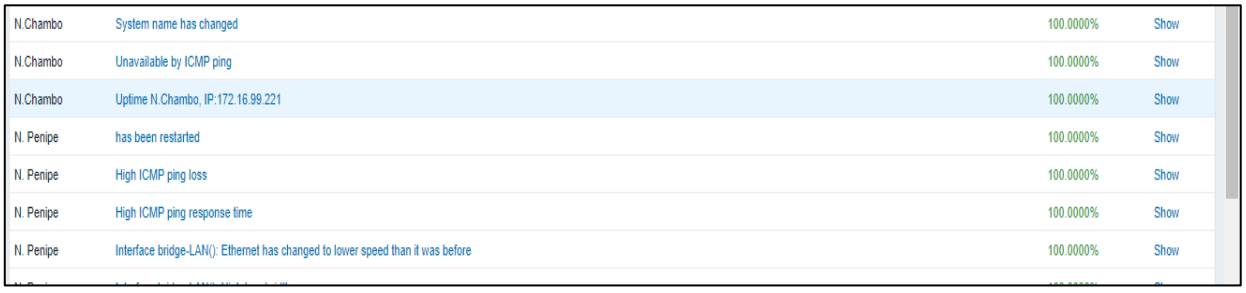
$$PDS \approx\ 99.99\%$$

Donde podemos observar que el porcentaje teórico se asemeja mucho con la información que nos proporciona zabbix en la Ilustración 5-4, nos va a salir exacto porque los datos se escogió solo viendo la gráfica, no se consideró el tiempo que se demora al estar 100 porciento funcionando y solo se tomó en cuenta este caso particular porque este router mikrotik muestra un extraño comportamiento que es software dude no pudo definir.

4.2.2 Nodo Chambo

Repetimos los mismo pasos anteriores donde primero buscamos el reporte donde está especificado el porcentaje de funcionamiento que zabbix en la parte superior se encuentra un buscador para mayor facilidad en el cual nos muestra todos los reportes que tiene el equipo.

A comparación del equipo anterior este a lo largo del tiempo que zabbix obtuvo datos no ha mostrado ninguna novedad cabe mencionar que este equipo es con fibra óptica que tiene casi 100 clientes según la información prestada por la empresa.



N.Chambo	System name has changed	100.0000%	Show
N.Chambo	Unavailable by ICMP ping	100.0000%	Show
N.Chambo	Uptime N.Chambo, IP:172.16.99.221	100.0000%	Show
N. Penipe	has been restarted	100.0000%	Show
N. Penipe	High ICMP ping loss	100.0000%	Show
N. Penipe	High ICMP ping response time	100.0000%	Show
N. Penipe	Interface bridge-LAN(): Ethernet has changed to lower speed than it was before	100.0000%	Show

Ilustración 5-4: Disponibilidad y caída en porcentaje del equipo en el nodo Chambo

Realizado por: Toapanta, Ángel, 2023

Después verificamos el grafico de barras que en este caso está funcionando exitosamente al 100 por ciento y no debe mostrar ningún porcentaje de la barra en rojo y también en la parte inferior esta un distintivo donde nos muestra un ok en color verde, problemas de color rojo.

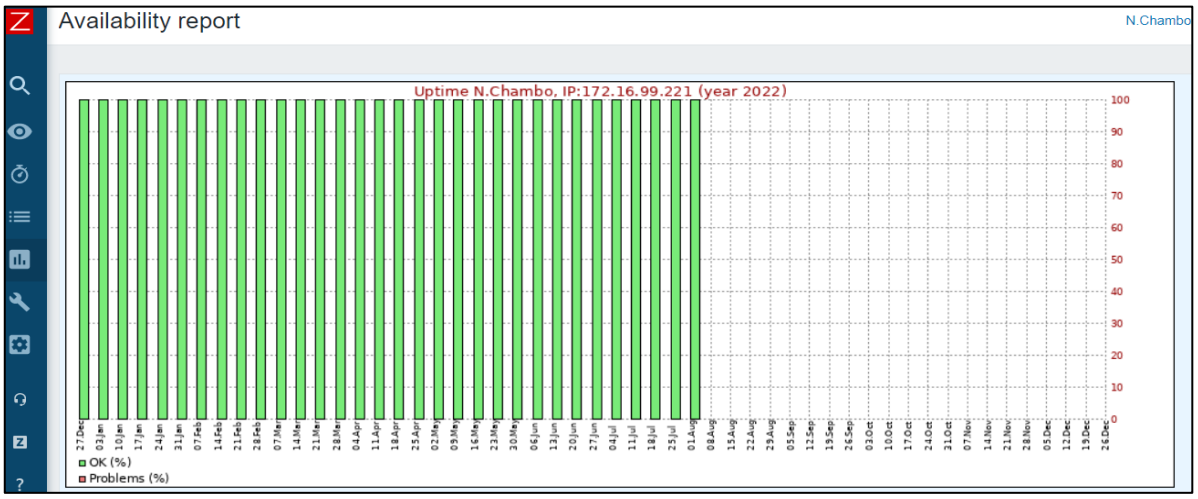


Ilustración 6-4: Disponibilidad del equipo representado en barras nodo Chambo

Realizado por: Toapanta, Ángel, 2023

Por último vemos que la gráfica de disponibilidad que está en forma lineal donde si funciona al 100 % no debe tener ninguna caída del servicio y debe ser continua cabe recalcar que los datos obtenidos anteriormente deben tener semejanza con la gráfica lineal.

La Ilustración 7-4 se encuentra en la interfaz del equipo en las últimas graficas que a mi parecer nos ayuda bastante en la búsqueda y ver el estado rápido de la disponibilidad.

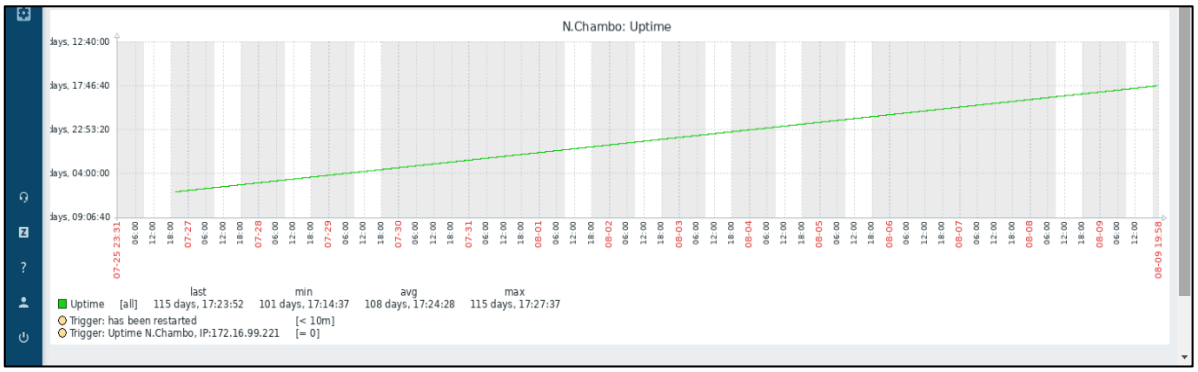


Ilustración 7-4: Disponibilidad del equipo en forma lineal nodo Cambo

Realizado por: Toapanta, Ángel, 2023

4.2.3 Nodo Penipe

Este router está funcionando al 100% que significa que no han presentado ninguna caída durante todo el tiempo que estaba monitoreada.

Así como anterior mente vimos una búsqueda del equipo facilita bastante para interactuar con la interfaz del equipo donde aparece de color verde el dato de 100%.

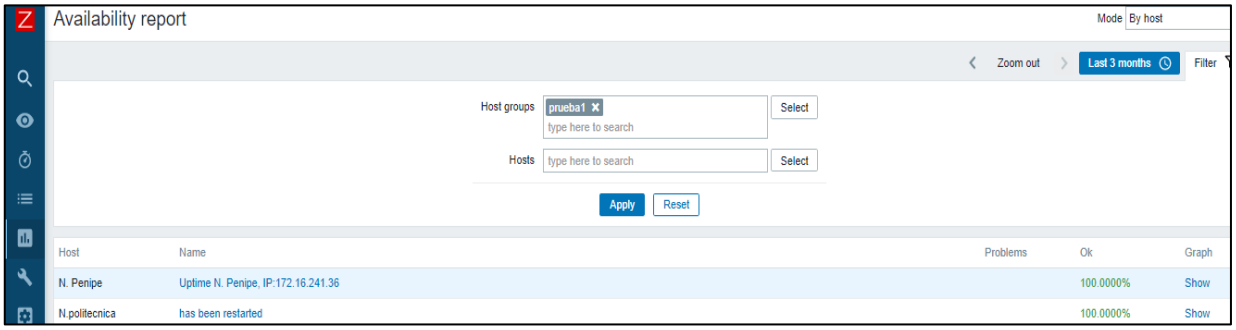


Ilustración 8-4: Disponibilidad y caída en porcentaje del equipo en el nodo Penipe

Realizado por: Toapanta, Ángel, 2023

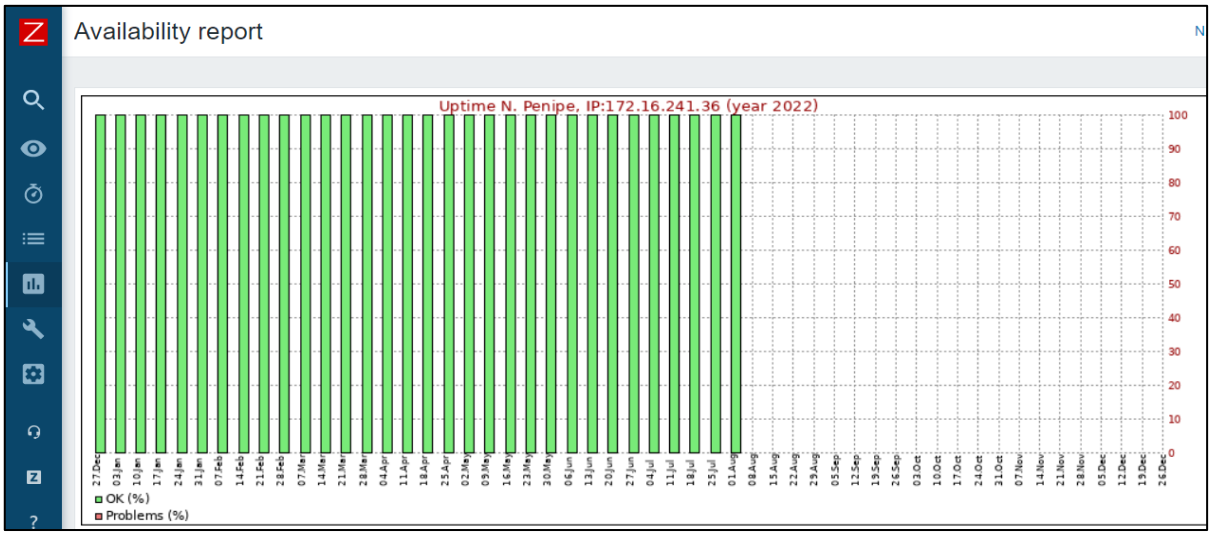


Ilustración 9-4: Disponibilidad del equipo representado en barras nodo Penipe

Realizado por: Toapanta, Ángel, 2023

El grafico lineal debe tener una semejanza de los datos anteriores es decir si está funcionando al 100% la gráfica lineal no debe presentar ninguna caída y en este caso también nos muestra desde que tiempo se levantó el servicio.

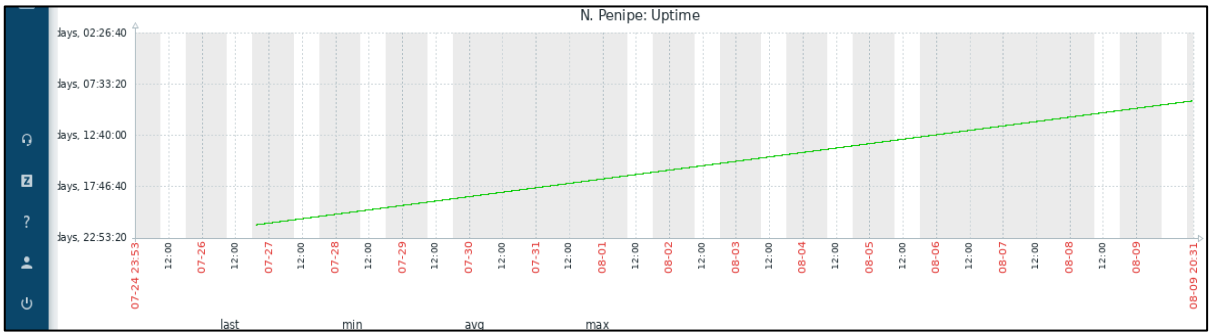


Ilustración 10-4: Disponibilidad del equipo en forma lineal nodo Penipe

Realizado por: Toapanta, Ángel, 2023

4.2.4 Nodo San Martin

Este equipo podemos observar que también están funcionando al 100% que significa que no han presentado ninguna caída durante todo el tiempo que estaba monitoreada. Que es una noticia buena ya que los clientes de ese nodo todo este periodo de tiempo tuvo el servicio de internet.

Ilustración 11-4: Disponibilidad y caída en porcentaje del equipo en el nodo San Martin

Realizado por: Toapanta, Ángel, 2023

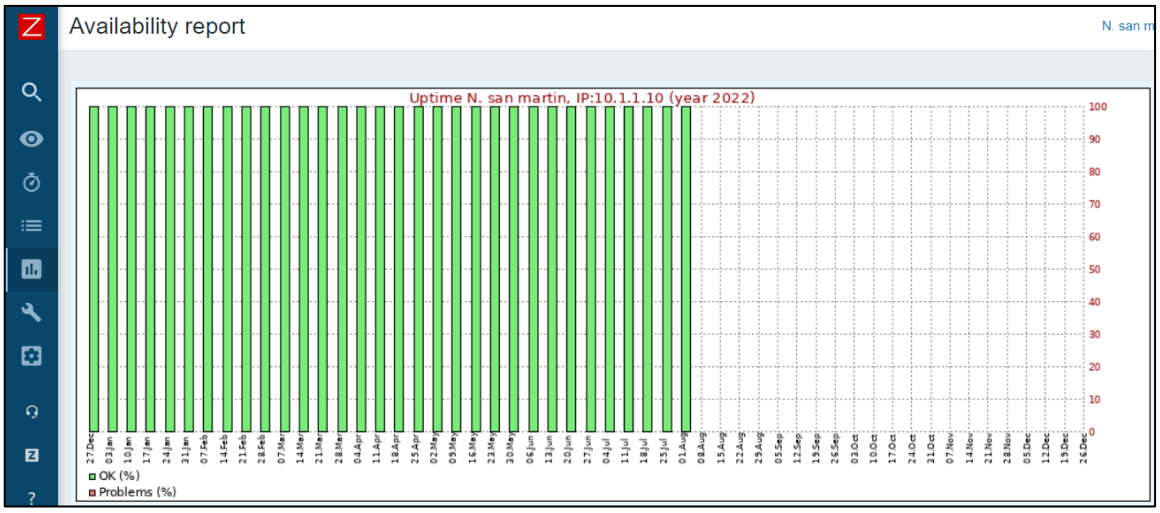


Ilustración 12-4: Disponibilidad del equipo representado en barras nodo San Martin

Realizado por: Toapanta, Ángel, 2023

El grafico lineal si está trabajando al 100% no debe presentar ninguna caída a lo largo del tiempo.

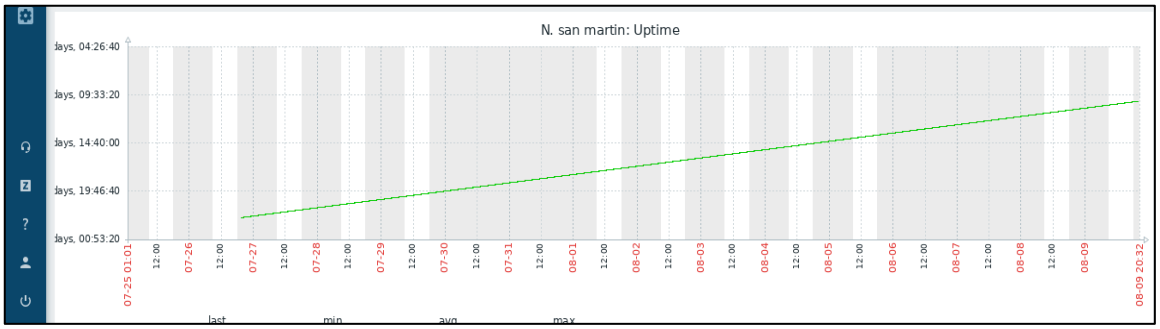


Ilustración 13-4: Disponibilidad del equipo en forma lineal San Martin

Realizado por: Toapanta, Ángel, 2023

4.2.5 Nodo San Vicente

Este router está funcionando al 100% que significa que no han presentado ninguna caída durante todo el tiempo que estaba monitoreada. Con una búsqueda del equipo podemos acceder al registro sin problemas.

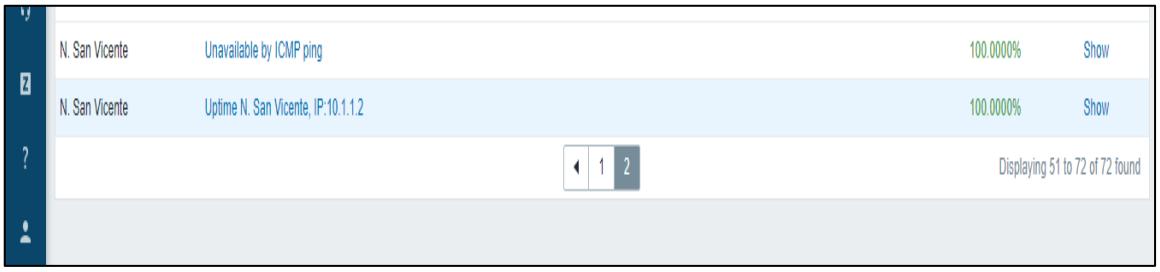


Ilustración 14-4: Disponibilidad y caída en porcentaje del equipo en el nodo San Vicente

Realizado por: Toapanta, Ángel, 2023

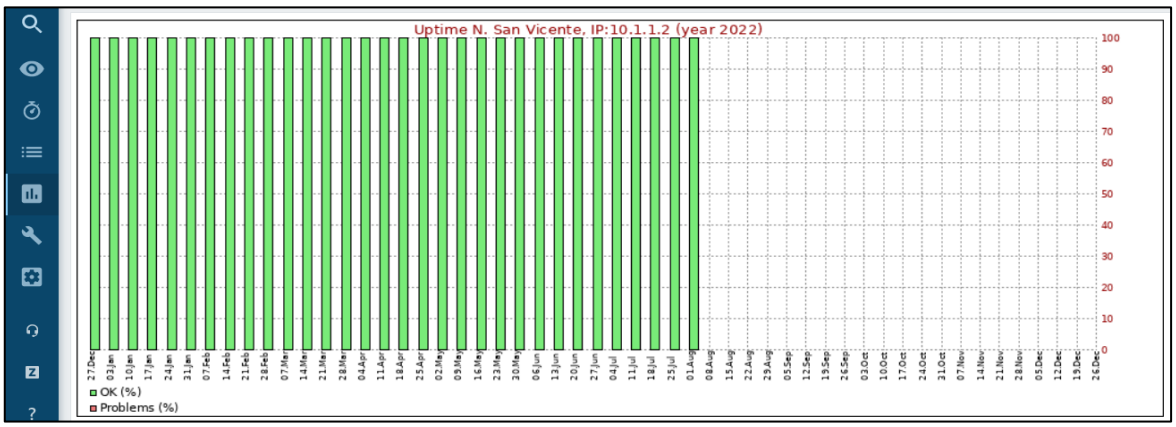


Ilustración 15-4: Disponibilidad del equipo representado en barras nodo San Vicente

Realizado por: Toapanta, Ángel, 2023

El grafico lineal si está trabajando al 100% no debe presentar ninguna caída a lo largo del tiempo. Y debe tener una semejanza con los demás datos obtenidos anteriormente.

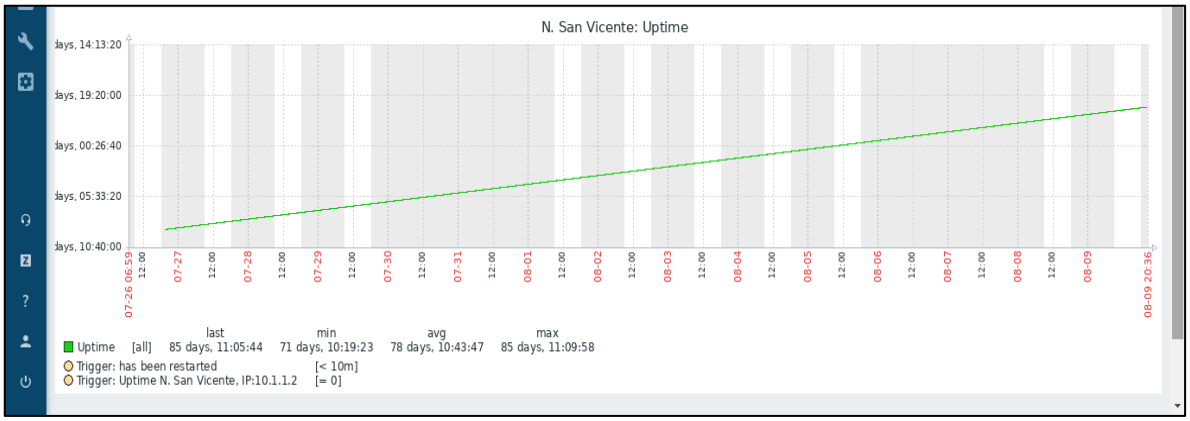


Ilustración 16-4: Disponibilidad del equipo en forma lineal San Vicente

Realizado por: Toapanta, Ángel, 2023

4.2.6 Nodo la Politécnica

Este nodo salió de operación por asunto de la gerencia de la empresa Maxxnet Internet, lo que podemos decir que zabbix guarda la información importante de este nodo dado el caso uptime no guarda la gráfica Ilustración 18-4, pero si guarda el informe hasta que tiempo estaba disponible como vemos en la Ilustración 17-4.

Ilustración 17-4: Disponibilidad del equipo representado en barras nodo Politécnica

Realizado por: Toapanta, Ángel, 2023

Como mencionamos antes el software no muestra el grafico porque ya pasaron varios días sin funcionar.

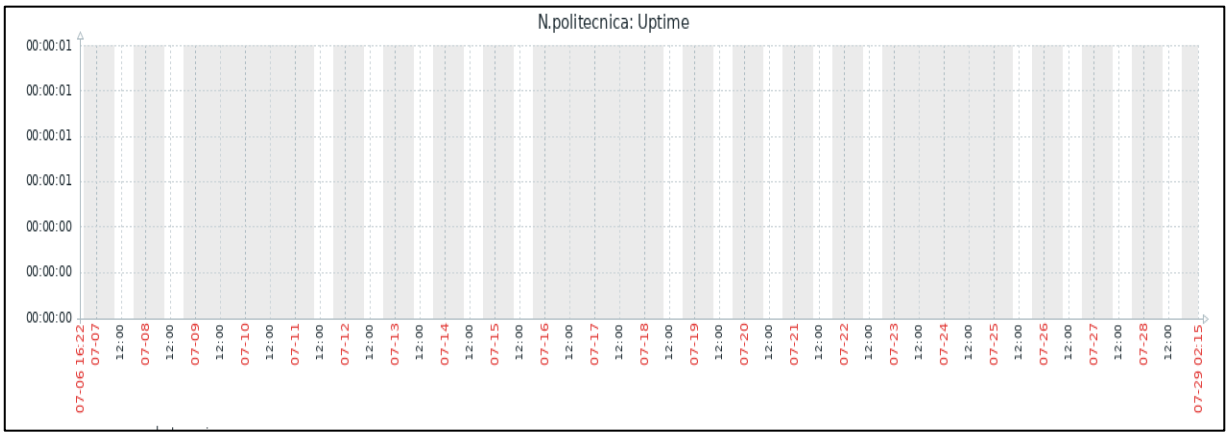


Ilustración 18-4: Disponibilidad del equipo en forma lineal nodo politécnica

Realizado por: Toapanta, Ángel, 2023

4.2.7 Cisco Core

El funcionamiento de este equipo depende bastante la empresa, el primer caso es el grafico donde se ubica la parte de porcentaje donde nos representa cuanto tiempo estuvo funcionando el sistema y la diferencia es cuánto tiempo está inactivo el equipo en otras palabra nos representa el UPTIME.

En la Ilustración 19-4 a lado derecho de la pantalla está el dato con números de color verdes.

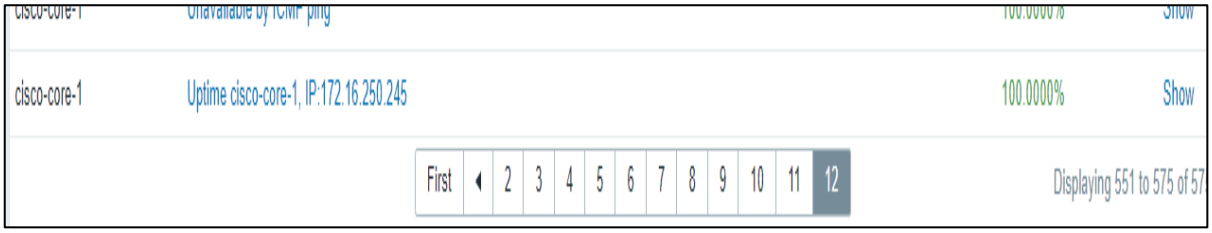


Ilustración 19-4: Disponibilidad y caída en porcentaje Cisco Core

Realizado por: Toapanta, Ángel, 2023

Otra forma de ver el estado es el grafico de barras donde nos muestra el rango de días que ha estado funcionando correctamente el Nexus.

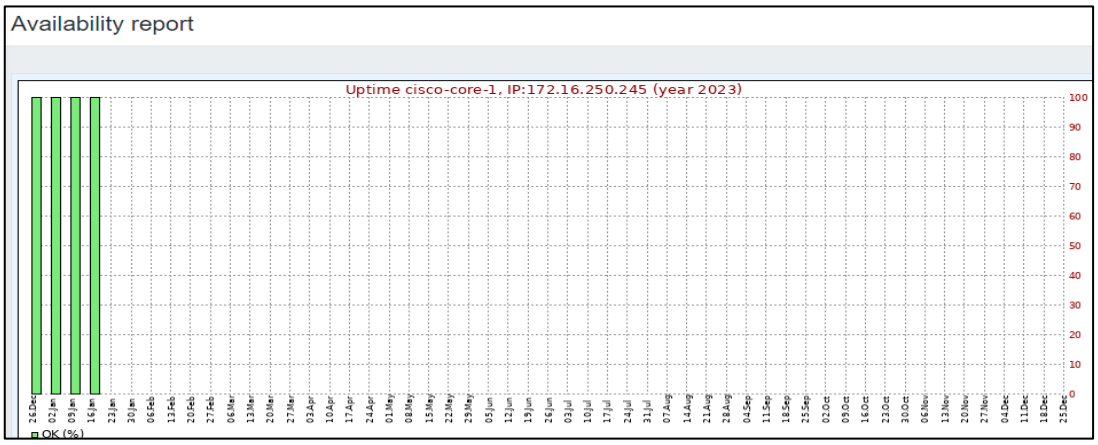


Ilustración 20-4: Disponibilidad del equipo representado en barras Cisco Core

Realizado por: Toapanta, Ángel, 2023

Por último el grafico de forma lineal es el más importante ya que él nos muestra el tiempo exacto de que día se levantó el sistema y que día se cayó el sistema con la hora exacta.

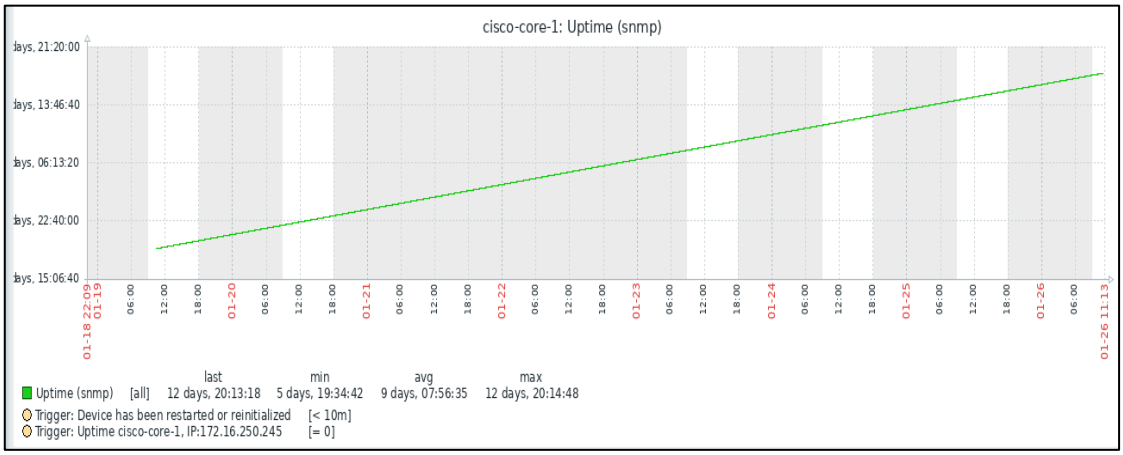


Ilustración 21-4: Disponibilidad del equipo en forma lineal Cisco Core

Realizado por: Toapanta, Ángel, 2023

Para concluir esta primera parte de la recolección de datos, los equipos que se ocuparon en este proyecto están en su mayoría están funcionando correctamente, el equipo de cacha presenta anomalías pero son un periodo de tiempo bastante bajo que puede ser por retrasos en los mensajes snmp que zabbix representa como caídas.

4.3 Análisis del Ancho de Banda

Para este proyecto un parámetro importante es el consumo del ancho de banda, el caso de zabbix es una herramienta muy útil y versátil ya que tenemos la opción visualizar el consumo del ancho de banda en tiempo real que tiene cada interfaz del equipo, al momento de vincular un host como un router el software reconoce al router y un aditivo adicional hace a la vez un descubrimiento de todas las interfaces que tiene el equipo.

Los equipos en estudio son equipos router mikrotik en operación que tienen en funcionamiento varios puertos por tal motivo solo vamos a visualizar una sola interfaz la cual nos representa el consumo del ancho de banda.

4.3.1 Nodo Cacha

El consumo del ancho de banda en el software zabbix viene expresado en dos parámetros del tráfico que son: los bits que manda el equipo, los bits que recibe el equipo dentro de la interfaz, al ver estos datos vemos unos picos donde el cual nos informa alto tráfico y también que en este caso el consumo se puede decir que es periódico.

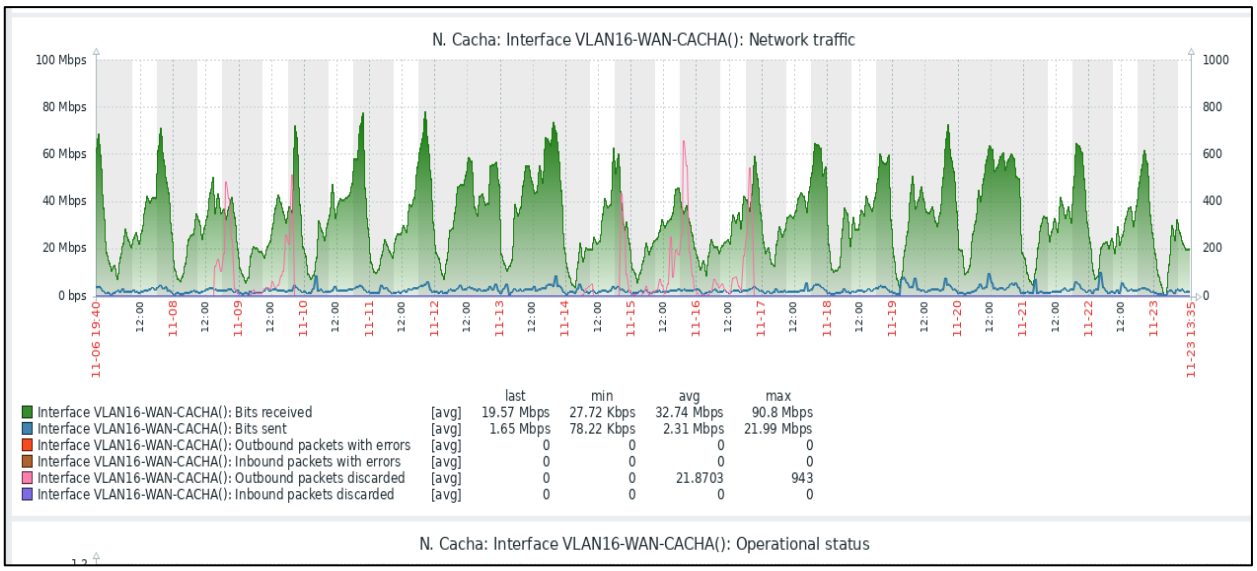


Ilustración 22-4: Consumo del ancho de banda en el nodo Cacha

Realizado por: Toapanta, Ángel, 2023

4.3.2 Nodo Chambo

El consumo del ancho de banda es más alto en este nodo ya que el tráfico también va a depender del número de clientes que este que este dentro de la interfaz, vamos a tener picos donde existe mayor tráfico.

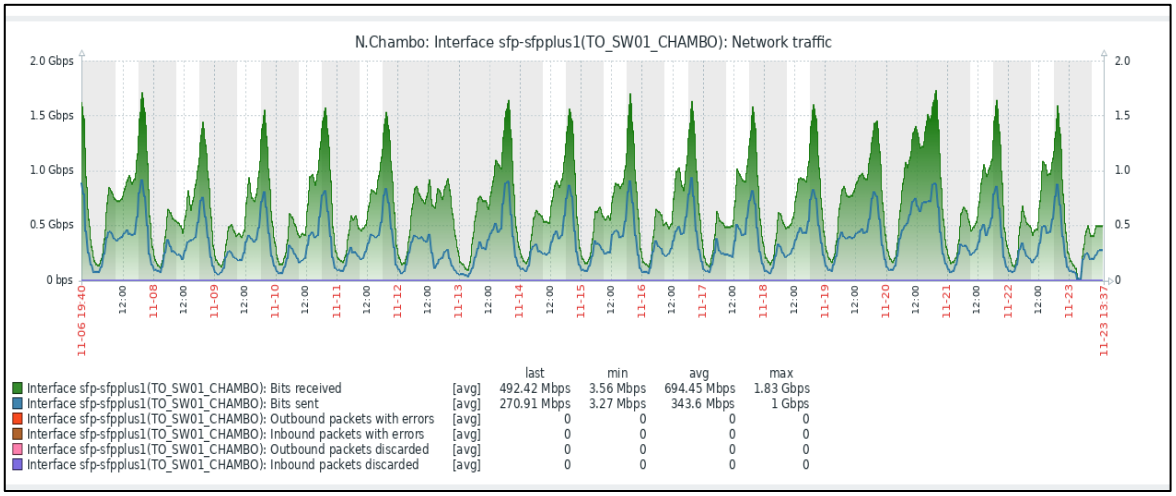


Ilustración 23-4: Consumo del ancho de banda en el nodo Cambo

Realizado por: Toapanta, Ángel, 2023

4.3.3 Nodo Penipe

En la Ilustración 24-4 no representa el tráfico existente en el ancho de banda que existe en la interfaz.

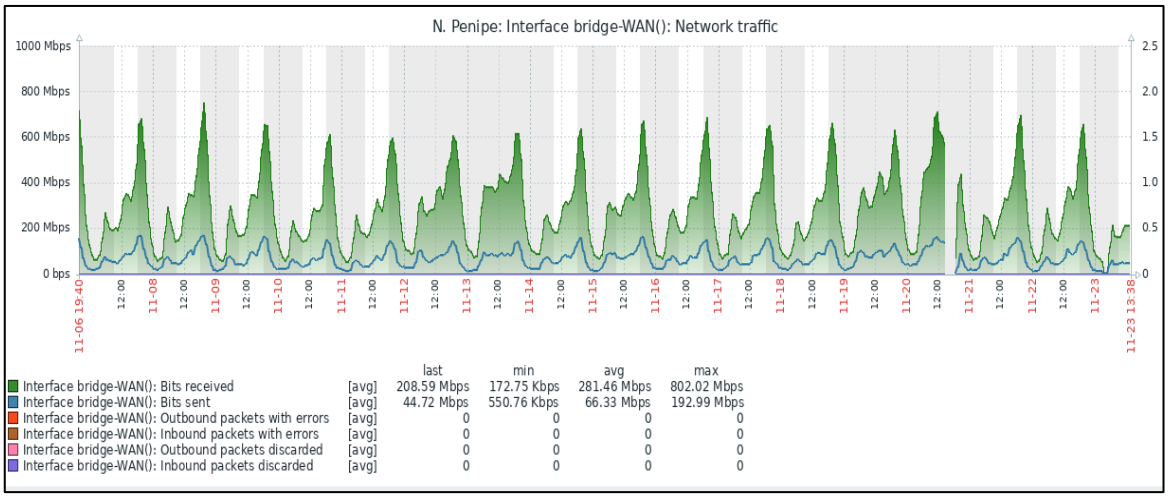


Ilustración 24-4: Consumo del ancho de banda en el nodo Penipe

Realizado por: Toapanta, Ángel, 2023

4.3.4 Nodo la Politécnica

Cabe recalcar que este nodo no está en operación por asuntos de gerencia pero para el caso de estudio se vio necesario explicar cómo el mismo zabbix sigue guardando la información pertinente de este nodo como los datos del tráfico que existió en esa instancia.

En la Ilustración 25-4 nos muestra hasta qué tiempo estuvo funcionando el sistema correctamente.

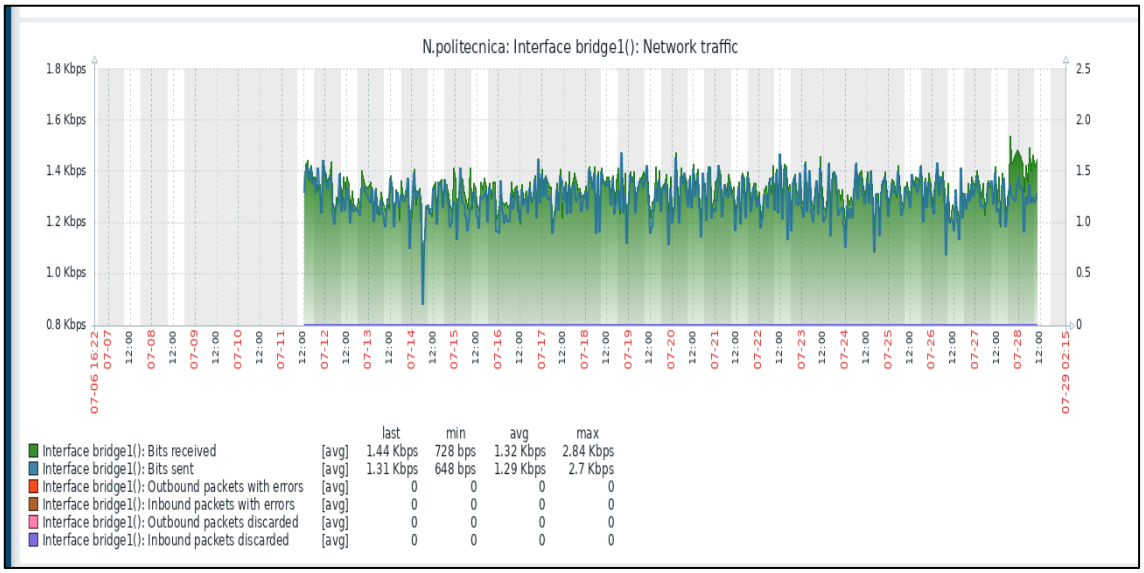


Ilustración 25-4: Consumo del ancho de banda en el nodo Politécnica

Realizado por: Toapanta, Ángel, 2023

4.3.5 Nodo San Martin

En Ilustración 26-4 nos representa el tráfico existente que tiene el nodo que también viene dado con los parámetros anteriormente explicados.

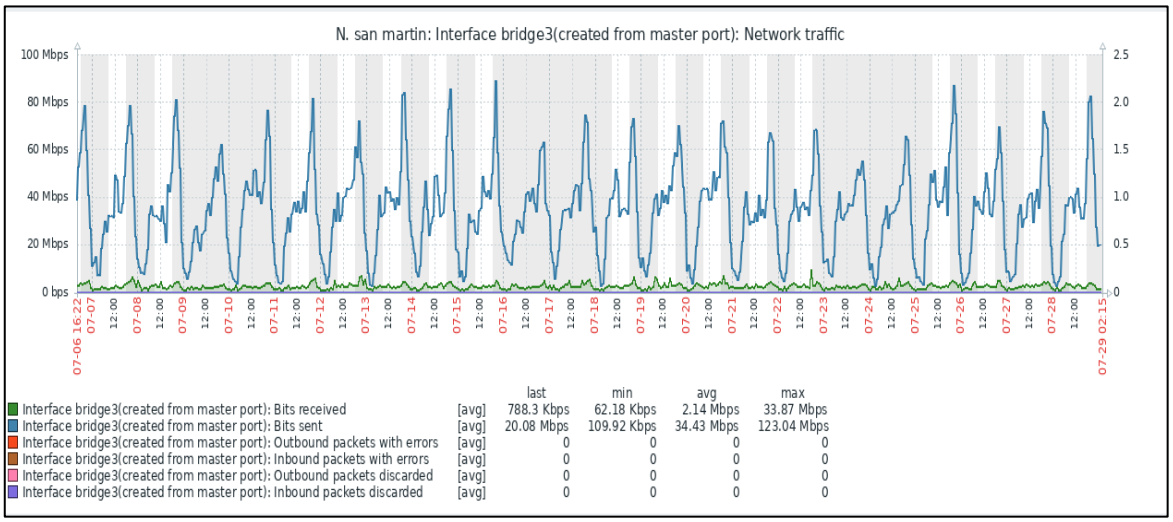


Ilustración 26-4: Consumo del ancho de banda en el nodo San Martin

Realizado por: Toapanta, Ángel, 2023

4.3.6 Nodo San Vicente

En la Ilustración 27-4 nos muestra picos de alto tráfico y cuanto tráfico tiene la interfaz, cabe mencionar que la gráfica viene dada con los dos parámetros de enviado y recibido de bits

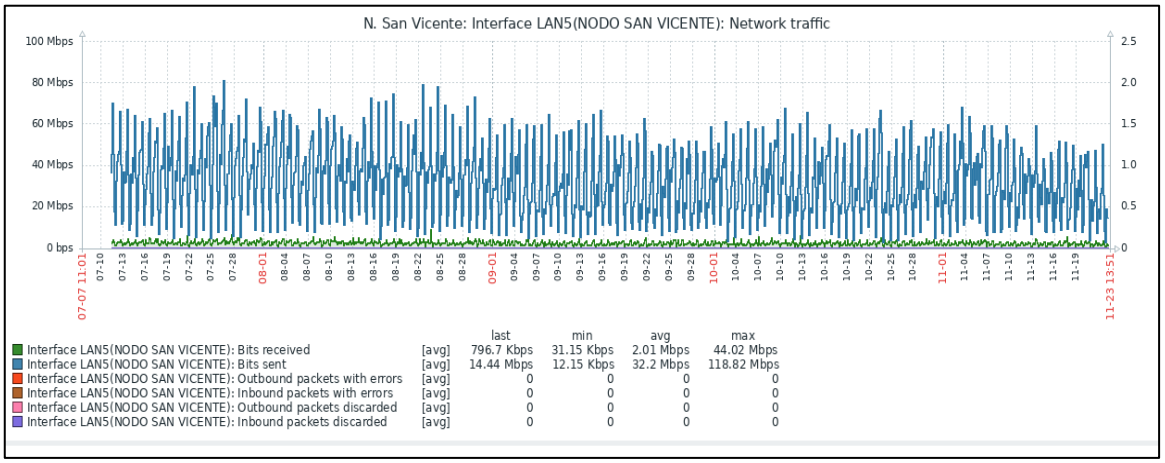


Ilustración 27-4: Consumo del ancho de banda en el nodo San Vicente

Realizado por: Toapanta, Ángel, 2023

El consumo del ancho de banda que tiene cada nodo del Core de la empresa Maxxnet Internet se puede visualizar los días y la hora del día que ha tenido mayor consumo, que están separados con números rojo para mayor facilidad.

4.3.7 Cisco Core

En este caso como el equipo tiene varias interfaz optaremos en visualizar el que tenga mayor consumo de tráfico, ya que en ese podemos visualizar los picos más altos que se encuentra en ese instante de tiempo.

En comparación de los demás equipos vemos que el consumo es mucho mayor ya que ese equipo maneja todas las interfaces de la red y es encargada de administrar las mismas.

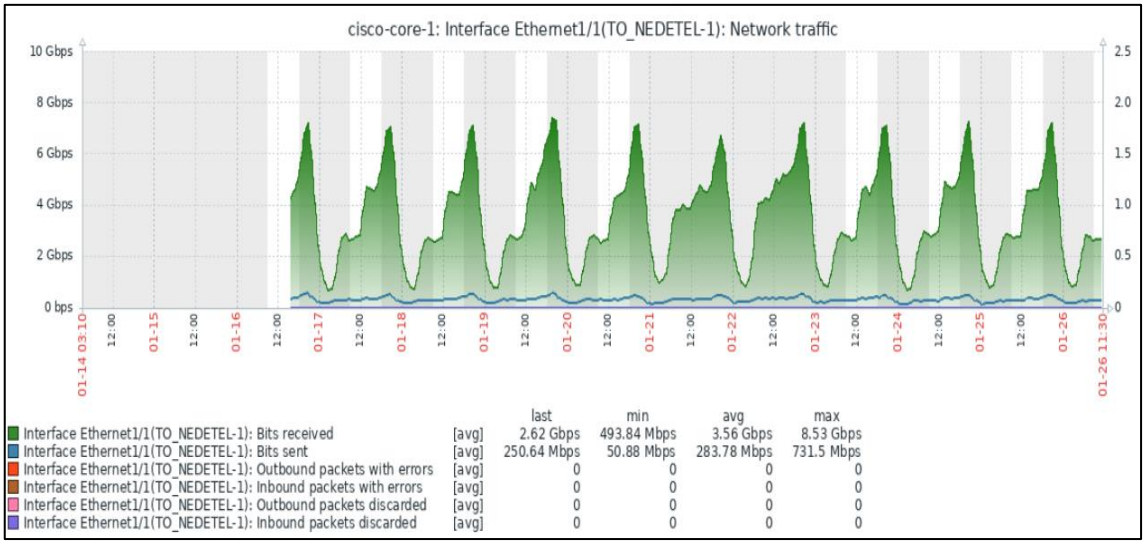


Ilustración 28-4: Consumo del ancho de banda del Cisco Core

Realizado por: Toapanta, Ángel, 2023

CONCLUSIONES

- El protocolo SNMPv3 nos da la ventaja de manejar la información de una forma modular y gestionar los datos mediante dos filtros que es la autentificación y la encriptación, para tener un control restringido de acceso mediante las políticas que maneja la empresa para evitar la suplantación de identidades o modificación de los mensajes que puedan alterar el funcionamiento de la red Core, por recomendación las claves de acceso sean robustas difícil de romper y solo las personas adecuadas tengan acceso.

- El software Zabbix es un sistema de monitoreo de redes Open Source que está diseñada para monitorizar a varios equipos como servidores, router, switch, cámaras, etc, de diferentes marcas pero lo más importante que los equipos soporte alguna versión (1,2,3) del protocolo SNMP, cabe mencionar que zabbix cuando utilice SNMPv3 solo abrirá un canal de comunicación con el equipo gestionado siempre y cuando tenga las claves de autentificación y encriptación para asegurar el sistema integral para no comprometer la información.

- La implementación del sistema de monitoreo en tiempo real se logró mediante la utilización de zabbix, gracias a las propiedades que brinda el programa como un diseño y configuración en la interfaz web amigable para el administrador para verificar el estado actual del equipo y como están esta los consumos del anchos de banda de cada interfaz con un aporte en materia de seguridad que es la utilización de SNMPv3 para garantizar un nivel óptimo de servicio para los clientes como rige el ente de control.

- Los resultados del diseño de monitoreo propuesto cumplieron en brindar información de los tres puntos que se base este proyecto en este caso son uptime o downtime y el consumo del ancho banda, que son puntos cruciales que pueden ayudar en dar un mejor diagnóstico de lo que está pasando con el equipo con el objetivo de tener un proceso de mantenimiento preventivo y satisfacer las necesidades de la empresa Maxxnet-Internet.

- Para concluir el sistema de monitoreo a través de Zabbix en la actualidad está trabajando 24/7 recolectando datos, alertando de los equipos que presentan alguna anormalidad que están en la red Core, cabe mencionar que el sistema está en ejecución y cumple con su propósito de impartir información del equipo.

RECOMENDACIONES

- Como es un caso real se recomienda que hagamos una etapa de prueba en ambientes controlados por ejemplo utilizando máquinas virtuales para familiarizarse con las configuraciones tanto en el servidor como en la interfaz web.

- Si está trabajando con zabbix los expertos recomiendan utilizar las últimas versiones liberadas de la página oficial ya que esas instancias se encuentran modificaciones en la integración de equipos que hacían falta en versiones anteriores por ejemplo para el cisco N9K-C93180YC-EX solo existen plantillas para la versión 6.4.

- Antes de programar un equipo se debe asegurar que tenga todos los permisos de acceso SNMP y conexión local entre ambos es decir que se reconozcan entre sí mediante un ping icmp.

- Una gran ayuda en este proyecto es verificar con programas auxiliares la conectividad snmpv3 con los equipos hacia el servidor que es SNMPWALK para determinar qué lado estaba dando error.

- Para los equipos que estén funcionando y dando servicio la configuración se debe realizar con cautela y verificando que la información que se administro sea la correcta ya que un mal comando puede que el equipo se mande a reiniciar.

- Para los error en la utilización de zabbix se recomienda pedir ayuda a la comunidad ya que ellos pueden dar diferentes puntos de vista y así resolver el problema rápidamente, también zabbix tiene una vasta información en internet de casos parecidos en errores que pueden ayudar para los proyectos.

BIBLIOGRAFÍA

A CRESPATA, R. Analisis del Protocolo SNMPv3 para el desarrollo en un Prototipo de Monitoreo de red segura [en línea] (Trabajo de Titulación). Escuela Superior Politécnica de Chimborazo, Riobamba, Ecuador. 2012. [Consulta: 08 octubre 2022]. Disponible en: https://1library.co/document/q7wx97oz-analisis-protocolo-snmpv-desarrollo-prototipo-monitoreo-red-segura.html.

CISCO NETWORKING ACADEMY.*¿Qué es un router? - Definición y usos* [blog]. 2021. [Consulta: 22 febrero 2023]. Disponible en: https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/what-is-a-router.html.

CODIFÍCAME. *Definición de Network Core* [blog]. 2012. [Consulta: 04 enero 2023]. Disponible en: https://www.codifica.me/definicion-de-network-core/.

COMPLETO, V. *Protocolo ASN1 y Protocolo SNMP* [blog]. 2019. [Consulta: 15 diciembre 2022]. Disponible en: http://everpec.blogspot.com/2013/11/protocolo-asn1-y-protocolo-snmp.html.

CÓRDOVA, R.R.D. Desarrollo de una plataforma de monitoreo de instancias Odoo, utilizando la herramienta Zabbix en infraestructura en la nube [en línea] (Trabajo de Titulación). Escuela Politécnica Nacional, Quito, Ecuador. 2019. [Consulta: 10 noviembre 2022]. Disponible en: https://bibdigital.epn.edu.ec/handle/15000/22175.

CYPRESS. *Understanding Bit-Error-Rate Hotlink [*en línea]. Ohio-EE.UU., 2010. [Consulta: 15 febrero 2023]. Disponible en: www.cypress.com.

DE REDFORT, G. *Introducción a SNMP* [blog]. 2008. [Consulta: 10 febrero 2023]. Disponible en: https://nsrc.org/workshops/2014/walc/raw-attachment/wiki/Agenda/snmp.pdf.

ISAIAS, D. & BARONA, V. Estudio de servidor zabbix en clientes corporativos de la urbe de Guayaquil [en línea] (Trabajo de Titulación). Universidad Politécnica Salesiana Sede Guayaquil, Guayaquil, Ecuador. 2016. [Consulta: 04 noviembre 2022]. Disponible en: https://dspace.ups.edu.ec/bitstream/123456789/12294/1/UPS-GT001620.pdf.

JUNCO ROMERO, G., & RABELO PADUA, S. "Los recursos de red y su monitoreo". *Revista cubana de informática médica* [en línea], 2018, vol. 8, no. 1, pp. 76–83. [Consulta: 02 enero 2023]. ISSN 0340-2672. Disponible en: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1684-18592018000100009.

LEÓN VASQUEZ, I. "RESOLUCION-STN-2011-0617". *Revista Arcotel* [en línea], 2011, vol. 4, no. 2, pp. 11–23. [Consulta: 11 febrero 2023]. ISSN 1140-0634. Disponible en: https://www.arcotel.gob.ec/wp-content/uploads/downloads/2013/07/snt_2011_0617_ge2.pdf.

MANAGEENGINE. *¿Qué es SNMP?* [blog]. 2023. [Consulta: 23 noviembre 2022]. Disponible en: https://www.manageengine.com/es/network-monitoring/what-is-snmp.html.

OMALIE, E., VICKSAI, M. y WILSON, M., 2018. Implementación y pruebas de monitoreo en una red LAN, basados en SNMPv3 [en línea] (Trabajo de Titulación). Escuela Politécnica del Litoral, Guayaquil, Ecuador. [Consulta: 28 diciembre 2022]. Disponible en: https://www.dspace.espol.edu.ec/bitstream/123456789/29720/1/Resumen de tesis MVenegas y Elsa Ochoa%2C director de tesis Mag. Washington Medina M. 5 junio 2014.pdf.

POZO, J.I. *Infancia y aprendizaje* [en línea]. Madrid-España: Editorial Vértice, 1995. [Consulta: 23 enero 2023]. Disponible en: https://doi.org/10.1080/02103702.1987.10822166.

RFC. *Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)* [blog]. 2002 [Consulta: 15 febrero 2023]. Disponible en: https://datatracker.ietf.org/doc/html/rfc3418.

RFC 1156. *Management Information Base for network management of TCP/IP-based internets* [blog]. 1990. [Consulta: 11 febrero 2023]. Disponible en: https://datatracker.ietf.org/doc/html/rfc1156.

SERVER ZEO. *What is Zabbix* [blog]. 2021. [Consulta: 8 enero 2023]. Disponible en: https://www.zabbix.com/documentation/current/en/manual/introduction/about.

STEWARD, P. *Uclm.es* [blog]. 2015. [Consulta: 15 febrero 2023]. Disponible en: https://www.dsi.uclm.es/personal/miguelfgraciani/mikicurri/docencia/LenguajesInternet0910/web_LI/Teori.

ANEXOS

ANEXO A: Plantilla del Switch Cisco nexus 9000-9500

```
zabbix_export:
  version: '6.0'
  date: '2022-11-28T08:35:59Z'
  template_groups:
    -
      uuid: 36bff6c29af64692839d077febfc7079
      name: 'Templates/Network devices'
  templates:
    -
      uuid: 80fc469750f84061924662a98c33580c
      template: 'Cisco Nexus 9000 Series by SNMP'
      name: 'Cisco Nexus 9000 Series by SNMP'
      description: |
        Template Cisco Nexus 9000 Series

          MIBs used:
          CISCO-ENHANCED-MEMPOOL-MIB
          CISCO-ENTITY-FRU-CONTROL-MIB
          CISCO-ENTITY-SENSOR-MIB
          CISCO-PROCESS-MIB
          ENTITY-MIB
          EtherLike-MIB
          IF-MIB
          SNMPv2-MIB
          SNMP-FRAMEWORK-MIB
          CISCO-IMAGE-MIB

        You can discuss this template or leave feedback on our forum https://www.zabbix.com/forum/zabbix-sugge
for-cisco

        Template tooling version used: 0.42
      groups:
        -
          name: 'Templates/Network devices'
      items:
        -
          uuid: 8eff7e6fc12c45f6b98a4fb89c44f03d
          name: 'ICMP ping'
          type: SIMPLE
          key: icmpping
          history: 7d
          valuemap:
            name: 'Service state'
```

```
          valuemap:
            name: 'Service state'
          tags:
            -
              tag: component
              value: health
            -
              tag: component
              value: network
          triggers:
            -
              uuid: 2b9b678cb9fc407cb485136ddcf5953c
              expression: 'max(/Cisco Nexus 9000 Series by SNMP/icmpping,#3)=0'
              name: 'Unavailable by ICMP ping'
              priority: HIGH
              description: 'The last three attempts returned a timeout. Check the connectivity of a device.'
              tags:
                -
                  tag: scope
                  value: availability
        -
          uuid: cb04f67d7ea04894a9f143a7d27db09a
          name: 'ICMP loss'
          type: SIMPLE
          key: icmppingloss
          history: 7d
          value_type: FLOAT
          units: '%'
          tags:
            -
              tag: component
              value: health
            -
              tag: component
              value: network
          triggers:
            -
              uuid: d32cffe7dcef4873ac8bb4d86119ddaa
              expression: 'min(/Cisco Nexus 9000 Series by SNMP/icmppingloss,5m)>{$ICMP_LOSS_WARN} and min(/Cisco Nexus 90
              name: 'High ICMP ping loss'
              opdata: 'Loss: {ITEM.LASTVALUE1}'
              priority: WARNING
              dependencies:
                -
```

ANEXO B: Ente de control ARCOTEL

ARTÍCULO 4: ÍNDICES DE CALIDAD DE LAS REDES DE ACCESO UNIVERSAL DE INTERNET CON INFRAESTRUCTURA PROPIA

Av. Diego de Almagro N31-95 y Alpallana, Edif. Senatel. Telfs: 2947800 Fax: 2901010 0003
Call Center 1-800SENATEL, Casilla 17-07-9777. www.conatel.gov.ec Quito-Ecuador

0617

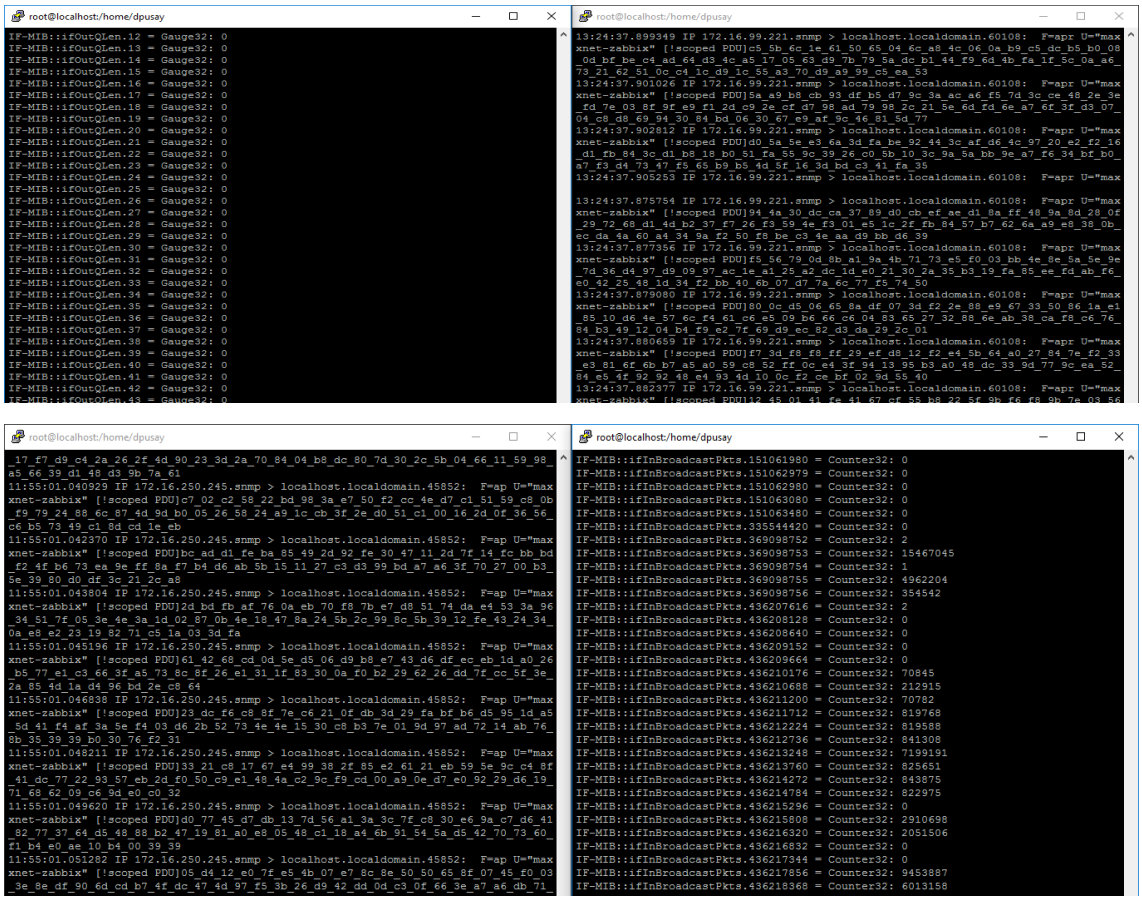
Los siguientes índices de calidad deberán ser cumplidos por los Proveedores de Redes de Acceso Universal de Internet que hayan obtenido el acto administrativo de operación a través de una Resolución del CONATEL, que construyan enlaces de la red de transporte y/o de acceso con infraestructura propia de las Redes de Acceso Universal de Internet.

PDA: Porcentaje de averías.
TRA: Tiempo medio de reparación de averías.
PR8: Porcentaje de averías con tiempo de reparación mayor a 8 horas.
PDS: Porcentaje de disponibilidad del servicio.

Para cada uno de los cuatro índices de calidad indicados, se establece un período de medición mensual, y todos los índices deben ser validados en un período total de un año para efectos de medición del cumplimiento de la Autorización para operar la Red de Acceso Universal de Internet. El Proveedor de la Red autorizada, deberá remitir trimestralmente a la SENATEL y a la SUPERTEL, la información conteniendo el valor obtenido para todos los indicadores y para cada uno de los meses del trimestre correspondiente, respetando todos los campos, según los formatos adjuntos en el Anexo 1 de la presente Resolución.

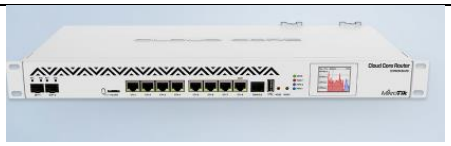
La Superintendencia de Telecomunicaciones podrá efectuar verificaciones de control trimestrales durante el primer año de operación de la Red de Acceso Universal de Internet.

ANEXO C: Verificacion de la comunicación SNMPv3 de la forma encriptada, la captura se realizo mediante TCPDUMP con las credenciales de cada equipo y direccion IP



Además zabbix ofrece más elementos de control como temperatura, espacio de memoria, espacio de disco, etc.

ANEXO D: Caracteristicas Equipos NEXUS y Mikrotik

Cisco Nexus	Mikrotik
	
Características. Part Number N9K-C93180YC-EX Ports 48 x 10/25-Gbps and 6 x 40/100-Gbps QSFP28 ports Downlink supported speeds 1/10/25-Gbps speeds CPU 4 cores System memory 24 GB SSD drive 64 GB System buffer 40 MB Management ports 2 ports: 1 RJ-45 and 1 SFP USB ports 1 RS-232 serial ports 1 Power supplies (up to 2) 650W AC, 930W DC, or 1200W HVAC/HVDC Typical power (AC/DC) 210W Maximum power (AC/DC) 470W Physical dimensions (H x W x D) 1.72 x 17.3 x 22.5 in. (4.4 x 43.9 x 57.1 cm) Weight (without power supplies or fans) 17.2 lb (7.8 kg)	Características. Product code CCR1036-8G-2S+, Architecture TILE, CPU TLR4-03680 CPU core count 36, CPU nominal frequency 1.2 GHz, Dimensions 443 x 193 x 44 mm, RouterOS license 6, Operating System RouterOS, Size of RAM 4 GB, Storage size 1GB, Storage type NAND, MTBF Approximately 200'000 hours at 25C, Tested ambient temperature -20°C to 60°C, IPsec hardware acceleration Yes Ethernet 10/100/1000 Ethernet ports 8, SFP DDMI Yes, SFP+ ports 2

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

DIRECCIÓN DE BIBLIOTECAS Y RECURSOS DEL APRENDIZAJE

UNIDAD DE PROCESOS TÉCNICOS

REVISIÓN DE NORMAS TÉCNICAS, RESUMEN Y BIBLIOGRAFÍA

Fecha de entrega: 03/ 04 / 2023

INFORMACIÓN DE LOS AUTORES
Nombres – Apellidos: Angel Santiago Toapanta Carvajal
INFORMACIÓN INSTITUCIONAL
Facultad: Informática y Electrónica
Carrera: Telecomunicaciones
Título a optar: INGENIERO EN ELECTRONICA, TELECOMUNICACIONES Y REDES
f. Analista de Biblioteca responsable: Ing. Fernanda Arévalo M.