ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

CARRERA TELECOMUNICACIONES

"DESARROLLO DE LA REINGENIERÍA DEL SISTEMA DEL MONITOREO DE RED PARA LA EMPRESA ELÉCTRICA AMBATO REGIONAL CENTRO NORTE S.A."

Trabajo de titulación

Tipo: Proyecto Técnico

Presentado para optar al grado académico de:

INGENIERO EN ELECTRÓNICA, TELECOMUNCACIONES Y REDES

AUTOR: ISRAEL SEBASTIÁN DUCHE VALLEJO

DIRECTOR: Ing. Alberto Arellano A. Msc.

Riobamba-Ecuador

2021

Yo, ISRAEL SEBASTIÁN DUCHE VALLEJO, declaro que el presente trabajo de titulación es de mi autoría y los resultados del mismo son auténticos. Los textos en el documento que proviene de otras fuentes están debidamente citados y referenciados.

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

Riobamba, 23 de diciembre de 2021

Israel Sebastián Duche Vallejo

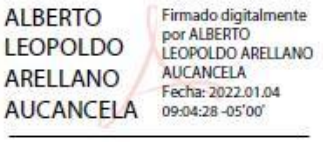
1804321824

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

CARRERA TELECOMUNICACIONES

El Tribunal de Trabajo de Titulación certifica que: El trabajo de titulación tipo: Proyecto Técnico, **"DESARROLLO DE LA REINGENIERÍA DEL SISTEMA DEL MONITOREO DE RED PARA LA EMPRESA ELÉCTRICA AMBATO REGIONAL CENTRO NORTE S.A."**, realizado por el señor **ISRAEL SEBASTIÁN DUCHE VALLEJO**, ha sido minuciosamente revisado por los Miembros del Tribunal de Trabajo de Titulación, el mismo que cumple con los requisitos científicos, técnicos, legales, en tal virtud el Tribunal Autoriza su presentación.

NOMBRE	FIRMA	FEHCA
Ing. Jorge Yuquilema I. **DELEGADO DEL DECANO**		2021-12-23
Ing. Alberto Arrellano A. Msc **DIRECTOR DEL TRABAJO DE TITULACIÓN**		2021-12-23
Ing. Diego Veloz Ch. Msc **MIEMBRO DEL TRABAJO DE TITULACIÓN**		2021-12-23

DEDICATORIA

El presente trabajo de titulación se lo dedico primeramente a Dios por darme la vida, salud, fuerza e inteligencia para siempre seguir adelante y permitirme llegar a este importante momento, a mis padres, por darme su apoyo tanto emocional como económicamente durante este arduo trayecto, a los docentes que compartieron su experiencia y conocimientos, supieron guiarme de la mejor manera a través de toda esta etapa académica y a la Empresa Eléctrica de Ambato Regional Centro Norte S.A. por abrirme las puertas y permitirme desarrollar este proyecto.

Israel Duche

AGRADECIMIENTO

Mi más sincero agradecimiento a Dios por darme siempre su infinita sabiduría e inteligencia, a mis padres por estar siempre a mi lado y ayudarme a superar obstáculos que se han presentado a lo largo de esta etapa académica, a la Escuela Superior Politécnica de Chimborazo, la Escuela de Telecomunicaciones y a sus docentes, que me supieron acoger en su seno y compartieron sus experiencias y conocimientos sin egoísmos, y la Empresa Eléctrica de Ambato Regional Centro Norte S.A. por brindarme la oportunidad de realizar este proyecto.

Israel Duche

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE GRÁFICOS

ÍNDICE DE ANEXOS

RESUMEN

El objetivo fue desarrollar la reingeniería del sistema de monitoreo de red de la Empresa Eléctrica Ambato Regional Centro Norte S.A. (EEASA). El desarrollo del proyecto se dividió en tres fases, la primera consistió en realizar una búsqueda bibliográfica en varias fuentes fiscas y digitales para recopilar información acerca de la administración y gestión de las redes de datos, estudio de los protocolos de gestión SNMP y Syslog, y las herramientas que se usa en el monitoreo y control de las redes de datos. La segunda fase se orientó al diseño e implementación del nuevo sistema de monitoreo de red para la EEASA, que constó de cuatro etapas, en la primera se realizó en una evaluación inicial de la red de la empresa, donde se analizó el número de equipos y el tráfico de datos generado, en la segunda se realizó un análisis del sistema de monitoreo de red usado por la empresa, donde se estudió las problemáticas de diseño y funcionamiento que tiene dicho sistema, a continuación se procedió a realizar el diseño y dimensionamiento de los equipos necesarios para el correcto desempeño del sistema de monitoreo de red, donde se analizó la arquitectura y protocolos a usarse, se definió la aplicación para el monitoreo de la red y se detalló los requerimientos de los equipos a implementarse. En la última fase del proyecto se realizó una evaluación final del sistema de monitoreo de red repotenciado para verificar que no existan los problemas que tenía el sistema anterior, así mismo se evaluó el rendimiento de los equipos y de la aplicación, de esta forma se comprobó que el nuevo sistema de monitoreo de red de la empresa se encuentra completamente operativo. De la misma forma se recomienda realizar evaluaciones periódicas al sistema de monitoreo de red para la verificación del correcto desempeño del sistema.

Palabras clave: <INGENIERÍA Y TECNOLOGÍA ELECTRÓNICA>, <REINGENIERÍA>, <SISTEMA DE MONITOREO>, <GESTIÓN DE RED>, <MONITOREO DEL RENDIMIENTO DE RED>, <ESTACIÓN DE GESTIÓN DE RED (NMS)>, <AGENTE DE GESTIÓN>, <BASE DE INFORMACION DE GESTIÓN (MIB)>.

ABSTRACT

It was aimed to develop the reengineering of the network monitoring system of Empresa Eléctrica Ambato Regional Centro Norte S.A. (EEASA). The project development was divided into three phases, the first one consisted of conducting a bibliographic search in various sources physical and digital to collect information about the administration and management of data networks, the SNMP and Syslog management protocols study, and the tools used in the monitoring and control of data networks. The second phase was oriented to design and implement the new network monitoring system for the EEASA, which consisted of four stages. In the first phase, an initial evaluation of the company's network was carried out where the number of equipment and the data traffic generated was analyzed. In the second phase, the network monitoring system analysis used by the company was carried out where the design and operation problems of the system were studied, then the design and dimensioning of the necessary equipment for the correct performance of the network monitoring system were conducted to analyze the architecture and protocols to be used, finally, the application for network monitoring was defined and the requirements of the equipment to be implemented were detailed. In the last phase of the project, a final evaluation of the repowered network monitoring system was carried out to verify that the problems of the previous system had did not exist anymore. In addition, the performance of the equipment and the application were evaluated to warrant that the company's new network monitoring system is fully operational. It is recommended to carry out periodic evaluations of the network monitoring system to verify the correct performance of the system.

Keywords: <ENGINEERING AND ELECTRONIC TECHNOLOGY>, <REENGINEERING>, <MONITORING SYSTEM>, <NETWORK MANAGEMENT>, <NETWORK PERFORMANCE MONITORING>, <NETWORK MANAGEMENT STATION (NMS)>, <MANAGEMENT AGENT>, <MANAGEMENT INFORMATION BASE (MIB)>.

INTRODUCCIÓN

Hoy en día, las redes de datos han crecido considerablemente, llegando a pasar de un simple conjunto de computadores que compartían información y recursos, a una amalgama compleja de dispositivos, sistemas y técnicas de comunicación que se han ido desarrollando en el transcurso del tiempo, sin embargo, siempre ha sido necesario llevar una correcta administración, control y gestión de las redes, las cuales permitan atender a fallos de una manera oportuna.

La Empresa Eléctrica de Ambato Regional Centro Norte S.A. (EEASA) es una empresa dedicada a brindar el servicio básico de energía eléctrica y alumbrado público a las provincias de Tungurahua, Pastaza, Napo y Morona Santiago. Esta empresa, mediante la implementación de las redes de datos a mejorado grandemente su gestión corporativa, por esta razón es indispensable que la red empresarial opere de una manera eficaz, corrigiendo a tiempo fallas que puedan presentarse, para esto se requiere un sistema de monitoreo de red el cual permita al administrador conocer los diferentes eventos que puedan ocurrir y de esta forma poder corregirlos sin causar problemas a la empresa.

En la actualidad, la EEASA para poder mejorar la calidad del servicio que entrega a sus clientes ha modernizado su infraestructura, tanto en subestaciones como en la red de distribución eléctrica, mediante la implementación de dispositivos de automatización, los cuales, es necesario que sean monitorizados de una manera continua dentro del sistema, para verificar que se tenga una alta disponibilidad y así poder responder de una manera adecuada a las incidencias que puedan presentarse en el transcurso del tiempo, por eso, además del monitoreo de dispositivos de red existentes en su infraestructura, es necesario que se controle la disponibilidad y el funcionamiento de los equipos automáticos.

Por lo tanto, para poder realizar el diseño y la implementación del sistema de monitoreo de red para la EEASA, es necesario efectuar una investigación bibliográfica para determinar la arquitectura, protocolos y programas que se adapten a las necesidades que requiere la empresa, para así poder comprender de una mejor manera las definiciones y terminologías con respecto al tema. A continuación, se procederá a realizar un estudio para evaluar el estado actual de la red empresarial y analizar el sistema de monitoreo de red que usa actualmente la EEASA para, de esta forma, determinar los parámetros y requerimientos que debe tener el nuevo sistema de monitoreo a implementarse, y que de esta manera se pueda realizar la administración y gestión de los equipos que se encuentran dentro de la red empresarial de una manera eficaz.

ANTECEDENTES

Dentro de la gestión y administración de redes de comunicaciones, la detección a tiempo de fallas y el monitoreo de los elementos que forman parte de la red son actividades de gran importancia para entregar calidad de servicio a los usuarios. Cuando una empresa entrega un determinado servicio, las redes son uno de los puntos más importantes a tener en cuenta, ya que, si la red deja de funcionar por cualquier motivo y no se llega a transmitir los datos necesarios, la empresa deja de prestar el servicio a sus clientes durante el tiempo que dure la caída, todo esto puede causar grandes pérdidas económicas a la empresa (Pandora FMS team 2017).

Por tal razón, es importante tener un sistema de monitoreo de red capaz de notificar las fallas ocurridas y de mostrar su comportamiento mediante el análisis y recolección de información que reporta el equipo. En la actualidad se pueden monitorear mediante diferentes protocolos y herramientas. Los elementos más usuales que se monitorean dentro de una infraestructura de red son: Base de datos, servidores, Estaciones de trabajo (CPU, Espacio en disco, etc.), *Routers* (Flujo de tráfico) y *Swicthes* (Romero y Padua 2018).

El monitoreo de las redes consiste en analizar el estado de los equipos y tráfico IP en una red para obtener métricas, medidas de efectividad e información estadística útil. Estos datos pueden ser utilizadas para mejorar la seguridad informática en las organizaciones, como, por ejemplo, una gran cantidad de computadores externos que envían paquetes de red hacia una maquina interna, podría causar una denegación de servicio (DoS) a la maquina receptora, un análisis de tráfico IP puede identificar el origen de dichos paquetes. Con esta información se pueden tomar acciones como, no aceptar paquetes provenientes de la maquina atacante (Echeverría 2018).

La Empresa Eléctrica Ambato Regional Centro Norte S.A. (EEASA), es una empresa distribuidora y comercializadora de energía eléctrica que opera como sociedad anónima; brinda este servicio a cuatro provincias que están bajo su responsabilidad en la región central del País, convirtiéndola así en la más grande área de concesión en el conjunto de empresas distribuidoras de este servicio. La empresa para mejorar su servicio de distribución y comercialización de energía eléctrica ha realizado la implementación de varios equipos automatizados como reconectadores, seccionadores, interruptores, RTU, subestaciones de distribución, entre otros, que permite brindar un servicio de calidad. También cuenta con las agencias de recaudación, oficinas, cámaras de vigilancia y diferentes equipos de red como *access points*, *switches* y *routers*, que se encargan de mantener la comunicación dentro de la empresa.

Debido a esto, el número de equipos que forma parte de la red de comunicaciones de la EEAS es muy extensa y es necesario contar con un sistema de monitoreo de red el cual permite tener una

correcta administración, control y gestión de los equipos que forman parte de la red, para poder prevenir y corregir fallas a tiempo sin que esto pueda perjudicar a la empresa.

La EEASA para poder realizar la gestión y administración de la red posee el software *Network Performance Monitor* (NPM) de la empresa SolarWinds, con un licenciamiento básico, el cual permite administrar y gestionar solamente 500 dispositivos, esto evita tener una mayor escalabilidad al momento de ingresar nuevos equipos al sistema de monitoreo, provocando así, un problema al administrador de la red, ya que no puede tener el control completo de todos los elementos del sistema.

FORMULACIÓN DEL PROBLEMA

La Empresa Eléctrica Ambato Regional Centro Norte S.A. en los últimos años ha tenido una gran expansión en su red de datos, ya que se ha incorporado un mayor número de dispositivos para poder mejorar el servicio de distribución y comercialización de energía eléctrica, dichos dispositivos se conectan a la red de datos empresarial, y deben ser monitoreados continuamente, ya que estos equipos deben operar de una manera eficaz para poder atender de forma oportuna las incidencias que se pueda presentar en la red eléctrica.

Para el monitoreo de la red empresarial se usa un sistema el cual consta de un computador con hardware de pocos recursos (procesador Intel Core i3 de 2.93 GHz, memoria RAM de 16GB y un disco duro de 148GB de almacenamiento) y la aplicación NPM de la empresa SolarWinds con un licenciamiento básico, el cual permite monitorear, administrar y gestionar a 500 dispositivos. Debido a estos inconvenientes el sistema de monitoreo de red no está funcionando adecuadamente, ya que varios de los equipos de la empresa no pueden ser monitoreados por el sistema, esto puede provocar varios problemas a futuro como, no identificar de manera oportuna fallas en los enlaces, intrusiones de extraños a la red o un análisis erróneo de tráfico. Por estas razones, la empresa necesita repotenciar su sistema de monitoreo de red, planteándose la siguiente problemática ¿Es necesario el desarrollo de una reingeniería en el sistema de monitoreo que tiene actualmente la Empresa Eléctrica Ambato Regional Centro Norte S.A.?

SISTEMATIZACIÓN DEL PROBLEMA

¿Qué protocolos de monitoreo se encuentran operando actualmente en la red?

¿Cómo se va a realizar el dimensionamiento para la implementación del nuevo sistema de monitoreo de red de la empresa?

¿Qué protocolo para el monitoreo de red se va a estudiar?

¿De qué forma se seleccionará los recursos de hardware y software necesarios?

¿De qué manera se hará la implementación del sistema de monitoreo y cómo se evaluará el correcto desempeño de este?

JUSTIFICACIÓN TEÓRICA

Una de las actividades más importantes de un administrador de red es la detección a tiempo de fallos y el monitoreo exhaustivo de toda la infraestructura que conforma su red de datos, estas acciones son de gran importancia dentro de una organización, ya que de esta forma se garantiza una calidad de servicio a los clientes. Por esta razón, en la actualidad es indispensable que una empresa cuente con un sistema capaz de mostrar el comportamiento de la red mediante la recolección de información que pueda brindar un determinado protocolo, a su vez, poder notificar los eventos ocurridos a tiempo para realizar el mantenimiento correctivo respectivo.

Dentro de un sistema de monitoreo de red es muy importante definir lo más claro posible las acciones que se desea realizar, y que seguimiento se hará dentro de la red, entre las características más importantes que se puede observar en un sistema de monitoreo se encuentran:

- Disponibilidad de los equipos que forman parte de la red.
- Consumo de recursos de los equipos como memoria RAM o CPU.
- Estado físico de los enlaces de la red.
- Utilización del ancho de banda de la red.
- Análisis de tráfico de los paquetes que viajan por la red.
- Los diferentes servicios con los que cuenta la empresa como web, correo, base de datos, etc.
- Latencia entre los distintos enlaces de la red.

Sin embargo, debido a que existe diversas maneras en la que se puede implementar un sistema de monitoreo por medio de diferentes herramientas existentes, es necesario que se analice diferentes características como: recursos humanos, económicos, infraestructura de red, etc.

Según (Romero y Padua, 2018), las notificaciones a alertas más importantes que un sistema de monitoreo de red de datos debería entregar a los administradores de red son:

- Alarmas de procesamiento.
- Alarmas de conectividad.
- Alarmas ambientales.
- Alarmas de utilización.
- Alarmas de disponibilidad.

La Empresa Eléctrica Ambato Regional Centro Norte S.A, es una institución que se encarga de la distribución del servicio de energía eléctrica y alumbrado público a cuatro provincias del Ecuador, por lo tanto, para la comunicación entre las diferentes instalaciones ubicadas en lo largo de las cuatro provincias, la empresa cuenta con una red de datos robusta, la cual garantiza el

correcto desempeño de esta, para que sus clientes puedan recibir un servicio de calidad. Por esta razón es muy importante que la EEASA cuente con un sistema de monitoreo eficaz que garantice la sostenibilidad de la red.

Para garantizar el correcto funcionamiento de la red empresarial, la EEASA cuenta con un sistema de monitoreo el cual se basa en el uso de la herramienta *Network Performance Monitor* (NPM), que brinda la empresa SolarWinds. Entre los aspectos principales que este sistema se encarga de monitorear dentro de la infraestructura de la red de datos de la empresa se tiene:

- Un sistema SCADA para el control de diferentes equipos de automatización, encargados de la distribución del suministro eléctrico.
- Equipos de subestaciones eléctricas.
- Equipos de red MPLS.
- Equipos de comunicaciones que se encuentran en las instalaciones de la EEASA como centras de recaudación, oficinas administrativas, bodegas, etc.
- Equipos de radio enlace que permiten la comunicación entre los varias partes de la empresa como, por ejemplo: el intercambio de información entre los equipos automáticos de control y el centro de control.

En la Figura 1. se muestra un ejemplo de cómo se proyectan los datos estadísticos en la herramienta NPM del sistema de monitoreo de la EEASA.

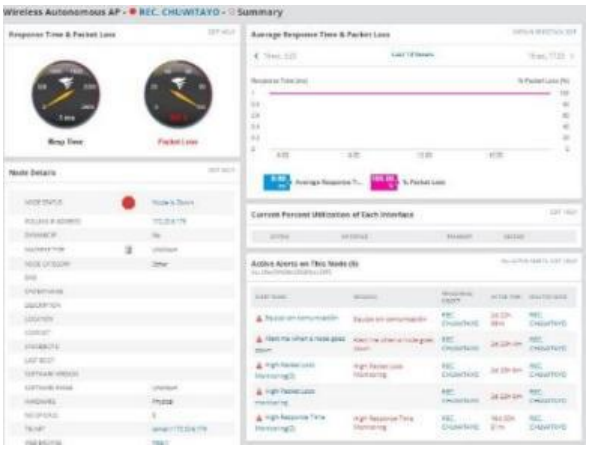


Figura 1. Ejemplo de datos estadísticos de equipo monitoreado

Realizado por: Duche, I. 2021

Para el funcionamiento del sistema de monitoreo la herramienta NMP cuenta con la licencia básica LS500, esta aplicación se encuentra instalada en un equipo informático con pocos recursos, este equipo usa el sistema operativo WINDOWS SERVER 2016 *Standar*, así mismo la base de datos que usa la aplicación para el almacenamiento de datos es SQL Server 2017 con un

licenciamiento *Express*, la cual se encuentra dentro del mismo computador de la aplicación de monitoreo.

Actualmente, la red empresarial de la EEASA se encuentra en proceso de expansión, ya que se estudia el desarrollo de diferentes proyectos como una reingeniería de la red de comunicaciones, incrementos de los puntos de control mediante equipos automáticos, implementación de nuevas subestaciones eléctricas, etc. Por lo tanto, es necesario que los equipos correspondientes a las nuevas implementaciones planificadas por la EEASA ingresen al sistema de monitoreo con el que cuenta la empresa.

Debido al crecimiento de la red empresarial que pasa actualmente la EEASA, se considera que el sistema de monitoreo que se encuentra en operación podría comenzar a presentar varios problemas, debido a la falta de recursos y a la mala arquitectura con la que ha sido diseñado anteriormente el sistema de monitoreo.

Entre los problemas más críticos que puede llegar a presentarse en un futuro dentro del sistema de monitoreo se tiene:

- Limitaciones de ingreso de nuevos nodos al sistema de monitoreo de red debido a la limitación del licenciamiento de la aplicación NPM.
- Una latencia muy alta al momento de acceder a las diferentes partes de la aplicación.
- Conflictos entre la base de datos y la aplicación debido a una mala arquitectura.
- Falta de espacio para el almacenamiento de datos históricos de eventos ocurridos en la red.

En la Figura 2. se puede observar que el número de nodos que se encuentran actualmente dentro del sistema de monitoreo está ocupando aproximadamente toda la capacidad que ofrece la licencia básica LS 500 de la aplicación NPM.

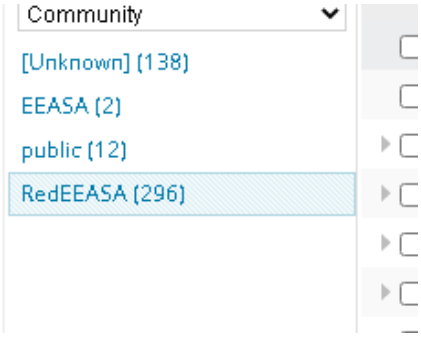


Figura 2. Numero de nodos existentes en aplicación NPM

Realizado por: Duche, I. 2021

Por estas razones, se ha visto la necesidad de realizar una reingeniería en el sistema de monitoreo de red de la EEASA, inicialmente se realizará una evaluación inicial de la red empresarial, para

proceder al estudio del dimensionamiento adecuado, de esta manera se conocerá los requerimientos necesarios para la implementación de hardware y software respetivamente para la implementación de un nuevo sistema de monitoreo que satisfaga las características que se desea monitorear dentro de la empresa. Además, se requiere que el nuevo sistema sea escalable, para evitar los errores que se podría presentar al momento de que la red pase por una nueva fase de crecimiento. Para concluir se realizará una evaluación final en la que se verifique el correcto funcionamiento y desempeño del sistema de monitoreo para la red empresarial.

JUSTIFICACIÓN APLICATIVA

La Empresa Eléctrica Ambato Regional Centro Norte S.A., para el monitoreo, administración y gestión de su red empresarial, usa la herramienta de monitoreo NPM, que brinda la empresa SolarWinds, y los protocolos de monitoreo y administración SNMP e ICMP. En los últimos años la EEASA ha tenido un gran incremento dentro de la red de la empresa debido al aumento de nuevas instalaciones que representa un aumento en los equipos de redes que se usa para la comunicación.

En la Figura 3, se puede observar una parte del sistema de distribución de la red eléctrica, así mismo en la Figura 4, se muestra una pequeña parte de la topología de red de fibra óptica con la que cuenta la empresa, que permite la comunicación entre las diferentes instalaciones que se encuentran distribuidas a lo largo de las cuatro provincias que la EEASA se encarga de brinda el servicio de distribución de energía eléctrica.

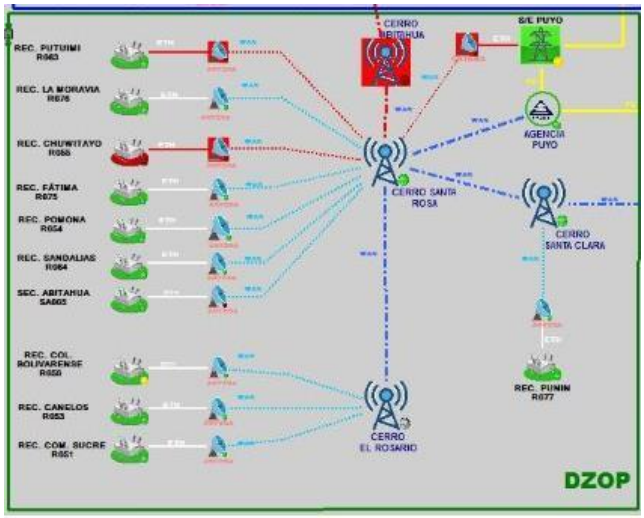


Figura 3. Parte de la red de distribución eléctrica en aplicación NPM

Realizado por: Duche, I. 2021

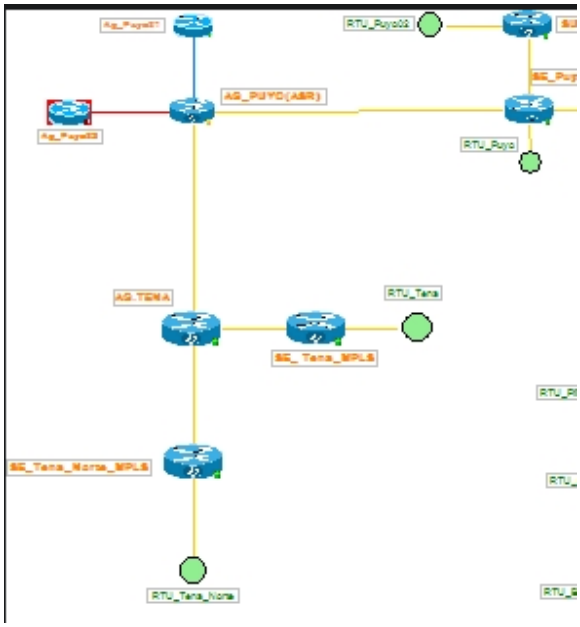


Figura 4. Parte del mapa de red mostrado en aplicación NPM

Realizado por: Duche, I. 2021

Por esta razón es necesario que el sistema de monitoreo de la red se encuentre completamente operativo, y que todos los equipos que pertenecen a la red corporativa de la EEASA se encuentren ingresados dentro del sistema de monitoreo, para verificar el correcto desempeño de la infraestructura de red, y en caso de que ocurra algún evento determinado, el administrador a cargo pueda realizar las medidas respectivas de corrección de fallo y así garantizar que la red empresarial se encuentre en correcto funcionamiento.

En la actualidad la red de datos de la EEASA pasa por un proceso de expansión, esto significa que el número de elemento que debe ser monitorizado también se ha incrementado, por esta razón, debido a las características que tiene el sistema de monitoreo, este podría presentar diversas fallas, las cuales no permitirán que se realice una correcta administración y gestión de los equipos que pertenecen a la red de datos.

Por lo tanto, se pretende realizar una reingeniería del sistema de monitoreo de red, para esto se requiere desarrollar una evaluación inicial de la red corporativa de la EEASA, para conocer su estado actual, esto también permitirá realizar un dimensionamiento adecuado para conocer los requerimientos necesarios tanto de hardware y software respectivamente, que garantice el correcto funcionamiento del nuevo sistema de monitoreo que se busca implementar. Así mismo, se debe realizar un análisis de la arquitectura que requiere un sistema de monitoreo de red, para de esta forma realizar un correcto diseño al momento de la planificación del nuevo sistema.

En la Figura 5. se muestra un ejemplo de la arquitectura de un sistema de monitoreo de red usando las herramientas que brinda la empresa SolarWinds para la administración y gestión de una infraestructura de red, tanto física como el análisis del flujo de tráfico.

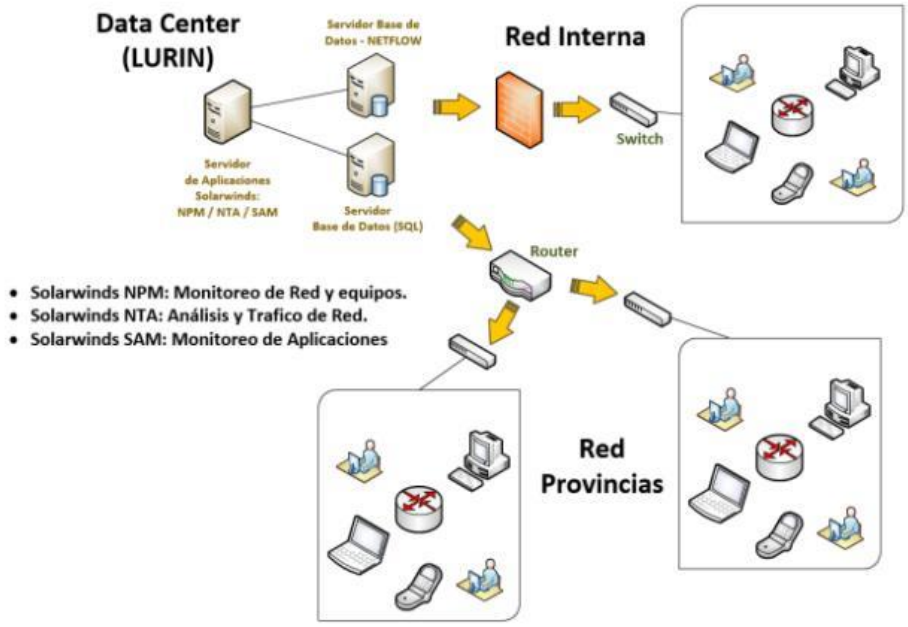


Figura 5. Ejemplo de arquitectura para sistema de monitoreo

Realizado por: Zambrano, M. 2019

También se requiere realizar un análisis adecuado acerca del licenciamiento que se va a utilizar para la aplicación y la base de datos respectivamente, se debe hacer una selección adecuada que satisfaga las necesidades de escalabilidad que se pretende tener en el sistema de monitoreo, de esta forma, se busca evitar gastos innecesarios para la empresa con costos elevados de licencias.

Para concluir se realizará una evaluación final del sistema de monitoreo, en el cual se verifique el correcto desempeño del nuevo sistema de monitoreo de red implementado en la empresa, garantizando así que se cumpla con todas las necesidades que el administrador requiere para controlar el funcionamiento de la red de la EEASA.

OBJETIVOS

OBJETIVO GENERAL

- Desarrollar la reingeniería del sistema de monitoreo de red para la Empresa Eléctrica Ambato Regional Centro Norte S.A.

OBJETIVOS ESPECÍFICOS

- Estudiar el estado actual del sistema de monitoreo de red que se encuentra operativo dentro de la EEASA.
- Realizar el estudio del estado actual de la red empresarial para conocer los requerimientos de hardware y de software que va a necesitar el sistema de monitoreo.
- Implementar el sistema de monitoreo dentro de la red empresarial de la EEASA, configurar y agregar todos los equipos de la empresa dentro del sistema.
- Evaluar el correcto desempeño del sistema de monitoreo de la red de la EEASA.

CAPÍTULO I

1. MARCO TEORICO REFERENCIAL

1.1. Introducción a la administración de redes

En la actualidad, la infraestructura de las redes de datos se encuentra en constante crecimiento, por lo que el detectar algún error o falla dentro de la infraestructura de red es una tarea muy compleja para realizarla de forma manual, por lo tanto, se ha vuelto indispensable que las empresas lleven una correcta administración de sus infraestructuras de red, para que, de esta forma se pueda tener un control completo sin importar su complejidad.

Según Gatera (2017, p.52), la administración de las redes de datos son funciones o actividades prioritarias que se realiza dentro de los sistemas informáticos de las empresas y organizaciones modernas, con el principal objetivo de conseguir un funcionamiento óptimo y continuo de toda la infraestructura de la red de datos empresarial, de esta forma se garantiza que se encuentren operativos los sistemas tanto de hardware como de software.

También se considera a la administración de redes como el control, organización, supervisión y toma de decisiones dentro de la infraestructura de la red de comunicaciones, para poder mantener un funcionamiento óptimo y eficaz, haciendo uso de herramientas, aplicaciones y dispositivos de red. Entre las principales actividades que se realiza dentro de la administración de la red se destacan: detección de fallos, evaluación de tráfico de datos, mantenimiento preventivo y correctivo de la red, control de acceso, etc. (Naranjo y Ortega 2006, p.1).

Otra definición, en base a la *Sonoma County Office of Education* (2013, pp.1-3), la administración de una red de datos consiste en la ejecución de varias actividades que permitan garantizar el funcionamiento correcto del sistema de telecomunicaciones tanto de hardware como de software, haciendo uso de varias herramientas que permitan proporcionar apoyo dentro de todos los niveles de la red de datos, además se encarga de controlar las operaciones relacionadas con los proveedores de redes de telecomunicaciones con lo que cuenta una empresas u organización ya sea privada o pública.

Generalmente, a medida que las infraestructuras de redes de datos se vuelven más complejas, el detectar un mal funcionamiento o incidencias dentro del sistema se hace una tarea complicada, por lo cual, la detección y corrección de fallos es una prioridad dentro de las redes de datos, por

lo que se requiere un enfoque profesional, sistemático y con experiencia, en la Figura 1-1, se muestra un ejemplo de un sistema de administración de red.

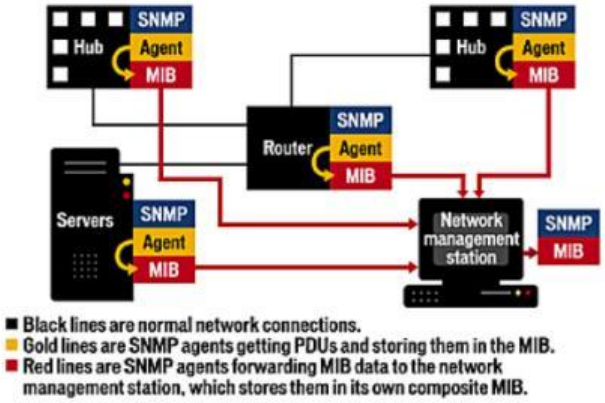


Figura 1-1. Ejemplo de arquitectura de administración

Realizado por: Gatera, T. 2017

A los profesionales encargados de realizar estas actividades se los denominan administradores de red, este profesional es responsable de planificar, organizar y controlar el sistema de telecomunicaciones, para así poder solucionar problemas que se puedan presentar en las diferentes situaciones o escenarios dentro de un sistema de telecomunicaciones.

Entre las principales actividades que un administrador de red se encarga de realizar dentro de un sistema de telecomunicaciones en una empresa u organización son:

- Supervisión del funcionamiento, desempeño y rendimiento de la red de datos de la empresa u organización.
- Evaluación periódica de los sistemas de telecomunicaciones, tanto de hardware como de software.
- Planificación del diseño de nuevos sistemas de telecomunicaciones tanto locales como de forma remota.
- Proporción de asistencia técnica y ayuda a los usuarios finales de la red de datos, en el caso de existir problemas en estaciones de trabajo.
- Administración de servidores tanto físicos como virtuales con los que cuenta de la empresa, en los diferentes sistemas operativos (Linux y Windows).
- Mantenimiento de la seguridad del sistema de comunicaciones, realizando métodos y técnicas que eviten que exista alguna intrusión a la red de datos de la empresa.

1.1.1. Objetivos de la administración de red

De acuerdo con Naranjo y Ortega (2006, p.2), los objetivos centrales con lo que debe cumplir la administración de las redes de datos son:

- Realizar el control de posibles fallos, incidencia o degradaciones en el rendimiento del sistema de telecomunicaciones, por medio del uso de herramientas tanto manuales como automatizadas que garanticen el óptimo funcionamiento de la red de datos de la empresa u organización.
- Establecer varias estrategias de administración que permita que el administrador pueda optimizar al máximo la infraestructura del sistema de telecomunicaciones ya existente dentro de la empresa.
- Buscar constantemente técnicas y método que permitan optimizar de la mejor manera posibles los recursos con lo que cuenta la red de datos, de esta forma se trata de conseguir mejorar el rendimiento de aplicación y servicios que son usados por los usuarios finales dentro de la organización.

(Brihuega 2015, p.136), también menciona que para poder mantener una red de telecomunicaciones de manera operativa, eficiente, segura y monitoreada constantemente es necesario que se cumpla con los siguientes objetivos:

- Buscar siempre la mejor manera de mantener la continuidad en las operaciones del sistema de telecomunicaciones, haciendo uso de técnicas y métodos adecuados de monitoreo y control, lo cual permita poder resolver problemas o incidencias que se puedan presentar dentro de la red y a su vez optimizar de la mejor manera los recursos.
- Usar de una manera óptima y eficiente la red de datos, buscando siempre la manera de mejorar el uso de los recursos del sistema, como por ejemplo el porcentaje de utilización del ancho de banda.
- Minimizar los costos de la empresa, garantizando que las aplicaciones y servicios que brinda el sistema de telecomunicaciones estén completamente operativos.
- Evaluar constantemente la seguridad de la red de datos, así mismo implementar mecanismos de seguridad que permita proteger a la empresa contra el acceso de entes no autorizados ajenas a la organización, y garantizando que la información se encuentre segura y no se encuentre comprometida de ninguna manera.
- Registra las actividades como cambios o actualizaciones que se realicen en el sistema de telecomunicaciones, de tal manera que cuando se tenga planeado algún mantenimiento programado esto ocasione el mínimo de interrupciones posibles, y de esta forma poder levantar lo antes posible el servicio.

1.1.2. Funciones de la administración de red

La administración de una infraestructura de red permite realizar actividades que garanticen que la red de datos funcione de una manera óptima y que la infraestructura del sistema de telecomunicaciones tenga el mejor rendimiento (Naranjo y Ortega 2006).

Para realizar estas actividades de una manera adecuada, la administración de red se basa en dos procedimientos, los cuales permiten llevar a cabo varias actividades de una manera eficaz, estos procedimientos son: monitoreo y control.

1.1.2.1. Monitoreo

Es uno de los procesos principales que permite la administración de una red de datos. El monitoreo es una técnica pasiva, donde el administrador se encarga del control mediante el uso herramientas informáticas, observando así el comportamiento del sistema de telecomunicaciones y el estado de sus componentes, por ejemplo equipos de red (Naranjo y Ortega, 2006, p. 2).

Además, se encarga de llevar un registro de todas las actividades que se realice dentro de la red de datos, de esta manera se obtiene información acerca del estado de los recursos que tiene la infraestructura de la red.

1.1.2.2. Control

El proceso de control es un método activo, el cual mediante la información recopilada o registrada por medio técnicas de monitoreo, se pueda realizar acciones sobre el comportamiento de la red administrada, de esta manera se optimiza los recursos y se garantiza el correcto funcionamiento de la misma (Naranjo y Ortega, 2006, p. 2).

Este proceso generalmente abarca la configuración y seguridad que el administrador le puede dar a la red de datos.

1.2. Monitoreo de redes

Según Cisco (Cisco Systems, 2021), el monitoreo de red es un proceso que proporciona información acerca de infraestructura de red a un administrador, el cual necesita determinar, en tiempo real, el funcionamiento óptimo de la red. Esto se lo realiza a través de herramientas de software de monitoreo, la cual permite a los administradores gestionar y optimizar la red de una manera eficaz.

La monitorización de los sistema o redes de datos es ampliamente usada por los administradores, ya que permite realizar varias actividades como: detectar y solucionar problemas, identificar el origen de los mismo, realizar tendencias y proyecciones que permitan predecir y evitar futuros problemas en la red, proporcionar datos sobre las actividades realizadas dentro del sistema tales como configuración o control de acceso, etc. (Limoncelli, Hogan y Chalup, 2007, p. 523).

Para el monitoreo de una red existen varios protocolos, los cuales se encargan de recolectar y enviar información del estado de los equipos hacia el centro de control de la infraestructura de red. Entre los protocolos más usados en el entorno de TI se puede encontrar: Netflow, Syslog, ICMP y SNMP

Para poder realizar el monitoreo de una red, existe dos métodos principales con lo que se puede realizar la supervisión de la infraestructura del sistema de telecomunicaciones, estos son:

- Realizar una recopilación o un registro de datos históricos de las actividades de la red tales como disponibilidad o uso, por medio de información que envían los equipos de red en intervalos de tiempo.
- Realizar un seguimiento en tiempo real de la red de datos para garantizar el correcto funcionamiento y que las fallas o incidencias puedan ser notificadas al administrador en el momento que sucede.

1.2.1. Monitoreo mediante datos históricos

El monitoreo o supervisión histórica se basa en la recopilación o registro de información de actividades en intervalos de tiempo. Esa información se la usa a largo plazo para que el administrador pueda evitar problemas a futuro y realice la toma de decisiones de actividades que permita la optimización dentro de la red, estas actividades se las visualizan de manera estadística para una mejor comprensión (Limoncelli, Hogan y Chalup, 2007, pp. 523-524).

Este método de monitoreo tiene dos componentes principales, los cuales son:

- Recopilación de datos.
- Visualización de datos.

La interpretación de los resultados obtenidos mediante la monitorización histórica se los presenta en forma de conclusiones, como, por ejemplo: El servicio web de la empresa funcionó el 99.99% del tiempo en el año pasado, el equipo del departamento de administración estuvo operativo el 95% del tiempo del año pasado, etc.

La información que se recopila por medio de este método de monitoreo es usada ampliamente al momento del diseño y planificación de la capacidad de un sistema de telecomunicaciones, por ejemplo: mediante la visualización grafica de los datos recopilados del año anterior del porcentaje de utilización del ancho de banda de la red, se puede realizar una reingeniería que permita mejorar el rendimiento del sistema de comunicaciones. Entre las herramientas más usadas por los administradores de red para realizar un monitoreo histórico se tiene: Cricket y Orca.

1.2.2. Monitoreo en tiempo real

En la actualidad este método de monitoreo es el más usado, ya que advierte al administrador de la red en tiempo real la existencia de algún fallo tan pronto este suceda. De esta forma se pueden tomar medidas correctivas de manera inmediata evitando así que se vea comprometido el funcionamiento y rendimiento del sistema de telecomunicaciones, garantizando que todos los servicios se encuentren operativos (Limoncelli, Hogan y Chalup, 2007, pp. 527-528).

Al igual que la monitorización histórica, el monitoreo en tiempo real consta de dos componentes principales, los cuales son:

- Componente de monitorización.
- Componente de alertas.

Estos dos componentes tienen una relación directa, ya que dentro de un sistema de monitoreo en tiempo real no tiene sentido que la estación de monitoreo conozca de algún fallo o incidencia, a menos que pueda avisar sobre el problema a un recurso humano, en este caso al administrador de red.

El objetivo principal del método de monitorización en tiempo real es que el administrador tenga la información del fallo en el momento que sucede la incidencia, antes de que los clientes o usuarios de los servicios se den cuentan de este evento. Gracias a esto las interrupciones son más cortas ya que los problemas son solucionados de manera inmediata y se garantiza la calidad de servicio al usuario final.

Una característica de la red muy importante que se puede analizar mediante el proceso de monitoreo en tiempo real es la seguridad, ya que, el administrador podrá tener conocimiento en el momento exacto de efectuarse un determinado ataque dentro de la red de datos y realizar las acciones respectivas para evitar que la información se vea comprometida por el atacante.

Las herramientas más usadas por los administradores de red para realizar un monitoreo en tiempo real son: Nagios y Zabbix.

.

1.3. Gestión de redes de comunicaciones

En la actualidad, el crecimiento agigantado de las redes de una empresa o institución se ha vuelto uno de los factores críticos que un administrador de red debe analizar. En los últimos años las redes se han hecho más grandes y complejas para poder dar soporte a un mayor número de aplicación y usuarios, por esta razón, a medida que las redes tiene una escala mayor, surgen dos problemas principales, los cuales son:

- Las aplicaciones distribuidas y los elementos de la infraestructura de red se vuelven indispensable dentro de una organización.
- A medida que las redes crecen, pueden existir un mayor número de elementos que puedan presentar fallos, dejando inoperable una parte de la red o bajar el rendimiento a un nivel inaceptable.

Por esta razón, cuando la red de datos tiene un tamaño considerablemente grande, la gestión de la infraestructura de red no se puede realizar solo el recurso humano, debido a la gran complejidad que esta implica.

Para poder solucionar esto, nace la necesidad de crear protocolos y herramientas que faciliten la gestión de una red. Además de esto, cabe resaltar que dentro de una infraestructura de red se tienen varios equipos heterogéneos, es decir que los instrumentos que se usen para llevar a cabo el proceso de gestión deben tener soporte para varias marcas de los equipos de red.

Torres (2015), menciona que, la gestión de red se puede definir como la agrupación de varias actividades enfocadas en el control, organización y supervisión de los recursos con los que cuenta la infraestructura del sistema de telecomunicaciones, para poder garantizar una calidad de servicio para el usuario final. El objetivo principal de la gestión es asegurar un adecuado nivel de servicio usando los recursos gestionados con el menor costo, gracias a esto es posible mejorar la disponibilidad y el rendimiento, de esta forma se puede incrementar la efectividad de la red.

Para poder realizar la gestión de red de manera óptima y sistemática, se ha desarrollado diversos modelos de gestión de redes, como se puede observar en la Figura 2-1, los cuales permiten que un administrador de red tenga una guía o una serie de pasos que le permita realizar un proceso adecuado de acción al momento de ocurrir algún tipo de evento inesperado dentro de la red de datos, a continuación, se menciona los modelos de gestión más usados para la gestión de redes:

- Modelo de gestión OSI.
- Modelo de gestión TCP/IP.
- Modelo de gestión TMN.

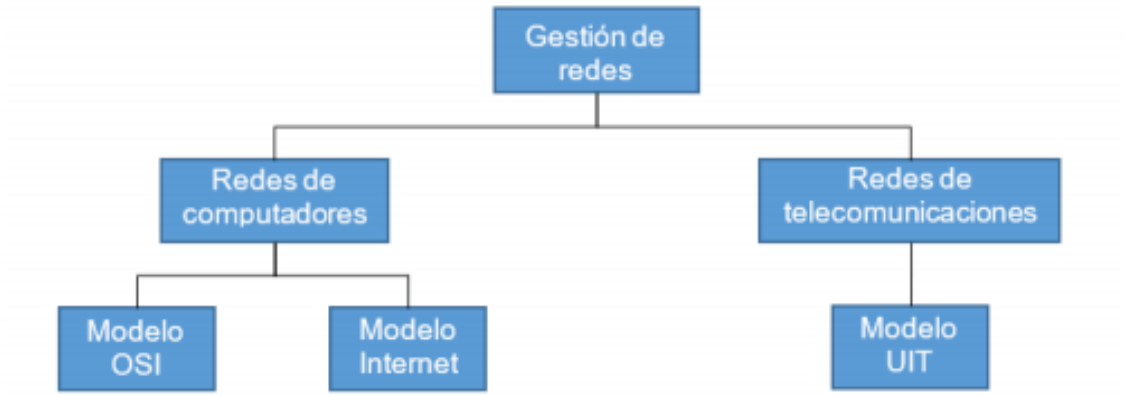


Figura 2-1. Mapa conceptual de modelos de gestión

Realizado por: Trujillo, J. 2019

1.3.1. Modelos de gestión

La gestión de redes de datos interconectadas son un conjunto de medidas que son fundamentales para garantizar la operatividad de manera eficaz del sistema y sus recursos, teniendo como eje principal incrementar la productividad y permitir el cumplimiento de los objetivos principales que tiene la organización.

Sin embargo, para realizar las diferentes actividades de gestión, hay que tener en cuenta que los sistemas de telecomunicaciones usan equipos de diferentes fabricantes, lo que hace que se tenga una infraestructura de red heterogénea, por esta razón se requiere que la gestión de red sea de manera integrada, para que de esta forma se pueda llevar a cabo el control de los equipos de una manera adecuada sin la necesidad de contar con un sistema de datos homogéneo (Duque, 2015, p.10).

Por esta razón surge la necesidad de que se presente distintos modelos de gestión de redes presentado por diferentes entidades. En base a Padilla y Ron (2015, p.10), un modelo de gestión se considera como la agrupación de varios criterios con el objetivo principal de gestionar una red de

la manera más óptima, y llevar a cabo el conjunto de actividades que se realizan dentro de la gestión de red de forma eficaz.

De acuerdo con Duque (2015, p. 12), los modelos de gestión presentado por las diversas entidades de telecomunicaciones, busca estandarizar de manera global la forma en la que se realiza las diferentes actividades de gestión, de esta forma se permite que sea integral y que pueda dar soporte a los sistemas de telecomunicaciones heterogéneos con los que cuentan las diferentes instituciones, organización o empresas. De esta forma se puede realizar la gestión integral con el mismo conjunto de herramientas, sin importar el fabricante de los equipos de telecomunicaciones.

Los modelos de gestión se basan en el paradigma gestor-agente, con lo que primero se realizan actividades de control y supervisión para luego proceder a ejecutar acciones por parte del gestor. Además, en base a Martí (Citado en Trujillo 2019), sin importar el modelo de gestión que se pretenda implementar, un sistema de gestión de red debe constar con una serie de funciones, las cuales se encuentran especificadas dentro del modelo FCAPS.

El modelo de función FCAPS, define un conjunto o serie de funciones que se encuentran detallas dentro de la norma ITU-M.3400, estas actividades son denominadas áreas funcionales de los sistemas de gestión, y esto permite la gestión integral de sistemas interconectados heterogéneos de forma estandarizada, independientemente del sistema de gestión de red que la organización o institución tenga implementada (Torres, 2015, p.10).

Las actividades que se propone en el modelo funcional FCAPS, son:

1. Gestión de fallos

El conjunto de funciones de la gestión de fallas o también conocido como mantenimiento permite al administrador de la red poder detectar, aislar y rectificar el funcionamiento del sistema de telecomunicaciones en el caso de existir un evento fuera de lo normal. Las métricas usadas para medir la gestión de fallas son la fiabilidad, disponibilidad y supervivencias o RAS: *reliability, availability* y *survivability* (Recomendación UIT-T M.3400, 2000, pp. 17-42).

2. Gestión de configuración

Dentro de este conjunto de funciones, la gestión de configuración permite tener un control para identificar, recoger datos y suministrar datos de los elementos de la red de telecomunicaciones (Recomendación UIT-T M.3400, 2000, pp. 43-60).

Entre las funciones más importantes se tiene:

- Planificación e ingeniería de la red.
- Instalación.

- Control.

3. Gestión de *accounting*

La gestión de la contabilidad permite la medición del uso de los servicios de red y la determinación del coste que representa para el proveedor de servicios, así como la cantidad que se ha de cobrar al cliente por el mencionado uso (Recomendación UIT-T M.3400, 2000, pp. 61-70).

Comprende los siguientes grupos de conjuntos de funciones:

- Medición de la utilización.
- Tarificación/fijación de precios.
- Control de la empresa.

4. Gestión de rendimiento

El grupo de funciones de la gestión de desempeño o rendimiento busca evaluar el comportamiento de los elementos de la red de telecomunicaciones y crear reportes al respecto, también estudia la relación de la efectividad que tiene el sistema (Recomendación UIT-T M.3400, 2000, pp. 6-17).

5. Gestión de seguridad

Estas funciones son las más importantes dentro de los modelos de gestión, ya que el conjunto de funciones de prevención o gestión de seguridad busca evitar la intrusión de personal no autorizado a la red de telecomunicaciones, para esto se realiza varias actividades como: control de seguridad de acceso físico, análisis del riesgo con él personal, evaluación del cifrado de seguridad que tiene la red de telecomunicaciones, etc. (Recomendación UIT-T M.3400, 2000, pp. 70-79).

1.3.1.1. Modelo de gestión OSI

La organización internacional de estándares OSI, ha definido una arquitectura para los sistemas de interconexiones abiertas, la cual a lo largo del tiempo se ha convertido en un modelo referencial dentro de los sistemas de telecomunicaciones para estandarizar y poder tener una interoperabilidad entre las diferentes marcas que existen en el mercado de las telecomunicaciones.

El modelo OSI define 7 capas, las cuales se pueden observar en la Figura 3-1, en donde se muestra la arquitectura de capas con la que se diseñó el modelo OSI.

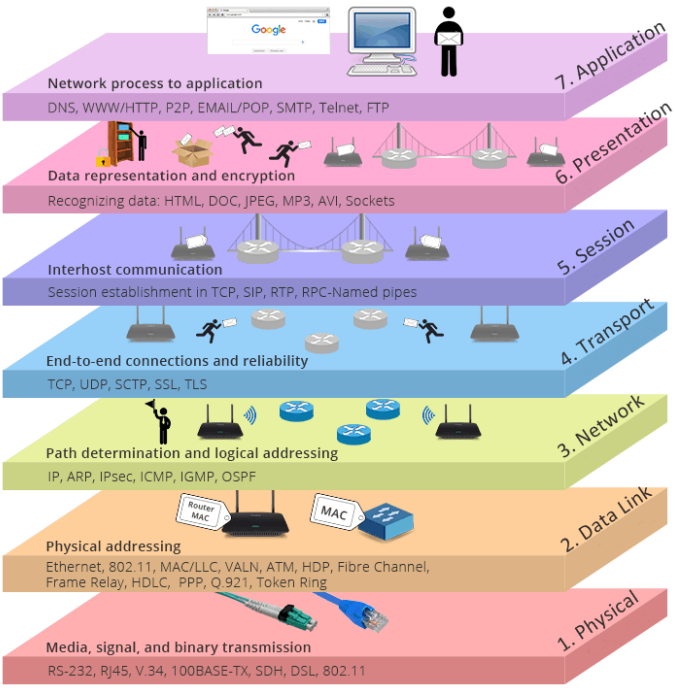


Figura 3-1. Capas del modelo OSI

Realizado por: FS *community*, 2019

Así mismo, OSI ha definido un modelo de gestión, cuyo principal objetivo es supervisar, controlar y mantener un sistema de telecomunicaciones, de esta forma se garantiza el funcionamiento óptimo de la red.

En base a Mercado (2008, p.12), dentro de este modelo de gestión se define de manera general tres formas principales de llevar a cabo una gestión en entornos OSI, los cuales son:

- Gestión de sistema.
- Gestión de nivel.
- Operación en nivel.

En la Figura 4-1, se muestra los niveles de gestión según OSI.

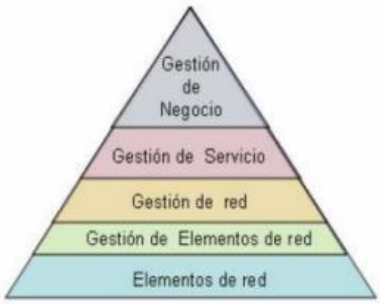


Figura 4-1. Niveles de gestión en el modelo OSI

Realizado por: Mercado, N. 2008

Para poder implementar este modelo de gestión, OSI usa los protocolos CMIP y CMIS, los cuales se los define en los estándares ISO/IEC 9595 y 9596, estos protocolos permiten gestionar los procesos de trasmisión de los datos, especifica las reglas de codificación de la gestión los procesos, y la arquitectura (Recomendación UIT-T X.711, 1997, pp. 12-23), como se observa en la Figura 5-1, de esta forma se logra la interpretación de la información.

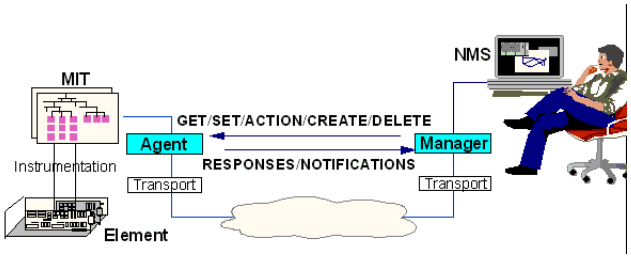


Figura 5-1. Operación del protocolo CMIP

Realizado por: Computación para ingenieros. 2010

1.3.1.2. Modelo de gestión TMN

El sector de normalización de las telecomunicaciones de la UIT, en base al modelo de gestión OSI, establece un nuevo modelo de gestión para los sistemas de telecomunicaciones denominado TMN (*Telecommunication Management Network*), el cual se encuentra definido dentro de la recomendación ITU-M.3010, en la cual se presentan conceptos básicos de la arquitectura del modelo de gestión de telecomunicaciones, así como un modelo de referencia lógico (Recomendación UIT-T M.3010 2000).

Debido a que el modelo de gestión TMN se basa en el modelo de gestión OSI, tiene varias características similares a este modelo de gestión, entre la cual se destaca el uso del paradigma Gestor-Agente y el paradigma orientado a objetos.

El modelo de gestión TMN define 3 arquitecturas diferentes para realizar la gestión de la red, estas son:

- Arquitectura física.
- Arquitectura funcional.
- Arquitectura de la información.

En el esquema de la Figura 6-1, se indica un ejemplo de la arquitectura física del modelo de gestión TMN.

Figura 6-1. Arquitectura física de TMN

Realizado por: López, R. 2010

1.3.1.3. Modelo de gestión TCP/IP

El modelo estándar para la conexión de internet TCP/IP, permite la conexión y comunicaciones entre equipos que se encuentran en diferentes redes, por medio del uso de diferentes aplicaciones como Telnet, FTP, HTTP, entre otros.

EL protocolo TCP/IP se encuentra conformado por:

- Protocolo de Control de Transmisión (TCP).
- Protocolo de Internet (IP).

En la Figura 7-1. se muestra la pila del protocolo TCP/IP.

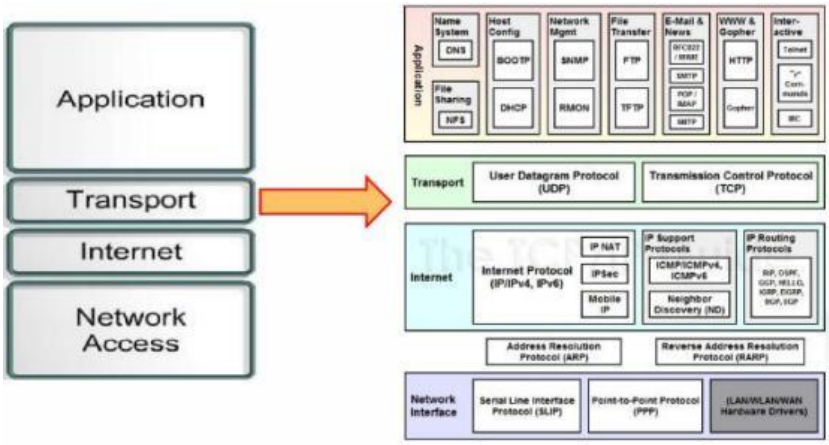


Figura 7-1. Pila del protocolo TCP/IP

Realizado por: Arellano, A. 2020

Al principio el protocolo ICPM (*Internet Control Message Protocol*), era usado para la gestión dentro del modelo TCP/IP, sin embargo, con el crecimiento de las redes se hizo necesario desarrollar un nuevo protocolo de gestión, de esta manera se creó el protocolo SNMP.

Para la gestión de las redes de datos, el protocolo SNMP consta de tres partes principales, las cuales son:

- Estructura de administración de información (SMI).
- Base de información de administración (MIB).
- Protocolo de administración de red simple (SNMP).

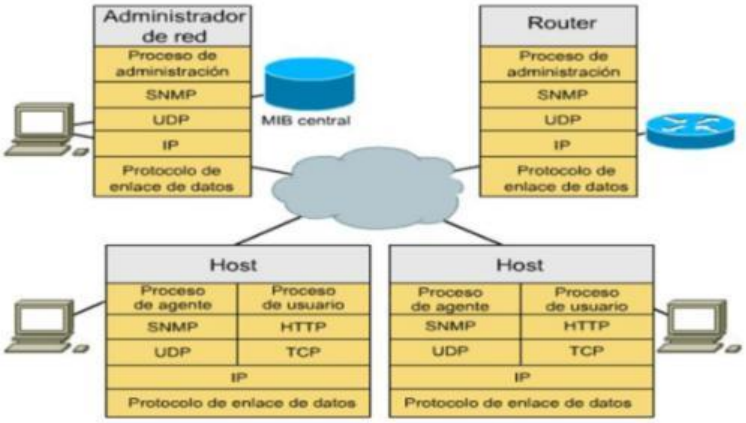


Figura 8-1. Ejemplo de la arquitectura SNMP

Realizado por: Pérez, L. 2013

1.4. Protocolo SNMP

El Protocolo Simple de Administración de Red (*Simple Network Management Protocol*, SNMP), es un protocolo de la capa de aplicación el cual fue diseñado como una estrategia para facilitar la administración y gestión de redes de telecomunicaciones basadas en el protocolo TCP/IP (Internet), mediante el intercambio de información entre los equipos que se encuentran dentro de sistema de administración de red.

De acuerdo con Stallings (1998, p.1), la versión original de protocolo SNMP (conocido actualmente como SNMPv1), se convirtió en el protocolo de monitoreo y supervisión más usado entre los administradores de redes independientes, sin embargo, a medida que su este protocolo era más demandado, sus deficiencias eran más notorias, entre las que se pueden destacar: falta de comunicación entre gestores, incapacidad de realizar envíos masivos de datos y la falta de

seguridad, por lo que para solucionar estos inconvenientes se desarrollaron las versiones SNMPv2 y SNMPv3.

En la Figura 9-1, se puede apreciar un ejemplo de una red gestionada mediante el uso del protocolo SNMP.

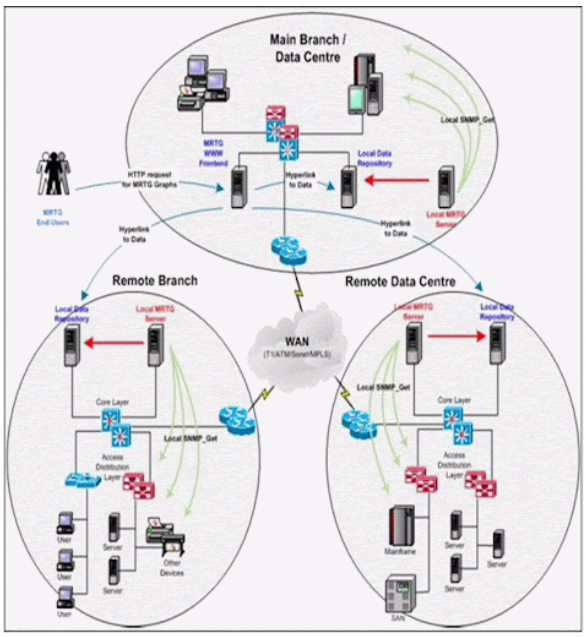


Figura 9-1. Red gestionada con SNMP

Realizado por: Pérez, L. 2013

Las especificaciones del protocolo SNMP se define en el RFC 1157, en la cual se puede encontrar los conceptos y definiciones básicas que usa el protocolo para la administración, tales como la arquitectura a emplearse, el formato del mensaje, la forma de operación del protocolo, etc. (RFC 1157, 1990).

1.4.1. Componentes básicos

Según Stallings (1998, p. 2), menciona que el modelo de gestión que utiliza el protocolo SNMP consta de 4 elementos claves los cuales son:

- Estación de gestión (NMS)

La estación de gestión generalmente es un dispositivo independiente, el cual sirve de interfaz entre el sistema de gestión y el gestor humano de la red que permite tener una supervisión y control de la red de datos. Una estación de gestión mínimo debe tener un conjunto de servicios que permita la gestión y análisis de datos, corrección de fallos, prevención de incidencias, etc.

- Agente de gestión

Son los equipos o entidades que serán gestionadas dentro del sistema de telecomunicaciones, estos equipos tendrán un software específico que les permita enviar información mediante el protocolo de gestión utilizado.

- Base de información de gestión (MIB)

La MIB es una estructura de datos en forma jerárquica de los objetos a ser administrados, para que así, de esta forma el NMS tenga una accesibilidad y pueda manipular el equipo vía SNMP. Dentro de las MIB se puede encuentra cuatro áreas bien definidas, las cuales son: Atributos del sistema, privadas, experimentales y de dirección (Ramirez, 2019).

- Protocolo de gestión de red

Para el intercambio de información de control, supervisión y gestión entre la estación de gestión y los agentes o entidades gestionados es necesario usar un protocolo el cual permita que la información pueda ser interpretada entres los equipos. En este caso el protocolo a usarse en el modelo de gestión será SNMP.

En la Figura 10-1, se puede identificar de manera clara cada uno de los elementos que utiliza el modelo de gestión SNMP.

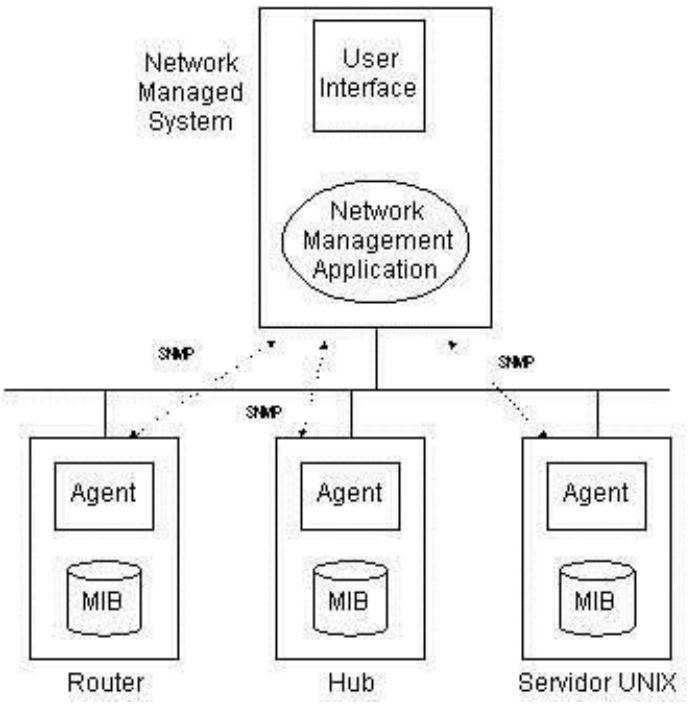


Figura 10-1. Elementos del modelo gestión de SNMP

Realizado por: Maraboli, M. 2010

1.4.2. Arquitectura

SNMP fue diseñado para ser un protocolo de la capa de aplicación de la pila del protocolo TCP/IP, para la transmisión de la información el agente por defecto utilizada el protocolo UDP, sin embargo, él envió de los datos también se puede realizar a través de TCP, como menciona Stallings (1998, p. 2), en el protocolo SNMP, el uso de TCP es muy bueno pero el uso de UDP es requerido.

En la Figura 11-1, se puede visualizar el proceso de encapsulación del PDU SNMP para el intercambio de la información.

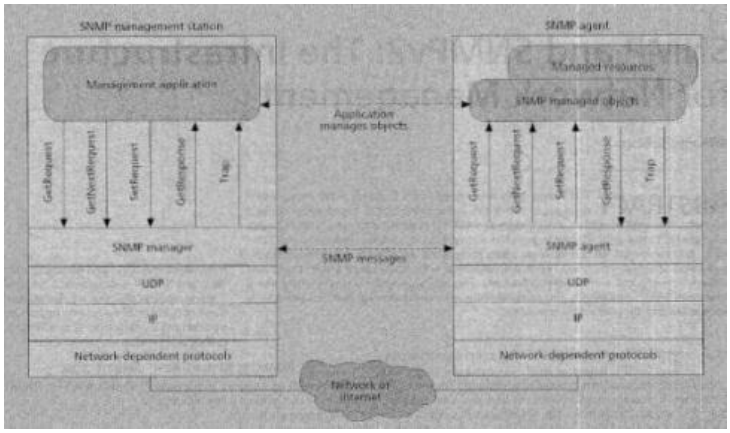


Figura 11-1. Funcionamiento de SNMP

Realizado por: Stallings, W. 1998

Desde la estación de gestión, se emiten 3 tipos de mensajes diferentes los cuales son: *GET, SET* y *TRAP*.

El mensaje *Get* es usado solo para lectura de la información que se genera en el sistema de gestión, este puede ser de tres tipos los cuales son: *GetRequest* y *GetNextRequest*, los cuales son usado para solicitar información desde la estación de gestión a un determinado agente mediante la inspección de las variables de la MIB y el *GetResponse*, el cual es el mensaje que envía el agente o entidad gestionada hacia la estación de gestión en respuesta a la solicitud que se haya requerido.

EL mensaje *SetReques*t, se usa para que la estación de gestión pueda realizar acciones de escritura, es decir este mensaje permite realizar cambios en las variables de la tabla MIB; el agente que recibe el mensaje responde a la estación de monitoreo con un mensaje *GetResponse*.

Los mensajes *Trap*, son unidireccionales, es decir el agente envía un mensaje a la estación de monitoreo al momento de ocurrir un determinado incidente, este mensaje no recibe una respuesta, tal y como se puede observar en la Figura 15-1.

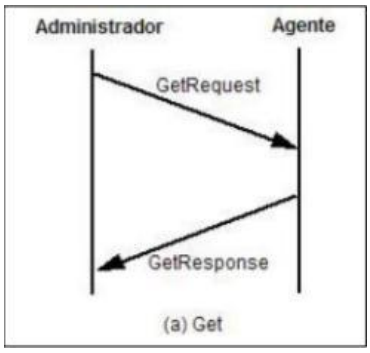


Figura 12-1. Intercambio de información con *Get*

Realizado por: Stallings, W. 1999

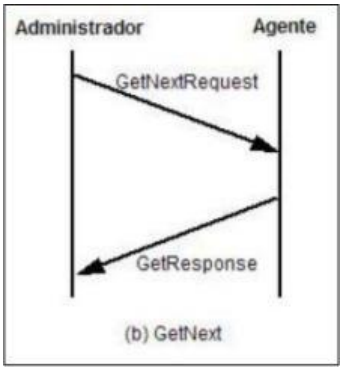


Figura 13-1. Intercambio de información con *GetNext*

Realizado por: Stallings, W. 1999

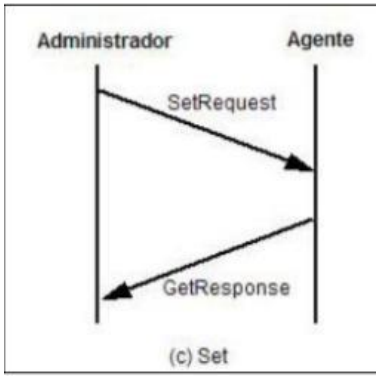


Figura 14-1. Intercambio de información con *Set*

Realizado por: Stallings, W. 1999

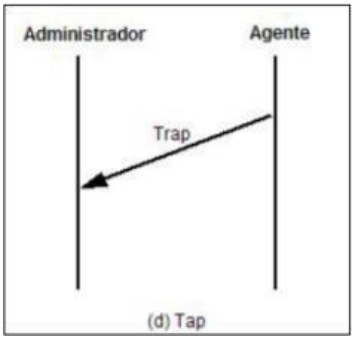


Figura 15-1. Intercambio de información con *Trap*

Realizado por: Stallings, W. 1999

1.4.3. Estructura del PDU

EL protocolo SNMP, para el transporte de la información lo realiza a través del protocolo UDP, por lo tanto, para transmitir un mensaje, la entidad SNMP crea un mensaje SNMP y la envía como datagrama UDP, usando por defecto el puerto 161, para realizar las consultas *Get* desde la estación de gestión a los agentes y el puerto 162 para que los agentes envíen los mensajes *Traps* hacia la estación de gestión (Ramirez, 2019, p.28).

Los campos de la estructura del datagrama UDP, se pueden visualizar en la Figura 16-1.

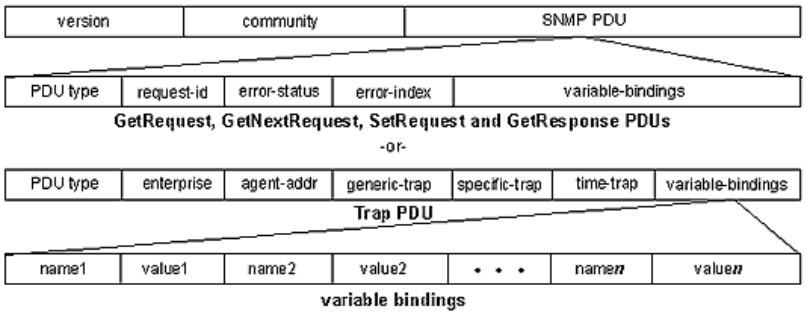


Figura 16-1. Estructura del PDU SNMP

Realizado por: DPS Telecom. 1999

Cada uno de los campos tiene una función bien definida, las cuales son:

- Versión: Indique la versión SNMP que se va a utilizar
- Comunidad: Relación que existe entre el agente y la estación de gestión
- SNMP PDU: Información que envía el agente SNMP

Los campos que se encuentra dentro del SNMP PDU, pueden variar dependiendo del tipo de mensaje que se enviar, tal como se muestra en la Figura 16-1, estos campos pueden ser:

Campos para los mensajes *GetRequest, GetNextRequest, SetRequest y GetResponse*:

- Tipo de PDU: especifica el tipo de mensaje que se va a enviar.
- *Request* ID: Es usado para distinguir entre las peticiones, cada petición tiene una identificación única.
- *Error-Status*: permite indicar que ha sucedido una irregularidad al momento de procesase la información.
- *Error-Index*: Cuando el campo *Error-Status*, avisa que existió un error, este campo proporciona información adicional del causando de la irregularidad.
- *Variable-bindings*: Este campo consiste en una secuencia de instancias de objetos referenciales, es decir contiene generalmente los datos solicitados por una determinada operación.

Campos para el mensaje *Trap*:

- *Enterprise*: Es el tipo de entidad que genero el mensaje *Trap.*
- *Agent-addr*: La dirección IP del equipo agente que envió el mensaje *Trap.*
- *Generic-trap*: Indica el tipo de *Traps* predefinidos.
- *Specific-trap*: Código específico que indica la naturaleza del *Trap.*
- *Time-traps*: Es el tiempo que paso desde la inicialización de la entidad que genero el *Trap* hasta la generación del *Trap*.

1.4.4. Versiones

1.4.4.1. SNMPv1

Es la primera versión desarrollada del protocolo SNMP, las únicas operaciones que se realiza en esta versión son las de inspección y alteración de las variables, específicamente estas acciones son:

- *SET*
- *GET*
- *TRAP*

En esta versión se encontró varias falencias entre las que se puede mencionar: la imposibilidad de variar la estructura de una tabla MIB, es decir no se puede agregar o borras instancias de objetos, no es posible enviar comandos para que el agente realice una acción determinada.

SNMPv1, solo proporciona acceso a un solo objeto del árbol de estructura de datos, es decir no se puede acceder a una tabla completa o a una fila de la tabla (Contreras, 2006, p.8).

Por estas restricciones el protocolo SNMPv1 tiene una facilidad de implementación, pero carece de ciertas características que limitan la gestión, por lo cual se desarrolló sus siguientes versiones.

1.4.4.2. SNMPv2

El protocolo SNMPv1 se popularizo rápidamente para la gestión de sistemas de telecomunicaciones, sin embargo, debido a las limitaciones que se encontró en este protocolo se desarrolló la versión SNMPv2. El protocolo SNMPv2 se encuentra definido dentro del RFC 3416, en el cual se especifica la operación del protocolo, arquitectura que se requiere, tipos de mensaje que envía, estructura del PDU, etc. (RFC 3416, 2002).

En base a Moreno y Serna (2013, p.26), este protocolo no incluye un mecanismo de seguridad, ya que sigue haciendo uso de las comunidades como método de autenticación del envió de la información, sin embargo, presenta mejoras en los sistemas de intercambio de la información de gestión.

Según Contreras (2006, p.17), las mejoras que se tiene en SNMPv2 sobre SNMPv1 son las siguientes:

- Desarrollo de una nueva base de información de gestión para esta versión de SNMP (MIB-II).
- Agregación de nuevas características a la estructura de información de gestión (SMI).
- Permite el intercambio de la información entre estaciones de gestión NMS (gestor-gestor).
- Aumento en el número de las operaciones definidas por el protocolo.
- Manejo de nuevas PDU.

La estructura del PDU es la misma usada por el protocolo SNMPv1, formada por los campos versión, comunidad y SNMP PDU, sin embargo, se han aumentado nuevos estados de error como se muestra en la Tabla 1-1, esto potencian la operación del protocolo SNMPv2.

Tabla 1-1: Nuevos estados de errores de SNMPv2.

Tipo de Error	Nº	Descripción
noAccess	6	Cuando se quiere acceder a un objeto del tipo not-accessible.
wrongType	7	Indica que se quiere establecer a una variable con un tipo de dato no permitido.
wrongLength	8	Indica que una variable se quiere establecer con una longitud superior a la permitida.
wrongEncoding	9	Indica una codificación errónea en el valor del objeto.
wrongValue	10	Indica que ese valor no puede ser asignado a la variable.
noCreation	11	Indica que no se puede cambiar el valor de la variable que no existe.
inconsistentValue	12	No se puede asignar el valor por su estado incoherente.
resourceUnavailable	13	No se cuenta con los recursos suficientes para realizar el cambio de valor.
commitFailed	14	Indica que existen fallas en las operaciones de escritura.
undoFailed	15	Debido a las fallas no se pueden revertir los valores.
authorizationError	16	Indica que el nombre de comunidad es incorrecto.
notWritable	17	Indica que la variable no permite realizar procesos de escritura.
inconsistentName	18	Indica el intento de cambiar el valor de una variable con nombre inconsistente.

Fuente: Moreno, A.; Serna, S. 2013

Realizado por: Duche, I, 2021

También el protocolo SNMPv2 añade nuevos mensajes, los cuales son:

- *GetBulkRequest*

Este PDU ayuda a disminuir el número de intercambios de información que se quiere para poder recuperar un gran volumen de información, esto quiere decir que mediante este mensaje se puede recibir una mayor cantidad de datos con una sola solicitud.

- *InformRequest*

Gracias al aumento de este mensaje, se logró el intercambio de la información entre las estaciones de gestión (gestor-gestor). Al momento de que una estación de gestión recibe un mensaje *InformRequest*, el gestor construye un mensaje de tipo *GetResponse* con los mismos valores que contiene el PDU de entrada en el caso de que la respuesta sea exitosa, caso contrario se indicara un error.

- *Trap* v2

El PDU *Trap* v2, cumple las mismas funciones que el PDU *Trap* en la versión SNMPv1, el cual es la de enviar un mensaje al gestor en caso de un determinado evento, sin embargo, este tipo de mensaje difiere en el formato para facilitar el procesamiento del mensaje en la estación de gestión.

La estructura del PDU es la misma que del mensaje *InformRequest*, y dentro del campo *variable-bindings* incluyen los objetos:

- *sysUpTime*
- *sysOID*

1.4.4.3. SNMPv3

Debido a la carencia de seguridad que se tenía en las versiones anteriores SNMPv1 y SNMPv2, se desarrolló la versión SNMPv3, lo cual mediante el uso de algoritmos de encriptación y autenticación se permite proteger a la información de amenazas de seguridad como:

- Modificación de la información
- Enmascaramiento
- Reenvió de los mensajes
- Falta de privacidad (*disclosure*)

Sin embargo, no se encuentra diseñado para prevenir tipos de ataques como:

- DDoS
- *Sniffer*

Sus características y especificaciones de encuentran definidas en el RFC 3414.

Como se ha mencionado, el protocolo SNMP funciona a través de entidades, lo cual permite encontrar al objeto dentro del sistema de gestión ya sea como un nodo agente o un nodo gestor, en la Figura 17-1, se enseña el diagrama de una entidad SNMPv3.

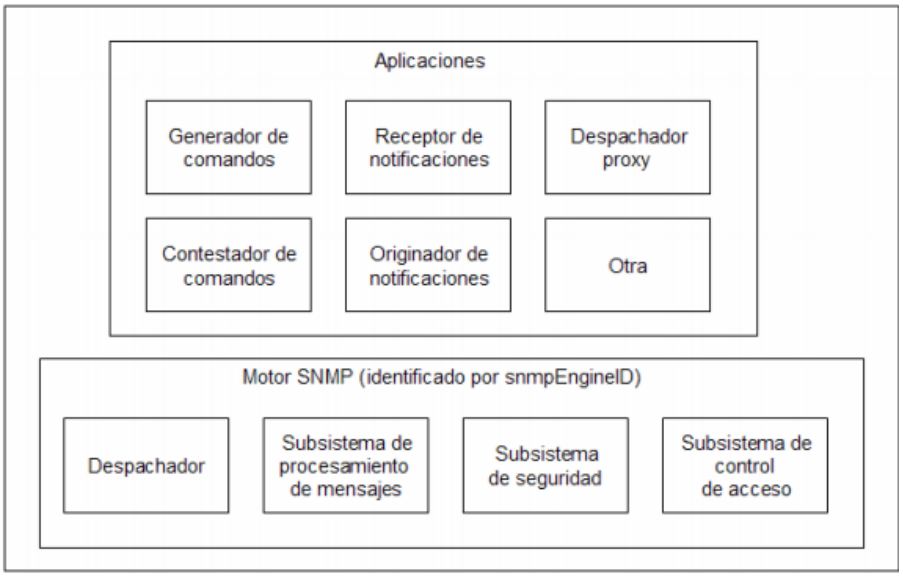


Figura 17-1. Estructura de una entidad SNMPv3

Realizado por: Botero, N. 2005

De la misma forma que con las versiones anteriores del protocolo, SNMPv3 agrega nuevos campos que mejoran el intercambio de información entre las diferentes entidades SNMP, tal como se muestra en la Figura 18-1.

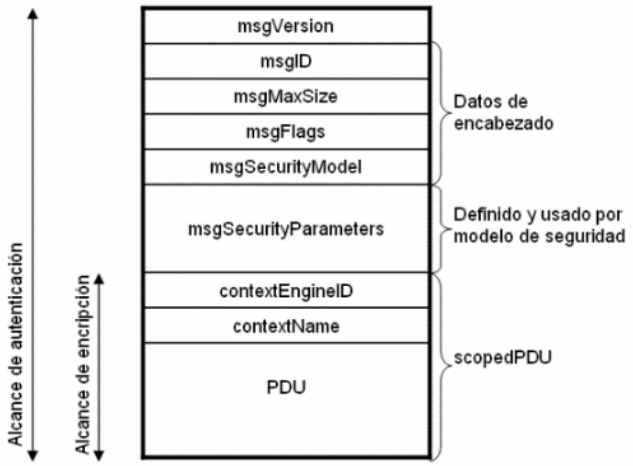


Figura 18-1. Campos de un mensaje SNMPv3

Realizado por: Botero, N. 2005

1.4.5. MIB

Dentro del protocolo SNMP, todos los objetos gestionados se encuentran organizados bajo una estructura jerárquica en forma de árbol, esta estructura es conocida como *Management Information Base* (MIB), la cual se encarga de almacenar la información de los agentes.

La información acerca de la MIB se encuentra contenida en el RFC 3418. Este es un componente indispensable dentro del protocolo SNMP, ya que gracias a la MIB es posible que el protocolo pueda gestionaran los nodos de una manera eficiente. Dentro de la tabla MIB, en las hojas del árbol de la estructura jerárquica se encuentra los objetos gestionados, lo cual representa la información, actividad o recurso que la estación de gestión haya solicitado al nodo administrado (RFC 3418, 2002).

La MIB, para poder definir su estructura en forma de árbol, lo hace a partir del agrupamiento de objetos dentro de conjuntos o grupos con características similares o que se relacionan de manera lógica, tal como se puede ver en la Figura 19-1.

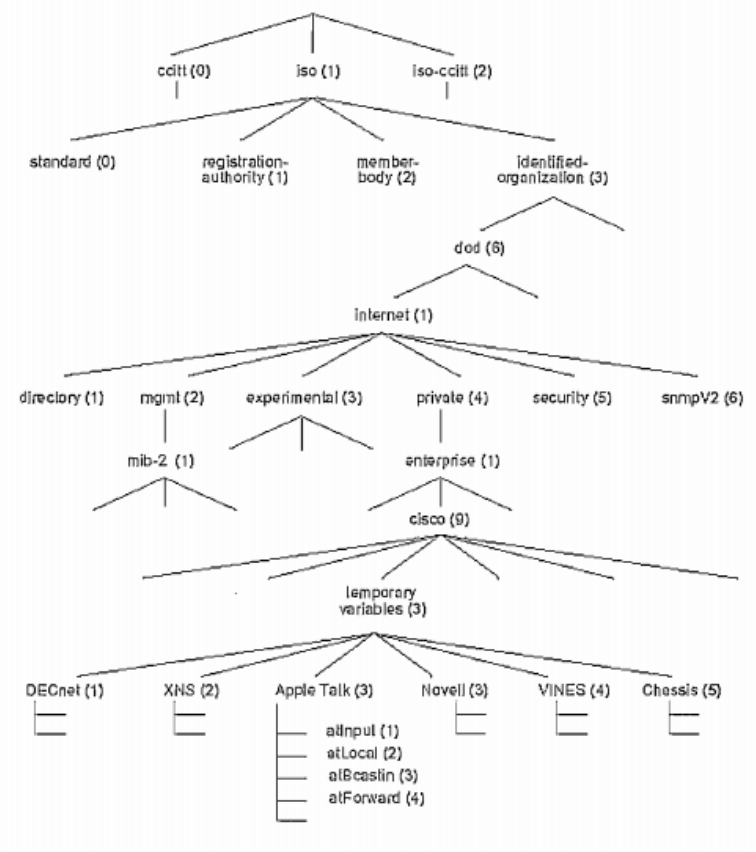


Figura 19-1. Ejemplo de una estructura MIB

Realizado por: Contreras, C. 2006

1.4.6. SMI

La Structure of Management Information (SMI), permite definir los nombres y la sintaxis de los objetos individuales a ser gestionados, es decir, la SMI ayuda a la identificación de los tipos de datos y los recursos que se pueden usar dentro de la MIB. Las especificaciones se encuentras

definidas según la versión, la SMIv1 se encuentra dentro del RFC 1155 y 1215, mientras que la SMIv2, la cual contiene actualización de la versión anterior se la puede encontrar en el RFC 2578.

Cada objeto gestionado contiene los siguientes atributos:

- OID, el cual permite la identificación única de cada objeto de forma individual.
- Tipo y Sintaxis, se define la sintaxis mediante el uso de ASN.1.
- Codificación.

Dentro de la SMI, se pueden clasificar los tipos de datos, para SMIv1 se tienen:

- Primitivos
- Estructurados
- Definidos o Etiquetados

Mientras que para la versión SMIv2 se han agregado nuevos tipos de datos, los cuales se pueden observar en la Tabla 2-1.

Tabla 2-1: Nuevos tipos de datos en SMIv2.

TIPO DE DATO	DESCRIPCIÓN
INTEGER32	Igual al tipo de dato INTEGER.
COUNTER32	Igual al tipo de dato COUNTER.
GAUGE32	Igual al tipo de dato GAUGE.
UNSIGNED32	Representa valores decimales entre 0 y $2^{32} - 1$, inclusive.
COUNTER64	Similar a COUNTER32, su valor máximo es $2^{64} - 1$.
BITS	Utilizado para enumerar bits no negativos.

Fuente: Moreno, A.; Serna, S. 2013

Realizado por: Duche, I, 2021

1.4.7. ANS.1

Es un tipo de lenguaje formal diseñado para poder definir la sintaxis de los tipos de dato que van a ser intercambiados entre sistemas heterogéneos, el ASN.1 (*Abstract Syntax Notation One*), se encuentra definida en las recomendaciones ITU-T X.208 y 209. Entre algunos ejemplos se puede encontrar:

- Telefonía (SS7)
- Aviación
- Redes de Datos (SNMP)
- Banca

Este lenguaje entrega un conjunto de reglas que permiten caracterizar la estructura de los objetos, es decir brinda una sintaxis a cada objeto individual de la SNMP MIB, definiéndolo de una manera formal, sin embargo, para tener una simplicidad solo se usan subconjuntos de elementos y características.

Entre los tipos de datos permitidos dentro de protocolo SNMP se pueden encontrar:

- Tipo Universal
- Tipo Aplicación-Extendida
- Tipo Contexto-Especifico
- Tipo Privada

A continuación, en la Figura 20-1, se puede visualizar los tipos de datos permitidos en la etiqueta identificador.

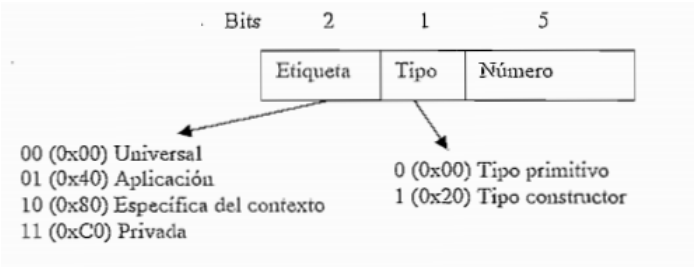


Figura 20-1. Datos permitidos en ASN.1

Realizado por: Contreras, C. 2006

1.4.8. OID

Dentro del protocolo SNMP, un componente muy importante son los OIDs (*Object IDentifier*), siendo estos las direcciones de un nodo que se encuentran dentro de una estructura MIB. Están conformadas por número enteros positivos y su separación se la realiza por medio de puntos.

Los OIDs, se forman al inicio con un punto el cual indica la raíz, a continuación, el objeto se le identifica mediante un sufijo, de acuerdo en el tipo de dato que retorna. Así mismo, contiene un valor único el cual puede ser un entero o una cadena de caracteres. Cabe recalcar que se utilizan sufijos distintos a cero para cada tabla, por ejemplo, el OID del nodo *system* se define como: .1.3.6.1.2.1.1

1.5. Logs

Los archivos *logs* son diferentes registros que se generan cuando sucede un determinado evento dentro de dispositivos como, servidores, computadoras de escritorios, equipos de red, etc. que se encuentran dentro de una empresa u organización. El contenido de estos archivos es la información que se relaciona con el evento especifico que haya ocurrido dentro del equipo, red o sistema (Vieda, 2020).

En base a Fiallos (2018, p.12), los *logs* se los considera como ficheros o archivos de texto en los cuales se almacena la información de eventos importantes que hayan ocurrido dentro de la red o sistema de telecomunicaciones. Entre las acciones más importantes que se almacena dentro de estos archivos son: conexiones remotas, inicios de sesión en un equipo, cambios realizados en el equipo, dirección de origen, etc.

Para la compresión de los archivos o registros *logs* de un sistema, se debe tener en cuenta determinadas definiciones y conceptos, los cuales son:

- Los *logs* son registros oficiales de un determinado evento ocurrido, los cuales se almacenan en el equipo en forma de archivo por un determinado periodo de tiempo.
- Al momento de ocurrir un determinado evento, el archivo *log* generado debe permitir al administrador responder las siguientes preguntas: ¿Qué?, ¿Quién?, ¿Cuándo?, ¿Dónde? y Por qué?

Para poder realizar una correcta gestión de los registros *logs*, según Fiallos (2018, pp. 12-17), se debe realizar 4 acciones principales, las cuales son:

- **Administración de *logs*:** Es el proceso por el cual se encarga de la generación, transporte, almacenamiento, análisis y reportes de los archivos logs. Existe dos formas de administrar la priorización de los archivos *logs*: los más importantes y los más significativos.

- **Análisis de *logs*:** Es la fase más importante y compleja que el administrador de la red debe realizar, ya que se debe hacer uso de los métodos de análisis de *logs*, esta tarea se puede complicar cuando el sistema es muy grande. Para realizar el análisis de *logs* se tiene 3 conceptos principales que se deben analizar, estos son: correlación de eventos, visualización y reportes.

- **Retención y reducción de *logs*:** En esta fase se analiza el almacenamiento por un determinado periodo de tiempo de los archivos *logs* generados por los diferentes equipos, de

acuerdo con las diferentes políticas que tenga la empresa, con la finalidad de que estos eventos puedan ser analizados posteriormente.

- **Rotación de *logs*:** Es la fase final, en la cual se estudia el cierre de un registro *log*, el cual ya haya sido analizado anteriormente y se logró solucionar el problema. Antes los archivos *logs* eran usados para la búsqueda y solución de errores, en la actualidad debido al gran número de equipos que pueden existir dentro de un sistema, los archivos *logs* son usados para realizar una mayor cantidad de acciones como: optimización del sistema, registro de actividades de los usuarios, seguridad, etc.

1.6. Protocolo Syslog

1.6.1. Definición

En base a Gómez (2014, p.8), Syslog permite a los servidores, computadores o equipos de telecomunicaciones (Origen), enviar información de los diferentes eventos que pueden ocurrir dentro de un sistema de telecomunicaciones, hacia los equipos encargados de recibir los mensajes de los eventos (Colectores), conocidos como servidores Syslog. Estos mensajes pueden ser almacenados localmente en el mismo dispositivo.

De acuerdo con Ramirez (2019, p.35), Syslog es un sistema de registros *logs*, cuyo objetivo principal es el manejo, control y administración del archivos *logs*, que generan los eventos ocurridos dentro del sistemas o red de telecomunicaciones. Este protocolo otorga una forma de transporte, para que el mensaje que envía los equipos que notifican del evento pueda llegar al equipo configurado con el protocolo Syslog como servidor.

También, como menciona Fiallos (2018, p. 12), Syslog es un estándar que sirve para la recopilación, administración y transporte de los mensajes de notificación de eventos que ocurren dentro de un sistema de telecomunicaciones, es decir permite el envió de la información de los *logs* del sistema, por lo tanto, se puede decir que este protocolo permite el procesamiento y manejo de los registros del sistema.

Por lo tanto, se puede decir que el estándar Syslog permite centralizar el transporte, manejo y captura de los archivos *log* que genera el sistema de telecomunicaciones. Sus especificaciones se encuentran registradas en la IETF dentro del RFC 5424, en el cual se encuentra la arquitectura, el formato del mensaje, conceptos del mapeo de transporte, descripción de los elementos de los datos estructurados, entro otros (RFC 5424, 2009).

1.6.2. Funcionamiento

Los equipos y servicios que soportan el registro y envío de archivos *logs*, puede formar parte del sistema y poder usar el protocolo Syslog, ya que podrán enviar cualquier tipo de mensaje *log* que se haya generado al momento de que exista algún evento inesperado. Entre los mensajes más comunes que son enviados se tiene: seguridad del sistema, errores, avisos, información, controles de acceso, entre otros. Sin embargo, el mensaje enviado por el equipo puede contener cualquier otro tipo de información, además de esto, el mensaje también incluye la fecha y hora del envío, el equipo que envía, la prioridad y otros datos adicionales que puedan servir para el análisis del registro.

La forma de operación del protocolo Syslog consiste en que los clientes (*Originator*), al momento de ocurrir algún evento que se registra como un *log*, envía un pequeño mensaje no mayor a 1024 bytes, a un equipo configurado como servidor Syslog (*Collector*), el cual será el encargado del procesamiento y almacenamiento de los mensajes enviados para ser analizados por el administrador posteriormente.

Estos mensajes generalmente son enviados hacia el servidor de Syslog en formato de texto plano, usando el protocolo UDP, por medio del puerto 514, sin embargo, existen aplicaciones las cuales permiten hacer uso del protocolo TCP reemplazando el protocolo UDP. También admiten el uso de *Stunnel* para que la información de los datos pueda viajar de una manera cifrada mediante SSL/TLS (Gómez, 2014, p.13).

En la Figura 21-1, se puede ver un esquema de diseño de un sistema de registros de *logs* del sistema haciendo uso del protocolo Syslog.

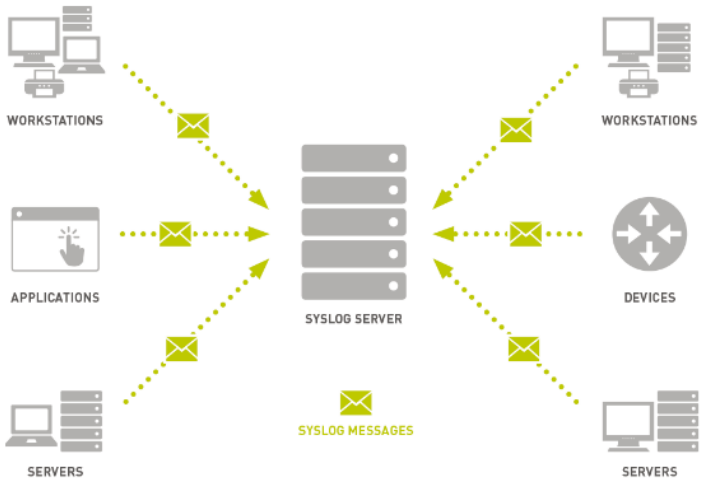


Figura 21-1. Esquema de sistema Syslog

Realizado por: Paessler. 2020

1.6.3. Arquitectura

En base al RFC 5424 (RFC 5424, 2009), define un modelo de capas para especificar la arquitectura del protocolo Syslog, dentro del RFC se ha definido tres capas las cuales son:

- Contenido Syslog

Esta capa se encarga de la gestión de la información y del contenido del mensaje Syslog que ha enviado el equipo.

- Aplicación Syslog

El principal objetivo de esta capa es la de gestionar la generación, interpretación, *routing* y almacenamiento de los mensajes Syslog enviados al sistema.

- Transporte Syslog

Esta capa se encarga de colocar el mensaje Syslog para su envío y recepción a través del sistema de red.

En la Figura 22-1, se puede observar la arquitectura de capas que tiene el protocolo Syslog, de acuerdo con el RFC 5424.

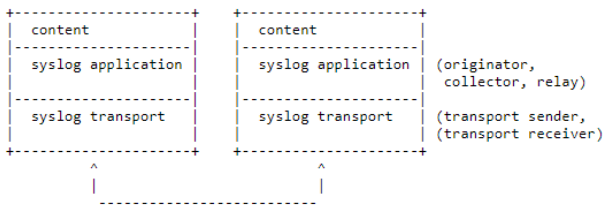


Figura 22-1. Arquitectura de capas de Syslog

Realizado por: RFC 5424. 2009

1.6.4. Componentes

En base al RFC 5424 (2009), el protocolo Syslog define 3 componentes principales, los cuales son:

- *Originator*

Son los equipos encargados de la generación del contenido de los mensajes cuando sucede algún evento inesperado.

- *Relay*

Son equipos encargados de reenviar los mensajes generados por los dispositivos *Originator,* hacia otros equipos *Relays* o hacia el equipo *Collector.*

- *Collector*

También conocido como servidor Syslog, es el equipo encargado de procesar y almacenar los mensajes que envían los equipos del sistema para su posterior análisis.

En la Figura 23-1, se muestra un ejemplo del posible escenario que se puede diseñar para la implementación del protocolo Syslog.

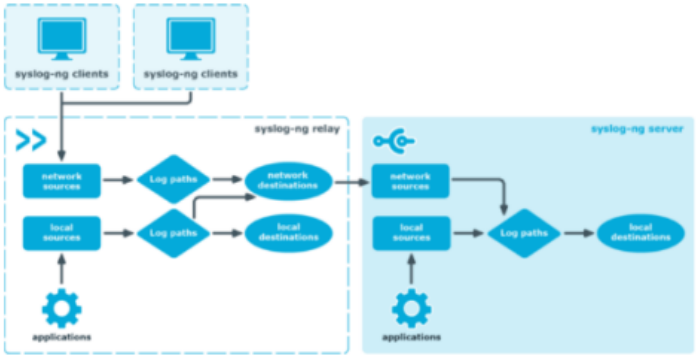


Figura 23-1. Arquitectura Syslog en modo cliente

Realizado por: Syslog-ng, 2021

1.6.5. Estructura del mensaje

La estructura del mensaje Syslog se conforma de tres partes principales los cuales son:

1. *Header*

Tiene varios campos los cuales ayudan a la identificación del tipo del mensaje que se envía, los campos más importes del *header* son los siguientes:

- PRI
- VERSION
- TIMESTAMP
- HOSTNAME
- APP-NAME
- PROCID
- MSGID

Dentro del campo PRI del *header*, se puede identificar dos aspectos importantes los cuales ayudan a la priorización del mensaje enviado, estos son: Recursos y Severidades.

En la Figura 24-1, se describe los valores que puede tener las severidades, mientras que en la Figura 25-1, se detalla los recursos que se pueden encontrar.

Keyword	Numeral	Description	
Emergency	0	System unusable	Severe
Alert	1	Immediate action required	
Critical	2	Critical Event (Highest of 3)	Impactful
Error	3	Error Event (Middle of 3)	
Warning	4	Warning Event (Lowest of 3)	
Notification	5	Normal, More Important	Normal
Informational	6	Normal, Less Important	
Debug	7	Requested by User Debug	Debug

Figura 24-1. Recursos *de* Syslog

Realizado por: Cisco, 2020

Código Numérico	Funcionalidades
0	*kernel messages*
1	*user-level messages*
2	*mail system*
3	*system daemons*
4	*security/authorization messages*
5	*messages generated internally by Syslogd*
6	*line printer subsystem*
7	*network news subsystem*
8	*UUCP subsystem*
9	*clock Daemon*
10	*security/authorization messages*
11	*FTP Daemon*
12	*NTP subsystem*
13	*log Audit*
14	*log alert*
15	*clock Daemon*
16	*local use 0 (local0)*
17	*local use 1 (local1)*
18	*local use 2 (local2)*
19	*local use 3 (local3)*
20	*local use 4 (local4)*
21	*local use 5 (local5)*
22	*local use 6 (local6)*
23	*local use 7 (local7)*

Figura 25-1. Severidades de Syslog

Realizado por: Cisco, 2021

2. Datos estructurados

Los datos estructurados (*Structured-Data*), se encargan de proporcionar un mecanismo de expresión de la información en un formato de datos bien definido y que sea fácilmente interpretable. Esta parte del mensaje puede tener cero, uno o varios datos estructurados los cuales se los define como Elementos SD.

3. Mensaje

Una vez analizados el *header* y la estructura de los datos, el resto del paquete Syslog será el texto del mensaje, el cual contiene la información sobre el proceso o evento que se generó en el equipo que envía dicha información.

En la Figura 26-1, se muestra un ejemplo de la estructura que puede tener un paquete Syslog.

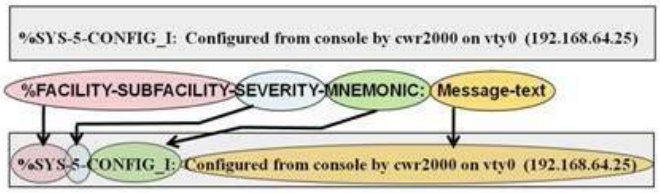


Figura 26-1. Ejemplo de mensaje Syslog

Realizado por: Cisco, 2021

1.7. Servidores

(Posey, 2021) menciona que, un servidor es un dispositivo informático físico o programa que proporciona un determinado servicio o recurso a un usuario, también denominado cliente, en un *Data Center*. Una computadora física que ejecuta un programa de servidor también puede ser denomino como tal, estas máquinas pueden dar servicios dedicados o puede usarse con otros fines como el de compartir recursos.

Los servidores son los encargados de brindar una gran variedad de servicios a los clientes, entre los que se puede encontrar: servicios de seguridad y autenticación, páginas web, correo electrónico, trasferencia de archivos, etc. Dentro de una red se puede tener un único servidor que proporcione varios servicios o un grupo de servidores, donde cada uno permita proporcionar un servicio en específico.

Un ejemplo de servidor fisco se lo puede observar en la Figura 27-1.

Figura 27-1. Servidor

Realizado por: Blancarte, O. 2021

1.7.1. Virtualización

En base a IBM, citado en (Fernández y García 2011), la virtualización es una estrategia la cual consiste en segmentar los recursos que tiene un computador físico en entorno de ejecución múltiple mediante el uso de conceptos informáticos, como la partición de recursos, tiempos compartidos, emulación de computadores, calidad de servicios, etc.

También, de acuerdo con Cabrera (2017, p.18), la virtualización consiste en la ejecución de varias máquinas de manera virtual dentro de una misma maquina física, donde a cada una de estas máquinas virtuales les corresponde un segmento de los recursos del servidor físico, así mismo, las distintas máquinas virtuales pueden operar con diferentes sistemas operativos y ejecutar varias aplicaciones dentro del mismo dispositivo físico.

(Sotaminga, Guerrero y Abad 2011) manifiesta que, el principal objetivo de la virtualización es poder tener varios sistemas operativos sobre uno ya existente, como se muestra en la Figura 28-1, sin que estos se vean afectados. Estas máquinas virtuales operar de una manera totalmente independiente gracias a que la virtualización genera una capa de software denominada *Virtual Machine Monitor*, de esta forma se crea una capa de abstracción entre el equipo fisco y el sistema operativo de la máquina virtual.

Figura 28-1. Ejemplo de servidor virtualizado

Realizado por: Blancarte, O. 2021

1.7.1.1. Hipervisor

Al momento que se realiza la virtualización, en este proceso se genera una capa de software intermedia entre la parte física y las máquinas virtuales, esta capa de virtualización requiere que tenga una supervisión (*Hypervisor*) la cual se encargue de asignar los recursos físicos a cada una de las máquinas virtuales, tal y como se observa en la Figura 29-1.

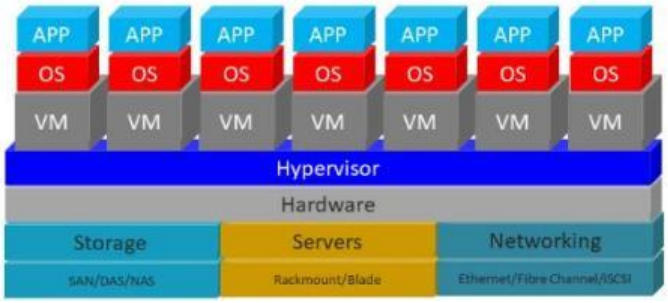


Figura 29-1. *Hypervisor*

Realizado por: Blancarte, O. 2021

El *Hypervisor* se encarga de generar el ambiente de las máquinas virtuales dentro de un equipo fisco, de esta forma se tiene un control maestro con los privilegios de más alto nivel, ya que este se encargará de la administración de una o más máquinas virtuales, también conocidos como sistemas operativos huéspedes (Fernández y García 2011).

Como se muestra en la Figura 30-1, los *Hypervisores* pueden ser clasificados en 2 tipos principales: virtualización alojada y virtualización nativa (*bare-metal*).

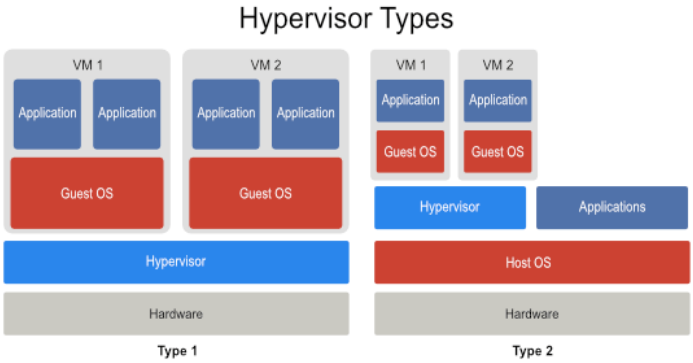


Figura 30-1. Tipos de *Hypervisor*

Realizado por: Blancarte, O. 2021

1.8. Software de monitoreo de red

Para el monitoreo y gestión de los sistemas de comunicaciones se requiere usar protocolos de monitoreo, los cuales permitan recopilar información que ayuden a la administración de la red de datos y garantice el funcionamiento óptimo. Sin embargo, como se muestra en la Figura 31-1, es necesario que la información de los datos recopilados se pueda visualizar de una forma organizada, para esto se requiere un software o aplicación específica que permita al administrador de la red observar los diferentes eventos que se presentan dentro de la infraestructura de la red de telecomunicaciones.

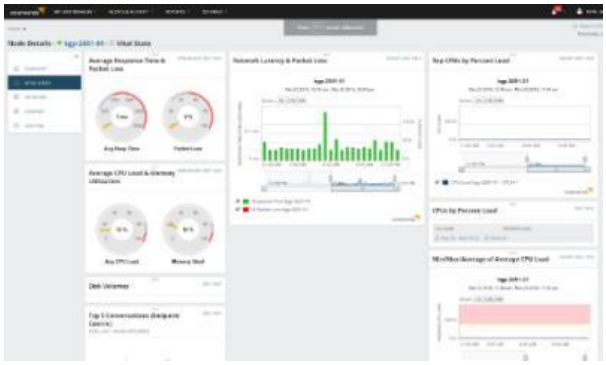


Figura 31-1. Ejemplo de aplicación de monitoreo

Realizado por: SolarWinds. 2021

Por lo general, el protocolo SNMP es el más usado para el monitoreo de los sistemas de telecomunicaciones. Por lo tanto, existen varios softwares, ya sean licenciados u *open source*, que permiten organizar y visualizar la información enviada por los equipos, entre los más se tiene: Zabbix, Cacti, Nagios y SolarWinds.

1.8.1. Network Performace Monitor (NPM)

SolarWinds, es una empresa dedicada al desarrollo de software y de herramientas para la infraestructura TI, esta brinda varias aplicaciones que permite el monitoreo de la red de datos, adaptándose a las necesidades del cliente, ya sea dependiendo del protocolo a usarse y de que parte de la infraestructura de red se desea administrar y gestionar.

La empresa distribuye sus productos por medio de licencias, las cuales, varían su precio entorno a la aplicación y el tipo de licenciamiento que se solicite, sin embargo, a pesar de que sus licencia tiene un alto costo, estas soluciones se recomienda para empresas grandes, ya que facilita la administración y gestión de sus infraestructuras de red (SolarWinds, 2021).

Para el uso del protocolo SNMP, SolarWinds ha desarrollado la aplicación *Network Performace Monitor* (NPM), el cual tiene varias características que lo hacen un software robusto al momento de realizar el monitoreo de red, ya que dentro de la aplicación existen varios servicios lo cuales permiten llevar un control adecuado de la infraestructura de red.

1.8.1.1. Características

La aplicación NPM es un potente software de monitoreo, el cual mediante sus servicios incorporados permite la detección, diagnóstico y resolución de problemas que se puede presentar en una infraestructura de red (SolarWinds, 2021).

De acuerdo con la página oficial de la herramienta NPM, sus características principales se mencionan en la Tabla 3-1.

Tabla 3-1: Características de aplicación NPM

CARACTERÍSTICA	DESCRIPCIÓN
Gestión de fallas, desempeño y disponibilidad	Permite la detección de fallas para poder dar un diagnóstico de la red y resolver el problema de una manera rápida evitando la inactividad de la red.
Análisis salto por salto en rutas críticas	visualización al detalle de la configuración de los equipos y el tráfico por medio del servicio NetPath™.
Cuadros de desempeño de la red del tipo arrastrar y detectar	Mediciones de desempeño de la red en tiempo real con cuadros y gráficos interactivos de los dispositivos de red.
Reportes personalizables de desempeño y disponibilidad	Permite la generación de reportes personalizados sobre las diferentes actividades gestionadas dentro de la aplicación.
Monitoreo del estado del hardware	La aplicación permite la medición de los recursos físicos de los equipos monitoreados.
Administración de redes inalámbricas	Realiza mediciones de equipos inalámbricos como Access Point y clientes.
Software de monitoreo de redes personalizable en un único panel	El administrador puede personalizar el *Dashboard* que ofrece la aplicación NPM, de acuerdo con su necesidad.
Referencias estadísticas dinámicas del desempeño de la red	Visualización de recursos monitoreados por medio de graficas estadísticas.
Monitoreo de red de varios proveedores	Soporta la gestión de los equipos de un gran número de marcas.
Monitoreo de varios servicios	Además de la gestión y monitoreo de equipos de red, la aplicación NPM permite el monitoreo de diferentes dispositivos como: Servidores, Equipos en la nube, UPS, RTU, etc.

Fuente: SolarWinds, 2021

Realizado por: Duche, I, 2021

1.8.1.2. Ventajas y desventajas

Dentro del campo de la gestión de redes, la aplicación NPM de SolarWinds se ha destacado, ya que es una herramienta muy completa al momento de monitorear una red de datos (SolarWinds, 2021). Las ventajas y desventajas más importantes que presenta la aplicación de monitoreo NPM se enumera a continuación:

1. Ventajas de aplicación NPM

- El Software NPM posee varios servicios que facilitan la gestión de la red.
- Interfaz web amigable con el usuario.
- Administración de equipos de manera intuitiva.
- Fácil configuración de alertas y eventos.
- Generación de reportes personalizados de los equipos monitoreados
- Detección rápida de problemas dentro de la infraestructura de red
- Visualizados de información por medio de graficas estadísticas que facilitan el análisis del desempeño de la red.
- Monitoreo de equipos por medio de varios protocolos de gestión como: SNMP, Syslog e ICMP.
- Soporta la gestión de varios equipos de diferentes marcas que forman parte de la infraestructura de red.
- El fabricante SolarWinds ofrece un soporte en caso de problemas con la aplicación.
- Soporte de seguridad que brinda el fabricante SolarWinds

2. Desventajas de aplicación NPM

- Funcionamiento de la aplicación NPM por medio de licencias.
- Costo elevado por las licencias requeridas para la gestión de los equipos.
- Limitación de agregación de equipos a la aplicación NPM por licenciamiento.
- Elevado consumo de recursos del equipo en el cual se aloja la aplicación NPM.
- Requiere personal capacitado y certificado por el fabricante SolarWinds para administración de la aplicación.
- Para su funcionamiento requiere un sistema operativo y base de datos específicos (Windows y Microsoft SQL Server).

CAPÍTULO II

2. MARCO METODOLÓGICO

Este capítulo contiene toda la información necesaria que se requiere para el desarrollo de la reingeniería del sistema de monitoreo de la red de datos para la Empresa Eléctrica Ambato Regional Centro Norte S.A. Cabe recalcar que cierta información no fue mencionada en este documento por motivo de confidencialidad de la empresa.

En la Figura 1-2, se describe el proceso para la implementación del sistema de monitoreo de red para la EEASA.

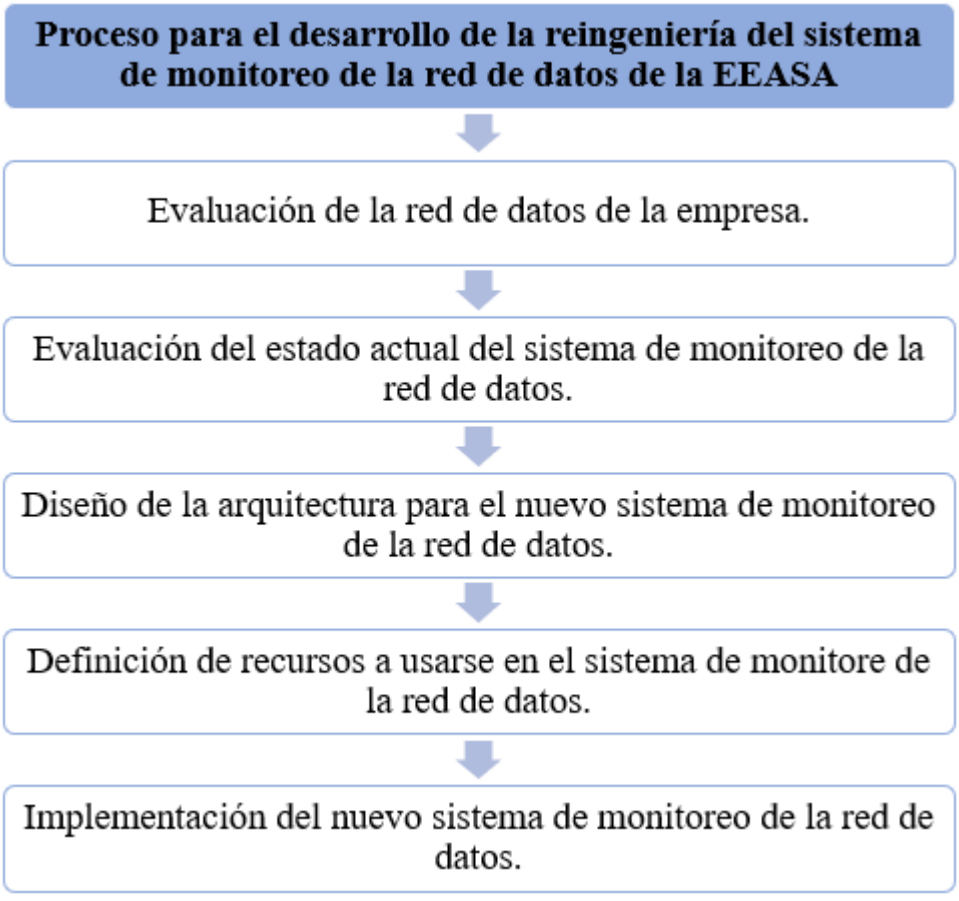


Figura 1-2. Proceso para implementación

Realizado por: Duche, I. 2021

2.1. Evaluación de la red al año 2020.

Actualmente la red empresarial de la EEASA se encuentra en un proceso de expansión y cambio debido al uso de nuevas tecnologías y la implementación de un mayor número de equipos para la comunicación dentro de la empresa en un futuro. La EEASA para las comunicaciones utiliza dos tipos redes de acuerdo con su medio de transmisión las cuales son:

- Red inalámbrica
- Red de fibra óptica,

Además, se cuenta con redes LAN en las instalaciones de la empresa para lo cual se utiliza cable de cobre.

Dentro de la red inalámbrica y de fibra óptica de la EEASA, se encuentra operativo un total de 441 equipos de red con una prioridad alta de monitoreo, y 218 cámaras de seguridad, las cuales se pretenden ingresar al sistema de monitoreo en un futuro, por lo que existe un total 659 dispositivos operativos dentro de la empresa. De la misma forma, se realizó el análisis de la tasa de tráfico de datos de los usuarios, donde se tiene una tasa de datos aproximado de 319.51 Mbps.

Estos resultados influyen para el estudio de dimensionamiento de los recursos requeridos por el sistema de gestión y administración de la infraestructura de red.

2.2. Evaluación del sistema de monitoreo de red de la empresa al año 2020

El sistema de monitoreo de la red de datos de la EEASA usa la herramienta NPM 2019.4 (*Network Performance Monitor*), esta aplicación opera bajo la modalidad de licenciamientos de acuerdo con el número de nodos, interfaces y volumen que van a ser monitoreados dentro de la red empresarial. La empresa usa el protocolo de gestión SNMP e ICMP para el monitoreo de los diferentes equipos que operan dentro de la infraestructura de red.

Como se puede observar en la Figura 2-2, la empresa posee el tipo de licencia SL500, la cual es una licencia básica que permite monitorear 500 nodos, 500 interfaces y 500 volúmenes (Memoria RAM, Disco Duro, CPU).

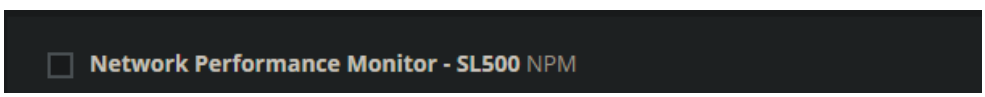


Figura 2-2. Licenciamiento de la aplicación NPM de la EEASA

Realizado por: Duche, I. 2021

Para la base de datos se tiene instalado la aplicación MS SQL Sever 2017 con la licencia *Express*, la cual se usa para la fase de prueba y desarrollo de la aplicación SQL server. Esta opción se presenta al momento de la instalación de la herramienta NPM en su versión de evaluación, por lo tanto, esta base de datos no es la adecuada para un sistema de monitoreo continúo debido a que tiene un límite de funciones y almacenamiento. Esto provoca que los datos estadísticos que se muestra en la aplicación de monitoreo no sean los correctos, además no cuenta con la capacidad suficiente para almacenar datos históricos que se requiere para realizar diferentes actividades dentro de la red de la empresa. Así mismo, esta base de datos no cuenta con un mecanismo de redundancia o de respaldo, esto quiere decir, que en el caso de algún fallo en el almacenamiento la información se perderá de manera permanente.

Como se muestra en la Figura 3-2. el sistema de monitoreo de red con el que opera la empresa no cuenta con un diseño de arquitectura en base a un modelo o protocolo de gestión, por esta razón se produce conflictos de operación dentro del sistema de monitoreo de red.

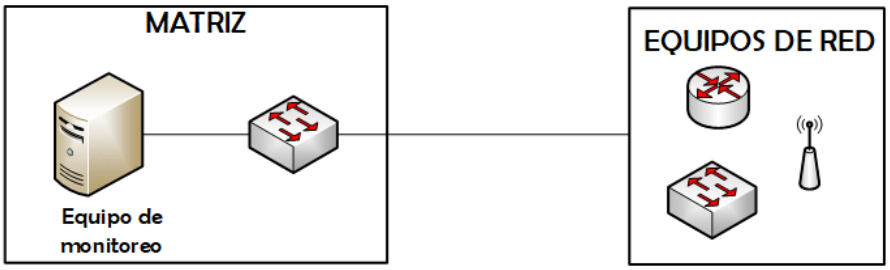


Figura 3-2. Topología de sistema de monitoreo de red de la EEASA

Realizado por: Duche, I. 2021

Las aplicaciones que usa la empresa para el monitoreo de la red de datos se encuentran alojadas en un único computador con pocos recursos que dificulta el funcionamiento óptimo del sistema, como se muestra en la Figura 4-2, los recursos del equipo son: procesador Intel Core i3 de 2.93GHz, memoria RAM de 16GB y disco duro de almacenamiento de 148GB, es decir, no se realizó un correcto análisis de diseño para la gestión de red al momento de la implementación del sistema. En base a este análisis se confirma que no se efectuó un estudio del crecimiento de la red, por lo que el sistema de monitoreo actual de la EEASA no es escalable.

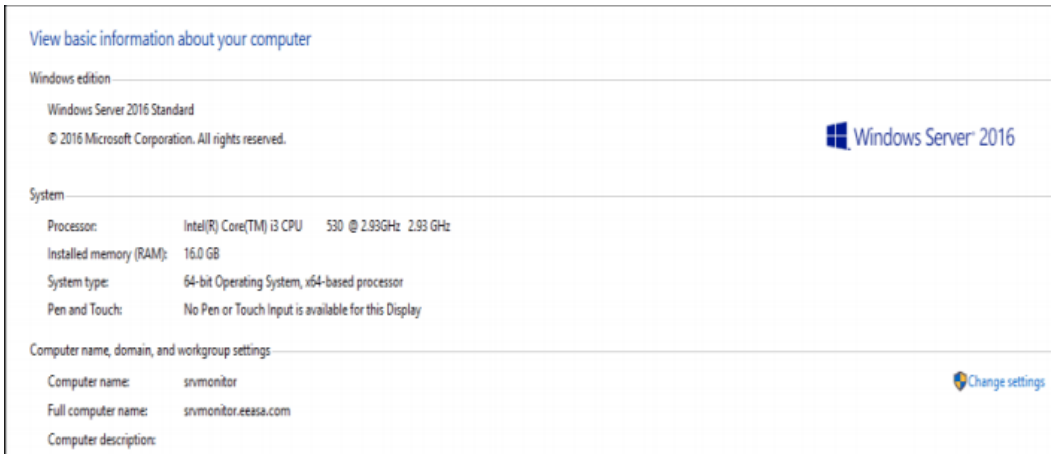


Figura 4-2. Recursos del servidor del sistema de monitoreo de red

Realizado por: Duche, I. 2021

Debido al elevado uso de recurso que requieren estas aplicaciones, dicho servidor impide el correcto desempeño del sistema de monitoreo, tal y como se puede evidenciar en la Figura 5-2, donde se observa que el consumo de memoria RAM sobrepasa el 90% de uso.

Figura 5-2. Consumo de memoria RAM

Realizado por: Duche, I. 2021

Dentro del sistema de monitoreo de red de datos de la EEASA, como se muestra en la Figura 6-2, se encuentra los siguientes elementos dentro del sistema:

- 451 nodos
- 500 interfaces
- 244 volúmenes

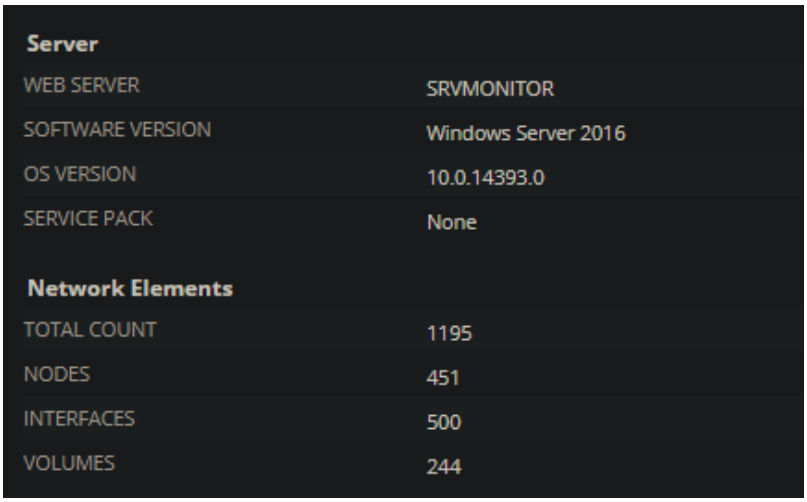


Figura 6-2. Elementos de red ingresados en el sistema

Realizado por: Duche, I. 2021

Como se puede analizar, el licenciamiento del software se encuentra ocupado aproximadamente al 100%, lo que limita el ingreso de nuevos dispositivos de red que deben ser monitoreados, por lo tanto, existen equipos dentro de la red empresarial que no pueden tener una administración adecuada. De la misma forma la red se encuentra en una etapa de expansión para la cual es necesario que el sistema de monitoreo de red tenga una alta escalabilidad.

Además, dentro del sistema de monitoreo se encuentran elementos que ya no forman parte de la red actual, por lo que se deberá realizar una depuración de estos equipos, ya que estos dispositivos ocupan licencias que podrían ser usadas para el monitoreo de otros equipos que tienen una prioridad de gestión más alta dentro de la red empresarial.

Las acciones que realiza el sistema de monitoreo de red son:

- Verificación de disponibilidad de equipos dentro de la red y estado de los equipos (Up o Down).
- Visualización mediante mapas lógicos de equipos de la red de datos de la empresa.
- Visualización de datos estadísticas de latencia y pérdida de paquetes de los equipos de la red.
- Direccionamiento de los equipos.
- Envió de alertas por medio de correos electrónicos al administrador de red.

Entre los principales problemas que se tiene a nivel aplicativo en el sistema de monitoreo de red de la EEASA se puede mencionar:

- Vulnerabilidad de seguridad por desactualización de aplicación NPM.

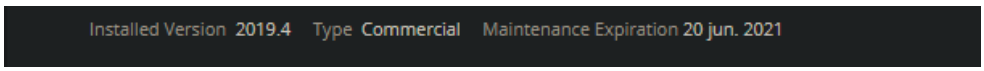


Figura 7-2. Versión de aplicación NPM

Realizado por: Duche, I. 2021

- Limitación de almacenamiento por licencia de la base de datos.

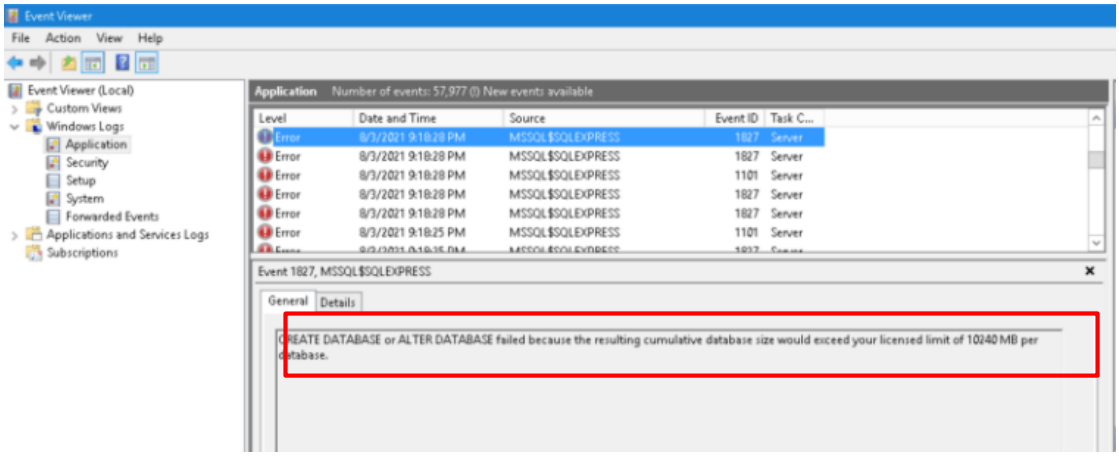


Figura 8-2. Error de base de datos por licenciamiento

Realizado por: Duche, I. 2021

- Insuficiente espacio de disco en el servidor.

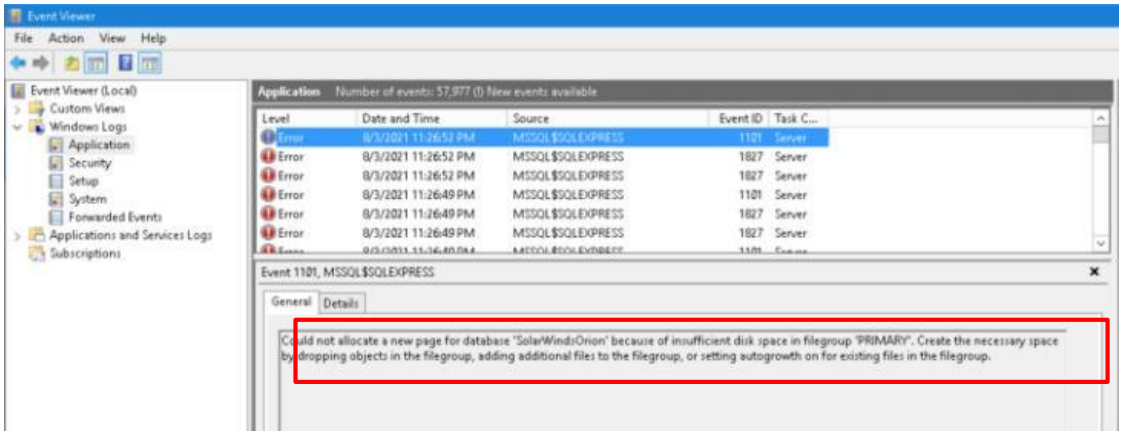


Figura 9-2. Error de espacio en disco del servidor

Realizado por: Duche, I. 2021

- Conflictos entre la base de datos y la aplicación de monitoreo.

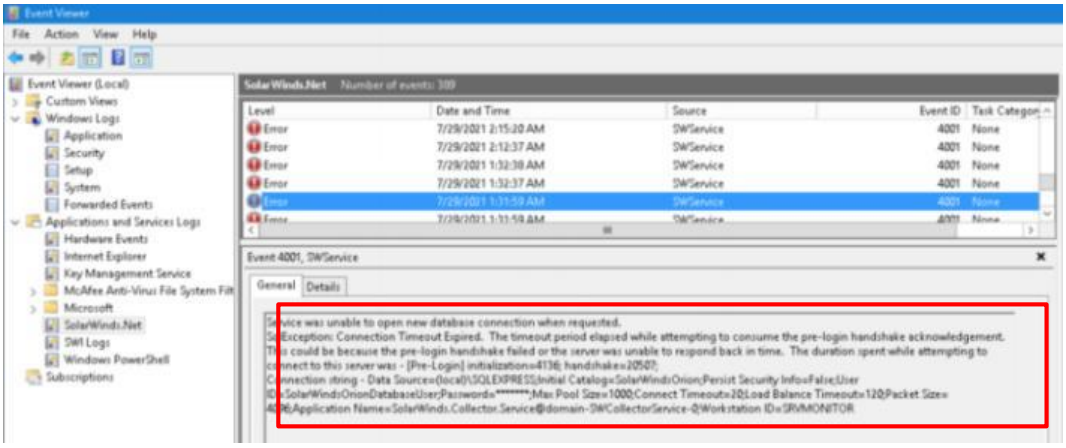


Figura 10-2. Error entre base de datos y aplicación de monitoreo

Realizado por: Duche, I. 2021

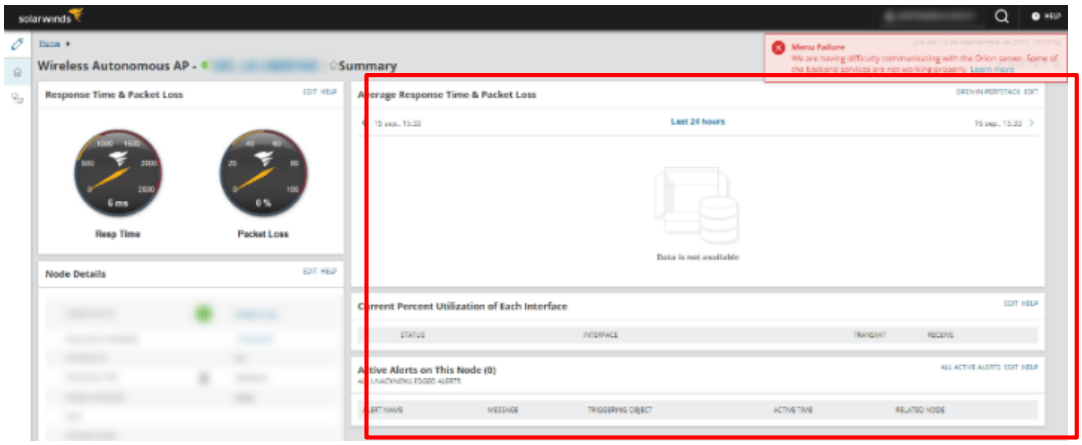


Figura 11-2. Error en el monitoreo de equipos de red

Realizado por: Duche, I. 2021

- Problemas de ingreso a la consola web.

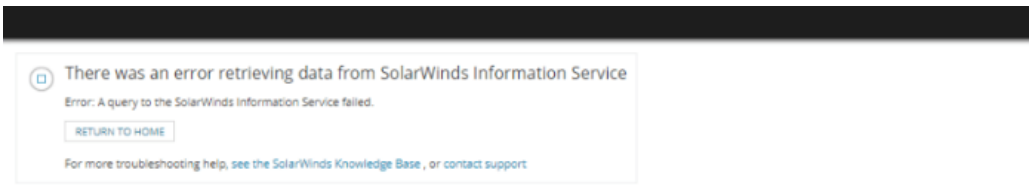


Figura 12-2. Error al ingreso de interfaz web de aplicación NPM

Realizado por: Duche, I. 2021

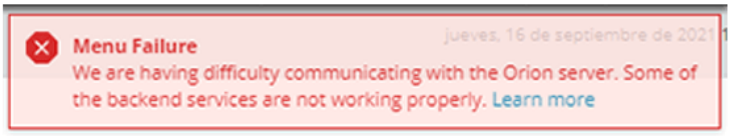


Figura 13-2. Falla en la comunicación son servidor NPM

Realizado por: Duche, I. 2021

- Desactivación de servicios de la aplicación de monitoreo.

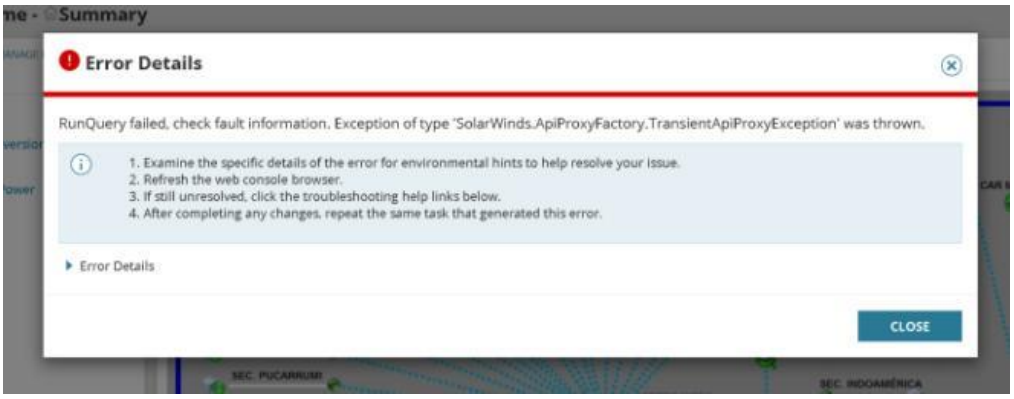


Figura 14-2. Error de servicios de la aplicación NPM

Realizado por: Duche, I. 2021

- Suspensión de servicios de la aplicación NPM

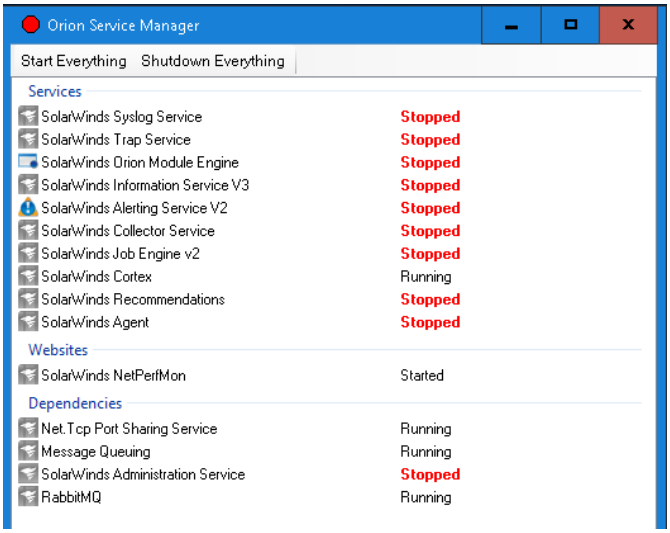


Figura 15-2. Fallo de servicios de aplicación NPM

Realizado por: Duche, I. 2021

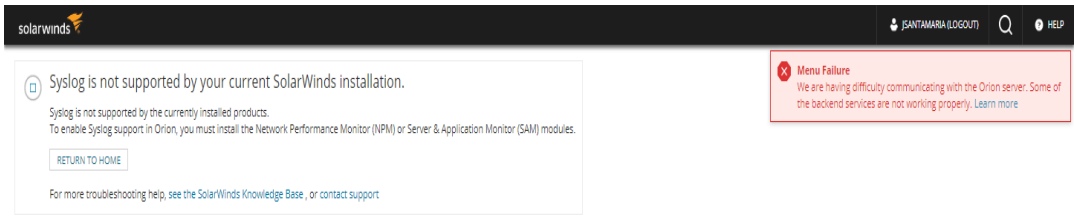


Figura 16-2. Fallo en el servicio Syslog

Realizado por: Duche, I. 2021

- Uso ineficiente de servicios como Syslog, *Traps* y Reportes.

Figura 17-2. Falta de uso de servicio Syslog

Realizado por: Duche, I. 2021

2.3. Posibles tendencias de crecimiento de la red de la EEASA

En base a la evaluación inicial realizada en la sección 2.1, se tiene un total de 441 equipos de red que necesita ser monitoreado con una alta prioridad, además el administrador requiere monitorear en un futuro un total de 218 cámaras, es decir se tiene 659 equipos que se debe ingresar al sistema de monitoreo repotenciado.

Por otro lado, el tráfico de datos promedio que se genera dentro de la red de la empresa es de 319.51Mbps.

Para buscar las posibles tendencias de crecimiento de la red de la empresa es necesario realizar proyecciones estadísticas para determinar el crecimiento del número de dispositivos que puede llegar a tener la red y el incremento del tráfico dentro de la misma, estos valores se obtendrán para un plazo de 5 años.

(CELADE, 1984, p. 30) Para el cálculo de las posibles tendencias a futuro, se hará uso de la siguiente fórmula:

$$c_n = c_0(1+i)^{n-1}$$

Siendo

c_n el número de equipos en el año final.

c_0 el número de equipos en el año inicial.

i el índice de crecimiento anual.

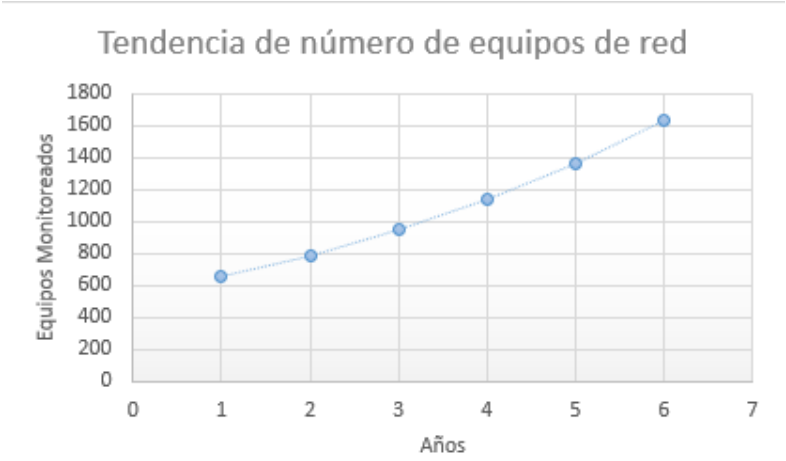
n el número de años.

Debido a que la empresa no cuanta con la información de datos histórico de años anteriores que permita determinar un índice o tasa de crecimiento de la red, el presente análisis se lo realizará con un índice de crecimiento del 20% de acuerdo con el criterio y experiencia del actual administrador de red, tanto para los equipos que se desean monitorear como para el tráfico de la red.

Por lo tanto, en base al índice de crecimiento del 20% anual, se tiene una proyección a 5 años de:

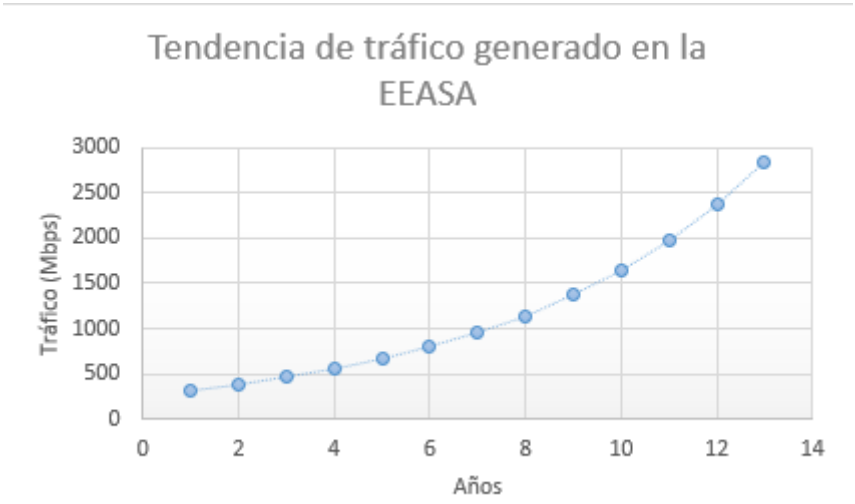
- 1640 equipos de red
- Incremento de tráfico en la red a 795.04 Mbps.

En la Gráfica 1-2 y Grafica 2-2, se muestras las estadísticas del incremento que tendrá en un futuro el número de equipos que se van a monitorear y el tráfico generado por la EEASA respectivamente.



Gráfica 1-2. Tendencia de crecimiento de número de equipos

Realizado por: Duche, I. 2020



Gráfica 2-2. Tendencia de crecimiento de tráfico en la red

Realizado por: Duche, I. 2020

Mediante estos datos se realizará el análisis para el dimensionamiento de los recursos de hardware requeridos para la implementación del sistema de monitoreo de red, para que de esta forma el sistema puede operar de manera correcta.

2.4. Solución propuesta

En base al análisis realizado, se determinó que es necesario desarrollar un nuevo diseño para el sistema de monitoreo de red, que permita monitorear los equipos de red por medio del protocolo SNMPv2, ya que es la versión que soporta la mayoría de los equipos que se encuentra dentro de la infraestructura de red de la empresa y el protocolo Syslog. Además, el sistema debe cumplir las características primordiales que un sistema de gestión de red debe realizar. Para lo cual, en las secciones posteriores se explica a detalle la solución propuesta.

2.5. Arquitectura

Para el diseño del nuevo sistema de monitoreo de red se usará la arquitectura que establece el modelo de gestión TCP/IP basado en el protocolo SNMP presentado en la sección 1.4.

EL nuevo diseño debe tener los componentes principales que propone el modelo de gestión, estos son:

- *Network Management Station* (NMS)
- Agentes de monitoreo
- Protocolo de monitoreo (SNMP)

En la Figura 18-2. se muestra el diseño de la arquitectura que tendrá el sistema de monitoreo.

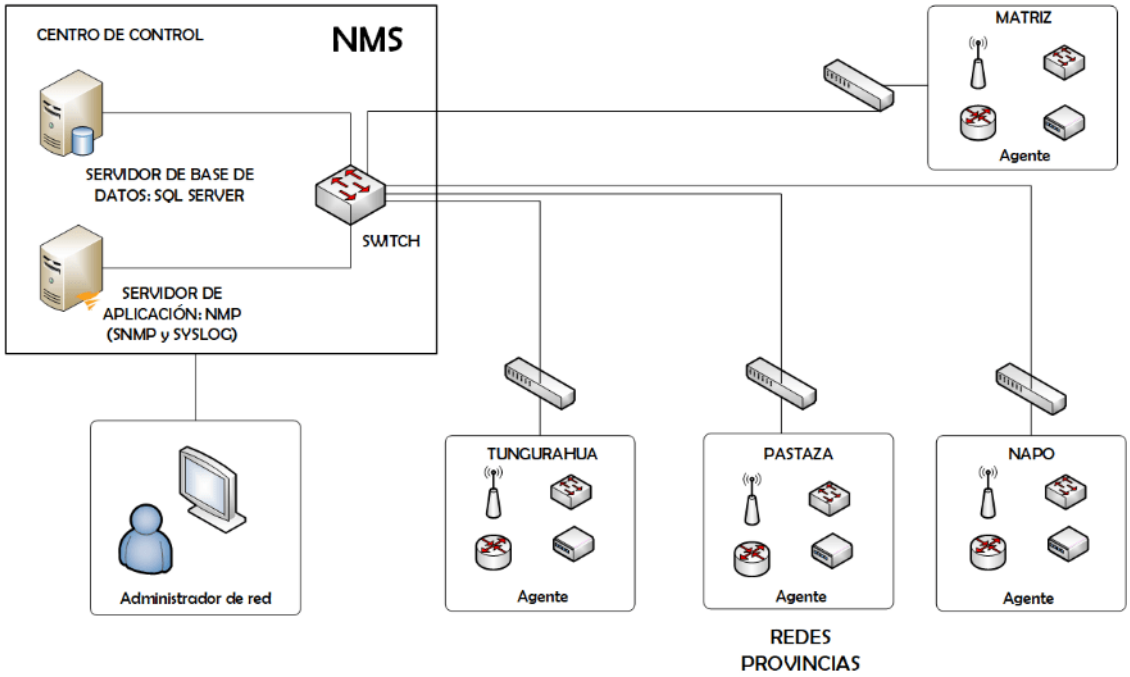


Figura 18-2. Arquitectura propuesta para el sistema de monitoreo de red

Realizado por: Duche, I. 2021

2.6. Requerimientos

En base a la arquitectura del modelo de gestión para un sistema de monitoreo, el protocolo SNMP requiere determinados elementos los cuales garantizan el funcionamiento óptimo del sistema. A continuación, se enumera los componentes requeridos y los equipos a ser utilizados en el sistema:

- Aplicación de monitoreo para protocolo SNMP.
- Sistema de gestión NMS (Servidor Aplicación y Base de datos).

2.6.1. Aplicación de monitoreo para el protocolo SNMP

2.6.1.1. Network Performance Monitor

Para la aplicación de monitoreo a usarse en el sistema de gestión de red, se decidió continuar con la herramienta NPM que brinda la empresa SolarWinds, la cual permite la gestión de equipos mediante el uso del protocolo SNMP. Esta aplicación soportar las 3 versiones del protocolo, además cuenta con otros servicios como el almacenamiento de mensajes Syslog, creación de reportes, administración de alertar, control de incidencias, diseño de mapas lógicos de red, entre otros, lo cual la hace una herramienta robusta para la gestión de redes.

Dentro de la aplicación NPM, además de monitorear equipos por medio de protocolo SNMP, permite realizar la gestión de equipos por medio de los protocolos Syslog e ICMP.

2.6.1.2. Licenciamiento

En base a la evaluación de la red realizada en la sección 2.1, para permitir el ingreso de todos los equipos al nuevo sistema de monitoreo, se requiere incrementar el licenciamiento de la aplicación. Para esto se escogió el tipo de licencia perpetuo SL2000. En la Figura 19-2, se muestra el licenciamiento que se ha escogido para el sistema.

License	Number of monitored elements
SL100	Up to 100 nodes, 100 interfaces, and 100 volumes (300 elements in total).
SL250	Up to 250 nodes, 250 interfaces, and 250 volumes (750 elements in total).
SL500	Up to 500 nodes, 500 interfaces, and 500 volumes (1500 elements in total).
SL2000	Up to 2000 nodes, 2000 interfaces, and 2000 volumes (6000 elements in total).
SLX	Virtually unlimited number of elements. With the default polling interval, one polling engine can monitor a maximum of 12,000 elements (the sum of nodes, interfaces, and volumes). To monitor over 12,000 elements, use additional polling engines (APEs). Each APE requires a license.

Figura 19-2. Tipo de licenciamiento seleccionado para la aplicación NPM.

Realizado por: Duche, I. 2021

2.6.2. Sistema de gestión NMS

2.6.2.1. Servidor para aplicación NPM y Base de datos

Para el sistema de gestión se hará uso de un servidor de la empresa que va a ser repotenciado, para realizar una virtualización de servidores por medio del *Hipervisor VMware vSphere*. Dentro de este equipo se alojará los servidores virtuales para la aplicación NPM y el servidor de Base de Datos respetivamente.

Para poder definir los recursos que se requieren para el correcto funcionamiento de los servidores del sistema de gestión, se realizar un dimensionamiento, para poder realizar una optimización de recursos.

2.6.2.2. Dimensionamiento

Para realizar el dimensionamiento adecuado de los equipos de hardware y que no exista un desperdicio de recurso, se ha tomado como puntos de referencia las recomendaciones y especificación del fabricante SolarWinds, para determinar los requerimientos más adecuados para el sistema de monitoreo de red. En la Tabla 1-2. se muestra los recursos que se requiere para el servidor de la aplicación NPM, mientras que en la Tabla 2-2. se puede visualizar los requerimientos recomendados para la base de datos para el correcto funcionamiento del sistema de gestión, en relación con la licencia que se requiere implementar (Network Performance Monitor, 2021).

Tabla 1-2: Recomendaciones para aplicación NPM

Recomendaciones del fabricante		
Aplicación NPM Medium SL2000		
Recurso	Mínimo	Recomendado
Memoria (RAM)	8GB	64GB
Procesamiento (CPU)	4 Núcleos a una frecuencia de 2.5 GHz	Superior
Almacenamiento	30 GB	40 GB o Superior

Fuente: SolarWinds, 2021

Realizado por: Duche, I, 2021

Tabla 2-2: Recomendaciones para aplicación SQL Server

Recomendaciones del fabricante		
Gestor de base de datos MS SQL Server		
Recurso	Mínimo	Recomendado
Memoria (RAM)	16GB	32GB
Procesamiento (CPU)	4 núcleos a una frecuencia de 2.5 GHz	Superior
Almacenamiento	50 GB	100 GB o Superior
Licencia	Standar	Enterprise

Fuente: SolarWinds, 2021

Realizado por: Duche, I, 2021

Para el servidor de base de datos, como lo menciona el fabricante, se requiere utilizar la aplicación MS SQL Server, para lo cual se usará la licencia *Enterprise*, de esta manera se podrá almacenar el volumen de información requerido por la empresa.

2.7. Presupuesto del proyecto

En base al dimensionamiento que se realizó para determinar los recursos requeridos para la implementación del nuevo sistema de monitoreo de red de la EEASA, la empresa ha destinado un presupuesto de $ 30.680,54, como se observa en la Figura 20-2.

DENOMINACIÓN DEL PROCESO	CÓDIGO CATEGORIA CPC A NIVEL 9	TIPO COMPRA (Bien, Obra, Servicio o consultoría)	CANTIDAD O GLOBAL	VALOR UNITARIO (USD)	VALOR TOTAL PROCESO SIN IVA (USD)	VALOR TOTAL PROCESO CON IVA (USD)	PROCEDIMIENTO (Subasta Inversa, Menor Cuantía, Cotización, Licitación, etc)
REPOTENCIACIÓN SISTEMA DE MONITOREO DE RED PARA LA EEASA	512900021	BIEN	GLOBAL	27.393,34	27.393,34	30.680,54	SUBASTA INVERSA

Figura 20-2. Presupuesto para sistema de monitoreo de red de la EEASA

Realizado por: Duche, I. 2021

Este presupuesto se encuentra destinado para realizar la compra de:

- Licencias perpetuas de aplicaciones NPM y SQL Server.
- Recursos para repotenciación de servidor fisco.
- Garantía por 12 meses.
- Mantenimiento de sistema de monitoreo de red por 12 meses.

Este monto se basa en la proforma emitida por el contratista encargado de brindar los equipos y licencias para la implementación del sistema. Para la obtención de los recursos necesarios para le implementación del sistema de monitoreo de red, se lo realizara por medio del portal de compras públicas.

2.8. Implementación

Para la implementación del sistema de monitoreo se realizará las siguientes actividades enumeradas a continuación:

- Repotenciación del servidor para aplicaciones.
- Instalación de aplicaciones.
- Instalación de licencias.

2.8.1. Repotenciación del servidor para las aplicaciones

Para la implementación de los servidores encargado de alojar las aplicaciones necesarias para el funcionamiento del nuevo sistema de monitoreo de red de la empresa, se lo realizara en un entorno virtualizado, debido a que se repotenció un servidor de la empresa el cual se encontraba subutilizado. Por esta razón se decidió usar dicho servidor, de esta forma se busca una optimización de recursos.

En la Figura 21-2, se muestra los recursos con los que cuenta el servidor después de la repotenciación, en este equipo se va a hospedar los servidores virtuales para las aplicaciones a usarse en el sistema de monitoreo de red.

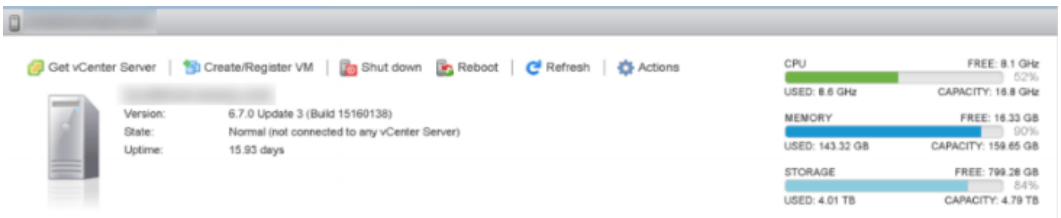


Figura 21-2. Recursos de servidor repotenciado

Realizado por: Duche, I. 2021

2.8.2. Instalación de aplicaciones

Una vez finalizado la repotenciación del servidor, se procede a la instalación y configuraciones de los servidores virtuales y las aplicaciones que van a intervenir en el sistema de monitoreo de red.

2.8.2.1. Instalación de aplicación de monitoreo NPM

Para la aplicación de monitoreo se creó una máquina virtual con los recursos que se puede observar en la Figura 22-2, esta asignación de recurso se realizó en base al dimensionamiento que se realizó en la sección 2.6.2.2.

Figura 22-2. Recursos para servidor virtual de aplicación NPM

Realizado por: Duche, I. 2021

Al momento de terminar la implementación del servidor virtual, se realizó la instalación del sistema operativo Windows Server 2016, en el cual se instalará la aplicación NPM 2020.2.6. A continuación, se realiza la migración de los datos contenidos en el equipo del sistema anterior, de esta manera no se pierde la información almacenada del sistema de monitoreo.

Para la configuración de la red, el administrador encargado asignó una nueva dirección IP, la cual se utilizará al momento de la configuración de los equipos a ser monitoreados.

Después de finalizar el proceso de migración, se levantó los servicios y se puso en operación la aplicación NPM.

2.8.2.2. Base de datos MS SQL Server

En la Figura 23-2, se muestra los recursos asignados para la creación del servidor virtual de la base de datos SQL Server.

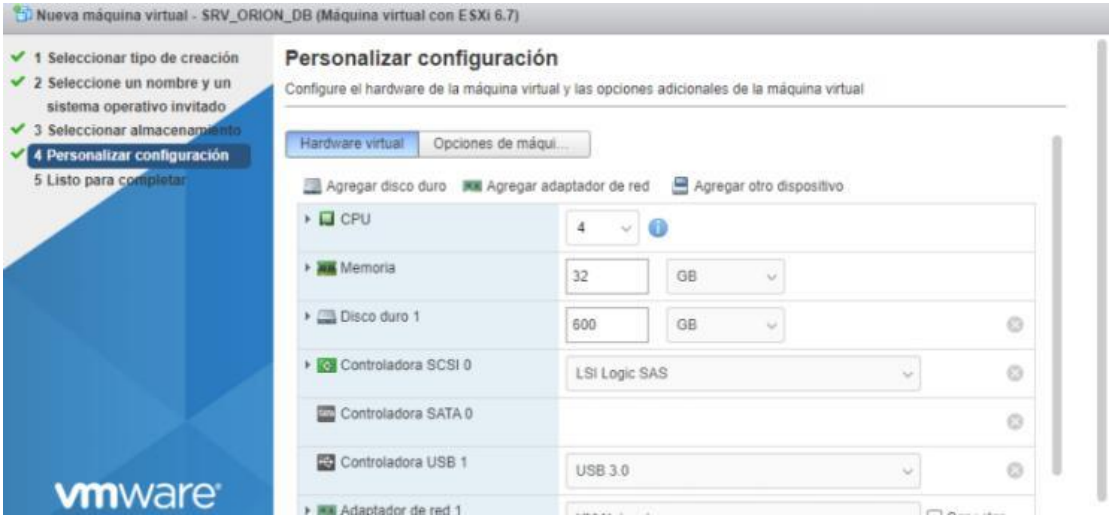


Figura 23-2. Recursos para base de datos

Realizado por: Duche, I. 2021

Terminado el proceso de creación de la máquina virtual, se procede a la instalación del sistema operativo Windows Server 2016 en la cual se alojará el sistema de gestión de base de datos Microsoft SQL Server 2019, el cual servirá para el almacenamiento de los datos recolectados por el servidor NPM. Una vez terminada la instalación se realizará la copia del *backup* realizado en el equipo anterior, de esta manera la información del sistema de monitoreo anterior no se perderá. Además, para el respaldo de la información se configuró un arreglo lógico de discos duros de tipo RAID 1, como mecanismo de redundancia. Para la configuración de red del servidor, se le asignó una dirección IP la cual se utilizará para vincular la base de datos con la aplicación NPM.

Finalizado de instalación de la aplicación SQL Server se realizó la configuración de la aplicación para optimizar al máximo los recursos que va a usar la base de datos, de esta forma se garantiza el correcto funcionamiento del equipo.

2.8.3. Instalación de las licencias

2.8.3.1. Licenciamiento de aplicación NPM

Para la aplicación NPM, se realizó la instalación de la licencia SL2000, mediante la cual se garantiza el ingreso al sistema de todos los equipos que la empresa requiera gestionar. En la Figura 24-2, se puede observar la licencia que se implementó para la aplicación.

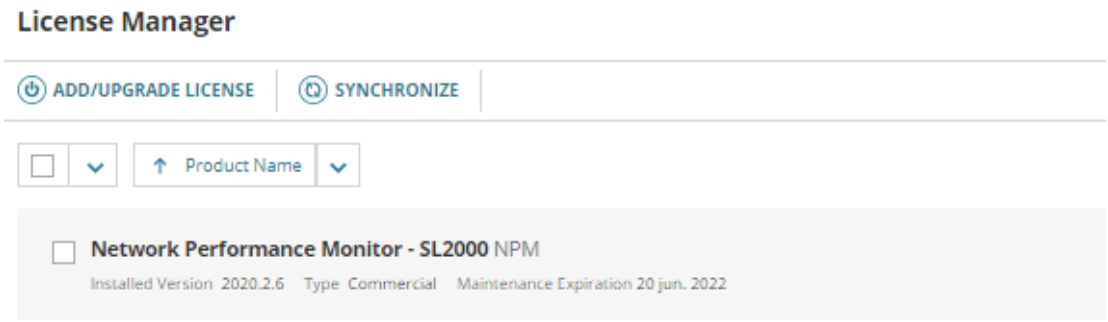


Figura 24-2. Licenciamiento en aplicación NPM

Realizado por: Duche, I. 2021

En la Figura 25-1, se observa que la licencia cuenta con soporte y mantenimiento por parte del fabricante de la aplicación, con lo cual se comprueba que la aplicación ha sido activada correctamente y cuanta con el licenciamiento legal por parte del *partner* de SolarWinds.

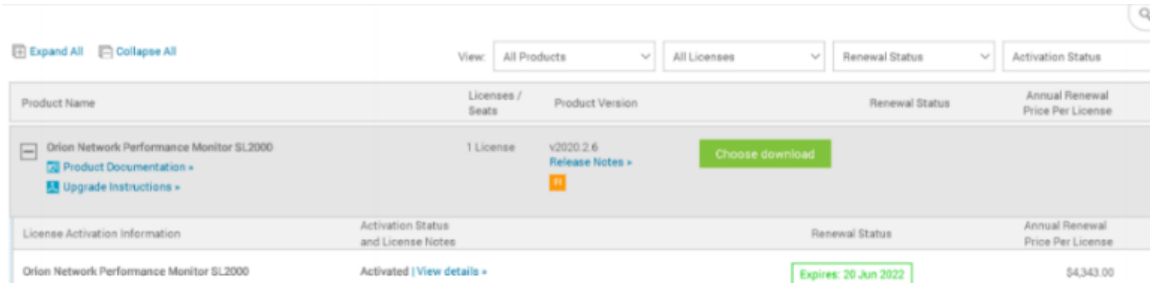


Figura 25-2. Licenciamiento registrado en *partner* de SolarWinds

Realizado por: Duche, I. 2021

2.8.3.2. Licenciamiento de aplicación SQL Server

Se realizó la instalación de la licencia *Enterprise* en la aplicación SQL Server, garantizando de esta forma el almacenamiento necesario para el sistema de monitoreo de red. En la Figura 26-2, se muestra el licenciamiento que usa la aplicación de base de datos SQL Server.

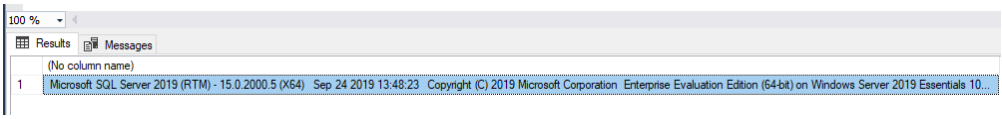


Figura 26-2. Licenciamiento en aplicación SQL Server

Realizado por: Duche, I. 2021

2.8.4. Agregación de equipos de red al sistema de monitoreo

2.8.4.1. Configuración de protocolo SNMP y Syslog en equipos de red de la EEASA

Una vez culminada la fase de implementación, se procede a realizar el ingreso de los equipos que la EEASA requiere que se monitoree, para esto, es necesario realizar la configuración de los protocolos de gestión SNMPv2 en cada uno de los equipos a ser monitoreados.

A continuación, se enumera la configuración de los equipos con los protocolos SNMPv2 y Syslog de diferentes marcas con los que cuenta la EEASA.

1. Configuración del protocolo SNMP en equipos a ser monitoreados

1.1. Equipos de radio enlace.

1.1.1.Equipos Mikrotik

- Creación de nueva comunidad SNMP

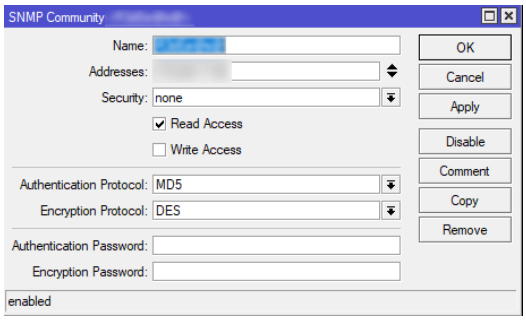


Figura 27-2. Creación de comunidad SNMP

Realizado por: Duche, I. 2021

- Configuración de SNMPv2

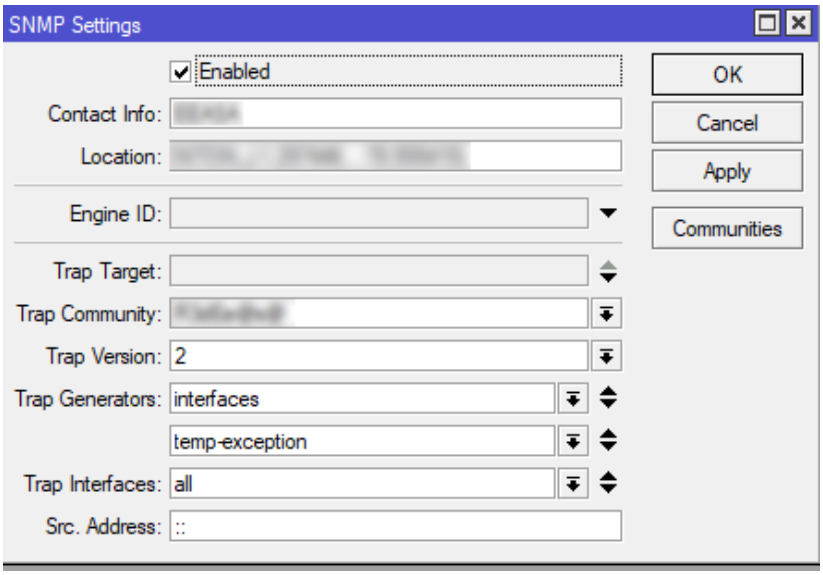


Figura 28-2. Configuración de SNMPv2 en equipo Mikrotik

Realizado por: Duche, I. 2021

1.1.2. Equipos Ubiquiti

- Configuración del equipo con el protocolo SNMP

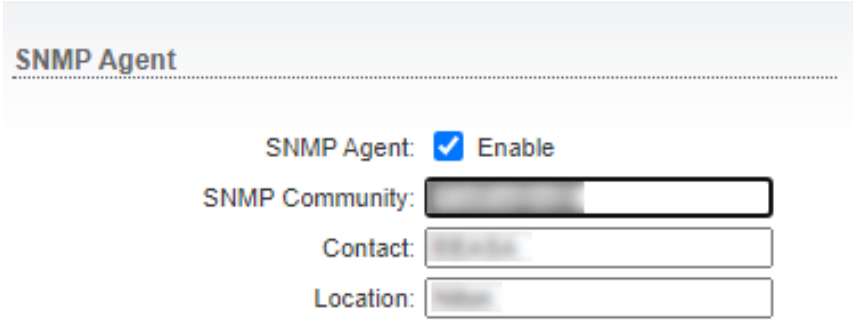


Figura 29-2. Configuración de SNMPv2 en equipo Ubiquiti

Realizado por: Duche, I. 2021

1.1.3.Equipos Proxim

- Configuración de nueva comunidad SNMP

Figura 30-2. Configuración de comunidad SNMPv2 en equipo Proxim

Realizado por: Duche, I. 2021

- Habilitación de *Traps*

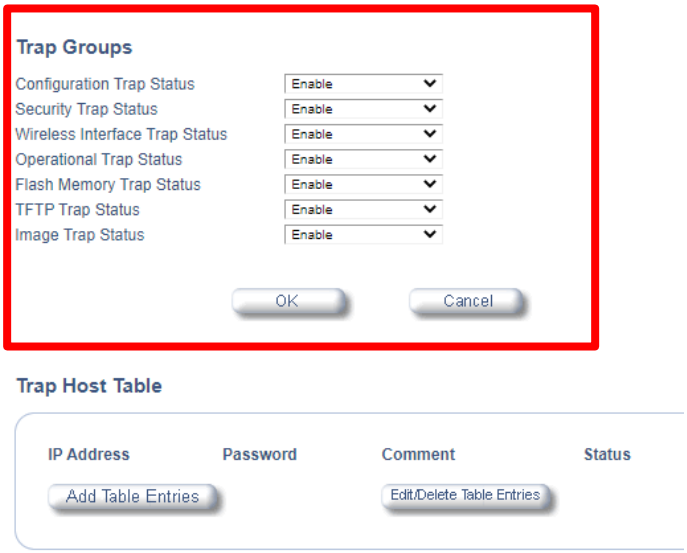


Figura 31-2. Habilitación de *Traps* en equipos Proxim

Realizado por: Duche, I. 2021

1.2. Equipos UPS

1.2.1.Equipos Schneider

- Configuración de comunidad SNMP

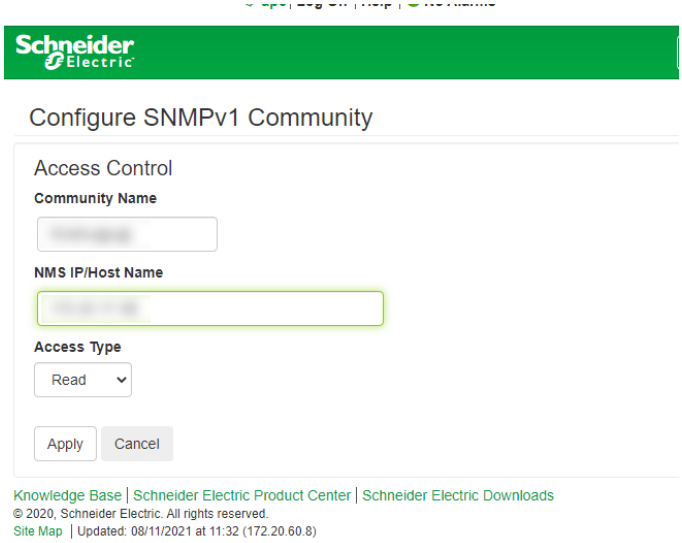


Figura 32-2. Configuración de comunidad SNMPv1

Realizado por: Duche, I. 2021

- Habilitación de protocolo SNMP

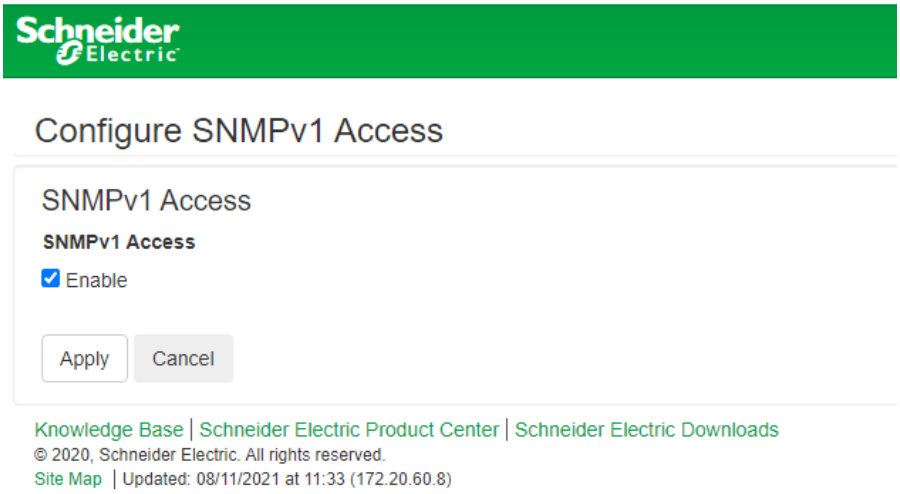


Figura 33-2. Habilitación del protocolo SNMPv1

Realizado por: Duche, I. 2021

1.2.2.Equipos Emerson

- Configuración de comunidad SNMP

Parameter	Description
Entry	Entry number of the access source.
IP Address	Configure network hosts interested in device information access. Note: Setting: IP Address = 0.0.0.0, Access = write, and Community = public, allows write access by any hosts, this may be a security risk to consider.
Access	Configure read and write access for network hosts.
Community	String identifying a "secret" known only by those hosts that are trusted for access. Note: The maximum length of the entry is 32 characters.
Clear	Clear the values of the parameters.

Edit Save Reset

Entry	IP Address	Access	Community	
1		read write		Clear

Figura 34-2. Configuración de comunidad SNMP en equipo Emerson

Realizado por: Duche, I. 2021

- Habilitación de protocolo SNMP

Parameter	Description
SNMP Agent	Enable or Disable the SNMP Network Agent. Note: Typically this feature is disabled when remote network management of the system is not needed.
Authentication Traps	When as SNMP request with an invalid community string is received, the web will issue SNMP Traps as security alerts, if enabled. Note: Typically this feature is enabled as a security measure to alert a management station that unintended/unauthorized requests are being received.

SNMP Agent: enabled

Authentication Traps: enabled

Edit Save Reset

Figura 35-2. Habilitación de SNMP en equipo Emerson

Realizado por: Duche, I. 2021

1.3. Equipos de Red

1.3.1.*Swicthes* Netonix

- Configuración de SNMPv2

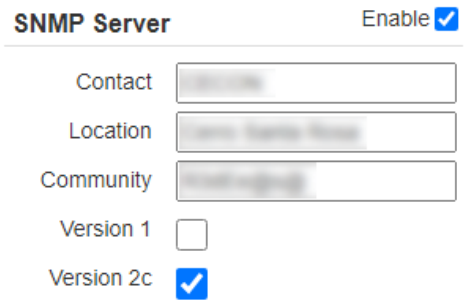


Figura 36-2. Configuración de SNMPv2 en equipo Netonix

Realizado por: Duche, I. 2021

1.3.2. *Routers y Switches* Cisco

- Configuración de comunidad y habilitación de *Traps* SNMPv2

```
!
snmp-server community [redacted] RO
snmp-server trap-source [redacted]
snmp-server location [redacted]
snmp-server contact [redacted]
snmp-server chassis-id [redacted]
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps vrrp
snmp-server enable traps pfr
snmp-server enable traps dsl
snmp-server enable traps transceiver all
snmp-server enable traps eigrp
snmp-server enable traps tty
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps bfd
snmp-server enable traps bgp
snmp-server enable traps bgp cbgp2
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps dhcp
snmp-server enable traps event-manager
snmp-server enable traps hsrp
snmp-server enable traps ipmulticast
snmp-server enable traps isis
snmp-server enable traps mpls rfc ldp
snmp-server enable traps mpls ldp
snmp-server enable traps mpls rfc traffic-eng
snmp-server enable traps mpls traffic-eng
snmp-server enable traps mpls fast-reroute protected
snmp-server enable traps msdp
snmp-server enable traps ospfv3 state-change
snmp-server enable traps ospfv3 errors
snmp-server enable traps slb real virtual csrp
snmp-server enable traps syslog
```

Figura 37-2. Configuración de SNMPv2 en equipo Cisco

Realizado por: Duche, I. 2021

Cabe resaltar que al momento de elegir la cadena de comunidad en determinados modelos de equipos CISCO, ciertos caracteres especiales están reservados para el protocolo SNMP, como por

ejemplo el caracter @ es reservado para la indexación de cadenas de comunidad SNMP (Cisco Systems, 2005).

Por lo tanto, al momento de configurar la comunidad en los equipos Cisco se tuvo cuidado de evitar el uso de los caracteres: @, #, /, \.

2. Configuración del protocolo Syslog en equipos a ser monitoreados

2.1. Equipos de radio enlace.

2.1.1.Equipos Mikrotik

- Configuración de IP de servidor remoto Syslog y habilitación de *Facility* y *Severity*

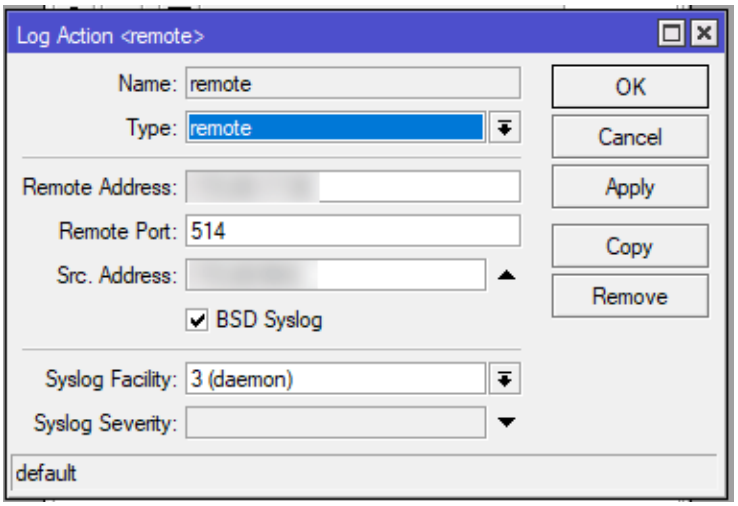


Figura 38-2. Configuración de IP de servidor remoto Syslog

Realizado por: Duche, I. 2021

- Determinación de mensajes a enviarse al servidor remoto Syslog

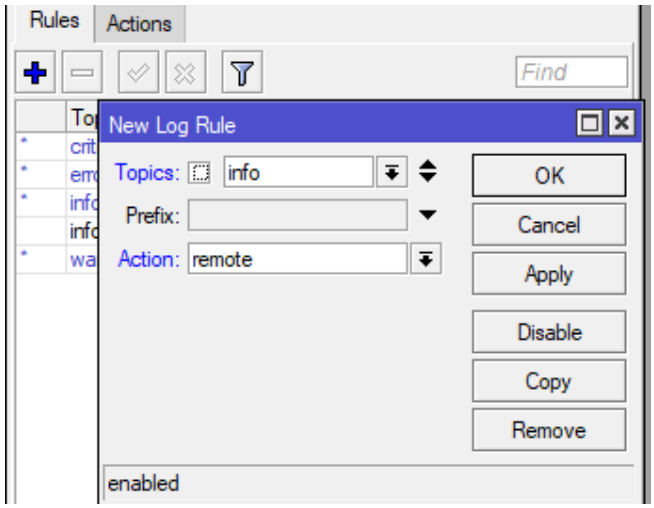


Figura 39-2. Configuración de mensaje

Realizado por: Duche, I. 2021

2.1.2.Equipos Ubiquiti

- Habilitación y configuración de dirección IP de servidor remoto Syslog

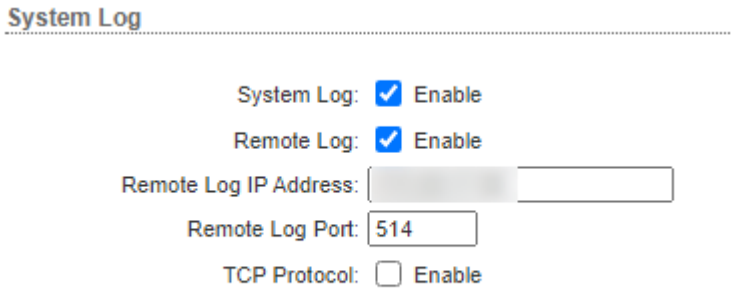


Figura 40-2. Configuración de Syslog en equipo Ubiquiti

Realizado por: Duche, I. 2021

2.1.3.Equipos Proxim

- Habilitación de protocolo Syslog y configuración de dirección IP de servidor remoto

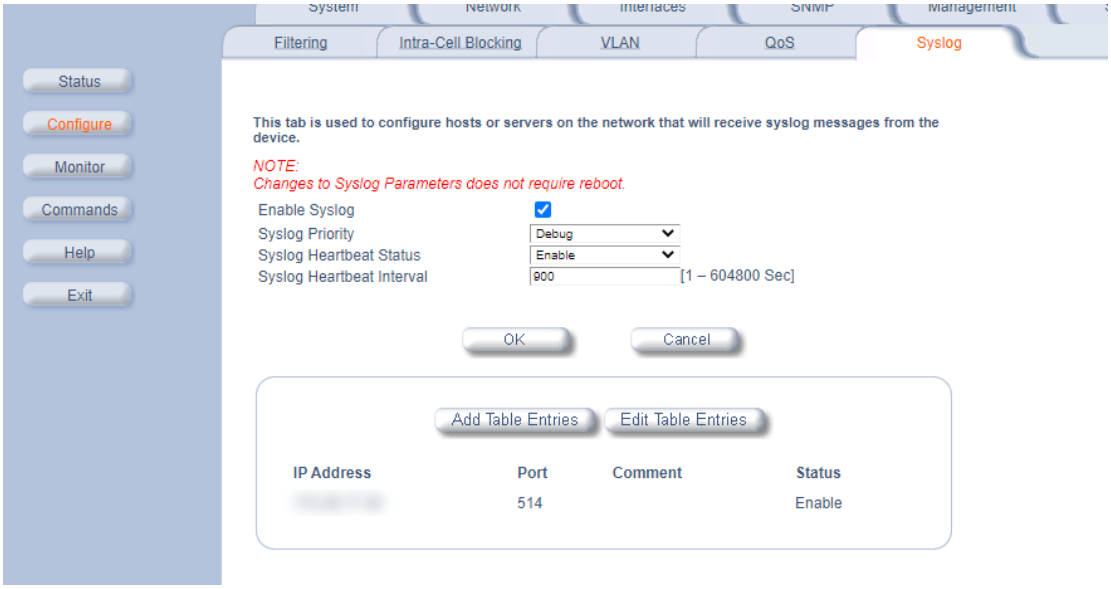


Figura 41-2. Configuración de Syslog en equipo Proxim

Realizado por: Duche, I. 2021

2.2. Equipos UPS

2.2.1.Equipos Schneider

- Configuración de dirección IP de servidor remoto Syslog

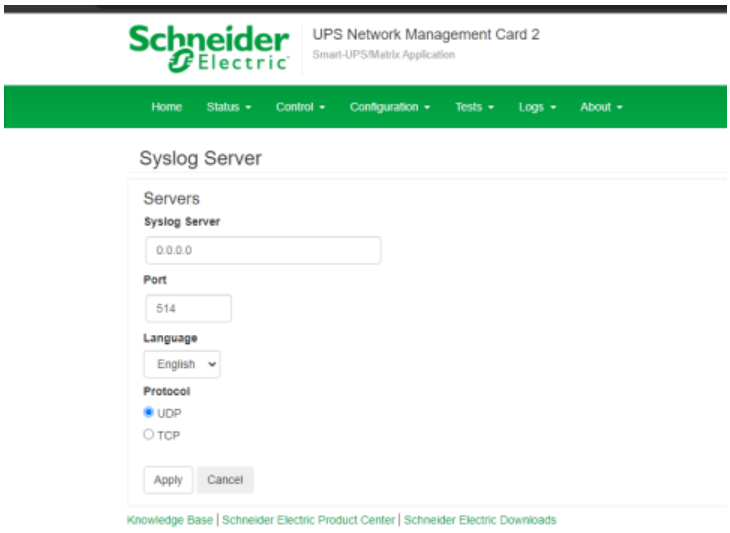


Figura 42-2. Configuración de IP de servidor remoto Syslog

Realizado por: Duche, I. 2021

- Configuración de *Facility* y *Severity*

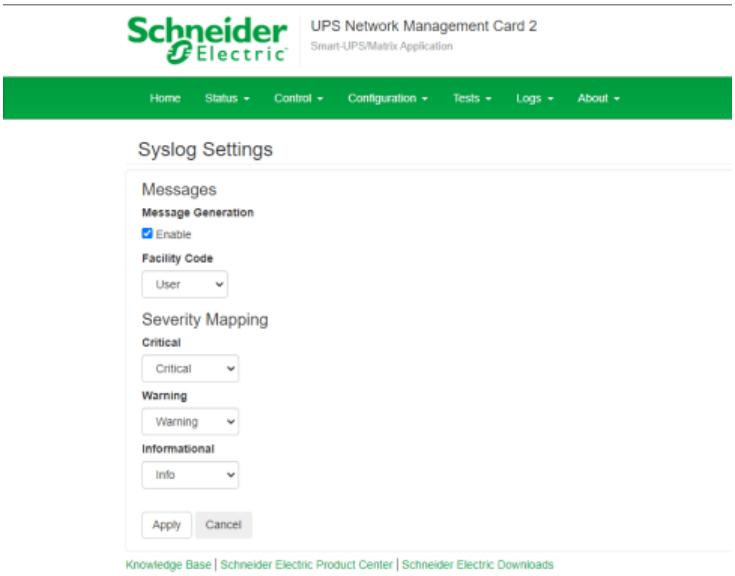


Figura 43-2. Configuración de *Facility* y *Severity*

Realizado por: Duche, I. 2021

2.3. Equipos de Red

2.3.1.*Swicthes* Netonix

- Habilitación y configuración de dirección IP de servidor remoto Syslog

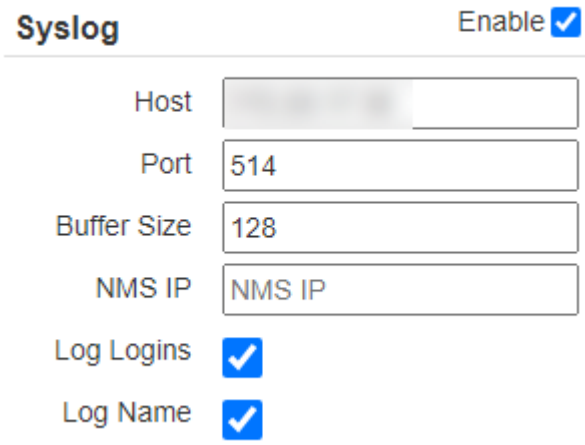


Figura 44-2. Configuración de Syslog en equipo Netonix

Realizado por: Duche, I. 2021

2.3.2.*Routers y Switches* Cisco

- Configuración de dirección IP de servidor remoto Syslog y habilitación de *Facility* y *Severity*.

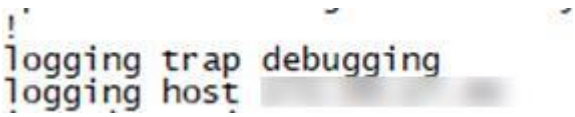


Figura 45-2. Configuración de Syslog en equipo en equipo Cisco

Realizado por: Duche, I. 2021

2.8.4.2. Ingreso de equipos a aplicación NPM

Una vez terminada la configuración de los protocolos SNMP y Syslog en los equipos de la empresa a ser monitoreados, se requiere agregar los agentes a la aplicación NPM, para la gestión por parte de la administración encargada de la red de la empresa.

Es necesario verificar que todos los equipos que se ingresan al sistema de monitoreo de red se encuentren operativos dentro de la empresa.

A continuación, se enumera los pasos que se debe seguir para el ingreso de los equipos de red al sistema de monitoreo.

1. Ingreso de datos básicos como dirección IP y comunidad para establecer relación entre el agente y la aplicación NPM.

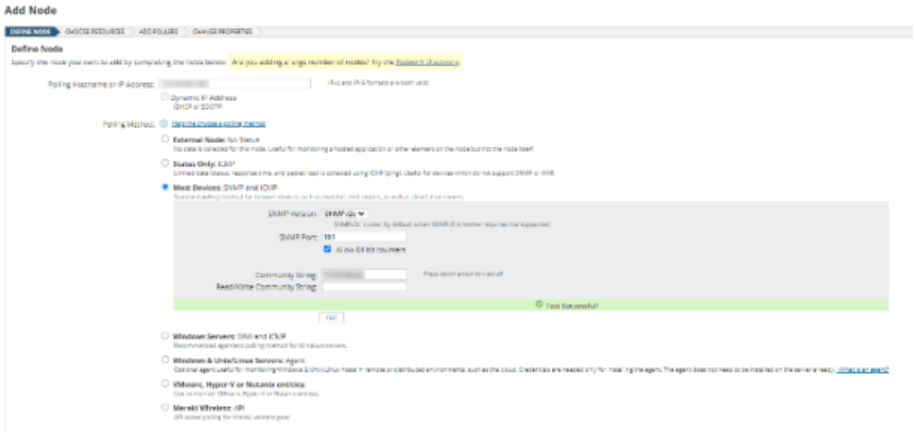


Figura 46-2. Ingreso de datos básicos para establecer relación.

Realizado por: Duche, I. 2021

2. Selección de recursos que se van a monitorear.

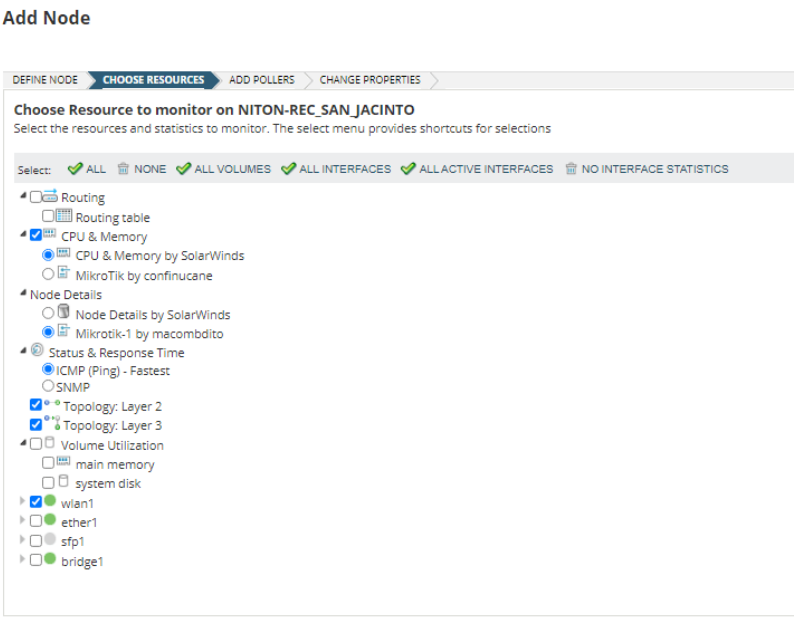


Figura 47-2. Selección de recursos.

Realizado por: Duche, I. 2021

3. Selección de *Pollings* personalizados.

De acuerdo con el equipo que se va a realizar la gestión, es necesario importar los archivos UnDP (*Universal Device Pollers*) de los dispositivos, ya que, por medio de estos archivos, la aplicación NPM podrá realizar un monitoreo personalizado haciendo uso del protocolo SNMP.

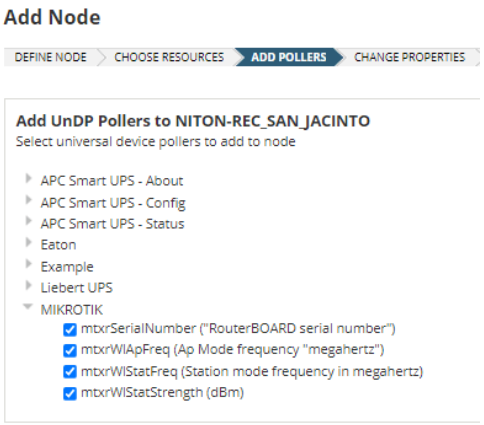


Figura 48-2. *Pollings* para equipos Mikrotiks

Realizado por: Duche, I. 2021

4. Confirmación de los datos del equipo a ingresarse.

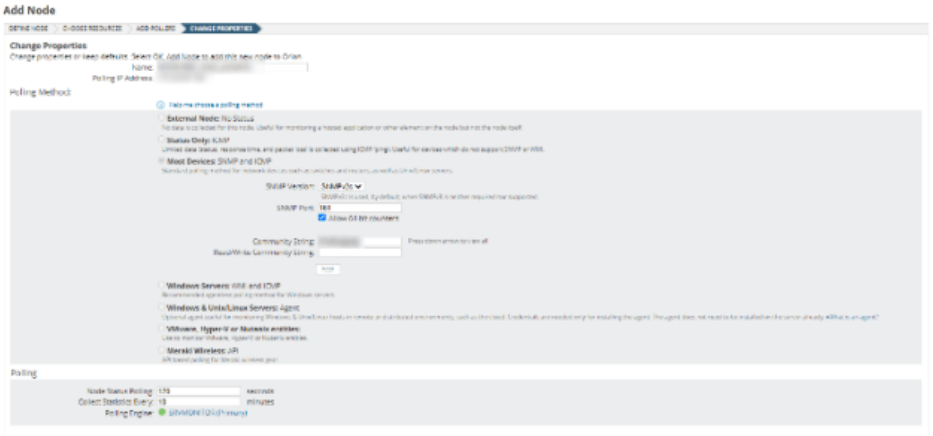


Figura 49-2. Finalización de proceso de ingreso de equipos

Realizado por: Duche, I. 2021

El proceso de implementación culminó en su totalidad el 06 de agosto del 2021.

CAPÍTULO III

3. MARCO DE ANÁLISIS Y RESULTADOS

En este capítulo se detallará los resultados obtenidos después de haber realizado la implementación del sistema de monitoreo de red para la Empresa Eléctrica Ambato Regional Centro Norte S.A. Para esto se realizará la verificación del correcto desempeño de los servicios implementados necesarios para la gestión de los equipos de red empresarial y se efectuará un análisis comparativo en el que se evidencie las mejoras con respecto al sistema anteriormente utilizado por la empresa, de esta forma se garantiza el óptimo funcionamiento y rendimiento del nuevo sistema. Cabe señalar que determinados resultados de las evaluaciones realizadas no pueden ser publicados en este documento por motivos de confidencialidad de la empresa.

3.1. Resultados del nuevo sistema de monitoreo de red implementado en la EEASA

Una vez culminada la implementación del sistema de monitoreo de red, se procedió a realizar la evaluación del sistema para verificar que las aplicaciones funcionen de una manera correcta, comprobando así que no se presente los errores del sistema anterior expuestos en el análisis de la sección 2.2.

Para realizar la evaluación del desempeño del sistema de monitoreo de red se usó la aplicación Visor de Eventos, en la cual se verifica que no exista mensajes de error en las aplicaciones, como era el caso del sistema anterior.

3.1.1. Verificación de errores en el servidor de la aplicación de monitoreo (NPM)

En la Figura 1-3 y Figura 2-3, se puede verificar que la aplicación NPM está funcionando de una manera óptima, ya que no presenta ningún registro de error de mal funcionamiento a nivel aplicativo.

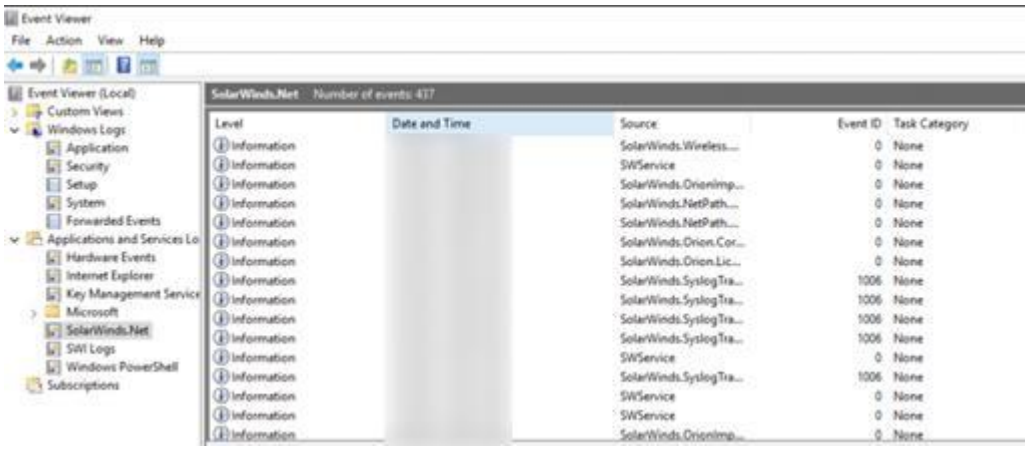


Figura 1-3. Registro de eventos del servidor de monitoreo NPM

Realizado por: Duche, I. 2021

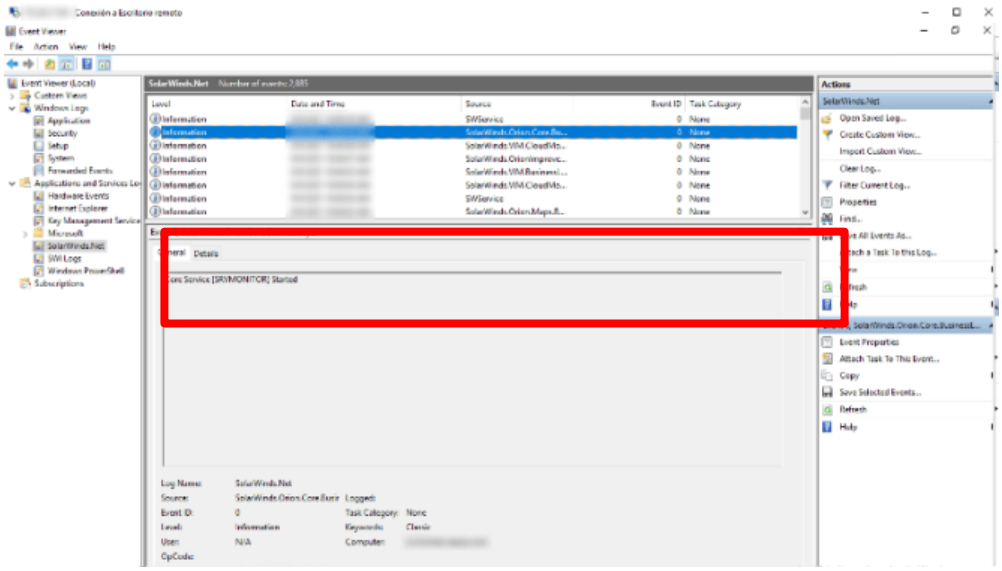


Figura 2-3. Mensaje informativo en servidor de monitoreo NPM

Realizado por: Duche, I. 2021

3.1.2. Verificación de errores en el servidor de la base de datos (SQL Server)

Para la base de datos, en la Figura 3-3 y Figura 4-3, se puede comprobar que la aplicación MS SQL Server está operando de manera correcta, debido a que dentro del Visor de Eventos del servidor no se encontró ningún error.

Figura 3-3. Registro de eventos del servidor de base de datos actual

Realizado por: Duche, I. 2021

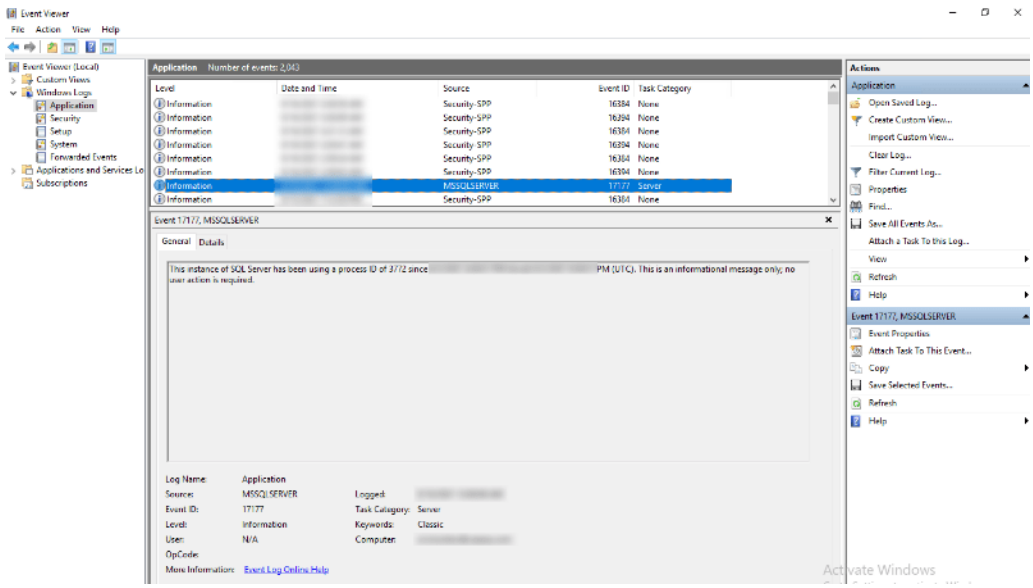


Figura 4-3. Registro de eventos del servidor de base de datos actual

Realizado por: Duche, I. 2021

3.1.3. Servicios de aplicación NPM

La aplicación NPM cuenta con varios servicios los cuales ayudan a la gestión de los equipos integrados al sistema de monitoreo de red, por lo cual se debe verificar que dichos servicios se encuentren operativos. En la Figura 5-3, se puede observar que todos los servicios que forman parte de la aplicación de monitoreo se encuentran ejecutándose de manera correcta.

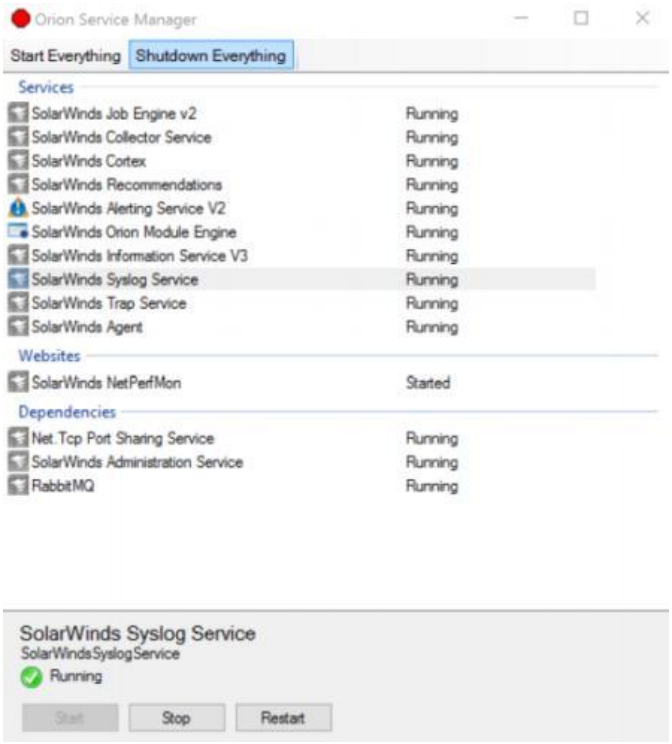


Figura 5-3. Servicios de aplicación NPM actual

Realizado por: Duche, I. 2021

3.2. Verificación de los protocolos SNMP y Syslog en el servidor

Dentro del servidor de la aplicación NPM se realizó un análisis de tráfico para verificar que los mensajes SNMP y Syslog enviados por los agentes hacia la estación de gestión son correctos, de esta forma se garantiza que el servidor está recibiendo la información correcta de los equipos administrados. Para el análisis de los paquetes se hizo uso de la aplicación Wireshark.

En la Figura 6-3, se puede observar el análisis del mensaje SNMP recibido por el servidor, en cual se comprueba el funcionamiento del protocolo SNMPv2 analizado en la sección 1.4.4.2.

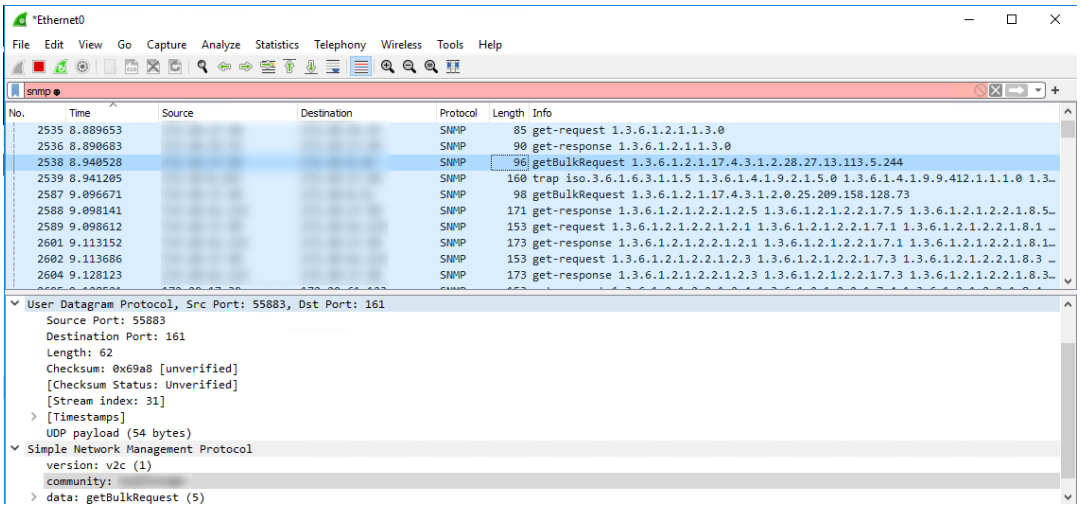


Figura 6-3. Análisis de paquete SNMP

Realizado por: Duche, I. 2021

En la Figura 7-3, se puede observar el análisis del mensaje Syslog recibido por la estación de gestión, en donde se demuestra que el mensaje Syslog enviado por el agente es correcto.

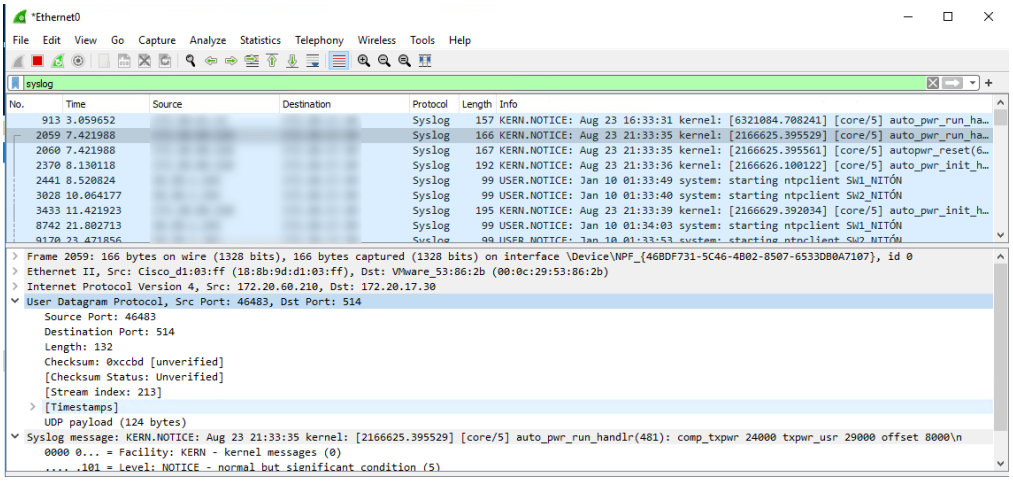


Figura 7-3. Análisis de paquete Syslog

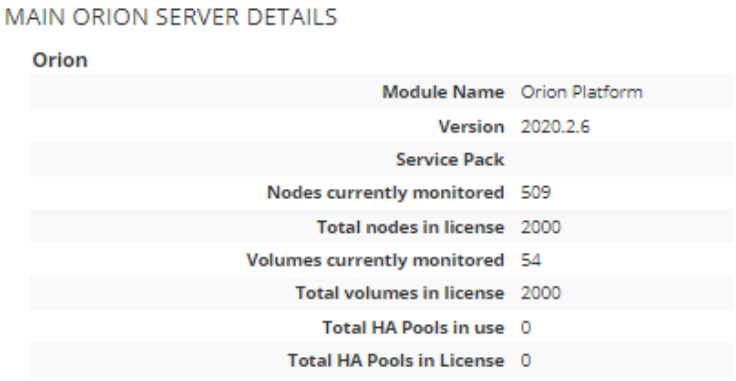
Realizado por: Duche, I. 2021

Después de haber finalizado la evaluación de los paquetes recibidos por la estación de gestión del sistema de monitoreo de red, se verifica que el servidor está recibiendo los mensajes correctos por parte de los agentes, de esta forma se garantiza que se está realizando el monitoreo de los equipos de red.

3.3. Evaluación de equipos ingresados al sistema de monitoreo

Finalizado el ingreso de los equipos dentro del nuevo sistema de monitoreo de red de la empresa, se procedió a realizar la evaluación para verificar que todos los dispositivos de red que se encuentran monitoreados estén operativos en la empresa, de esta forma se evita el desperdicio de licencia de la aplicación NPM, y se corrige los errores que tenía el sistema anterior como: equipos duplicados, equipos no operativos y equipos retirados.

Como se muestra en la Figura 8-3, el número total de equipos ingresados actualmente dentro del sistema de monitoreo es de 509. Como se puede notar, desde la fecha del estudio de la evaluación de la red hasta la finalización de la incorporación de los equipos de red al sistema, se tiene un incremento de 68 dispositivos.


MAIN ORION SERVER DETAILS

Orion

Module Name	Orion Platform
Version	2020.2.6
Service Pack	
Nodes currently monitored	509
Total nodes in license	2000
Volumes currently monitored	54
Total volumes in license	2000
Total HA Pools in use	0
Total HA Pools in License	0

Figura 8-3. Nodos monitoreados por aplicación NPM

Realizado por: Duche, I. 2021

En las siguientes tablas se puede visualizar el número de equipos que se encuentran operativos dentro de la infraestructura de red de la empresa.

Tabla 1-3: Equipos de radio enlaces operativos

Equipos de radio enlaces			
Marca del equipo	MikoTik	Ubiquiti	Proxim
Numero de equipos	245	40	6

Fuente: Empresa Eléctrica Ambato Regional Centro Norte, 2021

Realizado por: Duche, I, 2021

Tabla 2-3: Equipos UPS operativos

Sistema de alimentación ininterrumpido (UPS)			
Marca del equipo	APC	Emerson	EATON
Numero de equipos	6	3	1

Fuente: Empresa Eléctrica Ambato Regional Centro Norte, 2021

Realizado por: Duche, I, 2021

Tabla 3-3: Equipos de red operativos

Equipos de red (Routers y Switches)		
Marca del equipo	Netonix	Cisco
Numero de equipos	12	76

Fuente: Empresa Eléctrica Ambato Regional Centro Norte, 2021

Realizado por: Duche, I, 2021

Además de los equipos de red, la empresa cuenta con equipos de control automáticos los cuales deben ser ingresados al sistema de monitoreo ya que es necesario que sean gestionados. Se tiene un total de 120 equipos de control en el sistema, entre los que se puede mencionar: Reconectadores, seccionadores, interruptores, medidores y RTUs

Una vez terminada la evaluación de los equipos ingresados al sistema de monitoreo de red, se comprobó que el 100% de los equipos se encuentran operativos y tiene una alta prioridad de gestión, de esta forma se garantiza que no existe un desperdicio de licencias.

3.4. Evaluación del funcionamiento de la aplicación NPM

Como se mencionó en el capítulo anterior, la aplicación NPM cuenta con varios servicios que mejora la gestión de los equipos, los cuales dentro del sistema anterior eran mal utilizados o se desconocía su funcionamiento, por lo tanto, se realizará una evaluación para comprobar que los servicios que ofrece la aplicación de monitoreo se encuentran funcionando de manera correcta.

3.4.1. Evaluación de monitoreo de equipo dentro de aplicación NPM

La aplicación NPM, por medio de los protocolos SNMP y Syslog, permite realizar la gestión de un gran número de funciones de los equipos de la red, sin embargo, el administrador requiere el monitoreo de determinadas actividades principales, las cuales van a ser de gran utilidad para un análisis de la red.

En la Figura 9-3, se puede visualizar un ejemplo del *dashboard* de un equipo monitoreado por la aplicación NPM.

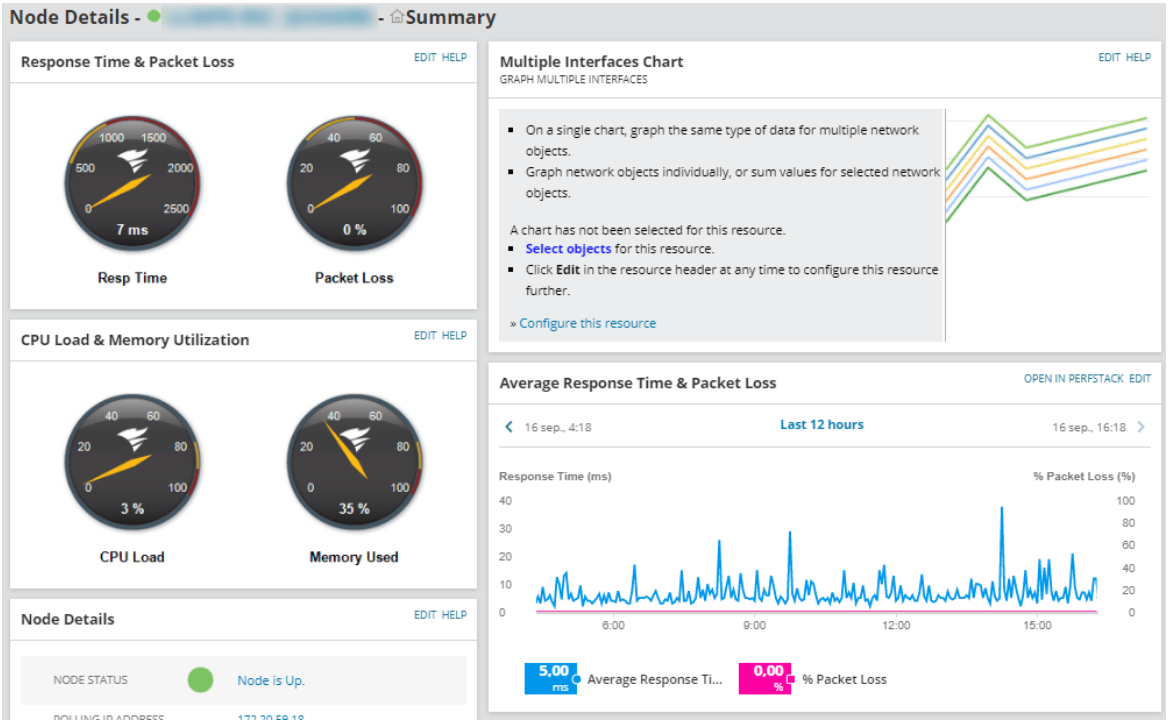


Figura 9-3. Nodos monitoreados por aplicación NPM

Realizado por: Duche, I. 2021

Las funciones principales que el administrador requiere monitorear son:

- Información básica de los equipos monitoreados.

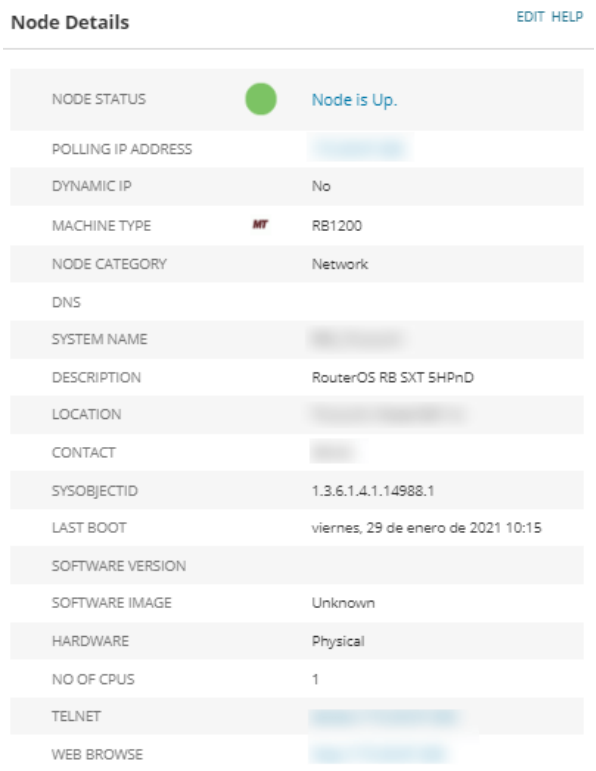


Figura 10-3. Detalles de equipo Mikrotik

Realizado por: Duche, I. 2021

- Latencia y pérdida de paquetes de los equipos.

Figura 11-3. Gráfico estadístico de latencia y pérdida de paquetes

Realizado por: Duche, I. 2021

- Estado de CPU y memoria RAM.

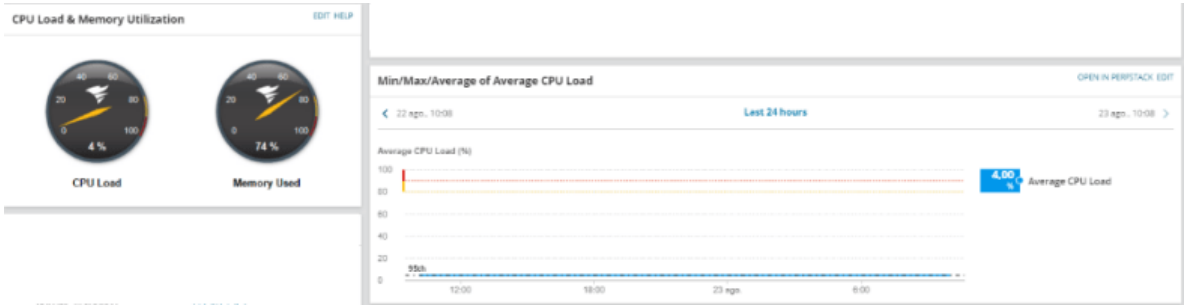


Figura 12-3. Utilización de CPU y memoria RAM del equipo

Realizado por: Duche, I. 2021

- Interfaces de los equipos.

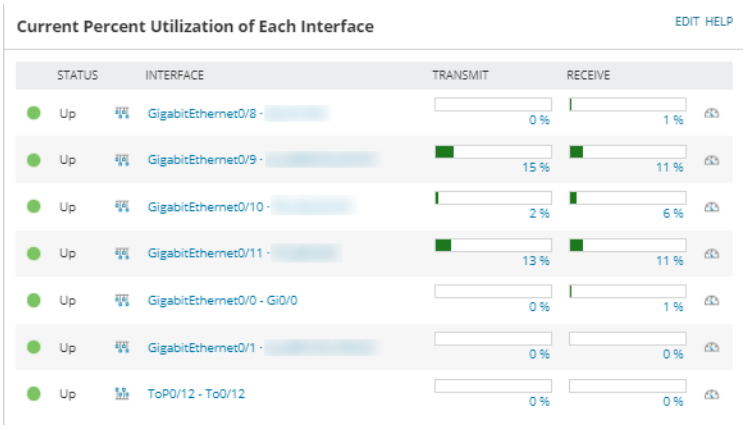


Figura 13-3. Interfaces de equipo Cisco monitoreado

Realizado por: Duche, I. 2021

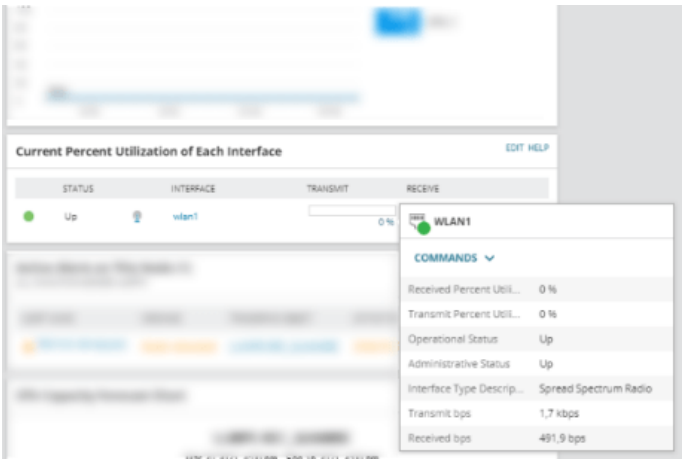


Figura 14-3. Interfaz de equipo inalámbrico

Realizado por: Duche, I. 2021

- Topología de equipos.

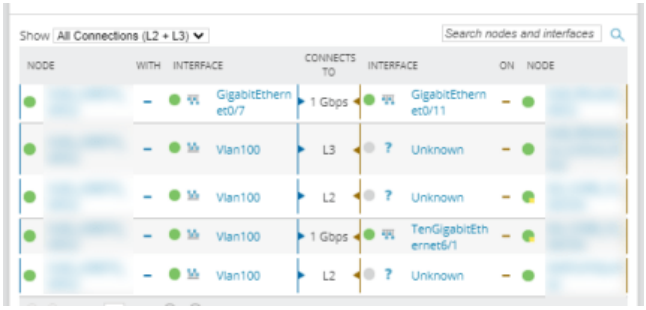


Figura 15-3. Topología lógica de equipo monitoreado

Realizado por: Duche, I. 2021

3.4.2. Evaluación de servicios de la aplicación NPM

Se realizó la evaluación de los servicios que la aplicación NPM brinda para verificar el correcto uso y funcionamiento.

Entre los servicios de la aplicación NPM que se usa para la gestión de la red se tiene:

- Recolección de mensajes Syslog.

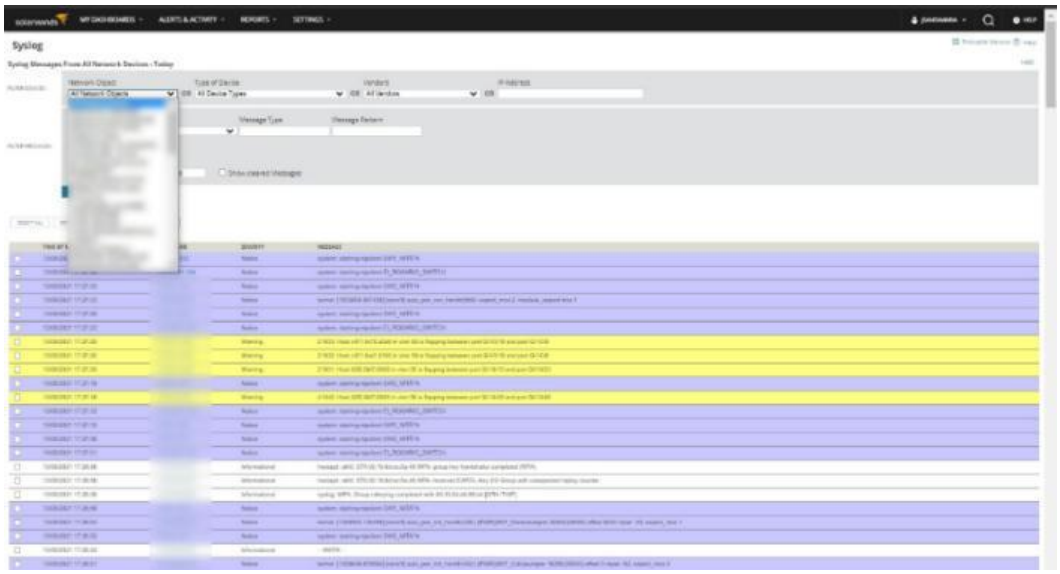


Figura 16-3. Mensajes Syslog recolectado por la aplicación NPM

Realizado por: Duche, I. 2021

- Visualización de mensajes *Traps*.

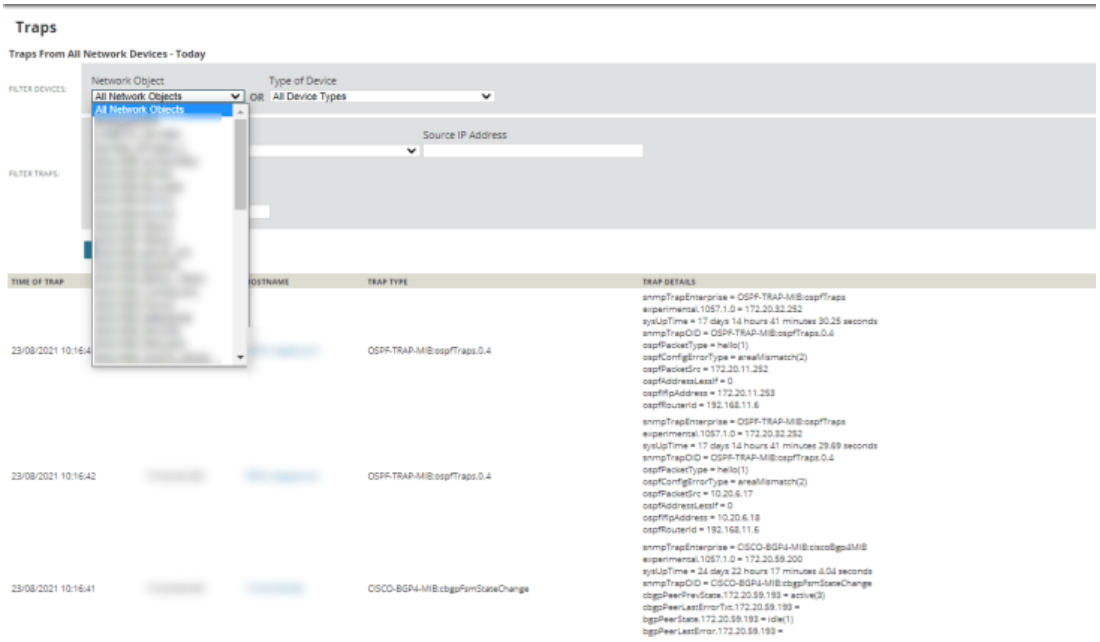


Figura 17-3. Mensajes *Traps* recolectados por la aplicación NPM

Realizado por: Duche, I. 2021

- Visualización de alertas y eventos ocurrido en la red.

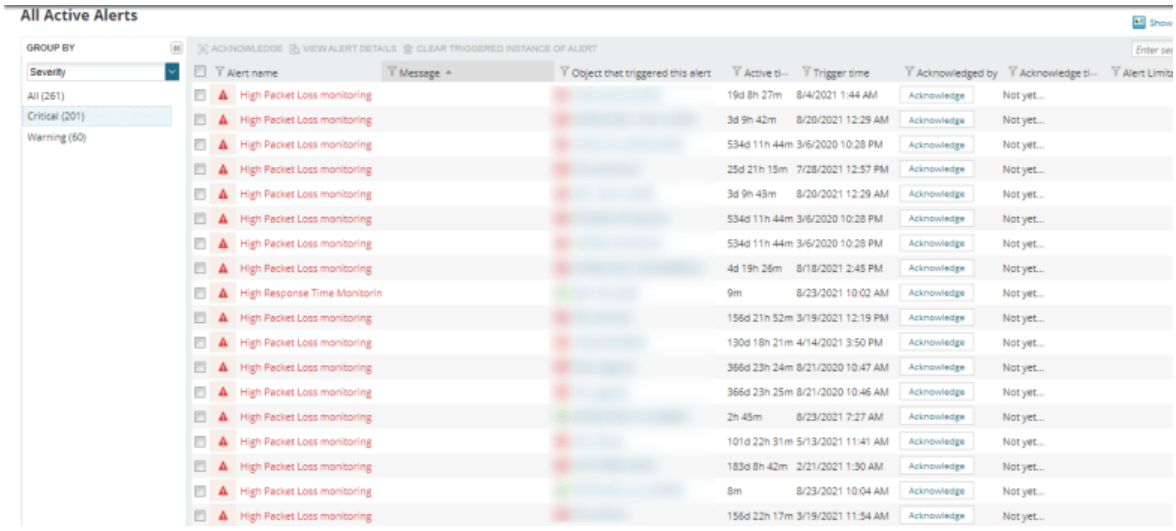


Figura 18-3. Mensajes de alertas críticas

Realizado por: Duche, I. 2021

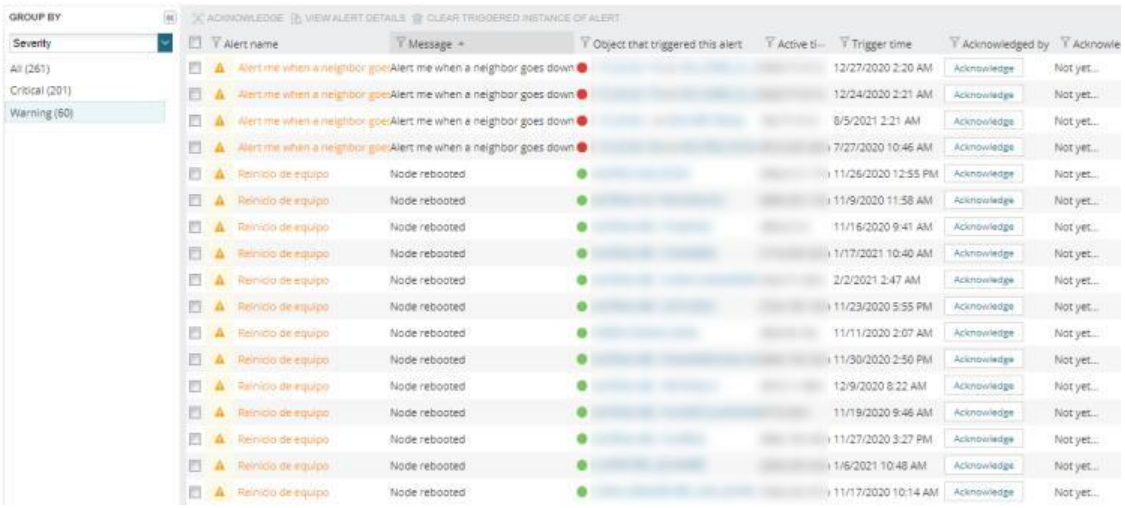


Figura 19-3. Mensajes de alertas de precaución

Realizado por: Duche, I. 2021

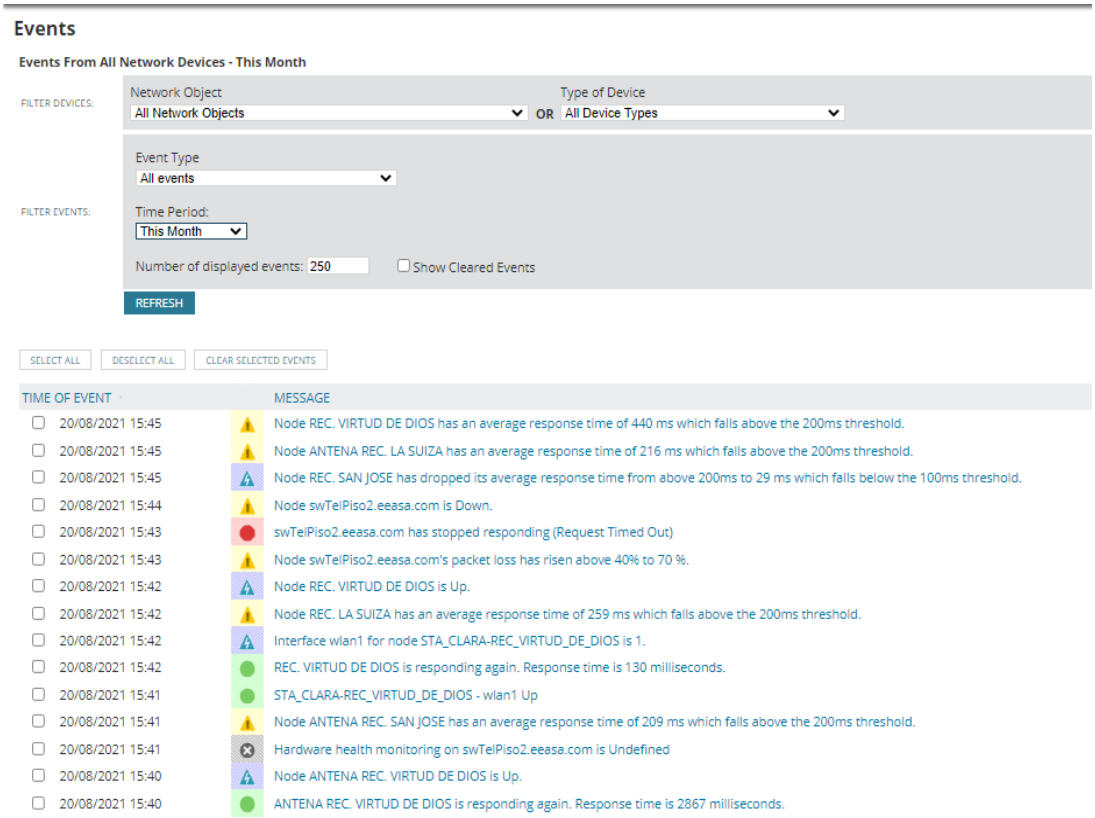
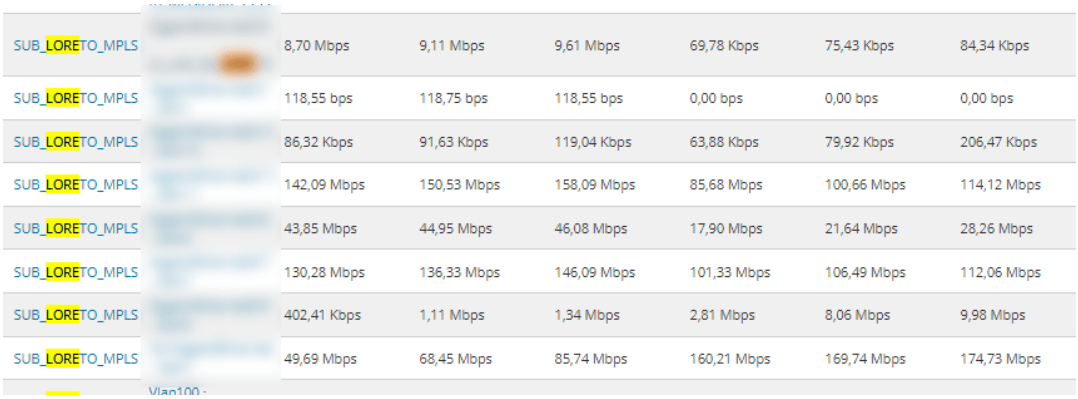


Figura 20-3. Mensajes de eventos ocurridos en los nodos

Realizado por: Duche, I. 2021

- Generación de reportes



SUB_LORETO_MPLS	8,70 Mbps	9,11 Mbps	9,61 Mbps	69,78 Kbps	75,43 Kbps	84,34 Kbps
SUB_LORETO_MPLS	118,55 bps	118,75 bps	118,55 bps	0,00 bps	0,00 bps	0,00 bps
SUB_LORETO_MPLS	86,32 Kbps	91,63 Kbps	119,04 Kbps	63,88 Kbps	79,92 Kbps	206,47 Kbps
SUB_LORETO_MPLS	142,09 Mbps	150,53 Mbps	158,09 Mbps	85,68 Mbps	100,66 Mbps	114,12 Mbps
SUB_LORETO_MPLS	43,85 Mbps	44,95 Mbps	46,08 Mbps	17,90 Mbps	21,64 Mbps	28,26 Mbps
SUB_LORETO_MPLS	130,28 Mbps	136,33 Mbps	146,09 Mbps	101,33 Mbps	106,49 Mbps	112,06 Mbps
SUB_LORETO_MPLS	402,41 Kbps	1,11 Mbps	1,34 Mbps	2,81 Mbps	8,06 Mbps	9,98 Mbps
SUB_LORETO_MPLS	49,69 Mbps	68,45 Mbps	85,74 Mbps	160,21 Mbps	169,74 Mbps	174,73 Mbps

Figura 21-3. Ejemplo de generación de reporte de tráfico de un equipo.

Realizado por: Duche, I. 2021

3.5. Análisis comparativo entre sistemas de monitoreo de red

Una vez finalizado la evaluación y verificación del correcto desempeño del nuevo sistema de monitoreo de red, se realizó el análisis comparativo con la finalidad de comprobar que se resolvieron los problemas que se encontró en la evaluación del sistema de monitoreo de red anterior expuestos en la sección 2.2. Por medio del análisis se demuestra que el nuevo sistema de monitoreo de red para la empresa se encuentra completamente funcional.

3.5.1. Comparación de rendimiento de la aplicación de monitoreo (NPM)

Una vez operativo el servidor de la aplicación NPM, se hizo una evaluación del rendimiento de los recursos de memoria (RAM) y procesamiento (CPU) del equipo, para comparar los resultados obtenidos con la información del rendimiento del servidor anterior, y comprobar el correcto desempeño del mismo.

En la Figura 22-3, se observa el consumo de memoria (RAM) del servidor anteriormente utilizados para alojar la aplicación de monitoreo, donde se visualiza que se está utilizando el 97% de memoria RAM del equipo, por esta razón la aplicación tenía constantes fallas de operación.

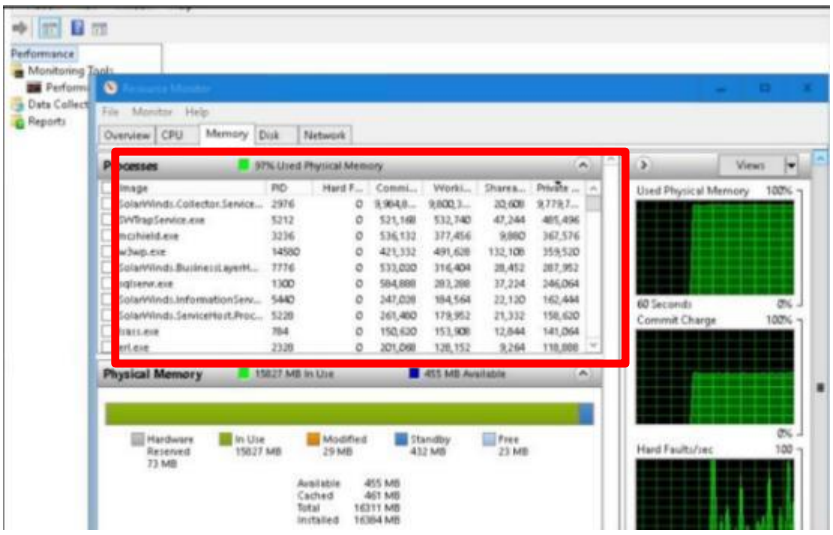


Figura 22-3. Consumo de memoria RAM de servidor de monitoreo anterior

Realizado por: Duche, I. 2021

A continuación, en la Figura 23-3, se muestra el consumo de memoria RAM que utiliza el nuevo servidor en el que se encuentra instalado la aplicación NPM, el cual es del 43%, lo que se considera un nivel óptimo para el correcto desempeño de la aplicación de monitoreo.

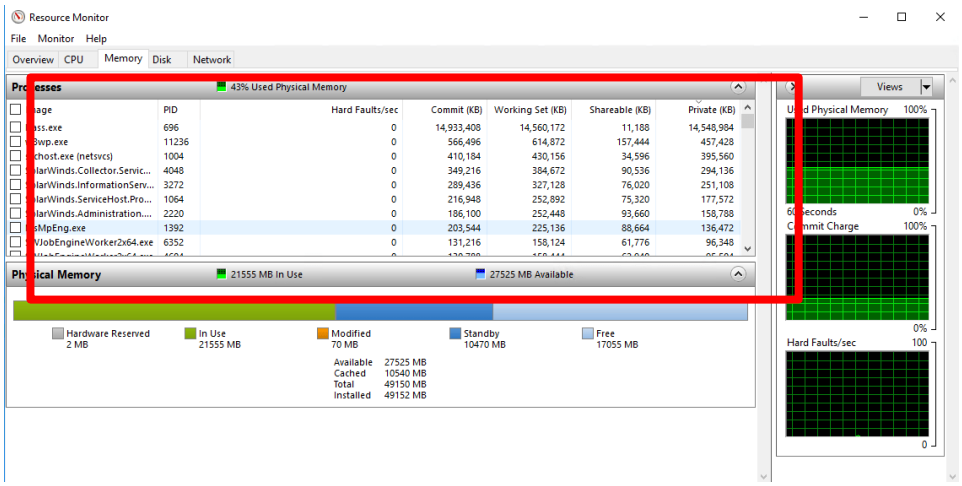


Figura 23-3. Consumo de memoria RAM en servidor NPM actual

Realizado por: Duche, I. 2021

Como se muestra en la Figura 24-3, el promedio del consumo de procesamiento en el servidor de monitoreo anteriormente utilizados es de 80,56%, lo cual es considerado un uso elevado de procesamiento, por lo tanto, esto repercutía en altas tiempo de latencia al momento de usar la aplicación de monitoreo.

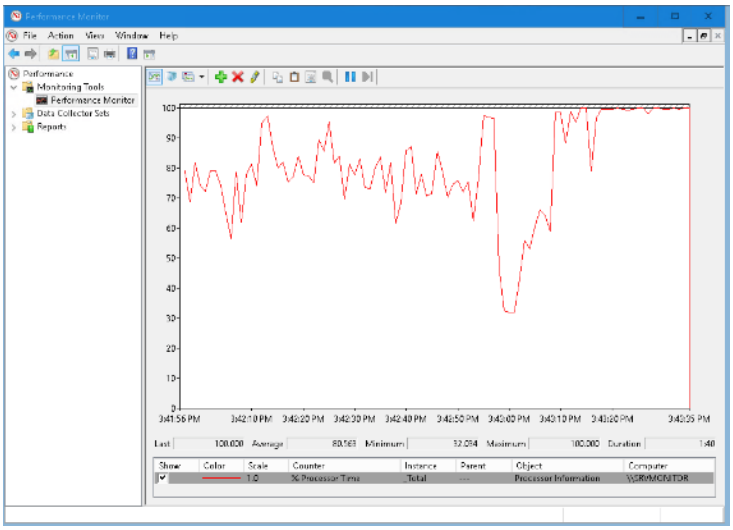


Figura 24-3. Consumo de procesamiento en servidor NPM anterior

Realizado por: Duche, I. 2021

Mientras que en la Figura 25-3, se puede visualizar que el consumo de procesamiento se encuentra en niveles mínimos, con un promedio de 8.16%, lo cual garantiza que el equipo está operando de una manera óptima.

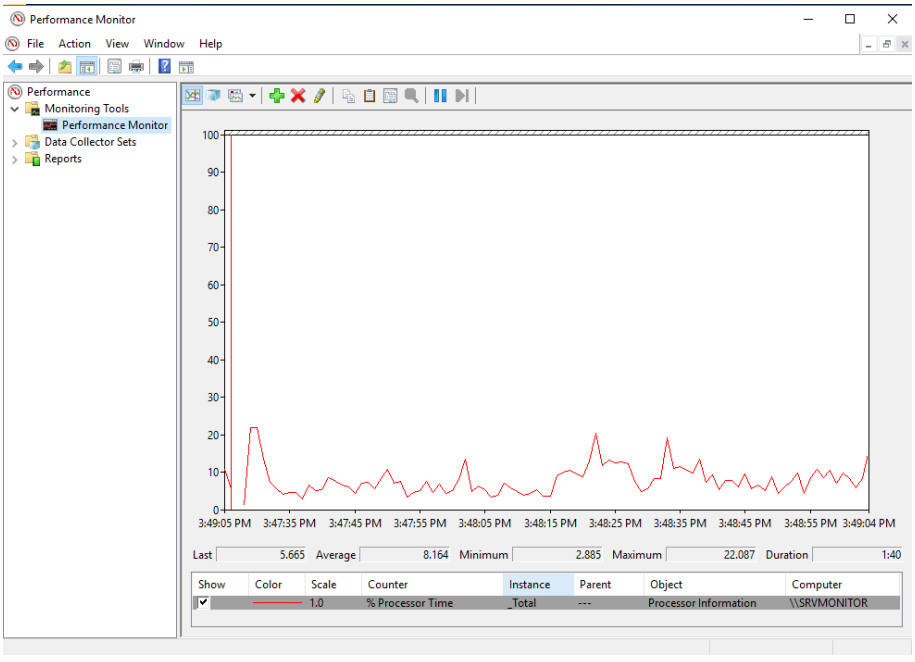


Figura 25-3. Consumo de procesamiento en servidor NPM anterior

Realizado por: Duche, I. 2021

Para finalizar en la Figura 26-3, se puede observar un resumen general del rendimiento del equipo de la aplicación NPM.

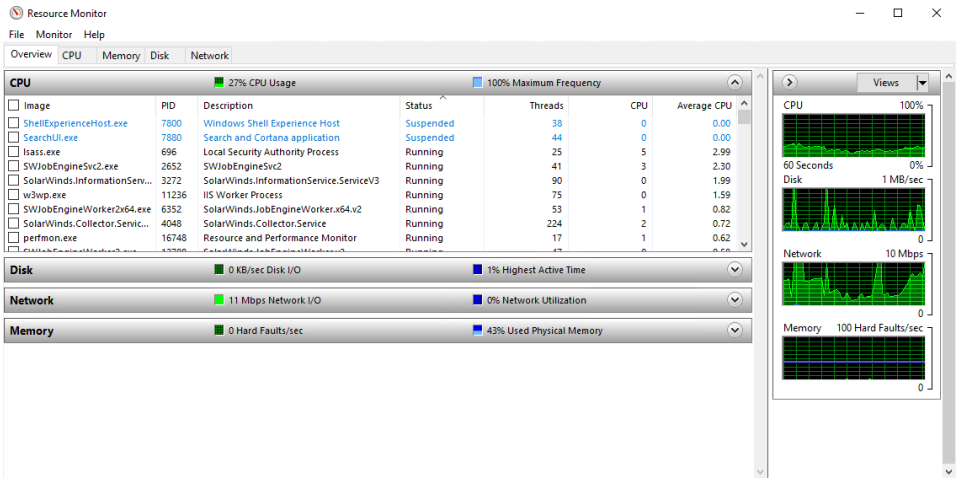


Figura 26-3. Resumen del rendimiento del servidor NPM

Realizado por: Duche, I. 2021

3.5.2. Comparación de rendimiento de la base de datos (SQL Server)

Al igual que con el servidor de la aplicación NPM, una vez puesto en marcha el servidor de base de datos (MS SQL Server), se realizó el análisis del rendimiento de memoria y procesamiento del equipo, para garantizar que el consumo de recursos se encuentre en niveles normales para su correcto funcionamiento.

En la Figura 27-3, se visualiza que el promedio del consumo del procesamiento de la base de datos en el servidor anterior es de 81.65%, lo cual provoca conflictos y problemas de operación de la base de datos.

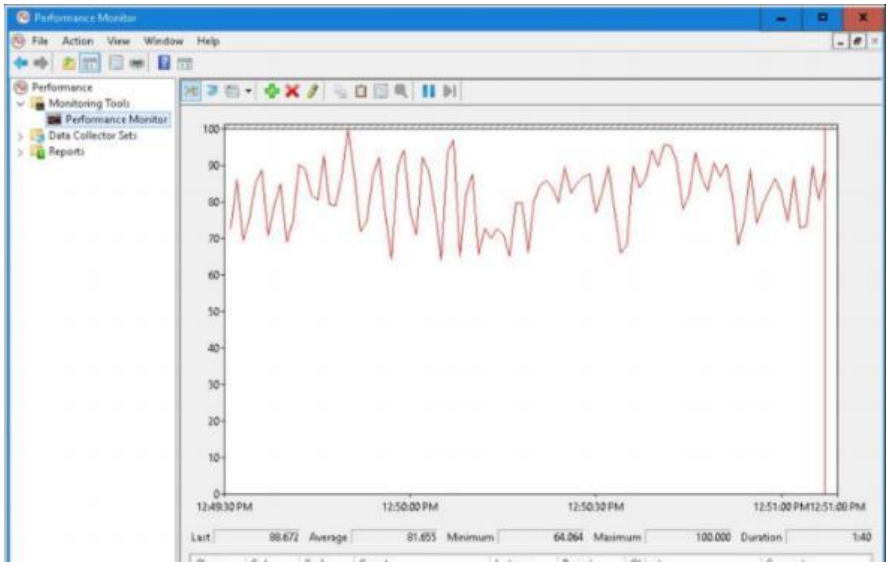


Figura 27-3. Consumo de procesamiento de base de datos MS SQL Server anterior

Realizado por: Duche, I. 2021

Mientras, en la Figura 28-3, se muestra que el promedio del consumo del procesamiento del servidor de base de datos usado actualmente en el sistema es de 4.22%, por lo que se puede garantizar que el servidor se encentra operando de una manera óptima.

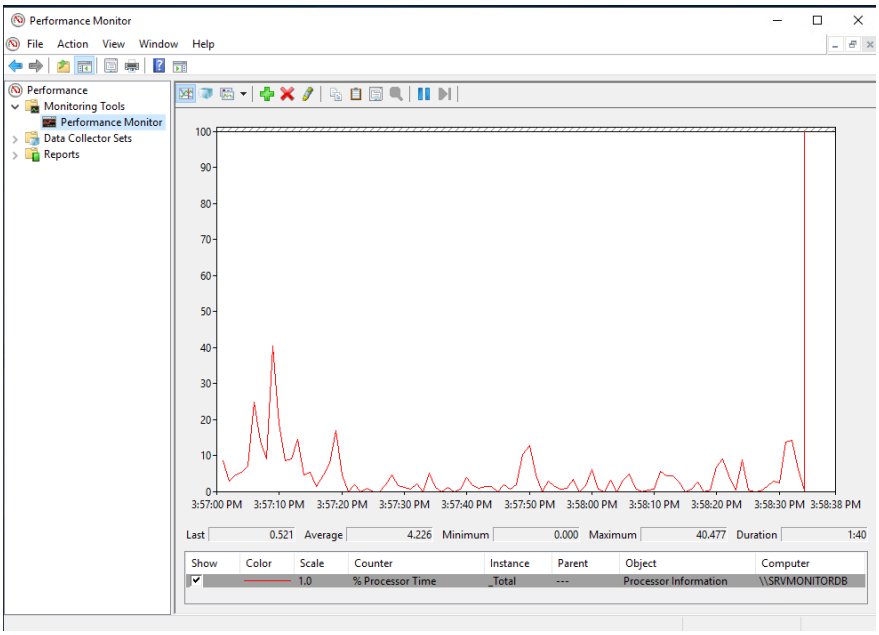


Figura 28-3. Consumo de procesamiento de base de datos MS SQL Server actual

Realizado por: Duche, I. 2021

En la Figura 29-3, se puede observar que el consumo de memoria del equipo en el cual se encuentra operando la aplicación para la gestión de base de datos SQL Server es del 97%, lo cual provoca conflictos al momento de su funcionamiento.

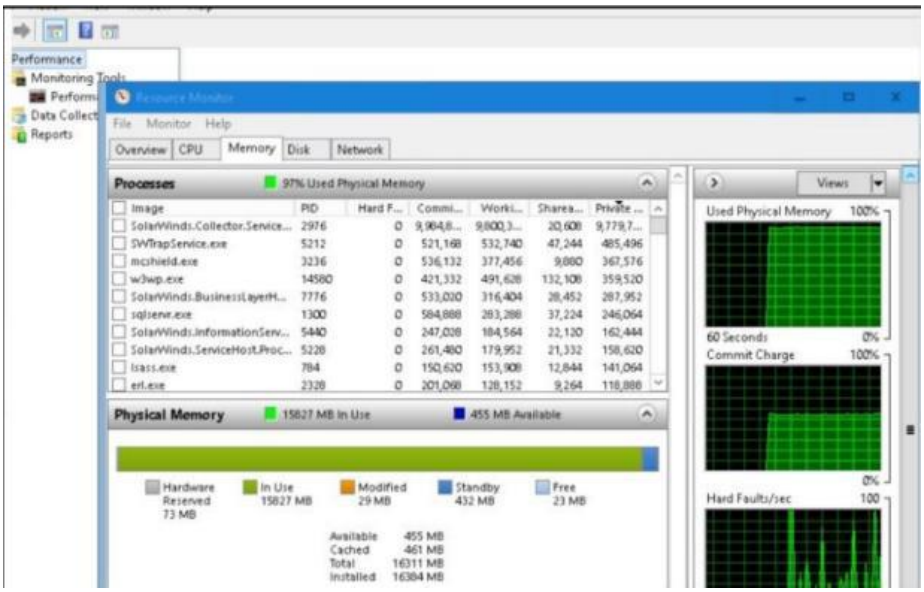


Figura 29-3. Consumo de memoria de base de datos MS SQL Server anterior

Realizado por: Duche, I. 2021

Sin embargo, como se muestra en la Figura 30-3, el consumo de memoria del servidor de base de datos SQL Server que se usa actualmente es del 20%, por lo que se verifica que el servidor de base de datos se encuentra completamente operativo.

Figura 30-3. Consumo de recurso de base de datos MS SQL Server actual

Realizado por: Duche, I. 2021

Para finalizar, en la figura 31-3, se puede visualizar un resumen general del rendimiento de los recursos usados por el servidor de base de datos SQL Serve.

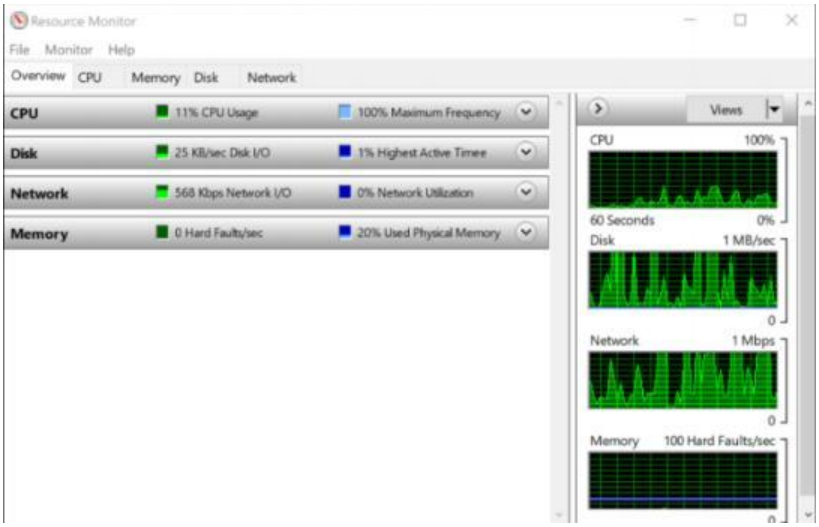


Figura 31-3. Resumen de recurso de base de datos SQL Server actual

Realizado por: Duche, I. 2021

CONCLUSIONES

- Después de haber realizado la evaluación del sistema de monitoreo de red usado por la empresa, se encontró varios problemas de funcionamiento, entre los que se puede mencionar: errores en el servidor de la aplicación de monitoreo, limitación de almacenamiento, limitación de licenciamiento, equipos innecesarios en el sistema, desconocimiento de gestión de red y problemas a nivel aplicativo, por lo cual se concluyó que la empresa requiere una repotenciación del sistema de gestión para la infraestructura de la red corporativa, ya que es indispensable que dicho sistema se encuentra completamente operativo y garantice la sostenibilidad de la red.
- Por medio del desarrollo de una evaluación adecuada de la red empresarial, en la que se analice métricas como: el número de equipos a ser monitoreados, el flujo de tráfico a través de la red, número de peticiones que recibe el servidor, posibles tendencias de crecimiento de la red corporativa y seguir recomendaciones del fabricante, se puede diseñar un correcto dimensionamiento de los recursos a usarse en el sistema de gestión de red, garantizando el correcto funcionamiento de los equipos implementados dentro del sistema, evitando fallas que causen la suspensión del servicio.
- En base a la búsqueda bibliográfica de la información sobre los modelos de gestión y los protocolos SNMP y Syslog, se facilitó el diseño de la arquitectura del sistema de monitoreo de red de la empresa, de esta forma se garantiza que la implementación del nuevo sistema va a funcionar de manera correcta y cumplirá con los requerimientos que necesita un sistema de gestión de una infraestructura de red.
- Una vez finalizada la evaluación y el análisis comparativo del sistema de monitoreo de red repotenciado de la empresa se concluyó que el sistema se encuentra completamente operativo, ya que cumple con las funciones principales de la gestión de red que son requeridas por el administrador, entre las que se encuentra: monitoreo de equipos que están operativos y tienen una prioridad alta de gestión, uso eficiente de servicios que brinda la aplicación NPM como recopilación de mensajes Syslog, *Traps*, alertas críticas y de precaución, visualización de eventos ocurridos en la red y generación de reportes personalizados. De la misma forma, el rendimiento de los equipos se encuentra en niveles normales, garantizando el correcto funcionamiento del sistema.

RECOMENDACIONES

- Se recomienda realizar evaluaciones periódicas de la red empresarial, de esta forma se puede tener datos históricos que pueda ayudar a realizar estudios de rendimiento y optimización de recursos de la infraestructura de red en un futuro, y poder realizar cualquier tipo de implementación y desarrollo que se requiera dentro de la red.
- Realizar un análisis continuo del desempeño del sistema de monitoreo de red, para verificar constantemente el funcionamiento correcto de los elementos que intervienen en el sistema como: rendimiento de servidores que alojan la aplicación, correcto funcionamiento de servicios de la aplicación NPM, revisión de licencias usadas por la aplicación y verificación de envío correcto de mensajes SNMP y Syslog por parte de los agentes.
- Debido a que el protocolo SNMPv2 no es seguro, se recomienda aplicar diferentes mecanismos de seguridad dentro de la infraestructura de red para resguardar la información que viaja por cada uno de los dispositivos, de la misma forma, para la gestión de los equipos monitoreados se requiere hacer uso de buenas prácticas al momento de agregar nuevos dispositivos dentro del sistema de gestión siguiendo las recomendaciones de los modelos de gestión de redes referenciales. Es necesario revisar la documentación oficial de los fabricantes de los equipos de red para la configuración correcta de los protocolos SNMP y Syslog.
- Se debe tener una capacitación continua con respecto a la herramienta de monitoreo de red NPM para poder explotar completamente el potencial de la aplicación, y poder hacer uso de todas sus funcionalidades, así mismo se recomienda buscar información de temas específicos de la aplicación en sitios oficiales de la empresa desarrolladora SolarWinds.

BIBLIOGRAFÍA

BRIHUEGA, D. *Administración de Redes Telematicas* [en línea]. Madrid-España: RA-MA Editorial, 2015. [Consulta: 2020-11-05]. Disponible en: https://elibro.net/es/ereader/espoch/106471?page=136

CABRERA, A. *Diseño e implementacion de virtualizacion con vSphere sobre servidores Blade, dentro de una zona desmilitarizada Linux para ambientes de pruebas de software en el departamento de desarrollo de la empresa Transoceánica Cia. Ltda.* [En línea] (Trabajo de titulación). Universidad Politécnica Salesiana Ecuador, Ingeniería de Sistemas. Guayaquil-Ecuador. 2017. pp. 18-23. [Consulta: 2020-11-09]. Disponible en: https://dspace.ups.edu.ec/bitstream/123456789/15005/1/UPS-GT002038.pdf

CELADE. *Métodos Para Proyecciones* [en línea]. San José-Costa Rica, 1984. [Consulta: 2021-03-05]. Disponible en: https://repositorio.cepal.org/bitstream/handle/11362/8754/S8400128_es.pdf

CISCO SYSTEMS, *Indexación de cadenas de comunidad SNMP*. [en línea]. [Consulta: 2021-04-15]. Disponible en: https://www.cisco.com/c/es_mx/support/docs/ip/simple-network-management-protocol-snmp/40367-camsnmp40367.html

CISCO SYSTEMS, *¿Qué es el monitoreo de red?* [en línea]. [Consulta: 2020-11-11]. Disponible en: https://www.cisco.com/c/es_mx/solutions/automation/what-is-network-monitoring.html

CONTRERAS, C. *Desarrollo de un sistema de monitoreo para la obtención de la información de red y el gráfico de su topología, basado en la utilización de los protocolos SNMP e ICMP*. [En línea] (Trabajo de titulación). Escuela Politécnica Nacional, Facultad de Ingeniería Eléctrica y Electrónica, Escuela de Ingeniería en Electrónica y Telecomunicaciones. Quito-Ecuador. 2006. pp. 8-15. [Consulta: 2020-11-09]. Disponible en: https://bibdigital.epn.edu.ec/bitstream/15000/5094/1/T2508.pdf

DUQUE, N. *Gestión de redes de datos a través de ontologías utilizando sistemas multiagentes*. [En línea] (Trabajo de titulación) (Maestría). Universidad Nacional de Colombia sede Manizales, Facultad de Ingeniería y Arquitectura, Maestría en Automatización Industrial. Manizales-Colombia. 2015. pp. 10-14. [Consulta: 2020-12-09]. Disponible en: https://repositorio.unal.edu.co/bitstream/handle/unal/55714/75071389.2015.pdf?sequence=1&isAllowed=y

ECHEVERRÍA, F. *Implementación y Evaluación de Sistema de Monitoreo de Seguridad basado en flujos de paquetes IP* [en línea] (Trabajo de titulación). Universidad de Chile. Facultad de Ciencias Físicas y matemáticas. Escuela de Ingeniería Civil en Computación. Santiago-Chile. 2008. pp. 16. [Consulta: 2020-11-23]. Disponible en: http://www.tesis.uchile.cl/tesis/uchile/2008/echeverria_fs/sources/echeverria_fs.pdf.

FERNÁNDEZ, Y. y GARCÍA, K., "Virtualización". *Telem@tíc.* [en línea], 2011, (Cuba) 10(3). pp. 61-73. [Consulta: 2020-12-20]. ISSN 1729-3804 Disponible en: http://148.202.167.116:8080/xmlui/bitstream/handle/123456789/2281/Virtualizaci%C3%B3n.pdf?sequence=1&isAllowed=y

FIALLOS, L. *Servicio de logs centralizado para los servidores del Centro de Cómputo de la UCSG, visualizado por medio de una aplicación web dentro de la red interna.* [en línea] (Trabajo de titulación). Universidad Católica de Santiago de Guayaquil. Facultad de Ingeniería. Escuela de ingeniería en Sistemas Computacionales. Guayaquil-Ecuador. 2018. pp. 12-17. [Consulta: 2021-01-13]. Disponible en: http://repositorio.ucsg.edu.ec/bitstream/3317/10003/1/T-UCSG-PRE-ING-CIS-171.pdf

GATERA, T. *Network Adminstration*. [en línea] (Tesis Pregrado). African Virtual University. Nairobi-Africa. 2017. pp, 51-64. [Consulta: 2020-11-20]. Disponible en: https://oer.avu.org/bitstream/handle/123456789/676/CSI%205100%20Network%20Administration1.pdf?sequence=1&isAllowed=y

GÓMEZ, J. *Implementación de un Servidor Syslog Centralizado en la Red Corporativa de ETECSA.* [en línea] (Trabajo de titulación). Universidad Central "Marta Abreu" de Las Villas. Facultad de Ingeniería Eléctrica. Departamento de Telecomunicaciones y Electrónica. Santa

Clara-Cuba. 2007. pp. 5-23. [Consulta: 2021-01-15]. Disponible en: https://dspace.uclv.edu.cu/bitstream/handle/123456789/6048/Yordy%20Rafael%20G%C3%B3mez%20Mera.pdf?sequence=1&isAllowed=y

LIMONCELLI, T.A., HOGAN, C.J. y CHALUP, S.R. *The Practice of System and Network Administration*. [en línea]. Segunda Edición. Boston-USA. Pearson Education. 2007. ISBN 978-0-321-49266-1. [Consulta: 2020-12-15]. Disponible en: http://index-of.co.uk/Addison-Wesley/The.Practice.of.System.and.Network.Administration.2nd.Edition.pdf

MERCADO, N. *Aplicaciones para la administración y operación de redes* [en línea] (Tesis Pregrado). Universidad Tecnológica de Bolívar. Minor en Comunicaciones y Redes. Cartagena de Indicas-Colombia. 2008. pp. 12-17. [Consulta: 2021-01-05]. Disponible en: https://biblioteca.utb.edu.co/notas/tesis/0043205.pdf

MORENO, A. y SERNA, S. *Diseño e implementacion de un prototipo de software para la administracion de red usando SNMPv3 sobre el sistema operativo Android.* [En línea] (Trabajo de titulación). Escuela Politécnica Nacional, Facultad de Ingeniería Eléctrica y Electrónica, Escuela de Ingeniería en Electrónica y Telecomunicaciones. Quito-Ecuador. 2013. pp. 26-39. [Consulta: 2021-02-25]. Disponible en: https://bibdigital.epn.edu.ec/bitstream/15000/5893/1/CD-4741.pdf

NARANJO, D. y ORTEGA, P. *Desarrollo de una aplicación gráfica basado en el sistema operativo Linux para el monitoreo y administración del tráfico de datos de redes LAN* [En línea] (Trabajo de titulación). Escuela Politécnica Nacional, Facultad de Ingeniería Eléctrica y Electrónica, Escuela de Ingeniería en Electrónica y Telecomunicaciones. Quito-Ecuador. 2006. pp. 1-6. [Consulta: 2020-12-03]. Disponible en: https://bibdigital.epn.edu.ec/bitstream/15000/2353/1/CD-0006.pdf

NETWORK PERFORMANCE MONITOR. *NPM 2020.2 System Requirements SolarWinds Worldwide* [En línea]. [Consulta: 2020-12-03]. Disponible en: https://documentation.solarwinds.com/en/success_center/NPM/content/system_requirements/NPM_2020-2_system_requirements.htm.

PADILLA, R. y RON, M. Propuesta de modelos de gestión de infraestrutura de red, basado en las mejores prácticas de gestipon de TI y los modeles estándar de gestión de red- Caso de estudio EP PETROECUADOR. [En línea] (Trabajo de titulación) (Maestría). Escuela Politécnica Nacional, Facultad de Ingeniería en sistemas. Quito-Ecuador. 2015. pp. 1-22. [Consulta: 2021-01-30]. Disponible en: https://bibdigital.epn.edu.ec/bitstream/15000/15092/1/CD-6904.pdf

PANDORA FMS TEAM. *Monitoreo de Red en 2021: qué debemos saber*. [blog]. 2017. [Consulta: 2020-11-20]. Disponible en: https://pandorafms.com/blog/es/monitoreo-de-red-que-debemos-saber/

POSEY, B. *What is a Server?*. [blog]. 2021. [Consulta: 2021-02-25]. Disponible en: https://whatis.techtarget.com/definition/server

RAMIREZ, E., 2019. *Alternativas de configuración con el uso de los protocolos Syslog y SNMP para la gestión de red de redes avanzadas.* Universidad Nacional Agraria de la Selva. Facultad de Ingeniería en Informática y Sistemas. Tingo María-Perú. 2019. pp. 17-35. [Consulta: 2021-03-01]. Disponible en: http://repositorio.unas.edu.pe/bitstream/handle/UNAS/1645/RDY_2019.pdf?sequence=1&isAllowed=y

RECOMENDACIÓN UIT-T M.3010. *Principios para una red de gestión de las telecomunicaciones.*

RECOMENDACIÓN UIT-T M.3400. *Funciones de gestión de la red de gestión de las telecomunicaciones.*

RECOMENDACIÓN UIT-T X.711. *Tecnología de la información – Interconexión de sistemas abiertos – Protocolo común de información de gestión: Especificación.*

RFC 1157. *A Simple Network Management Protocol (SNMP).*

RFC 3416. *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP).*

RFC 3418. *Management Information Base (MIB) for the Simple Network Management Protocol (SNMP).*

RFC 5424. *The Syslog Protocol.*

ROMERO, G. y PADUA, S. "Los recursos de red y su monitoreo" *Revista Cubana de Informática Médica*. [en línea], 2018, 10(1), pp. 76-83. [Consulta: 2020-11-20]. ISSN 1684-1859. Disponible en: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1684-18592018000100009

SOLARWINDS. *Network Performance Monitor, SolarWinds Worldwide* [en línea]. [Consulta: 2020-11-20]. Disponible en: https://www.solarwinds.com/es/network-performance-monitor. pendiente

SONOMA COUNTY OFFICE OF EDUCATION. *Network Administrator*. [En línea]. 2013. [Consulta: 2020-11-26]. Disponible en: https://www.scoe.org/blog_files/Network%20Administrator%20JD%209-13.pdf

SOTAMINGA, M., GUERRERO, C. y ABAD, A. *Implementación de un ambien Virtualizado para el manejo de múltiples servidores de VoIP sobre una plataforma común de hardware.* [en línea] (Trabajo de titulación). Escuela Superior Politécnica del Litorel, Facultad de Ingenieria en Electricidad y Computacion. Guayaquil-Ecuador. 2011. pp. 7-17. [Consulta: 2021-03-01]. Disponible en: https://www.dspace.espol.edu.ec/bitstream/123456789/19405/1/TESIS-SOTAMINGA-GUERRERO-ABAD-U.pdf

STALLINGS, W. "SNMP and SNMPv2: The Infrastructure for Network Management". *IEEE Communicactions Magazine*. (United State of America), 1998. pp. 37-43.

TORRES, L. *Administración y gestión de la red inalámbrica del gobierno autónomo descentralizado (GADIP) del cantón cayambe basada en el modelo funcional FCAPS de la OSI*. (Trabajo de titulación). Universidad Técnica del Norte. Facultad de Ingeniería en Ciencias Aplicadas. Ibarra-Ecuador. 2015. pp. 1-6.

TRUJILLO, L. *Sistema de gestión de red para Internet de las Cosas*. [en línea] (Tesis de maestría), Pontificia Universidad Javeriana. Faculta de Ingeniería. Departamento de Electrónica. Bogotá-Colombia. 2019. pp. 4-13. [Consulta: 2020-11-20]. Disponible en: https://repository.javeriana.edu.co/bitstream/handle/10554/45208/Documento.pdf?sequence=1&isAllowed=y

VIEDA, M. *Administración de Logs.* [blog]. [Consulta: 2021-02-25]. Disponible en: https://manuelvieda.com/blog/administracion-de-logs/.

ANEXOS

ANEXO A. Empresa Eléctrica Ambato Regional Centro Norte S.A.

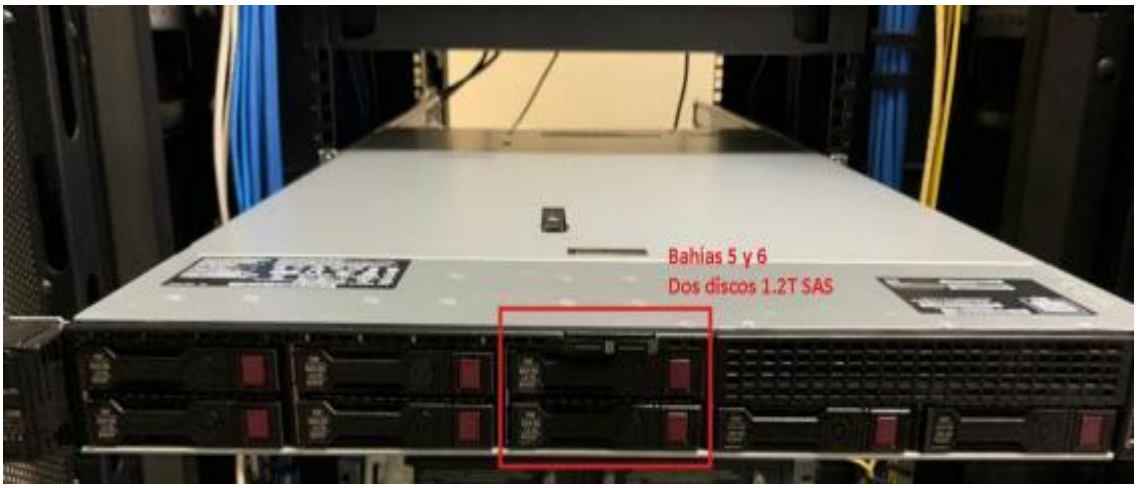
1. Instalación Matriz de EEASA.

2. Centro de Control en complejo Loreto de EEASA.

ANEXO B. Equipos utilizados para implementación de sistema de monitoreo.

1. Servidor a usarse para sistema de monitoreo de red de la empresa.

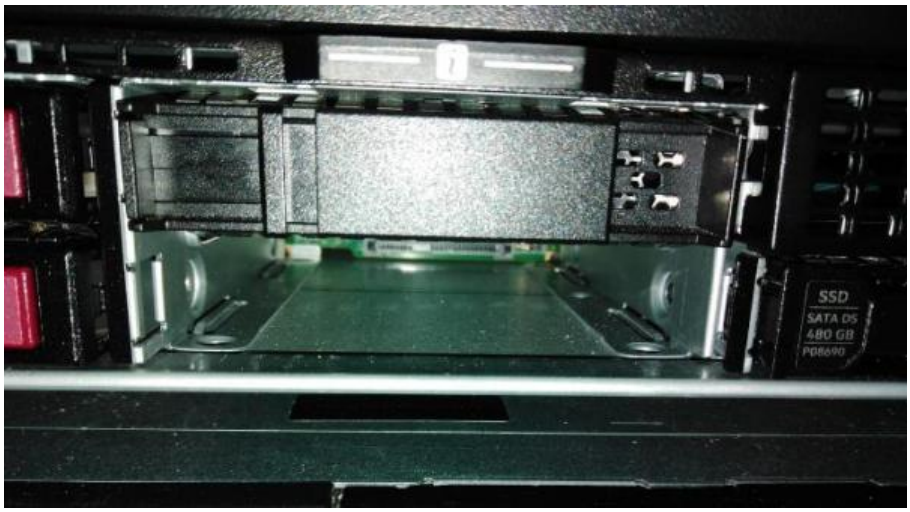
2. Servidor repotenciado para sistema de monitoreo de red de la empresa.



ANEXO C. Implementación de sistema de monitoreo de red para la EEASA.

1. Implementación de recursos de memoria RAM al servidor

2. implementación de discos duros en bahías del servidor



ANEXO D. Evaluación de sistema de monitoreo de red de la EEASA.

1. Pruebas de monitoreo a equipo de radio enlace Mikrotik

2. Pruebas de monitoreo a equipo de red Cisco.

ANEXO E. Certificado de verificación

EMPRESA ELECTRICA AMBATO
REGIONAL CENTRO NORTE S.A.

Trabajando con energía..!

EEASA

CERTIFICACIÓN

Por la presente, como administrador de red de la EEASA, comunico que el señor **ISRAEL SEBASTIÁN DUCHE VALLEJO**, estudiante de la Escuela Superior Politécnica de Chimborazo, Facultad de Informática y Electrónica, Carrera de Ingeniería Electrónica, Telecomunicaciones y Redes, ha culminado con éxito la tesis con el tema: **"DESARROLLO DE LA INGENIERIA DEL SISTEMA DE MONIOTOREO DE RED PARA LA EMPRESA ELÉCTRICA AMBATO REGIONAL CENTRO NORTE S.A."**, los resultados expuestos en el documento son correctos y el sistema de monitoreo de red se encuentra completamente operativo, además la información presentada en el documento guarda la confidencialidad de la empresa.

Atentamente

EMPRESA ELECTRICA AMBATO REGIONAL CENTRO NORTE S.A.
EEASA
DEPARTAMENTO SUBTRANSMISION

Ing. Diego Ocaña

CI: 180393678-8

Jefe de Área 2

Área de Redes y Comunicaciones

Ambato diciembre 09, 2021

Av. 12 de Noviembre 11-29 y Espejo Casilla 18-01-446
Telf: (03) 2998600 Reparaciones: 136 Fax: (03) 2421265
www.eeasa.com.ec e-mail: presidencia@eeasa.com.ec
Ambato - Ecuador

SGS UKAS ISO 9001