ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA EN SISTEMAS

"ANÁLISIS DE HERRAMIENTAS OPENSOURCE DE ADMINISTRACIÓN Y MONITOREO BASADO EN SNMP, APLICADO A LA RED DE DATOS DEL ILUSTRE MUNICIPIO DE AMBATO"

TESIS DE GRADO

Previa la obtención del título de

INGENIERO EN SISTEMAS INFORMÁTICOS

Presentado por:

JUANA KARINA ARELLANO AUCANCELA

ERIKA NATHALY CALDERÓN CAJAS

RIOBAMBA – ECUADOR

2011

Muchas han sido las personas que de manera directa o indirecta nos han ayudado en la realización de esta tesis. Queremos dejar constancia de todos ellos y agradecerles con sinceridad su participación.

Agradecemos infinitamente a Dios por permitirnos llegar hasta dónde estamos y por bendecirnos todos los días de nuestras vidas, guiándonos por el camino del bien y así culminar exitosamente nuestros sueños trazados, a nuestros padres por su eterno amor, su admirable abnegación, ya que siempre han estado inculcándonos el valor de la verdad, la vida, el respeto y la fortaleza para siempre luchar por nuestros propósitos.

Nuestro agradecimiento a nuestro director, Ingeniero Diego Ávila P. por su tiempo, paciencia, y acertada orientación la misma que nos ha llevado a culminar con éxito nuestro trabajo investigativo, en el ha primado su laboriosidad, y extensos conocimientos. Muchas Gracias.

Así mismo un agradecimiento muy especial al presidente del tribunal de nuestra tesis, Ingeniero Alberto Arellano A. por su amistad incondicional, confianza, sus apreciados y relevantes aportes, críticas, y sugerencias y sobre todo por su gran apoyo en la ejecución de nuestro trabajo final.

Dejamos constancia de nuestro profundo agradecimiento al departamento de Informática del Ilustre Municipio de Ambato, por habernos dado la oportunidad de aplicar nuestros conocimientos adquiridos, en especial al Ing. Francisco López quien nos brindó toda su ayuda y aprobación en cuanto a las tareas de estudio realizadas.

No quisiéramos concluir sin expresar nuestro agradecimiento a nuestros amigos de siempre, gracias por vuestra paciencia, palabras y apoyo en los momentos justos y sobre todo por vuestra compañía incondicional.

A mi Señor, Jesús, quien me dio la fe, la fortaleza, la salud y la esperanza para terminar este trabajo.

A mis padres, José Alberto y María Teresa quienes me enseñaron desde siempre a luchar para alcanzar mis metas. Mi triunfo es el de ustedes papis, ¡los amo!

A mis hermanos/as, quienes supieron brindarme su comprensión y cariño el cual me ha ayudado e impulsado a seguir adelante.

A mis adorados y muy queridos sobrinos David, Emily, Camila, Anhalis y Cyndel, quienes son el complemento de mi alegría, mis pequeños amores.

Es inevitable no hacer una dedicación especial a mi hermano y siempre AMIGO Alberto, quien me brindó su cariño, su estímulo y su apoyo constante y sobre todo me motivó siempre con sus palabras, "No te rindas" y "Sé fuerte". ¡ Mil Gracias.!

Finalmente quiero dedicar a mis amigos, quienes caminaron junto a mí en la batalla, con sus palabras de aliento. Gracias Amigos míos…!!

Juana Karina Arellano Aucancela

A mis padres quienes han sabido formarme con buenos sentimientos, hábitos y valores, lo cual me ha ayudado a salir adelante buscando siempre el mejor camino, sin decaer ante los fracasos y adversidades, a mis abuelitos quienes me dieron todo lo que soy como persona, mis valores, mis principios, mi perseverancia y mi empeño, y todo ello con una gran dosis de amor y sin pedir nunca nada a cambio, a mis hermanas y a toda mi familia que siempre me han apoyado para que siga adelante. También dedico este trabajo a mis amigos quienes siempre me ayudaron cuando más lo necesitaba brindándome su amistad, confianza y apoyo para salir adelante.

Erika Nathaly Calderón Cajas

NOMBRE	FIRMA	FECHA
Ing. Iván Ménes **DECANO FACULTAD DE INFORMÁTICA Y ELECTRÓNICA**	.....	.....
Ing. Raúl Rosero **DIRECTOR ESCUELA INGENIERÍA EN SISTEMAS**	.....	.....
Ing. Diego Ávila **DIRECTOR DE TESIS**	.....	.....
Ing. Alberto Arellano A. **MIEMBRO DEL TRIBUNAL**	.....	.....
Ing. Carlos Rodríguez **DIRECTOR DPTO DOCUMENTACIÓN**	.....	.....

NOTA DE LA TESIS .....

“Nosotras, Juana Karina Arellano Aucancela y Erika Nathaly Calderón Cajas somos responsables de las ideas, doctrinas y resultados expuestos en esta Tesis, y el patrimonio intelectual de la misma pertenecen a la ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO”.

Juana Karina Arellano Aucancela	**Erika Nathaly Calderón Cajas**

ÍNDICE GENERAL

Contenido

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

En la actualidad las redes de datos de las empresas se vuelven cada vez más complejas y diversas, y la necesidad y exigencia de su correcta operación es cada vez más crítica para el éxito de las mismas. Con el avance de la tecnología las redes soportan mucho más aplicaciones y servicios; además, su crecimiento constante y la incorporación de nuevas tecnologías van complicando y en algunas ocasiones degradando el desempeño de la red.

Al igual que han crecido en tamaño y capacidades, las redes también han crecido en términos de su importancia para las instituciones, por lo que hoy por hoy es primordial contar con un sistema de Administración y Monitoreo de redes que nos asegure su correcto funcionamiento. Anteriormente, las redes eran simples y con pocos elementos a ser administrados, esto se debía a que no eran parte fundamental de las empresas, por lo que su administración era una tarea sencilla para sus encargados. Hoy esto ha cambiado, el tamaño y la complejidad han aumentado, por lo que la Administración y Monitoreo de las mismas se ha convertido en un factor preponderante para que se pueda mantener un adecuado funcionamiento en la misma. Ahora los administradores realizan diversas funciones como monitorear, administrar y gestionar la red, con el objetivo de saber el estado de cada uno de los equipos, y así evitar problemas que puedan afectar en el desarrollo de las actividades cotidianas de cada institución.

El correcto desempeño de la red, implica que cada uno de los elementos que intervienen en la comunicación ha de estar operativo y configurado de una determinada manera; cualquier cambio no esperado puede dar lugar a errores en la transmisión si no se detecta y corrigen sus efectos a tiempo, esto quiere decir que la red se debe monitorear en todo momento, se debe recopilar información sobre niveles de desempeño, utilización y estado operativo. Esa información se debe guardar y poner a disposición

para su análisis, para que se puedan realizar seguimientos de tendencias y se puedan generar informes, de esta manera se podrá tomar medidas correctivas o preventivas a tiempo. La administración y monitoreo de la red no puede prevenir todos los problemas, pero puede minimizar la pérdida de servicio y el impacto del tiempo que no funcione.

Las tendencias actuales apuntan a que los sistemas de administración de red pasarán, en los próximos tres a cinco años, de ser complementos en la oferta de elementos de red a constituirse en una parte esencial de ellos, siendo en algunos casos el elemento decisorio en la compra, ya que con la distribución de procesos y datos, los entornos distribuidos son más potentes y más flexibles, pero también más críticos, lo que hace que su gestión sea una pieza clave para garantizar la disponibilidad y grado de servicio requerido a la red.

CAPÍTULO I

MARCO REFERENCIAL

1.1 Problematización

El Municipio de la ciudad de Ambato cuenta con un Departamento de Informática, el cual es el encargado de la Administración de toda la Red del Municipio, además de todo lo que tiene que ver con problemas y cambios en su infraestructura tecnológica tanto hardware como software.

El Municipio de Ambato viene trabajando durante varios años brindando servicios a la ciudadanía ambateña con constante mejoría, pero aun así no cuenta con ninguna herramienta que sea capaz de realizar una Administración y Monitoreo de los equipos de Red de una manera eficaz.

Actualmente la tarea de administrar y monitorear la red del Municipio de Ambato es compleja, tanto por el número de equipos instalados como por la ubicación que

tienen los mismos, ya que en ciertos casos las distancias varían considerablemente y para los administradores de la red, llevar a cabo estas tareas se torna bastante tedioso ya que deben inspeccionar los mismos y en el peor de los casos les toca verificar personalmente cada uno de los equipos, haciendo uso de tiempo y recursos.

Hoy en día ciertamente no se puede diagnosticar los problemas y fallas y peor tomar medidas preventivas en cuanto a solucionar o controlar problemas en la red del Municipio de Ambato. Una buena opción para la administración y monitoreo de una red de datos es emplear alguna herramienta que permita realizar estas actividades de monitoreo en tiempo real, es por eso que entre las herramientas a ser objeto de análisis para llevar a cabo la presente investigación contamos con: Cacti, Zenoss y Zabbix.

La necesidad de comunicación entre otras entidades bajo la administración de IMA hace que se instalen más dispositivos y esto simultáneamente hace crecer la red del Municipio de Ambato a medida que resulta difícil poseer una administración de red eficiente.

Se pretende implantar una herramienta para administrar y Monitorear la red local de manera sencilla y segura. Se basa en la utilización de recurso de administración definido en el estándar SNMP que se encuentra disponible en la plataforma Linux y el uso de un equipo que tomará el rol de administrador/servidor. Se configura el protocolo SNMP en todos y cada uno de los dispositivos a ser administrados, además se utilizan agentes que se instalan en las máquinas administradas y recaban toda la información especificada en el estándar SNMP, para luego ser concentradas en el centro administrador, el cual las organiza y las presenta en un ambiente Web.

En general esta investigación tiene relación sobre el análisis e implantación de una herramienta OpenSource, el cual trabaja en un ambiente distribuido y que permite la organización, configuración, monitoreo, y control de los principales dispositivos de una red local, con el fin de apoyar a una administración eficiente de la red.

1.1 Justificación

En la actualidad en el Ilustre Municipio de Ambato surge la necesidad de proteger sus rede de datos, cualquier cambio no esperado en su red puede dar lugar a errores en la transmisión de datos importantes si no se detecta y corrigen sus efectos a tiempo, por lo que resulta esencial disponer de un sistema de administración y monitoreo de red adecuado a los requerimientos que demandan los usuarios.

La administración de la red del Municipio de Ambato es una actividad indispensable debido a la alta oferta tecnológica disponible actualmente. Se ha vuelto de mucha importancia la necesidad de saber el estado de cada equipo que hace parte de la red, con el objetivo de prevenir fallos en ella y así detectar los posibles efectos que pueden ocasionar a la hora de prestar cierto servicio a los usuarios y ventajosamente poder anticiparse a ellos, prepararse para buscar soluciones y reaccionar en el caso que se produzcan.

De esto se deriva la importancia de contar con una herramienta capaz de notificarnos las fallas en la red del Municipio de Ambato y de mostrarnos su comportamiento mediante el análisis y recolección de información del dispositivo.

El desarrollo del proyecto se basa principalmente en el requerimiento del Ilustre Municipio de Ambato de usar herramientas OpenSource y se sustenta en el decreto No. 1014 emitido por el presidente de la república del Ecuador Rafael Correa en donde se establece como política pública para las entidades de la administración pública central la utilización de Software Libre en sus sistemas y equipamientos informáticos.

Se conoce como Software Libre a los programas de computación que se pueden utilizar y distribuir sin restricción alguna y que permiten su acceso a los códigos y fuentes y que sus aplicaciones pueden ser mejoradas.

Los programas de computación incluyen las siguientes libertades; utilización del programa con cualquier propósito de uso común; distribución de copias sin restricción alguna; estudio y modificación del programa (requisito: código fuente disponible); y publicación del programa mejorado (requisito; código fuente disponible).

Asimismo, las entidades de la administración pública central, previa la instalación del Software Libre en sus equipos, deberán verificar la existencia de la capacidad técnica que brinde el soporte necesario para el uso de este tipo de software. Además, el decreto faculta la utilización de software propietario (no Libre), únicamente cuando no exista una solución de Software Libre que supla las necesidades requeridas, o cuando esté en riesgo la seguridad nacional, o cuando el proyecto informático se encuentre en un punto de no retorno.

El artículo 5 del Decreto, precisa que tanto para Software Libre como para software propietario, siempre y cuando satisfagan los requerimientos, se debe preferir 6 soluciones: nacionales que permitan autonomía y soberanía tecnológica; regionales con componente nacional; regionales con proveedores nacionales; internacionales con componente nacional; internacionales con proveedores nacionales; e internacionales.

Según el Decreto 1014, la Subsecretaría de Informática será el órgano regulador y ejecutor de las políticas y proyectos informáticos y realizará el control y seguimiento del decreto en mención. El uso de software libre contempla ventajas como:

- *Contar con una licencia*. Siempre será mejor usar un producto Open Source a usar uno propietario pirateado.

- Tener la fuente. Siempre podemos modificarlo y adaptarlo a nuestras necesidades. Incluso podemos reparar errores que detectemos o incluir parches realizados por otros usuarios. O modificarlo para que se ejecute en otro sistema operativo, contra otra base de datos, etc.

En este sentido, planteamos el Análisis e Implementación de Herramientas OpenSource basadas en SNMP para la Administración y Monitoreo de la red del Ilustre Municipio de Ambato, que sirva para ayudar en la supervisión y mantenimiento, entre estos, monitorear de manera constante la disponibilidad y funcionalidad de los dispositivos de red de datos con la detección oportuna de fallas, dando seguimiento a todos los eventos ocurridos en los dispositivos de red, facilitando así la resolución de problemas de forma ordenada, rápida y eficiente, ayudando a los responsables a llegar a una satisfactoria y rápida solución, garantizando la explotación eficiente de los recursos de la institución, de esta manera se logrará mejorar el servicio.

1.2 Objetivos Generales y Específicos

1.2.1 Objetivo General

Analizar las Herramientas OpenSource de Administración y Monitoreo de Redes basadas en SNMP, para determinar la mejor de acuerdo a su utilidad y eficiencia, y aplicarla en el Municipio de Ambato.

1.2.2 Objetivos Específicos

- Analizar la infraestructura de red actual con el que cuenta el Ilustre Municipio de Ambato.

- Analizar las herramientas OpenSource para la administración y monitoreo de la red, que permitan resolver las necesidades del Municipio de Ambato.
- Implantar la herramienta seleccionada para realizar la Administración y Monitoreo de la red de datos del Municipio de Ambato.
- Administrar, Monitorear y mantener funcionando con calidad la red.
- Controlar el estado de los equipos y dispositivos de red existentes en la infraestructura del Municipio de Ambato.

1.3 Hipótesis

"La implementación de una Herramienta OpenSource basado en SNMP para la Administración y Monitoreo de la red del Municipio de Ambato mejorará la gestión del administrador y la productividad de la red de datos."

1.4 Métodos y Técnicas

1.4.1 Métodos

1.4.1.1 Inductivo – Deductivo

- Sigue un proceso analítico sintético, en el cual la inducción y la deducción se complementan.
- El método inductivo es aquel que parte de lo particular a lo general, de las partes al todo.
- El método deductivo va de lo general a lo particular. Parte del concepto a los principios, definiciones o afirmaciones de las cuales se extrae conclusiones y consecuencias.

1.4.1.2 Método Comparativo

- La presente investigación no se limita al estudio de una sola herramienta sino al estudio comparativo de varias para el análisis multidimensional de datos.

1.4.1.3 Método Científico

- Permite descubrir variedades científicas. Se utilizará este método para la recolección de información y desarrollo de la investigación.

1.4.1.4 Método Experimental

- Se fundamenta en el método científico, comprueba en forma objetiva una ley o una verdad científica, enriquece la calidad de información, datos y vivencias que contribuyen a interpretar la realidad y a actuar sobre ella conscientemente.

1.4.2 Técnicas

1.4.2.1 Fuentes

Son hechos o documentos a los que accede el investigador y que le permiten obtener información que puede ser primaria o secundaria.

- Primaria: Se utilizarán las siguientes técnicas:
  - Observación
  - Entrevista
  - Encuestas
  - Lluvia de ideas
- Secundarias: Se tomará información de medios como:
  - Internet

CAPÍTULO II

MARCO TEÓRICO CONCEPTUAL DE REFERENCIA

2.1. Qué es Administración y Monitoreo de Redes.

El término Administración y Monitoreo de redes es definido como la suma total de todas las políticas y procedimientos que intervienen en la planeación, configuración, control, monitoreo de los elementos que conforman una red, con el fin de asegurar el eficiente y efectivo empleo de sus recursos. Lo cual se verá reflejado en la calidad de los servicios ofrecidos. Dicho de una manera más sencilla, es un servicio que emplea una variedad de recursos para ayudar a los administradores de la red, en la supervisión y mantenimiento de la misma.

2.1.1. ADMINISTRACIÓN

La administración de redes consiste en la organización, control, toma de precauciones y supervisión de la red, para mantener su funcionamiento eficiente, mediante el empleo de herramientas de red, aplicaciones y dispositivos.

La administración de la red se vuelve más importante y difícil si se considera que las redes actuales comprendan lo siguiente:

- Mezclas de diversas señales, como voz, datos, imagen y gráficas.
- Interconexión de varios tipos de redes, como WAN, LAN y MAN.
- El uso de múltiples medios de comunicación, como par trenzado, cable coaxial, fibra óptica, satélite, láser, infrarrojo y microondas.
- Diversos protocolos de comunicación, incluyendo TCP/IP, OSI.
- El empleo de muchos sistemas operativos, como DOS, Netware, Windows NT, UNIX, OS/2.
- Diversas arquitecturas de red, incluyendo Ethernet, Fast Ethernet, Fiber channel, Gigabit.

2.1.1.1. Tres dimensiones de la Administración de Redes.

a) Dimensión Funcional. Se refiere a la asignación de tareas de administración por medio de áreas funcionales.

b) Dimensión Temporal. Se refiere a dividir el proceso de administración en diferentes fases cíclicas, incluyendo las fases de planeación, implementación y operación.

c) Dimensión del escenario. Se refiere al resto de los escenarios adicionales al de administración de redes, como son administración de sistemas, administración de aplicaciones, etc.

2.1.1.2. Objetivos de la Administración de Redes

- Asegurar que los usuarios de una red reciben el servicio con la calidad que ellos esperan.
- Planeación estratégica y táctica de la ingeniería, operaciones y mantenimiento de una red y sus servicios.

- Ayudar al personal técnico a enfrentar las complejidades de la red y asegurar que la información se mueva a través de ella con la máxima eficiencia y transparencia para los usuarios.
- Mejorar la continuidad en la operación de la red con mecanismos adecuados de control y monitoreo, de resolución de problemas y de suministro de recursos.
- Hacer uso eficiente de la red y utilizar mejor los recursos.
- Controlar cambios y actualizaciones en la red de modo que ocasionen las menos interrupciones posibles, en el servicio a los usuarios.

2.1.1.3. Pasos básicos de la Administración de Redes

El sistema de administración de red opera bajo los siguientes pasos básicos:

1.- Colección de información acerca del estado de la red y componentes del sistema. La información recolectada de los recursos debe incluir: eventos, atributos y acciones operativas.

2.- Transformación de la información para presentarla en formatos apropiados para el entendimiento del administrador.

3.- Transportación de la información del equipo monitoreado al centro de control.

4.- Almacenamiento de los datos coleccionados en el centro de control.

5.- Análisis de parámetros para obtener conclusiones que permitan deducir rápidamente lo que pasa en la red.

6.- Actuación para generar acciones rápidas y automáticas en respuesta a una falla mayor.

La característica fundamental de un sistemas de administración de red moderno es la de ser un sistema abierto, capaz de manejar varios protocolos y lidiar con varias arquitecturas de red. Esto quiere decir: soporte para los protocolos de red más importantes.

2.1.2. MONITOREO

Es la realización del estudio del estado de los recursos. Las funciones del monitoreo de red se llevan a cabo por agentes que realizan el seguimiento y registro de la actividad de red, la detección de eventos y la comunicación de alertas.

El monitoreo de una red abarca 4 fases:

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

Los tipos de monitoreo son:

- Local.
- Remoto.
- Automático.
- Manual.

Los elementos monitoreados pueden ser:

- En su totalidad.
- En Segmentos.

El monitoreo puede ser realizado en forma:

- Continua.
- Eventual.

2.1.2.1. Objetivos del Monitoreo

- Identificar la información a monitorear.
- Diseñar mecanismos para obtener la información necesaria.
- Utilizar la información obtenida dentro de las distintas áreas funcionales de administración de red.
- Tomar nuevas medidas sobre aspectos de los protocolos, colisiones, fallas, paquetes, etc.
- Almacenar la información obtenida en Bases de Información de gestión para su posterior análisis.
- Del análisis, obtener conclusiones para resolver problemas concretos o bien para optimizar la utilización de la red.

Dentro del monitoreo de la actividad de la red, los eventos típicos que son monitoreados suelen ser:

- Ejecución de tareas como la realización de copias de seguridad.
- Registro del estado de finalización de los procesos que se ejecutan en la red.
- Registro de las entradas y salidas de los usuarios en la red.
- Registro del arranque de determinadas aplicaciones.
- Errores en el arranque de las aplicaciones, etc.

En función de la prioridad que tengan asignados los eventos y de la necesidad de intervención, se pueden utilizar diferentes métodos de notificación o alerta tales como:

- Mensajes en la consola: método en el que se suele codificar en función de su importancia.
- Mensajes por correo electrónico: mediante el cual se envía contenido el nivel de prioridad y el nombre del evento ocurrido.

- Mensajes a móviles: método utilizado cuando el evento necesita intervención inmediata del administrador de red.

2.2. Arquitectura de la Administración y Monitoreo de Redes

La mayoría de las arquitecturas para la administración de redes utilizan la misma estructura y conjuntos básicos de relaciones. Las estaciones terminales, como los sistemas de cómputo y otros dispositivos de red, utilizan un software que les permite enviar mensajes de alerta cuando se detecta algún problema. Al recibir estos mensajes de alerta las entidades de administración son programadas para reaccionar, ejecutando una o varias acciones que incluyen la notificación al administrador, el cierre del sistema, y un proceso automático para la posible reparación del sistema.

Las entidades de administración también pueden registrar la información de las estaciones terminales para verificar los valores de ciertas variables. Esta verificación puede realizarse automáticamente o ejecutada por algún administrador de red.

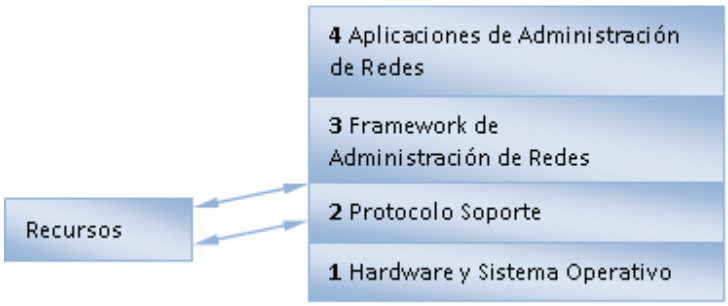


Figura II.1 : Arquitectura de la Administración de Redes
Fuente: http://www.chaco.gov.ar/UTN/AdmRedes/Traduccion/cap1.doc

1) Hardware y el sistema operativo

2) Protocolo soporte, el cual incluye:

- Capas por debajo de la capa de aplicación en OSI, UDP/IP en Internet.
- Protocolos de administración tales como SNMP, CMIP, etc.
- Conversión de diferentes protocolos y multi-protocolos que soporte protocolos heterogéneos.

3) Provee la base de varias aplicaciones de administración de redes:

- Funciones de agente y administración.
- Soporte de bases de datos tales como las bases de datos relacionales y orientadas a objetos para almacenar datos de muchas funciones de administración de redes y soporte para aplicaciones.
- Soporte para la interface de usuario.
- Funciones de administración de redes, tales como configuración y administración de fallas.

4) Provee un mercado muy amplio y que tiene un potencial alto de producir aplicaciones innovadoras tales como aplicaciones de administración de negocios, aplicaciones de fácil uso para facilitar la tarea del administrador y aplicaciones de diagnóstico de fallas.

2.3. Recursos a ser Administrados

La administración y monitoreo de redes de computadoras abarca monitoreo y control de hardware y componentes de software de redes diferentes.

2.3.1. Hardware

Estos son algunos de los componentes de hardware:

1. Conexiones físicas: incluye equipo relacionado con las capas físicas y de enlace. Los protocolos usados son FDDI, frame relay, BISDN, ATM, SONET. Además incluye switches y concentradores.

2. Componentes de Computadora: incluye dispositivos de almacenamiento, procesadores, impresoras y otros. Ethernet, Token Ring y Token Bus se consideran parte de los componentes de computadoras.
3. Componentes de interconexión y conectividad: se refiere a los componentes de hardware tales como repetidores, bridges, ruteadores, gateways, hubs y modems.
4. Hardware de telecomunicaciones: estos son modems, multiplexadores y switches.

2.3.2. Software

El software típico incluye:

1. Software del sistema operativo: DOS, Windows NT, OS/2 Warp.
2. Herramientas de software y software de aplicación: el software de aplicación hace a las computadoras más populares y productivas.
3. Software del sistema en modelo cliente servidor: NetWare servers.
4. Software de interconexión: software usado en repetidores, bridges, ruteadores, gateways, hubs y modems.
5. Software de aplicación en modelo cliente servidor: incluye servidores de base de datos, servidor de archivos y servidores de impresión.
6. Software de telecomunicaciones y comunicación de datos: software de administración relacionado a la comunicación de datos y protocolos de telecomunicación tales como FDDI, frame relay, ATM.
7. Software de telecomunicaciones backbone.

2.4. Elementos involucrados en la Administración y Monitoreo de Redes

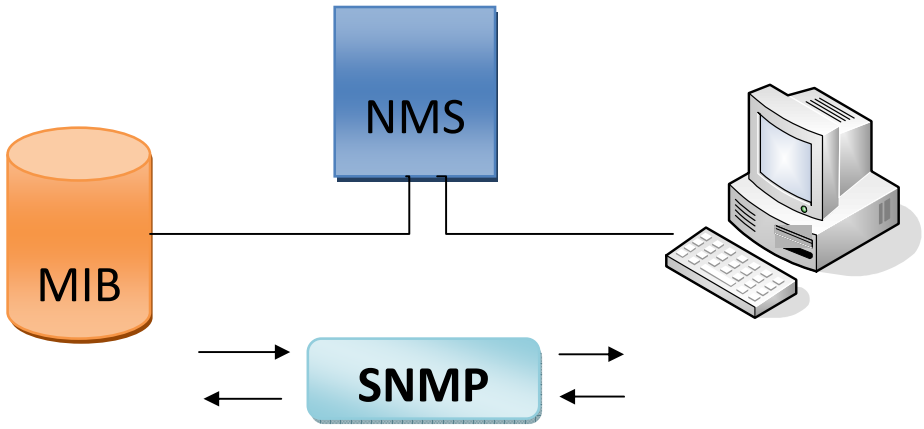


Figura II.2 : Componentes de la Administración y Monitoreo de Redes.
Fuente: http://www.scribd.com/doc/11526277/Proyecto-Monitoreo-Y-Gestion-de-la-Red-Final

2.4.1. SNMP (Protocolo Simple de Administración de Redes)

SNMP es un protocolo ubicado en la capa siete del modelo OSI, facilita la administración de los equipos en la red, permitiendo a los administradores supervisar, encontrar y resolver problemas de una manera mucho más fácil y cómoda.

El SNMP se ha convertido en un estándar de gestión de red sobresaliente y la mayoría de los equipos de interconexión (switches, routers, hubs, puentes) dispositivos de encaminamiento, estaciones de trabajo y Pcs ofrecen agentes SNMP para ser gestionados.

Se implementa fácilmente y consume un tiempo moderado del procesador y de recursos de red. Basado en paquetes UDP, es decir, es un protocolo "no orientado a la conexión". Cabe destacar que el protocolo sencillo de administración de redes (SNMP) es un protocolo de administración de red estándar utilizado en Internet.

Un posible modelo de SNMP puede ser el que a continuación se muestra, allí se administran cuatro componentes:

- Nodos de administración
- Estaciones administradas
- Información de administración
- Un protocolo de administración

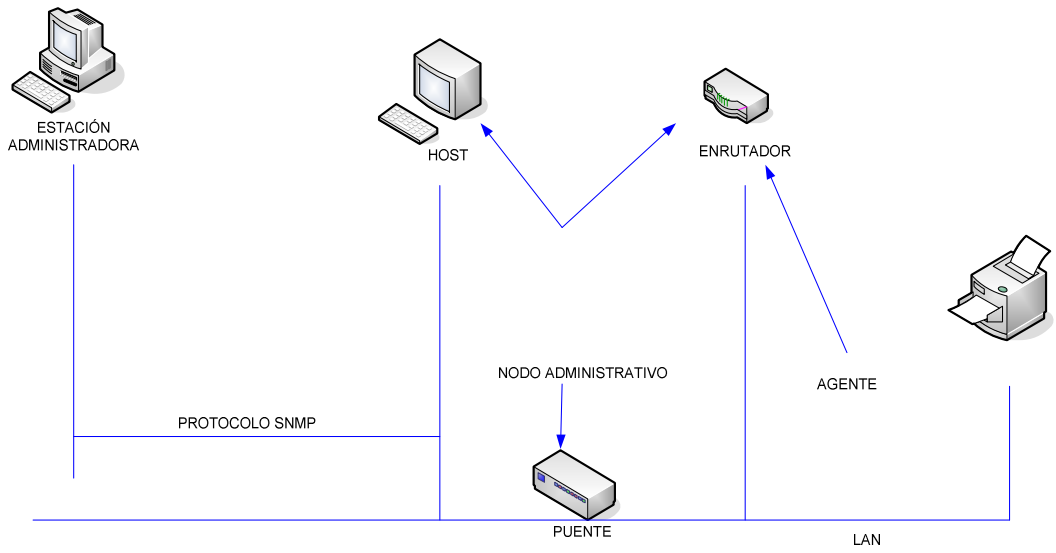


Figura II.3 : Proceso de Administración

Fuente: http://www.scribd.com/doc/8740389/Manual-Monitoreo-Uptime-en-Windows-Server- 2003

Los nodos administradores pueden ser enrutadores, host, puentes, impresoras u otros dispositivos capaces de comunicar información de estado al mundo exterior.

Cuando se hace referencia a un agente, se refiere, a aquel que mantiene una base de datos local de variables que describe su estado; comunicación entre el administrador y el agente.

Por ende, el protocolo SNMP describe la información precisa y exacta de cada tipo de agente que tiene que administrar y el formato con que este le proporciona los datos; pero lo más importante es la definición de quien tiene que llevar el registro y como se comunica la información.

Cuando nos referimos a objetos y/o al conjunto de todos los posibles objetos de una red, estos se dan en la estructura de datos llamados **MIB**, lo que hace realmente es que cada dispositivo administrado por el SNMP, mantiene una o más variables que describen su estado, y estas variables son llamadas **Objetos;** cada uno tiene un modo de acceso, solo lectura o solo escritura por que la mayor parte de los SNMP consiste en un tipo de comunicación de **Consulta-Respuesta**.

Cuando existen sucesos no planeados (las líneas pueden desactivarse y levantarse de nuevo) y ocasionan congestión en la red, cada uno de los sucesos significativos son definidos en un modulo MIB, e inmediatamente lo informa a las estaciones administradoras, llamado **Interrupción SNMP,** que indica lo ocurrido y es responsabilidad de la estación administradora, emitir consultas para informarse de los detalles.

El agente en SNMP es el equivalente a un servidor en Internet, esto quiere decir que un agente SNMP es un sistema que responde a cierta solicitud sobre el estado y condición de la red, que les hecha desde una estación cliente o estación administrativa.

Dependiendo de la aplicación que utilicemos podemos decidir que se puede monitorear por ejemplo:

- Monitorear la gestión de prestaciones (Tráfico y Retardo)
- De fallos (Cambios de Estados)
- De configuraciones (Inventario de la Red) entre otros.

El protocolo SNMP permite y da la facilidad de monitorear y administrar la red.

2.4.1.1. Arquitectura de un modelo SNMP

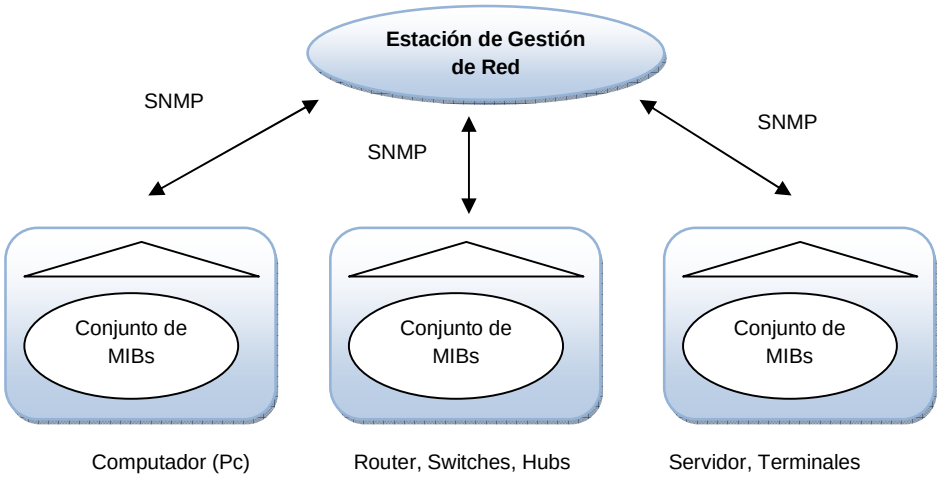


Figura II.4 : Arquitectura de un modelo SNMP

Fuente: http://redalyc.uaemex.mx/pdf/784/78430108.pdf

Este protocolo permite monitorear y controlar redes que operan bajo TCP/IP, además que permite capturar información de la red, el administrador de red puede utilizar este protocolo para diagnosticar y corregir problemas en la red utilizando un host remoto o host administrativo de red, routers, hubs, switches.

2.4.1.2. Ventajas y Desventajas de SNMP

2.4.1.2.1. Ventajas de SNMP

La ventaja fundamental de usar SNMP es que su diseño es simple por lo que su implementación es sencilla en grandes redes y la información de gestión que se necesita intercambiar ocupa pocos recursos de la red. Además, permite al usuario elegir las variables que desea monitorizar sin mas que definir:

- El título de la variable.
- El tipo de datos de la variable.
- Si la variable es de sólo lectura o también de escritura.
- El valor de la variable.

2.4.1.2.2. Desventajas de SNMP

La primera deficiencia de SNMP es que tiene grandes fallos de seguridad que pueden permitir a intrusos acceder a información que lleva la red. Todavía peor, estos intrusos pueden llegar a bloquear o deshabilitar terminales.
Para solucionar esto en versiones posteriores se han añadido mecanismos como:

- Privacidad de los datos, que los intrusos no puedan tomar información que va por la red.
- Autentificación, para prevenir que los intrusos manden información falsa por la red.
- Control de acceso, que restringe el acceso a ciertas variables a determinados usuarios que puedan hacer caer la red.

El mayor problema de SNMP es que se considera tan simple que la información está poco organizada. Esto se debe en gran parte a que SNMP se creó como un protocolo provisional y no ha sido sustituido por otro de entidad.

2.4.1.3. Versiones de SNMP

El protocolo SNMP ha ido avanzando a medida que han surgido las necesidades, principalmente de seguridad. Aunque SNMP es un protocolo flexible, extensible a gran tipo de redes, es un protocolo simple y difícil de implementar por eso fue adquiriendo avances para mejorar su funcionamiento.
Su primera versión fue:

- **SNMP v1:**

Esta versión fue muy simple y utiliza como método la autenticación basada en 'comunidades'. Se define por arquitectura, física (gestor-agente), en la aparte de seguridad introduce el cifrado con clave pública y firma digital. La forma sencilla de autenticarse en esta versión por el método de comunidades son tipos de mensaje como: get, get- next , get-response , set-request y trap no tiene ninguna seguridad implementada.

Ventajas

- Es un estándar de mercado
- Simple y fácil de usar

Desventajas

- Limitaciones en el mecanismo de la obtención de información
- Limitaciones de las capacidades de modelado de datos

- **SNMP v2:**

Esta versión contiene mejoras en cuanto a la v 1, aunque sigue utilizando comunidades ha mejorado en los tipos de datos y operaciones, pero sigue quedando corto en cuanto a seguridad.

Ventajas:

- Admite mecanismos de seguridad como la autentificación y el cifrado
- Permite la comunicación entre estaciones de gestión.

Desventajas

- Su incompatibilidad con la versión SNMP y la mayor complejidad añadida a las plataformas están desestimando su futura implementación.

- **SNMP v3**

Esta nueva versión ha estado buscando mejoras en cuanto a la seguridad aunque no se ha implementado mucho todavía se puede implementar para cualquier medio de seguridad, ofrece autenticidad e integridad utilizando claves de usuarios y mensajes con huellas digitales también ha mejorado en la privacidad al cifrar los mensajes y valida temporalmente sincronizando relojes y una ventana de 150 segundos con chequeo de secuencia

Ventajas:

- Las áreas a las que SNMPv3 va enfocado son primordialmente mejorar la seguridad y la administración respecto a SNMPv2.

Desventajas:

- Aún no es muy conocido y poco implementado.

2.4.1.4. Proceso de envió de un Mensaje SNMP

El envío de mensajes SNMP se realiza por medio del siguiente proceso:

- **Transmisión**

  Se construye UDP

  Se involucra el servicio de autenticación con la dirección de transporte.

  Se construye el mensaje SNMP

  Se codifica

- **Recepción**

  Comprobación sintáctica

  Verificación de la versión utilizada

  Autentificación, Verifica si falla

  Proceso de petición

- **Mensaje SNMP**

  Mensaje SNMP <---------->Datagrama UDP

  Disminuye el procesado de mensajes y complejidad del agente.

IMPORTANTE: *Por el puerto 161 UDP son recibidos los mensajes SNMP y los Traps por el puerto 162.*

2.4.1.5. Mensajes enviados por SNMP

Get Request: Solicita uno a mas atributos de un objeto. Es transmitido por el NMS (o nodo administrador) y recibido por el agente (o nodo administrado).

Get Next Request: Solicita el siguiente atributo de un objeto. Es transmitido por el NMS (o nodo administrador) y recibido por el agente (o nodo administrado).

Get Bulk Request: Presente en SNMP v2, solicita un amplio conjunto de valores en vez de ir solicitando uno por uno. Es transmitido por el nms (o nodo administrador) y recibido por el agente (o nodo administrado).

Set Request: Actualiza uno o varios atributos de un objeto. Es transmitido por el NMS (o nodo administrador) y recibido por el agente (o nodo administrado).

Set Next Request: Actualiza el siguiente atributo de un objeto. Es transmitido por el NMS (o nodo administrador) y recibido agente (o nodo administrado).

Get Response: Devuelve los atributos solicitados. Es transmitido por el agente (o nodo administrado) y recibido por el NMS (o nodo administrador).

Trap: informa de fallos en el agente (como perdida de la comunicación, caída de un servicio, problemas con la interfaz, etc). Es transmitido por el agente (o nodo administrado) y recibido por el NMS (o nodo administrador).

Inform Request: Describe la base local de información de gestión MIB para intercambiar información de nodos administradores entre sí. Es trasmitido por el NMS (o nodo administrador) y recibido por el agente (o nodo administrado).

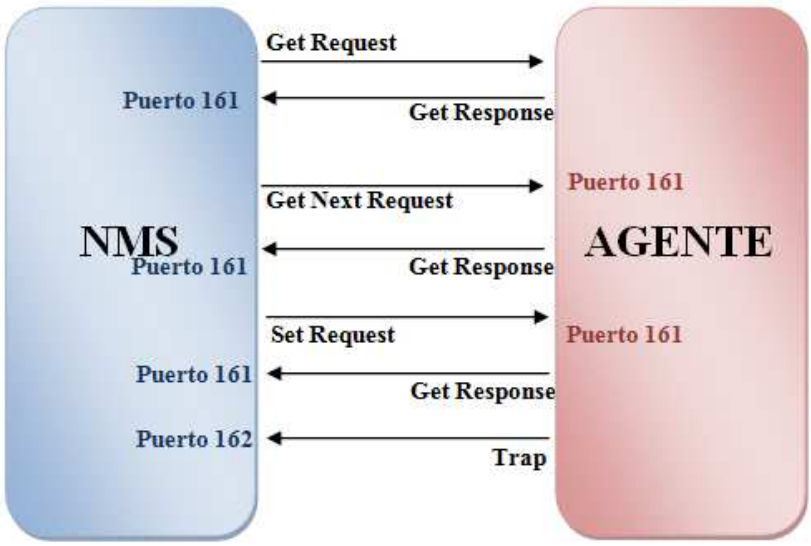


Figura II.5 : Estructura del Mensaje SNMP

Fuente: http://www.scribd.com/doc/11526277/Proyecto-Monitoreo-Y-Gestion-de-la-Red-Final

El **NMS** envía un mensaje *Get Request* solicitando el atributo de un objeto, el ***Agente*** devuelve un *Get Response* con los atributos solicitados, luego el NMS envía un *Get Next Request* solicitando el siguiente atributo del objeto, el agente a su vez responde de nuevo con un *Get Response,* el NMS envía un *Set Request* para actualizar los atributos de un objeto, el agente le envía un *Get Response*.

2.4.2. MIB

Es una base de datos de objetos administrados que son accesibles por el agente y manipulados vía SNMP para lograr la administración de la red, es una información jerárquica estructurada en forma de árbol de todos los dispositivos gestionados en una red.

2.4.2.1. Estructura de una MIB

Los objetos que se guardan en las MIB tienen un identificador único. Este identificador de objetos se llama **(OID)** es una secuencia de números enteros no son negativos y están separados por puntos que sale de un árbol estandarizado mundialmente conformado por ramas y nodos.

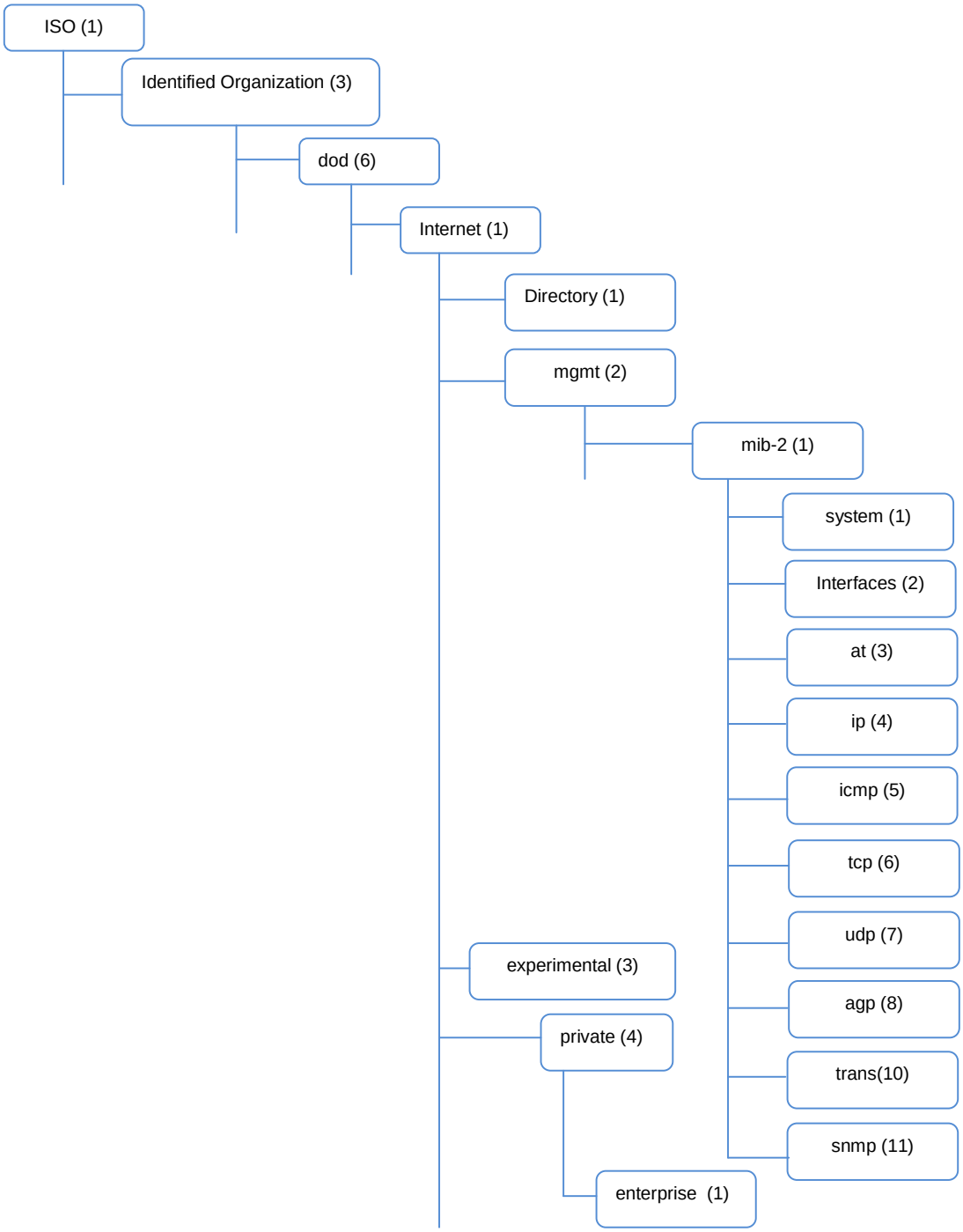


Figura II.6 : Estructura de una MIB

Fuente: http://www.scribd.com/doc/11526277/Proyecto-Monitoreo-Y-Gestion-de-la-Red-Final

Tienen 8 niveles de registro que son:

GRUPO	VARIABLE	SIGNIFICADO
System (sys)	sysUpTime	Tiempo desde el último arranque.
Interfaces (intf)	ifNumber	Número de Interfaces.
Interfaces (intf)	ifInErrors	Número de paquetes entrantes en los que el agente ha encontrado error.
Addess Traslation (add trs)		Número de paquetes recibidos.
Internet Protocol (ip)	ipInReceives	
Internet Control Message (icmp)	icmpInEchos	Número de solicitudes ICMP recibidas.
Transmision Control Protocol (tcp)	tcpInSegs	Número de paquetes TCP recibidos
User Datagram Protocol (udp)	udpInDatagrams	Número de datagramas UDP recibidos.

Tabla II.I: Niveles de registro de una MIB

Fuente: http://www.scribd.com/doc/11526277/Proyecto-Monitoreo-Y-Gestion-de-la-Red-Final

Las **MIB** están escritas utilizando la sintaxis **ASN.1.** Esta es utilizada para descubrir estructuras de datos que se definen para guardar la información de gestión. Luego que definimos las estructuras se debe definir la sintaxis de transferencia, para saber la forma en la que van hacer transmitidos los datos en la red; a esto se le conoce como las reglas de codificación básicas **(BER)**. Es la codificación utilizada para la transmisión de información escrita en sintaxis ASN.1 a otras aplicaciones mediante una sintaxis que define y permite definir el formato de cómo se van a enviar los datos.

En el ASN.1 se definen tres tipos de objetos:

1. **Tipos (Types)**---->define nuevas estructuras de datos y comienzan en mayúsculas.
2. **Valores (Values)**----->son variables de un tipi y se escriben en minúsculas.
3. **Macros**---->usados para cambiar la gramática y son escritas en mayúsculas.

2.4.3. Sistema de Gestión de Red (SGR, en inglés Network Management System o NMS)

Es un programa encontrado en una estación de trabajo, tiene la habilidad de buscar los agentes usando SNMP, es el sistema empleado para controlar y monitorizar la actividad de los componentes de la red, mediante SNMP. El término SGR se puede aplicar a un dispositivo dedicado empleado para la gestión de red, o bien a la aplicación que se ejecuta en dicho dispositivo. Existen una gran variedad de aplicaciones de gestión disponibles para usar con SNMP, que van desde sencillas aplicaciones de línea de comandos (como por ejemplo, el paquete NET-SNMP para sistemas Unix) hasta sofisticadas y potentes aplicaciones con interfaces de usuario gráficos.

2.4.4. AGENTE SNMP

Es el componente de software dentro del dispositivo gestionado que mantiene los datos del mismo e informa a los gestores acerca de ellos, cuando haga falta.

2.5. Operaciones de la Administración y Monitoreo de Redes

Las operaciones principales de un sistema de administración y monitoreo de red son las siguientes:

Administración de fallas.

Maneja las condiciones de error en todos los componentes de la red, en las siguientes fases:

a) Detección de fallas.
b) Diagnóstico del problema.
c) Darle la vuelta al problema y recuperación.
d) Resolución.
e) Seguimiento y control.

Control de fallas.

*T*iene que ver con la configuración de la red (incluye dar de alta, baja y reconfigurar la red) y con el monitoreo continuo de todos sus elementos.

Administración de cambios.

Comprende la planeación, la programación de eventos e instalación.

Administración del comportamiento.

Tiene como objetivo asegurar el funcionamiento óptimo de la red, lo que incluye: El número de paquetes que se transmiten por segundo, tiempos pequeños de respuesta y disponibilidad de la red.

Servicios de contabilidad.

Provee datos concernientes al cargo por uso de la red. Entre los datos proporcionados están los siguientes:

- Tiempo de conexión y terminación.
- Número de mensajes transmitidos y recibidos.
- Nombre del punto de acceso al servicio.
- Razón por la que terminó la conexión.

Control de Inventarios.

Se debe llevar un registro de los nuevos componentes que se incorporen a la red, de los movimientos que se hagan y de los cambios que se lleven a cabo.

Seguridad.

La estructura administrativa de la red debe proveer mecanismos de seguridad apropiados para lo siguiente:

- Identificación y autentificación del usuario, una clave de acceso y un password.
- Autorización de acceso a los recursos, es decir, solo personal autorizado.
- Confidencialidad. Para asegurar la confidencialidad en el medio de comunicación y en los medios de almacenamiento, se utilizan medios de criptografía, tanto simétrica como asimétrica.

2.6. Enfoques de Administración y Monitoreo de Redes

Existen, al menos, dos puntos de vista para abordar el proceso de monitorear una red: el enfoque activo y el enfoque pasivo. Aunque son diferentes ambos se complementan.

2.6.1. Enfoque Activo

Este tipo de monitoreo se realiza inyectando paquetes de prueba en la red, o enviando paquetes a determinadas aplicaciones midiendo sus tiempos de respuesta. Este enfoque tiene la característica de agregar tráfico en la red. Es utilizado para medir el rendimiento en una red.

2.6.1.1. Técnicas de monitoreo activo.

- *Basado en ICMP*
  - Diagnosticar problemas en la red
  - Detectar retardo, pérdida de paquetes.
  - RTT
  - Disponibilidad de host y redes.

- *Basado en TCP*
  - Tasa de transferencia
  - Diagnosticar problemas a nivel aplicación

- *Basado en UDP*
  - Pérdida de paquetes en un sentido (one-way)
  - RTT (traceroute)

2.6.2. Enfoque Pasivo

Este enfoque se basa en la obtención de datos a partir de recolectar y analizar el tráfico que circula por la red. Se emplean diversos dispositivos como *sniffers*, ruteadores, computadoras con software de análisis de tráfico y en general dispositivos con soporte para snmp, rmon y netflow.
Este enfoque no agrega tráfico en la red como lo hace el activo. Es utilizado para caracterizar el tráfico en la red y para contabilizar su uso.

2.6.2.1. Técnicas de monitoreo pasivo.

- **Solicitudes remotas**

  Mediante SNMP

  Esta técnica es utilizada para obtener estadísticas sobre la utilización de ancho de banda en los dispositivos de red, para ello se requiere tener acceso

a dichos dispositivos. Al mismo tiempo, este protocolo genera paquetes llamados *traps* que indican que un evento inusual se ha producido.

Otros métodos de acceso

Se pueden realizar scripts que tengan acceso a dispositivos remotos para obtener información importante para monitorear. En esta técnica se pueden emplear módulos de perl, ssh con autenticación de llave pública, etc.

- **Captura de tráfico**

  Se puede llevar a cabo de dos formas:

  1) Mediante la configuración de un puerto espejo en un dispositivo de red, el cual hará una copia del tráfico que se recibe en un puerto hacia otro donde estará conectado el equipo que realizará la captura; y

  2) Mediante la instalación de un dispositivo intermedio que capture el tráfico, el cual puede ser una computadora con el software de captura o un dispositivo extra. Esta técnica es utilizada para contabilizar el tráfico que circula por la red.

- **Análisis de Tráfico**

  Se utiliza para caracterizar el tráfico de la red, es decir, para identificar el tipo de aplicaciones que son más utilizadas. Se puede implementar haciendo uso de dispositivo *probe* que envíen información mediante RMON o a través de un dispositivo intermedio con una aplicación capaz de clasificar el tráfico por aplicación, direcciones IP origen y destino, puertos origen y destino, etc.

- **Flujos**

  También utilizado para identificar el tipo de tráfico utilizado en la red. Un flujo es un conjunto de paquetes con

  - La misma IP origen y destino

- El mismo puerto TCP origen y destino
- El mismo tipo de aplicación.

Los flujos pueden ser obtenidos de ruteadores o mediante dispositivos que sean capaces de capturar tráfico y transformarlo en flujos. También es usado para tareas de facturación (billing).

2.7. Estrategias de Administración y Monitoreo de Redes

Antes de implementar un esquema de monitoreo se deben tomar en cuenta los elementos que se van a monitorear así como las herramientas que se utilizarán para esta tarea.

2.7.1. ¿Qué monitorear?

Una consideración muy importante es delimitar el espectro sobre el cual se va a trabajar. Existen muchos aspectos que pueden ser monitoreados, los más comunes son los siguientes:

- Utilización de ancho de banda
- Consumo de CPU
- Consumo de memoria
- Estado Físico de las conexiones
- Tipo de tráfico
- Alarmas
- Servicios (Web, correo, base de datos)

Es importante definir el alcance de los dispositivos que van a ser monitoreado, puede ser muy amplio y se puede dividir de la siguiente forma.

- Dispositivos de Interconexión
  - Ruteadores, switches, hubs, firewall

- Servidores
  - Web, Mail, DB
- Red de Administración
  - Monitoreo, Logs, Configuración.

2.7.2. Métricas

La definición de métricas permitirá establecer patrones de comportamiento para los dispositivos que serán monitoreados. También hay diversos tipos de métricas que pueden ser declarados, dependerán de las necesidades particulares de cada red. Las métricas deben ser congruentes con los objetos a monitorear. Algunos ejemplos son:

- Métricas de tráfico de entrada y salida
- Métricas de utilización de procesador y memoria
- Métrica de estado de las interfaces
- Métrica de conexiones lógicas

A cada métrica se le asigna un valor promedio, el cual identifica su patrón de comportamiento.

2.7.3. Alarmas

Las alarmas son consideradas como eventos con comportamiento inusual. Las alarmas más comunes son las que reportan cuando el estado operacional de un dispositivo o servicio cambia.

Existen otros tipos de alarmas basado en patrones previamente definidos en las métricas definidas, son valores máximos conocidos como umbrales o *threshold.* Cuando estos patrones son superados se produce una alarma, ya que es considerado como un comportamiento fuera del patrón. Algunos tipos de alarmas son:

- Alarmas de procesamiento
- Alarmas de conectividad
- Alarmas ambientales
- Alarmas de utilización
- Alarmas de disponibilidad (estado operacional)

2.7.4. Elección De Herramientas

Existe un gran número de herramientas para resolver el problema del monitoreo de una red. Hoy en día las hay tanto comerciales como basadas en software libre. La elección depende de varios factores, tanto humanos, económicos como de infraestructura:

a) El perfil de los administradores, sus conocimientos en determinados sistemas operativos;

b) Los recursos económicos disponibles

c) El equipo de cómputo disponible.

2.8. ¿Cómo escoger una herramienta de Administración y Monitoreo de Red?

Características a tomar en cuenta al escoger un sistema de administración y monitoreo de red:

- **Interfaz simple:**
  Todo lo que se necesita debe ser accesible fácilmente. No debe haber necesidad de monitorizar varias ventanas o aplicaciones. Lo ideal sería buscar un sistema de gestión de red con interfaz web personalizable, con posibilidad de manejar interfaces personalizadas para cada administrador.

- **Establecer líneas base:**

  Para poder reportar errores y eventos relativos a seguridad el sistema de gestión de red debe permitir establecer una línea base la cual le permita reconocer el normal funcionamiento de la red. La habilidad de distinguir entre un funcionamiento normal o anormal de la red reduce los reportes falso positivos, evitando muchas molestias al administrador de red.

- **Reportes útiles:**

  No es cuestión de simplemente reportar los eventos acontecidos en la red, sino también brindarnos herramientas útiles para actuar ante esta información brindada, la misma ventana debería mostrar la información y la herramienta para lidiar con ella.

- **Auto descubrimiento:**

  La herramienta descubre computadores y componentes en la infraestructura tecnológica sin necesidad de ser ingresado por una persona. Esta se encarga de enviar paquetes a varios dispositivos en la red identificándolos de esta forma. Ciertos sistemas cuentan adicionalmente con un sistema de visualización en forma de mapas, incluso georeferenciados, permitiendo la importación o exportación de la información en diferentes formatos.

- **Importación de configuración y análisis:**

  La configuración y optimización de una red puede tomar cientos de horas, y un error en la misma puede hacerte perder todo el trabajo previo. El poseer una herramienta de importación y análisis nos permite integrar configuraciones preexistentes y políticas de dispositivos de red. Adicionalmente esto permite retornar la configuración a su estado original.

- **Auditoría basada en políticas:**

  El proceso de auditoría confirma periódicamente que la configuración desplegada cumple con los estándares configurados para la red.

Adicionalmente detecta errores e inconsistencias en la red. Una habilidad muy deseable es la capacidad de enviar alertas a través de correos electrónicos o telefonía móvil.

- **Recolección de información en tiempo real e informe de los mismos:**
  La habilidad de colectar continuamente información y reportarla en tiempo real es esencial para mantener una red saludable. Una monitorización proactiva de la red nos permite reconocer problemas de desempeño en la misma y resolverlos antes de convertir a la red inoperable, de la misma manera se pueden determinar las posibles fuentes de problemas futuros en la red.

- **Soporte:**
  Es necesario contar con un soporte adecuado de la herramienta a utilizar, en nuestro caso al ser software libre, se debe contar con un buen grupo de usuarios con los cuales sea factible intercambiar información ya sea mediante foros o wikis.

- **Madurez de la herramienta:**
  Si nuestra intención es utilizar la herramienta en un ambiente de producción lo ideal es que se cuente con una herramienta probada y con la menor cantidad posible de fallos o bugs, usualmente una herramienta con un alto número de usuarios es una herramienta bastante depurada (al menos en lo que tiene que ver con el software libre).

- **Documentación:**
  Es imprescindible contar con una herramienta bien documentada, que brinde al usuario novel y al experto toda la información necesaria que lo lleve desde la obtención de paquetes y posterior instalación, hasta la configuración y puesta a punto del sistema, con información de errores más usuales y posibles problemas planteados.

2.9. HERRAMIENTAS OPENSOURCE PARA LA ADMINISTRACIÓN Y MONITOREO DE REDES BASADO EN SNMP.

Existe un gran número de herramientas de monitoreo en el mercado, las cuales se diferencian en distintos aspectos. En dependencia de los objetivos que se persigan una u otra herramienta podrá resultar más idónea en correspondencia con su funcionamiento y las preferencias de los administradores.

2.9.1. CACTI

Cacti es una solución completa para la monitorización de redes mediante gráficos y recopilación de datos, todo ello gracias a la potencia de RRDTool‘s. Podremos tener información prácticamente a tiempo real sobre nuestros routers, switches o servidores, tráfico de interfaces, cargas, cpu, temperaturas, etc.

Este sistema de monitorización, contiene un recolector de datos excelente, un sistema avanzado de creación de plantillas y gráficos y una completa interfaz de gestión de usuarios. Su instalación no es realmente compleja, lo que lo hace uno de los sistemas más completos y además, OpenSource del momento.

La aplicación está construida en PHP, y utiliza MySql para el almacenamiento de información sobre los gráficos y datos recogidos. El protocolo utilizado para la comunicación con los distintos equipos es SNMP.

Tiene una interfaz de usuario fácil de usar, que resulta conveniente para instalaciones del tamaño de una LAN, así como también para redes complejas con cientos de dispositivos. Es un potente software con el que podremos controlar en todo momento el estado de nuestra red. Cacti es un programa publicado bajo la licencia GNU GPL.

2.9.1.1. RRDTool

RRDTool es el acrónimo de Round Robin Database tool, se trata de una herramienta que trabaja con una BD que maneja Planificación Round-Robin. Esta técnica trabaja con una cantidad fija de datos y un puntero al elemento actual. El modo en que trabaja una base de datos utilizando Round Robin es el siguiente; se trata la BD como si fuera un círculo, sobrescribiendo los datos almacenados, una vez alcanzada la capacidad de la BD. La capacidad de la BD depende de la cantidad de información como historial que se quiera conservar.

2.9.1.1.1. Tipo de datos que pueden ser almacenados en una RRD

Se puede almacenar cualquier tipo de datos, siempre que se trate de una serie temporal de datos. Esto significa que se tiene que poder realizar medidas en algunos puntos de tiempo y proveer esta información a la RRDTool para que la almacene.

Un concepto ligado a las RRDtool es el de SNMP, acrónimo de Simple Network Management Protocol. Este protocolo puede ser usado para realizar consultas a dispositivos acerca del valor de los contadores que

ellos tienen (ej: una impresora). El valor obtenido de esos contadores es el que queremos guardar en la RRD.

2.9.1.1.2. Uso de RRDtool

Con esta herramienta a través de Cacti se puede representar gráficamente los datos almacenados en la RRD: uso de conexión a internet, datos como temperatura, velocidad, voltaje, número de impresiones, etc. La RRD va a ser utilizada para almacenar y procesar datos recolectados vía SNMP.

En definitiva, para hacer uso de una RRDtool, lo que se necesita es un sensor para medir los datos y poder alimentar al RRDtool con esos datos. Entonces, la RRDtool crea una base de datos, almacena los datos en ella, recupera estos datos y basándose en ellos, Cacti crea gráficos en formato PNG.

2.9.1.2. Características de CACTI

Cacti cuenta con las siguientes características:

- ***Fuente de datos***

Para manejar la recopilación de datos, se le puede pasar a Cacti la ruta a cualquier script o comando junto con cualquier dato que el usuario necesitare ingresar; Cacti reunirá estos datos, introduciendo este trabajo en el cron (para el caso de un sistema operativo Linux) y cargará los datos en la BD MySQL y los archivos de Planificación Round-robin que deba actualizar.

Una fuente de datos también puede ser creada. Por ejemplo, si se quisiera graficar los tiempos de ping de un host, se podría crear una fuente de datos, utilizando un script que haga ping a un host y devuelva el valor en mili segundos.

Después de definir opciones para la RRDtool, como ser la forma de almacenar los datos, uno puede definir cualquier información adicional que la fuente de entrada de datos requiera, como ser en este caso, la IP del host al cual hacer el ping. Luego que una fuente de datos es creada, es automáticamente mantenida cada 5 minutos.

- ***Gráficos***

Una vez que una o más fuentes de datos son definidas, una grafica de RRDtool puede ser creada usando los datos obtenidos. Cacti permite crear prácticamente cualquier gráfica, utilizando todos los estándares de tipos de gráficas de RRDtool y funciones de consolidación. No sólo se puede crear gráficos basados en la RRDtool, sino que también hay varias formas de mostrarlas. Junto con una "lista de vistas" estándar y una "vista preliminar", también existe una "vista en árbol", la cual permite colocar gráficos un árbol jerárquico, para propósitos organizacionales.

- ***Manejo de Usuarios***

Dadas las muchas funciones que ofrece Cacti, la herramienta cuenta con la funcionalidad de manejo de usuarios embebida, para así hacer posible agregar un usuario y darle permisos a ciertas áreas de Cacti. Esto permite tener usuarios que puedan cambiar parámetros de un gráfico, mientras que otros sólo pueden ver los gráficos. Asimismo, cada usuario mantiene su propia configuración de vista de gráficos.

- ***Plantillas***

Cacti puede escalar a un gran número de fuentes de datos y gráficos a través de plantillas. Esto permite la creación de una única plantilla de gráficos o fuente de datos, la cual define cualquier gráfico o fuente de datos asociada con esta plantilla. Las plantillas de hosts permiten definir las capacidades de un host, así Cacti puede utilizar esta información a la hora de agregar un nuevo host.

2.9.1.3. Requisitos Software

Para la instalación de Cacti se debe tener algunas aplicaciones ya funcionando, aunque en algunos casos Cacti instala dichas aplicaciones, estos requerimientos son los que se muestran a continuación:

- RRDTool 1.0.49 o 1.2.x o superior
- MySQL 4.1.x o 5.x o superior
- PHP 4.3.6 o superior, 5.x más recomendable para funciones avanzadas
- Un Servidor Web ejemplo. Apache o IIS

2.9.1.4. Principios de Funcionamiento

El funcionamiento Cacti puede ser dividido en tres tareas diferentes:

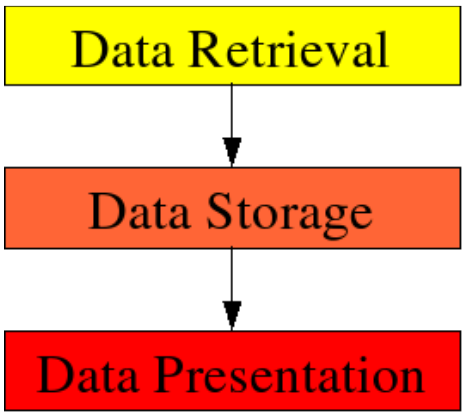


Figura II.7 : Principios de funcionamiento de CACTI
Fuente: http://www.cacti.net/downloads/docs/pdf/manual.pdf

2.9.1.4.1. Data Retrieval - Recuperación de Datos

La primera tarea es de recuperar datos. Cacti hará así la utilización de su Poller. El Poller es ejecutado del planificador del sistema operativo, p.ej. crontab para OSES Unix condimentado.

En las instalaciones actuales de TI, que está tratando con una gran cantidad de dispositivos de diferentes tipos, por ejemplo, servidores, equipos de red, aplicaciones, etc. Para recuperar los datos de objetivos a distancia / hosts, cactus, principalmente utilizará el Simple Network Management Protocol SNMP. Por lo tanto, todos los dispositivos capaces de utilizar SNMP tendrán derecho a ser controlado por Cacti.

2.9.1.4.2. Data Storage - Almacenamiento de datos

Hay muchos enfoques diferentes para esta tarea. Algunos pueden utilizar una base de datos (SQL), archivos de otros planos. Cacti utiliza RRDtool para almacenar datos.

RRDtool realizará algunas tareas específicas. Se lleva a cabo la consolidación de combinar los datos en bruto (un punto de datos primaria en la jerga de rrdtool) a los datos consolidados (un punto de datos consolidados). De esta manera, los datos históricos se comprimen para ahorrar espacio. RRDTool sabe diferentes funciones de consolidación: promedio, máximo, mínimo y ultimo.

2.9.1.4.3. Data Presentation - Presentación de Datos

Una de las características más apreciadas de RRDtool es la función integrada de gráficos. Esto viene útil cuando se combina esto con algún

servidor web de uso común. Tal, es posible acceder a los gráficos desde cualquier navegador en cualquier Plataforma.

La representación gráfica se puede hacer de maneras muy diferentes. Es posible, a un gráfico o muchos elementos en un gráfico con leyendas que denota características como mínimo, el máximo promedio, y mucho más.

2.9.1.5. Arquitectura de CACTI

Básicamente Cacti consta de los siguientes elementos:

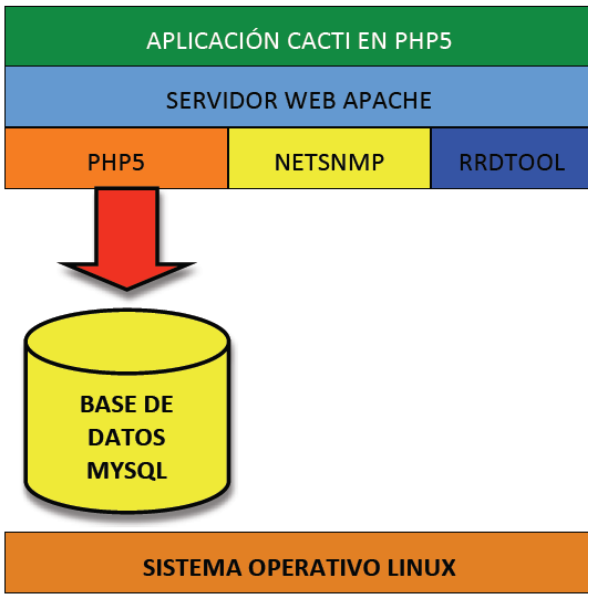


Figura II.8 : Arquitectura de Cacti sobre Linux

Fuente: http://www.scribd.com/doc/30455122/Procedimiento-Para-La-Instalacion-de-Cacti

2.9.2. ZENOSS

Zenoss es una aplicación de monitoreo de código abierto, es una plataforma para la gestión de red y servidores basada en el servidor de aplicaciones Zope. Liberado bajo la Licencia Pública General de GNU (GPL) versión 2, Zenoss Core provee una interfaz web que permite a los administradores de sistemas, monitorear la disponibilidad, inventario/configuración, desempeño y eventos. Erik Dahl comenzó el desarrollo de Zenoss en el 2002 y en agosto del 2005 fundó Zenoss, Inc., con Bill Karpovich. Zenoss, Inc. patrocina el desarrollo de Zenoss Core y vende una versión empresarial basada en la versión básica.

Sus principales funciones son dejar a la vista la configuración de red, la supervisión de la actividad de red, la gestión de la ocurrencia de eventos y la alarma. De forma automática, Zenoss permite visualizar las relaciones entre cada elemento de la red. Entre los protocolos utilizados, se encuentran SNMP, WMI y Telnet/SSH. Cada técnica de modelado produce una diversa riqueza de la información en el modelo. SNMP a menudo proporciona la más completa información del modelo, y SSH/Telnet se suele utilizar para aumentar el modelado cuando un agente SNMP no da una información crítica sobre alguna pieza específica. Los datos se registran en una base de datos exportable a XML, y el seguimiento de la actividad de la red se hace a través de tests SCMP y TCP programados.

La administración de Zenoss se realiza desde una interface web lo que simplifica la tarea a personas novatas en la aplicación y posibilita la configuración de la herramienta prácticamente sin la necesidad de modificar archivos de configuración.

Zenoss nos permite realizar monitoreo de sistemas operativos Windows y Linux prácticamente sin la necesidad de instalar agentes en los sistemas operativos. Es la herramienta de monitorización elegida por earthweb como uno de los diez proyectos más innovadores de software libre.

La aplicación y todas sus características están preparadas para funcionar bajo un entorno de software libre, como son las distribuciones Linux, pero también trabaja en plataformas Unix y sistemas Mac. Mención aparte sobre Windows; aunque Zenoss no fue diseñado para trabajar en el, es totalmente compatible y utilizable en este sistema.

La implementación en Windows es posible gracias a la simulación que ofrece la aplicación VMplayer, que permite hacer funcionar Zenoss con todas sus características en los sistemas operativos de Microsoft.

2.9.2.1. Tecnología

Zenoss combina programación original y varios proyectos de código abierto para integrar el almacenamiento de datos vía web con una interfaz de usuario basada en:

- ***Zope:*** Servidor de aplicaciones orientadas a objetos, para la construcción de sistemas de gestión de contenidos, intranets, portales y aplicaciones personalizadas, trabajado en la web escrito en Python.
- ***Python:*** extensible lenguaje de programación.
- ***Twisted:*** herramienta para interconexión de redes dirigida por eventos escrito en Python.
- ***NetSNMP***: protocolo de monitoreo que recolecta información sobre la situación de los sistemas.
- ***RRDtool:*** grafica y guarda registros de series temporales de datos.
- ***MySQL:*** Una base de datos de código abierto.

2.9.2.2. Características

Usando la tecnología de agentes, Zenoss monitorea toda la infraestructura de TI, incluyendo la red, servidores, e incluso aplicaciones. En su nivel más alto, el sistema se compone de estas áreas principales:

- Descubrimiento y configuración
- Rendimiento y disponibilidad
- Falla y gestión de eventos
- Alerta y remediación
- Generación de informes

Zenoss unifica estas áreas en un solo sistema con una interfaz moderna e interactiva de usuario Web.

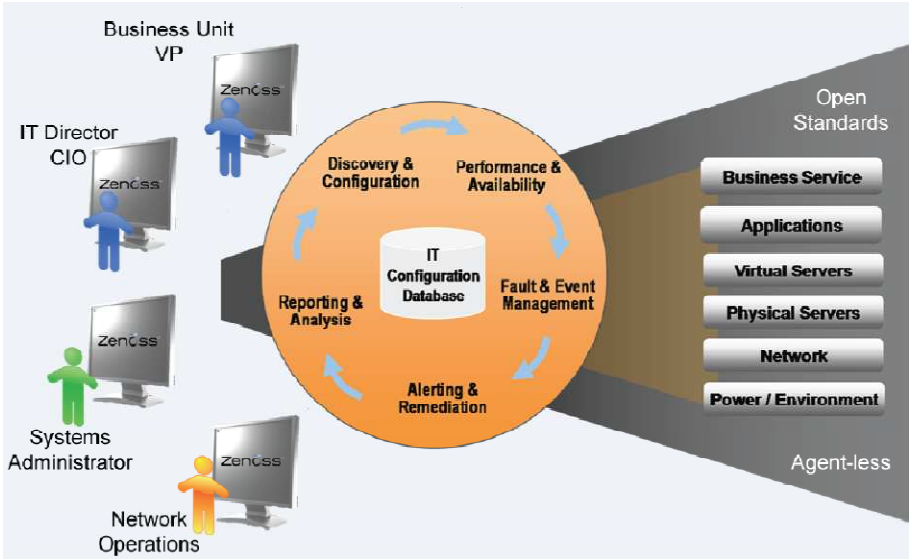


Figura II.9 : Vista de alto nivel Zenoss

Fuente: http://ufpr.dl.sourceforge.net/project/zenoss/Documentation/zenoss-3.0.x-docs/zendocs3.0.3/Zenoss_Administration_06-102010-3.0-v03.pdf

Sus principales características son:

- ***Tablero de control web:*** el dashboard web de Zenoss es customizable por el usuario final y provee vistas basadas en geografías, dispositivos y servidores e incluso aplicaciones de negocio.

- ***Administración y monitoreo de eventos:*** Mantener la disponibilidad y performance de su red. Obtener información de logs y eventos de diferentes fuentes como syslog, traps SNMP y el event log de Windows.

- ***Monitoreo de performance:*** las capacidades de colección, análisis y de gráficos de Zenoss permiten monitorear el estado de salud de la red.

- ***Reportes y alertas:*** Zenoss provee visibilidad de la disponibilidad y monitoreo de performance, administración de cambios y de configuración e incluso información de administración de información de eventos.

- ***Remediación automática:*** cuando ocurre un problema, Zenoss puede actuar tomando acciones correctivas basadas en reglas y políticas.

- ***Visualización de la red:*** a medida que su red crece Zenoss incluye mapeo de dependencias, visualización de topologías de red de capa 3 y la posibilidad de integrarse con Google Maps.

- ***Reportes comunitarios:*** le permiten a los usuarios finales generar sus propios reportes en el momento en que lo necesiten dentro de los cuales podemos encontrar reportes históricos o en tiempo real de dispositivos, eventos, performance, usuarios y mucho más.

- ***Monitores comunitarios:*** la encapsulación provista por Zenoss permite reutilizar configuraciones preexistentes.

Todas estas funciones se realizan por medio de SNMP o WMI para los sistemas Windows.

2.9.2.3. Versiones

Zenoss se ofrece en tres tipos de producto:

- ***Zenoss Core.-*** es la versión libre y gratis que se puede descargar y utilizar.
- ***Zenoss Professional.-*** versión comercial
- ***Zenoss Enterprise.-*** versión comercial

Figura II.10 : Versiones Zenoss

Fuente: http://www.scribd.com/doc/8756072/Manual-de-Monitoreo-de-Zennos

Las dos últimas son versiones comerciales, que se distinguen por ofrecer un soporte más profesional y algunas herramientas adicionales, no indispensables.

La versión Core, es la disponible y elaborada por la comunidad, solo que en esta version se le deben integrar los ZenPacks necesarios (viene listo para SNMP y SSH básico, se debe instalar el soporte para monitoreo WMI).

2.9.2.3.1. Zenoss Core

Es la versión disponible y elaborada por la comunidad, es una herramienta de monitorización premiada, que gestiona efectivamente la configuración, salud y desempeño de las redes, servidores y aplicaciones, a través de un único paquete integrado. Es una tecnología de código abierto de vigilancia y gestión de software.

2.9.2.3.1.1. Características

Las características que Zenoss Core ofrece**,** se demuestran en la potencia de sus módulos, el soporte brindado por parte de los propios usuarios y por el grado de usabilidad que demuestra frente a otras aplicaciones similares. Es muy configurable, y está diseñado para realizar una eficiente administración centralizada, de todas las herramientas tecnológicas de la empresa.

- Vigilancia de la disponibilidad de dispositivos de red mediante SNMP.
- Seguimiento de los servicios de red (HTTP, POP3, NNTP, SNMP, FTP).
- Seguimiento de acogida de los recursos (procesos, el uso de disco) en la mayoría de los sistemas operativos de red.
- Series cronológicas de la supervisión de la ejecución de los dispositivos.

- Descubrir automáticamente los recursos de la red y los cambios en la configuración de la red.
- Sistema de alerta basado en las notificaciones de conjuntos de reglas y de atención continúa.

Zenoss Core al ser un software OpenSource, existe una comunidad que aporta con packs de monitoreo, llamados ZenPacks, pueden añadir reglas de acción, clases de evento, evento comandos, comandos del usuario, las clases de servicios, fuentes de datos, gráficos, plantillas de resultados, informes, Modelo del producto extensiones o Definiciones, agregan soporte para más dispositivos, características nuevas o mejoras en performance a dispositivos ya soportados. Los ZenPack también pueden añadir nuevos demonios de la interfaz de usuario y nuevas características como los menús. Extiende y modifica Zenoss puede ser tan simple como añadir nuevas clases de dispositivos o la ejecución de plantillas o tan compleja como la que se prorroga el modelo de datos y proporcionar nueva colección demonios.

Una característica realmente interesante es la funcionalidad de Thresholds predictivos que lo acerca a su rival BMC Proactive Net, funcionalidad que permite manejar umbrales dinámicos (permite manejar valores distintos de acuerdo a la realidad de nuestra organización, por ejemplo para un banco el día 30 sus servidores reciben una mayor carga pero eso es un comportamiento normal por lo que no es necesario alertar, pero si el mismo comportamiento ocurre un día 10 entonces si estamos frente a un problema. Esto no lo permite hacer BMC Performance Manager Portal ni Nagios).

Otra característica importante es el soporte para monitoreo de infraestructura de servidores virtuales VMware ESX 4 (vSphere) ya que está acreditado por Vmware.

Una de las grandes herramientas de Zenoss es el Dashboard Configuration. Esta herramienta permite identificar a cada uno de los equipos, recursos y dispositivos tecnológicos de la organización. Provee de datos de ubicación, hora de conexión, entre otros de suma importancia. Las posibilidades de esto son impresionantes.

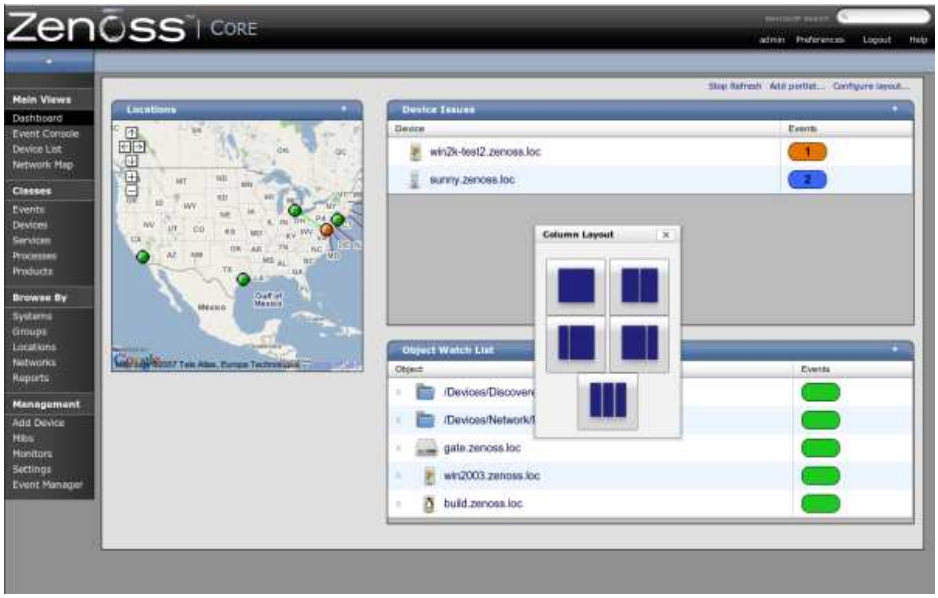


Figura II.11 : Herramienta Dashboard o de Localización

Fuente: http://www.aplicacionesempresariales.com/zenoss-monitorizacion-de-tecnologia-en-la-empresa.html

A propósito de la herramienta de localización o Dashboard; Zenoss permite integración con Google Maps, permitiendo localizar gráficamente en los mapas que ofrece Google, a las unidades y dispositivos tecnológicos fuera de la empresa.

2.9.2.4. Principios Clave

Zenoss ha sido diseñado con estas ideas importantes en su núcleo:

• Modelado

El modelo de sistema que permite entender el entorno en que opera. A través de sofisticadas y análisis detallado, Zenoss determina la manera de supervisar y administrar entornos de TI complejos. El núcleo del modelo estándar describe la información básica sobre el sistema operativo de cada dispositivo y el hardware. El modelo es basado en objetos, y se extiende fácilmente a través de la herencia de objetos.

• Descubrimiento

Con un sofisticado modelo, la introducción manual de datos y el mantenimiento es un reto. Para hacer frente a este desafío, Zenoss descubrimiento utiliza para rellenar el modelo. Durante el descubrimiento, el sistema accede a cada dispositivo de seguimiento en su infraestructura y se interroga en detalle, la adquisición de información acerca de sus componentes, integración de redes, y dependencias.

• Normalización

Debido a que Zenoss recopila información de diferentes plataformas ya sea través de diferentes protocolos, la cantidad y formato de la información disponible varía. Por ejemplo, la información del sistema de archivos obtenidos de un servidor Linux se diferencia de información similar obtenida de un servidor de Windows. Zenoss estandariza los datos recogidos, para que puedan realizar comparaciones válidas de cifras recogidas por diferentes métodos y sistemas diferentes.

• Recogida de datos sin agente

Para recopilar información, Zenoss se basa en el agente de recolección de datos. Al comunicarse con un dispositivo a través de uno o de varios protocolos (incluyendo SNMP, SSH, Telnet, y WMI), que minimiza el impacto sobre los sistemas de seguimiento.

• Total de Infraestructura de TI

A diferencia de otras herramientas, el enfoque del sistema inclusivo unifica todos los ámbitos de la infraestructura de TI - redes, servidores, y aplicaciones - para eliminar su necesidad de acceso a múltiples herramientas.

• La herencia de configuración

Zenoss extiende el concepto de herencia en lenguajes orientados a objetos para la configuración. Toda la configuración en base a parámetros (propiedades de configuración) y las direcciones de vigilancia (monitoreo plantillas) para describir la herencia cómo un dispositivo debe ser vigilado. La herencia le permite describir, en un nivel alto, cómo los dispositivos deben ser monitoreados.

• Compatible con varias plataformas de seguimiento

Zenoss monitorea el rendimiento y la disponibilidad de los sistemas operativos heterogéneos (incluyendo Windows, Linux y Unix), SNMP habilitado para los dispositivos de red (tales como Cisco), y una variedad de aplicaciones de software (por ejemplo, como WebLogic y VMware).

• Escala

Puede implementar el sistema en un solo servidor para manejar cientos de dispositivos.

• **Extensibilidad**

Mecanismo del sistema de extensión, ZenPacks, permite además una rápida modificación para personalizar su el medio ambiente.

2.9.2.5. Disponibilidad de vigilancia en Zenoss:

Se ejecutan pruebas en la infraestructura para determinar si está funcionando adecuadamente Ejemplos: ping de pruebas, proceso de ensayos, pruebas y servicio.

2.9.2.6. Eventos de Zenoss:

Los eventos se generan cuando los demonios detectan un fallo en el sistema genera un evento, estos incluyen syslog y trampas SNMP.

2.9.2.7. Supervisión y ejecución de Zenoss:

Zenoss puede recoger información a través de SNMP, scripts (ZenCommands) o XML-RPC.

2.9.2.8. Arquitectura de Zenoss

El siguiente diagrama ilustra la arquitectura del sistema.

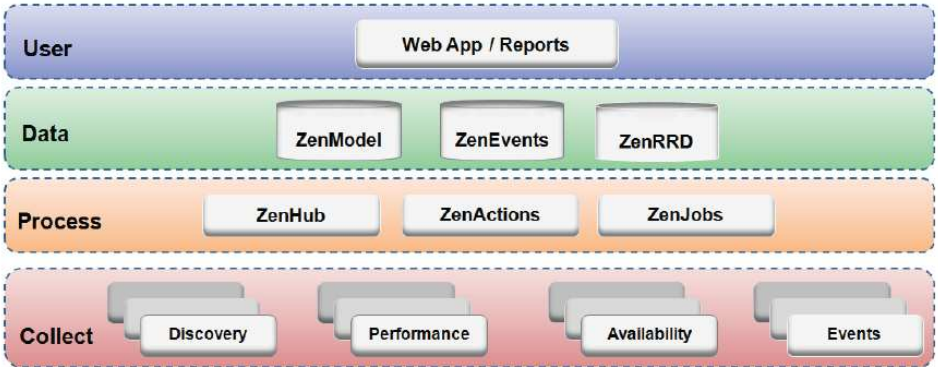


Figura II.12 : Arquitectura de Zenoss

Fuente: http://ufpr.dl.sourceforge.net/project/zenoss/Documentation/zenoss-3.0.x-docs/zendocs-3.0.3/Zenoss_Administration_06-102010-3.0-v03.pdf

Zenoss es un sistema escalonado de cuatro partes principales:

• Capa de Usuario
• Capa de Datos
• Capa de Procesamiento
• Capa de Colección

2.9.2.8.1. Capa de usuario:

La capa de usuario se manifiesta como una consola Web / Portal. Esta capa se compone de la interfaz gráfica de usuario (GUI), que permite al usuario el acceso a los siguientes datos:

- Trabajar con los dispositivos, redes y sistemas
- Supervisar y responder a eventos
- Gestión de usuarios
- Crear y ejecutar informes

La capa de usuario interactúa con la capa de datos y traduce la información para mostrar en la interfaz de usuario.

2.9.2.8.2. Capa de datos:

Es donde se almacena la totalidad de la información del sistema, esta capa se compone de los Zenoss, demonios y zeoctl (back-end objeto de base de datos que almacena la configuración).

- ***Front-end:*** Estado inicial de un proceso.
- ***Back-end:*** Estado final de un proceso.

La configuración y recolección de información se almacena en la capa de datos, en tres bases de datos separadas:

- **ZenRRD -** Utilizando RRDtool, almacenes de datos de rendimiento de series de tiempo. Dado que los archivos RRD se almacenan localmente para cada colector, ningún resultado cuellos de botella de la escritura a una sola base de datos como los coleccionistas se añaden nuevos.

- **ZenModel -** Sirve como modelo de configuración básica, que abarca los dispositivos y sus componentes, grupos y lugares. Contiene los datos del dispositivo en la base de datos ZEO back-end.

- **ZenEvents -** Almacena los datos de eventos en una base de datos MySQL.

DEMONIOS	CARACTERISTICAS
ZenrRRD	Reúne series cronológicas de datos y actúa como un RRDtool.
Zenevents	Interactúa con la base de datos MySQL Eventos.
Zenmodel	Configuración del modelo de Zope (objeto de base de datos)
Zenhub	Broker de información entre la capa de datos y la recogida de los demonios.

Tabla II.II : Bases de Datos de Zenoss

Fuente: http://www.slideshare.net/ces1227/zenoss-manual-presentation

2.9.2.8.3. Capa de Proceso:

El nivel de proceso gestiona la comunicación entre las capas de colección y de datos. También se ejecuta de back-end, trabajos periódicos, así como los trabajos iniciados por el usuario (ZenActions y ZenJobs). La capa de proceso utiliza Twisted PB (un sistema bidireccional de RPC) para las comunicaciones.

2.9.2.8.4. Capa de Colección:

La capa de colección está compuesta por servicios que recogen y alimentan los datos a la capa de datos. Estos servicios son proporcionados por demonios que llevan a cabo numerosos modelos, el monitoreo y las funciones de gestión de eventos.

El sistema de modelado utiliza SNMP, SSH y WMI para recopilar información desde máquinas remotas. La información en bruto se

alimenta en un sistema de extensiones (plugins de modelado) que normaliza los datos en un formato que coincida con el modelo básico.

Monitoreando demonios para visualizar la disponibilidad y el rendimiento de la infraestructura de TI. Usando múltiples protocolos, ellos almacenan la información de rendimiento local en archivos RRD, permitiendo así que los collectors se extendiendan entre muchos collectors. La información de estado y disponibilidad, como los fallos de ping y las infracciones de threshold, se devuelven a través de ZenHub para el sistema de eventos.

Los servicios que recogen los datos se realiza gracias a los demonios de recolección, estos se clasifican en 5 áreas distintas:

Automatizado de Modelado de los demonios:

DEMONIOS	CARACTERISTICAS
Zendisc	Encargado de descubrir todas las redes activas, para encontrar direcciones ip y dispositivos.
ZenwinModeler	Se utiliza para el auto-descubrimiento de Windows Servicios (WMI) se ejecuta en un cuadro de las ventanas.
ZenModeler	Se utiliza para alto rendimiento, modelo que utiliza SNMP, SSH, Telnet

Tabla II.III : Automatizado de modelado de los demonios

Fuente: http://www.slideshare.net/ces1227/zenoss-manual-presentation

Disponibilidad de modelos de demonios:

DEMONIOS	CARACTERISTICAS
Zenping	Supervisión del estado del ping para ICMP
Zenstatus	Realiza pruebas de conexión TCP remoto de los demonios
Zenprocess	Permite la supervisión de proceso utilizando los recursos de acogida SNMP MIB.

Tabla II.IV : Disponibilidad de modelos de demonios

Fuente: http://www.slideshare.net/ces1227/zenoss-manual-presentation

Evento de colección de demonios:

DEMONIOS	CARACTERISTICAS
Zensyslog	Es la recogida y clasificación de syslog de eventos.
Zeneventlog	Se utiliza recoger (WMI) de registro de eventos de eventos.
Zentrap	Recoge trampas SNMP. Recibe las trampas y los convierte en los acontecimientos.

Tabla II.V : Evento de colección de demonios

Fuente: http://www.slideshare.net/ces1227/zenoss-manual-presentation

Monitoreo de desempeño de demonios:

DEMONIOS	CARACTERISTICAS
ZenperfSNMP	Realiza un alto rendimiento asincrónico SNMP.(Rendimiento de colección)
ZenperfxMLrpc	Se utiliza para XML RPC colección
Zencommand	Utiliza para XML RPC, permite el funcionamiento de Nagios y Cacti y plug-ins local o remotamente a través de SSH.

Tabla II.VI : Monitoreo de desempeño de demonios

Fuente: http://www.slideshare.net/ces1227/zenoss-manual-presentation

Respuesta automática Demonios:

DEMONIOS	CARACTERISTICAS
Zenactions	Se utiliza para alertas (SMTP, SNPP y mantenimiento Windows)

Tabla II.VII : Respuesta automática demonios

Fuente: http://www.slideshare.net/ces1227/zenoss-manual-presentation

2.9.2.9. Enfoque del Monitoreo

Zenoss utiliza un enfoque basado en modelos de seguimiento, la combinación de descubrimiento y el modelo que permite el seguimiento automático.
Esta estrategia reduce los gastos generales de mantenimiento del sistema y asegura que los nuevos dispositivos y aplicaciones son monitoreadas como vienen en línea.

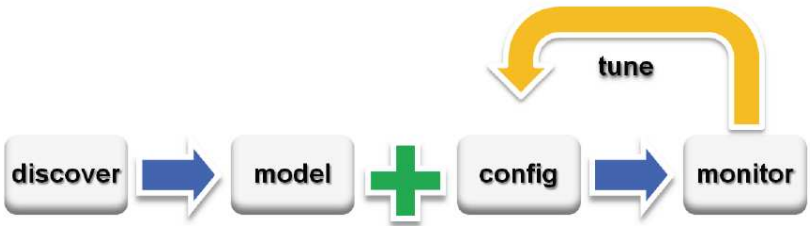


Figura II.13 : Flujo de trabajo: Control de Model-Driven
Fuente: http://ufpr.dl.sourceforge.net/project/zenoss/Documentation/zenoss-3.0.x-docs/zendocs-3.0.3/Zenoss_Administration_06-102010-3.0-v03.pdf

Como se muestra en la ilustración anterior, el control basado en modelos se inicia con el descubrimiento, que se rellena el modelo. Este continúa con una configuración definida en el modelo que es automáticamente aplicado y monitoreado. Como el sistema funciona, la configuración es más afinada.

El Model-Driven se demuestra por el siguiente escenario de monitoreo de archivo del sistema.

Monitoreo de Sistema de Archivo

De forma predeterminada, el sistema está configurado con un threshould de sistema de archivos de 90% de utilización. Cada vez que se descubre un archivo del sistema, este threshould se aplica automáticamente al sistema de archivos, y comienza el monitoreo.

Figura II.14 : Monitoreado de archivos de sistema

Fuente: http://ufpr.dl.sourceforge.net/project/zenoss/Documentation/zenoss-3.0.x-docs/zendocs-3.0.3/Zenoss_Administration_06-102010-3.0-v03.pdf

Esta ilustración muestra el resultado de un sistema que está siendo monitoreado, utilizando la configuración por defecto. El gráfico muestra que el threshould del 90% ha sido superado en numerosas ocasiones. Dado que los datos en el modelo se normalizan, los threshould se aplicarán con independencia del mecanismo de recolección (SNMP, SSH y WMI).

2.9.3. ZABBIX

Zabbix fue creado por Alexei Vladishev, y actualmente está desarrollado y soportado por Zabbix SIA.

Zabbix es una herramienta para monitorear los recursos de un equipo en forma remota que consume pocos recursos, permite centralizar la información en un servidor que permite visualizar el monitoreo de múltiples hosts.

Zabbix es un software que controla numerosos parámetros de una red y la la integridad de los servidores. Zabbix utiliza un mecanismo de notificación flexible que permite a los usuarios configurar alertas basadas en correo electrónico para cualquier evento. Este permite una reacción rápida a los problemas del servidor. Todos los informes Zabbix y estadísticas, así como los parámetros de configuración se acceden a través de una interfaz basada en web. Un front-end basado en web se asegura que el estado de la red y la salud de los servidores se puede apreciar desde cualquier lugar. Zabbix es libre de costo. Zabbix se escribe y se distribuye bajo la GPL General Public License versión 2. Esto significa que su código fuente se distribuye libremente y disponible para el público en general. El soporte es gratuito y comercial está disponible y realizado por la empresa Zabbix.

2.9.3.1. Características

A continuación expondremos algunas funcionalidades más destacadas de Zabbix.

- Permite también monitoreos simples sin agente ni SNMP, por ejemplo, solo hacerle ping a un servidor o verificar que desde la red esté disponible un cierto puerto TCP o UDP.
- Permite el uso de plantillas (Templates) para facilitar el modelamiento de dispositivos a monitorear
- **Interfaz web integrada**

  Zabbix tiene un único interfaz web en la cual se integran la parte de monitorización, representación gráfica de los datos obtenidos, configuración de los monitores y alertas, y administración de los usuarios, permitiendo personalizar las funcionalidades visibles en función del perfil del usuario.
- **Posibilidad de especificar condiciones complejas de alerta**

  Podemos especificar condiciones de alerta bastante complejas, pudiendo combinar varios monitores, incluso de diferentes servidores, y sobre ellos disparar alertas en base a la suma, media o valores mínimos o máximos en un periodo de tiempo determinado, o en los últimos N valores.
- **Niveles de gravedad de alertas**

  Para todas las monitorizaciones puede definirse la gravedad de la misma (desde informativa hasta crítica), y en base a esa gravedad podemos establecer la acción a tomar (a quién se avisa, el medio utilizado o la acción a realizar).
- **Escalabilidad de acciones**

  Zabbix permite designar una sucesión de escalabilidad de acciones a realizar ante un evento. Por ejemplo, puede ejecutar un script de autocorrección cuando se produce la incidencia por primera vez, enviar un aviso por correo electrónico si pasado un tiempo no se ha solventado el problema, emitir avisos por SMS si el problema sigue sin resolverse en una tercera comprobación.

  Esta utilidad es especialmente útil para la adopción de medidas proactivas en caso de incidencias que pudieran ser solventables de forma

automática. Por ejemplo, ante la caída de un servicio web fuera de horario laboral, que como primera medida intente un reinicio del servicio, y que en caso de que esa acción no solvente el problema, realice el aviso al técnico correspondiente.

- **Autodescubrimiento**

  Podemos especificar un rango de direcciones IP en el que hay equipos que queremos monitorizar, y el propio sistema comienza a testear todas las IPs de ese rango y los puertos abiertos en cada uno de ellos, y es capaz de crear los correspondientes monitores para los equipos detectados.

  Esto es muy útil para por ejemplo monitorizar todos los equipos de un aula de informática, simplemente hay que encender todos los equipos y poner a funcionar la auto detección.

- **Plantillas**

  Podemos definir una serie de plantillas sobre las cuales determinamos los monitores y disparadores de alerta correspondientes. Cada vez que demos de alta a un nuevo dispositivo, simplemente le asociamos las plantillas que deseemos usar y ya tenemos la máquina configurada, con sólo especificar nombre, dirección IP y plantillas asociadas.

  Podemos definir plantillas genéricas para un servidor Linux, para servidores web, servidores de correo, UPS, switches, etc. Así, cuando necesitemos monitorizar un servidor Linux que presta servicio de correo IMAP e interfaz web, simplemente damos de alta el nombre de equipo, la IP y le asociamos las tres plantillas correspondientes.

- **Representación gráfica de cualquier monitorización**

  Zabbix almacena los valores obtenidos de cada monitorización en una base de datos MySQL, y a partir de ellos elaborar una gráfica de líneas. No es necesario hacer nada al respecto. Simplemente creando el monitor se crea su gráfica correspondiente, no tenemos que preocuparnos de crearla.

Si lo consideramos necesario, podemos especificarle la cantidad de valores que queremos que almacene, por si nos preocupa el posible incremento de la base de datos.

- **Creación de gráficas personalizada (multimonitor y multiservidor)**

  A partir de los valores obtenidos a través de los monitores, podemos realizar gráficas que impliquen diferentes monitores, que pueden además ser de diferentes servidores.

  Con esta utilidad podemos crear gráficas para comparar de un vistazo el tamaño de las colas de los diferentes servidores SMTP, o el espacio ocupado en las diferentes particiones de un mismo servidor.

- **Monitorización Web**

  Podemos simular la "experiencia de usuario" a la hora de navegar por nuestras páginas web, almacenando el tiempo de respuesta y la velocidad de transferencia de datos. Podemos especificar los valores a rellenar en un formulario web, y simular la sucesión de descargas de varias páginas.

- **Mapas, pantallas y slideshows**

  Podemos condensar toda la información recopilada en tres posibles representaciones visuales, en pantallas, mapas y slideshows. En un mapa podemos representar sobre un dibujo de fondo (en muchas ocasiones un mapa de localización) el estado de diferentes dispositivos y de las interconexiones que tengan. En una pantalla podemos incluir diferentes gráficas, tablas, mapas, y páginas web, permitiendo tener una completa visualización del estado de nuestras infraestructuras, y en un slideshow podemos diseñar una presentación con una sucesión de pantallas.

  Esto nos permite diseñar unas pantallas para que técnicos no directamente implicados en el control de los sistemas monitorizados (por ejemplo, técnicos de soporte y ayuda al usuario final), directivos de perfil no técnico, o incluso usuarios finales de nuestros servicios, puedan obtener de una forma clara y condensada datos sobre el estado de nuestras infraestructuras TIC.

- **Monitorización distribuida. Agentes Proxy**

  El Agente proxy es un proceso ligero que recolecta los datos monitorizados en lugar del servidor centralizado, descargando a este último de parte del proceso de recolección de datos. El agente proxy le pasa los datos obtenidos de manera concentrada al servidor central. También se suele utilizar para recolectar los datos de ubicaciones remotas, optimizando la comunicación de datos.

2.9.3.2. Requisitos software

Zabbix se articula en torno moderno servidor web Apache, los motores de base de datos, y el lenguaje de script PHP.

El siguiente software es necesario para ejecutar Zabbix:

Software	Versión	Descripción
Apache	1.3.12 o superior	
PHP	4.3 o superior	
PHP módulos: **php-gd** **php-bcmath**	4.3 o superior	Módulo PHP GD debe ser compatible con las imágenes PNG
MySQL **php-mysql**	3.22 o superior	Requerido si se usa MySQL como base de datos de backend.
Oracle **php-sqlora8**	9.2.0.4 o superior	Requerido si Oracle se utiliza como base de datos de backend.
PostgreSQL **php-pgsql**	7.0.2 o superior	Requerido si se utiliza PostgreSQL como base de datos. Considere el uso de PostgreSQL 8.x o posterior para un rendimiento mucho mejor.
SQLite **php-sqlite3**	3.3.5 o superior	Requerido si se utiliza SQLite como base de datos de backend.

Tabla II.VIII : Software necesario para ejecutar Zabbix

Fuente: Investigador

Nota: Zabbix puede funcionar en versiones anteriores de Apache, MySQL, Oracle y PostgreSQL también.

2.9.3.3. Arquitectura

Zabbix ofrece muchas maneras de controlar los diferentes aspectos de su infraestructura de TI y, de hecho, casi cualquier cosa que desee conectar a la misma. Puede ser caracterizada como un sistema de control semi-distribuida con gestión centralizada. Aunque muchas instalaciones tienen una base de datos única y central, es posible utilizar distribuido de vigilancia en los nodos y los apoderados, y la mayoría de instalaciones se utilizan agentes de Zabbix.

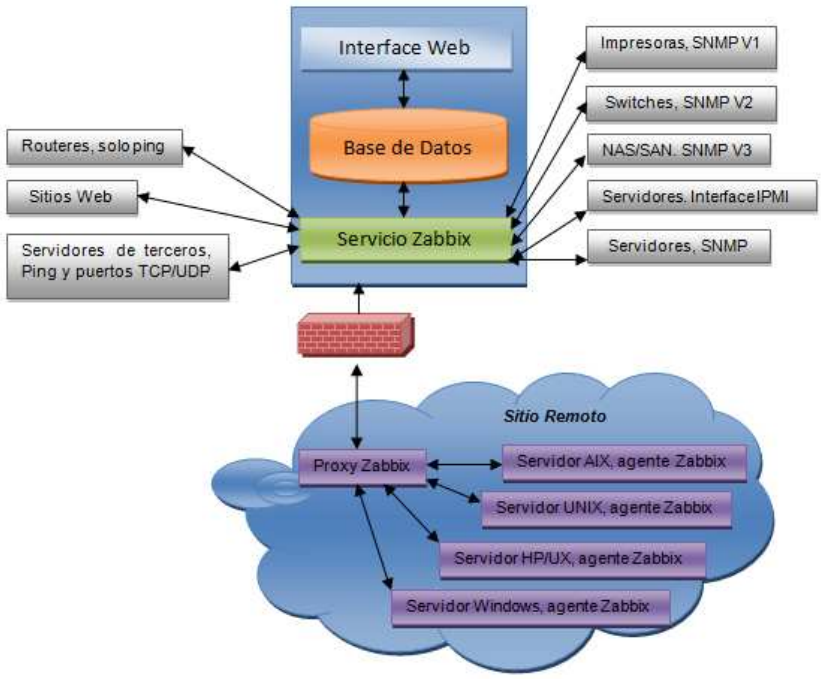


Figura II.15 : Arquitectura de Zabbix

Fuente: http://revistalinux.net/articulos/duerme-mejor-con-zabbix/

Internamente Zabbix está integrado por tres componentes principales, a saber:

- La base de datos
- La interface web (el front-end)
- El servicio o daemon Zabbix en sí mismo.

Esta arquitectura distribuida permite que Zabbix pueda gestionar decenas o incluso cientos de miles de dispositivos en instalaciones muy grandes y complejas ya que esto sumado a la posibilidad de configurar satélites o nodos adicionales de monitoreo permite distribuir la carga entre múltiples máquinas para poder alcanzar niveles enormes de escalamiento.

CAPÍTULO III

ANÁLISIS COMPARATIVO DE HERRAMIENTAS OPENSOURCE PARA LA ADMINISTRACIÓN Y MONITOREO DE REDES BASADAS EN SNMP

3.1. Análisis de la infraestructura actual de networking del Ilustre Municipio de Ambato.

En la actualidad el Ilustre Municipio de Ambato mantiene bajo su control un conjunto de dispositivos conectados a la red que proporcionan varios servicios. Este control implica el mantenimiento de los dispositivos en forma preventiva y también la necesidad de responder en tiempo y forma ante eventuales caídas de servicios. Actualmente se carece de una notificación temprana y eficaz de las fallas que puedan ocurrir dentro del conjunto de dispositivos mantenidos, el fallo se detecta cuando se recibe la notificación de un usuario o por algún control realizado por administradores del departamento de sistemas; ante esta situación y por la necesidad de detectar caídas de servicios que se tornan vitales, para el IMA de forma más rápida y segura surge la

necesidad de implantar una solución que provea la detección automática de fallas y notifique al personal sobre sus ocurrencias. Esta solución puede consistir en la instalación de una herramienta que monitoree, identifique problemas y los notifique a las personas indicadas para su resolución.

A continuación se muestra la infraestructura actual de networking del IMA:

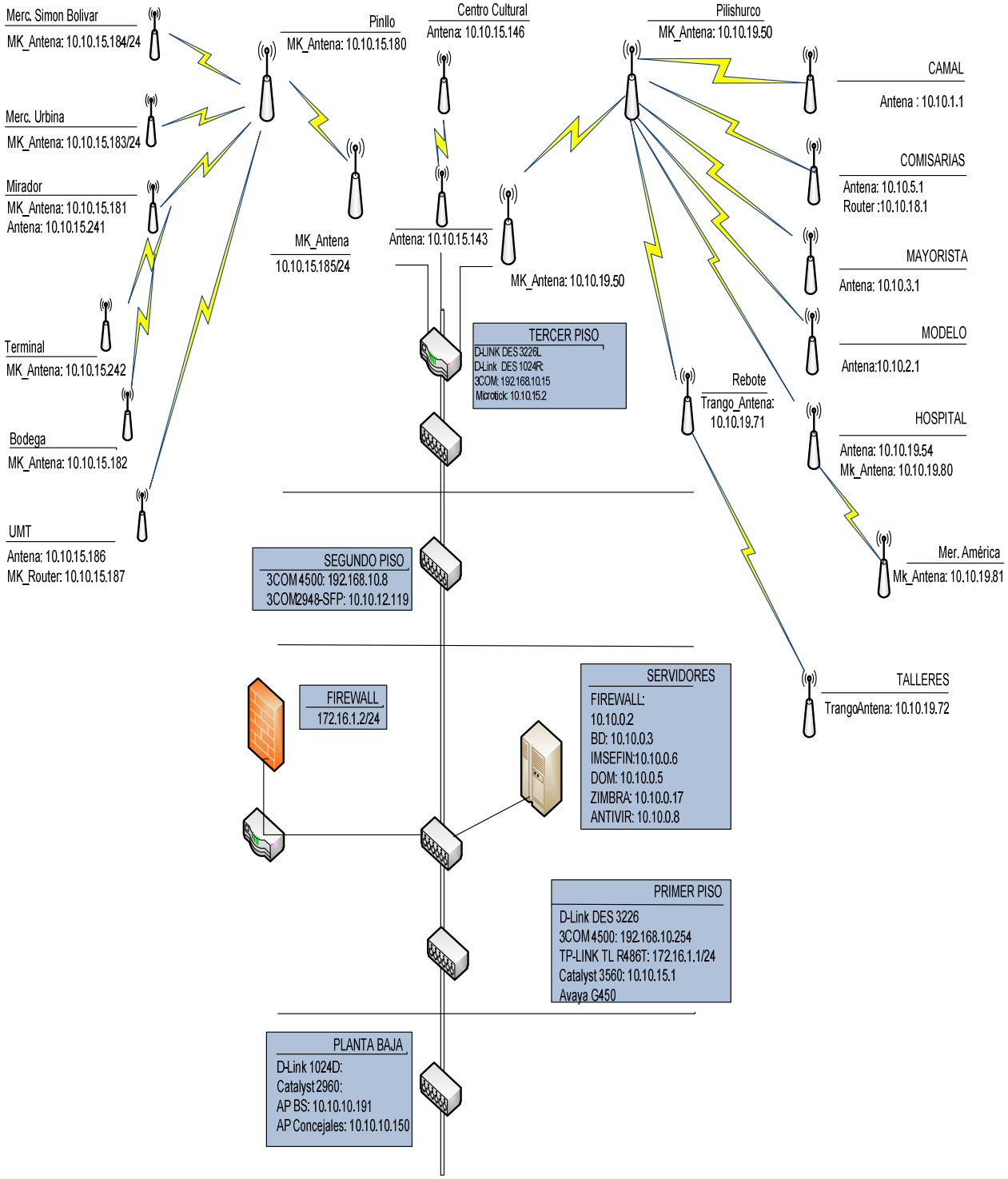


Figura III.16 : Infraestructura actual de networking IMA
Fuente: Departamento de Informática del Ilustre Municipio de Ambato

La red del IMA está conformada por varias subredes, distribuidas entre los diferentes pisos de la institución y sus dependencias. Los rangos de las subredes mencionadas son:

Edificio del Ilustre Municipio de Ambato

- **Planta Baja y Primer Piso:** 10.10.10.0/24, en esta subred se encuentran los diferentes servidores con los que cuenta la institución.
- **Segundo y Tercer Piso:** 10.10.12.0/24
- Centro Cultural, Terminal, Bodega: 10.10.15.0
- Mayorista, Camal: 10.10.19.0
- Comisarias: 10.10.18.0
- Desarrollo Social: 10.10.16.0
- UMT: 10.10.17.0

Actualmente la red del Municipio de Ambato es bastante extensa, ya que aparte de las instalaciones donde funciona la Institución esta cuenta con otras dependencias ubicadas en distintos sectores de la ciudad de Ambato, para lo cual el IMA en su infraestructura tiene instaladas dos radio bases Microtick principales, que son los puntos clave para la comunicación entre el Municipio y los lugares que administra, estas antenas están ubicadas en los sectores de Pillishurco y Pinllo.

PINLLO: 10.10.15.180
PILLISHURCO: 10.10.19.51

Equipos que forman parte de la red del IMA

En la red del Municipio de Ambato existen equipos de diferentes marcas y modelos, algunos administrables y otros no, a continuación se describen todos y cada uno los dispositivos que forman parte de la red:

	NOMBRE	S.O	IP
SERVIDORES	Base de Datos	Windows Server 2003	10.10.0.3
	Correo (zimbra)	Linux Red Hat	10.10.0.17
	Dominio	Windows Server 2003	10.10.0.5
	Antivirus	Windows Server 2008	10.10.0.8
	Firewall	Linux Red Hat	10.10.0.2
	Aplicaciones	S.O Windows Server 2003	10.10.0.6

Tabla III.IX : Servidores de la red de networking del IMA
Fuente: Departamento de Informática del Ilustre Municipio de Ambato

	NOMBRE	IP
MICROTICK	Mercado Simón Bolívar	10.10.15.184
	Mercado Urbina	10.10.15.183
	Mirador	10.10.15.181
	Mirador-Terminal	10.10.15.241
	Terminal	10.10.15.242
	Bodega	10.10.15.182
	UMT	10.10.15.186
	IMA-Pinllo	10.10.15.185
	IMA-Pilishurco	10.10.19.50
TRANGO	Hospital	10.10.19.80
	Mercado América	10.10.19.81
	Camal	10.10.1.1
	Comisarias	10.10.5.1
	Hospital	10.10.19.54
	Mercado Mayorista	10.10.3.1
	Mercado Modelo	10.10.2.1
	Rebote Talleres	10.10.19.71
	Talleres	10.10.19.72

Tabla III.X : Equipos Trango y Microtick de la red de networking del IMA
Fuente: Departamento de Informática del Ilustre Municipio de Ambato

	NOMBRE	IP
ROUTER	Comisarias	10.10.18.1
	Desarrollo Social	10.10.15.252
	Municipio	10.10.15.2
	UMT	10.10.15.187

Tabla III.XI : Routers de la red de networking del IMA

Fuente: Departamento de Informática del Ilustre Municipio de Ambato

	NOMBRE	IP
SWITCH	Switch 3Com 4500	192.168.10.254
	Switch 3Com 2948	10.10.12.119
	Switch 3Com 4500	192.168.10.15
	Switch 3Com 4500	10.10.12.100
	Switch Catalyst 3560	10.10.15.1
	Tp-Link TL-R480 2 D-link DES 10240 D-Link DES 3226 D-Link DES 3226L D-Link DES 1024R* Switch Catalyst 2960	NO ADMINISTRABLE

Tabla III.XII : Switch de la red de networking del IMA

Fuente: Departamento de Informática del Ilustre Municipio de Ambato

3.2.Determinación de los parámetros de comparación

Los parámetros que a continuación se definirán para la realización del estudio comparativo entre las herramientas de Administración y Monitoreo de redes Cacti, Zenoss y Zabbix, están basados en los requerimientos planteados por el Ilustre

Municipio de Ambato, y según los criterios de las autoras de la tesis. Los criterios que se van a considerar en general en este estudio son los siguientes:

PARÁMETRO	DEFINICIÓN
Usabilidad	Interfaz amigable. Facilidad de instalación, configuración, implementación y uso.
Gestión de Usuarios	Se refiere al tipo de seguridad ofrecida por la herramienta para acceder a la información que está recolectando. Posibilidad de manejar interfaces personalizadas para cada administrador.
Recolección de Información en tiempo real	Habilidad de colectar continuamente información y reportarla en tiempo real.
Soporte	Soporte en línea a través de wikis, foros, comunidades.
Reportes	Forma de presentar los datos obtenidos en el monitoreo para su análisis o estudio.
Alertas	Realizar un llamado de atención sobre futuros daños para poder tomar medidas correctivas y evitar que ocurran daños mayores.
Alarmas	Notificación por algún medio de que ocurrió algún daño o evento de importancia dentro de la infraestructura de red.
Autodescubrimiento de Dispositivos	Descubrir computadores y componentes en la infraestructura tecnológica sin necesidad de ser ingresado por una persona.
Mapas	Representación gráfica de la distribución y conectividad de los diferentes equipos que forma parte de la infraestructura de una red.

Tabla III.XIII : Parámetros de Comparación

Fuente: Investigador

3.3. Definición de Escalas

La forma para evaluar las herramientas de Administración y Monitoreo de Redes en base a los parámetros mencionados anteriormente, se calificarán utilizando una escala que va desde 1 hasta 5, a continuación su descripción.

Cuantitativa	**1**	**2**	**3**	**4**	**5**
Cualitativa	Insuficiente	Regular	Bueno	Muy bueno	Excelente

Tabla III.XIV : Escalas de Equivalencias

Fuente: Investigador

3.4. Implementación de Herramientas OpenSource en un ambiente de pruebas

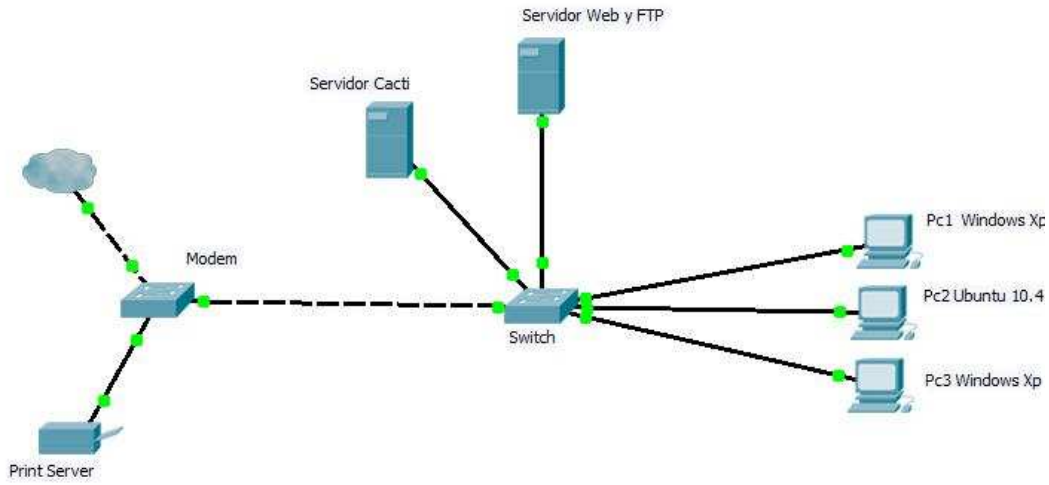


Figura III.17: Ambiente de pruebas

Fuente: Investigador

Para hacer el análisis respectivo de todas y cada una de las herramientas, se ha creado un escenario en el cual se instalarán las herramientas.

3.4.1. Pruebas con la herramienta de Administración y Monitoreo CACTI

Abrimos un navegador web y digitamos la siguiente dirección:

http://localhost/cacti

Seguido nos aparecerá una interfaz como la siguiente:

Figura III.18 : User Login – Cacti
Fuente: Investigador

El usuario por defecto para hacer el login es admin y contraseña admin, luego la podemos editar para mayor seguridad. A continuación la interfaz de gestión de Cacti:

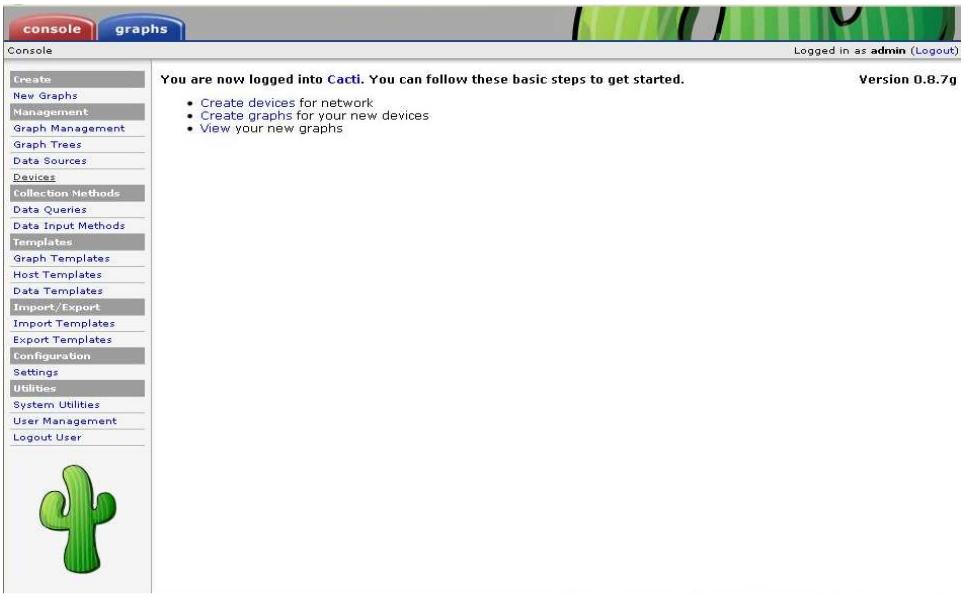


Figura III.19 : Interfaz de gestión – Cacti
Fuente: Investigador

En esta herramienta se puede observar en esta pestaña todos los dispositivos que están siendo objeto de monitoreo.

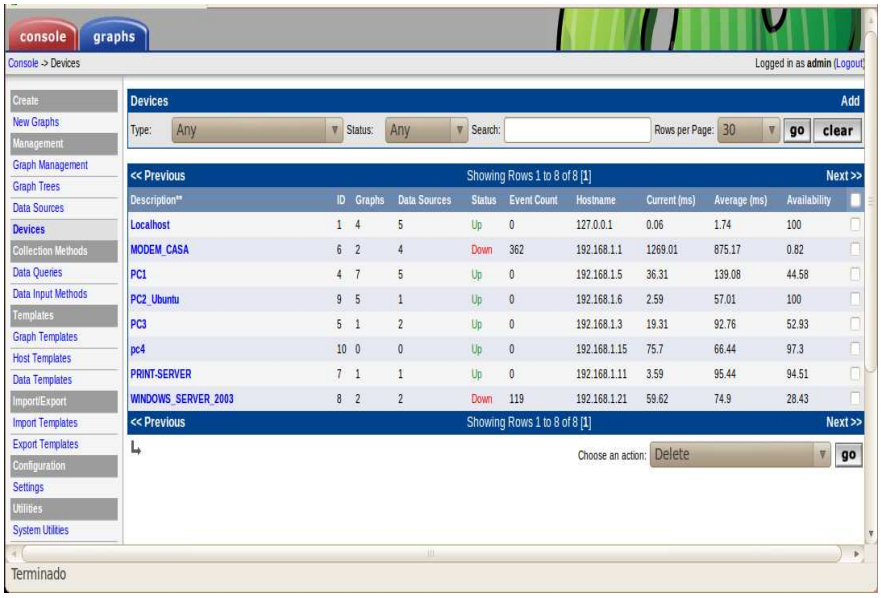


Figura III.20 : Dispositivos Monitoreados – Cacti

Fuente: Investigador

Para crear los gráficos dar click en el link Create Graphs for this Host en donde se podrá indicar qué gráficas se desea generar.

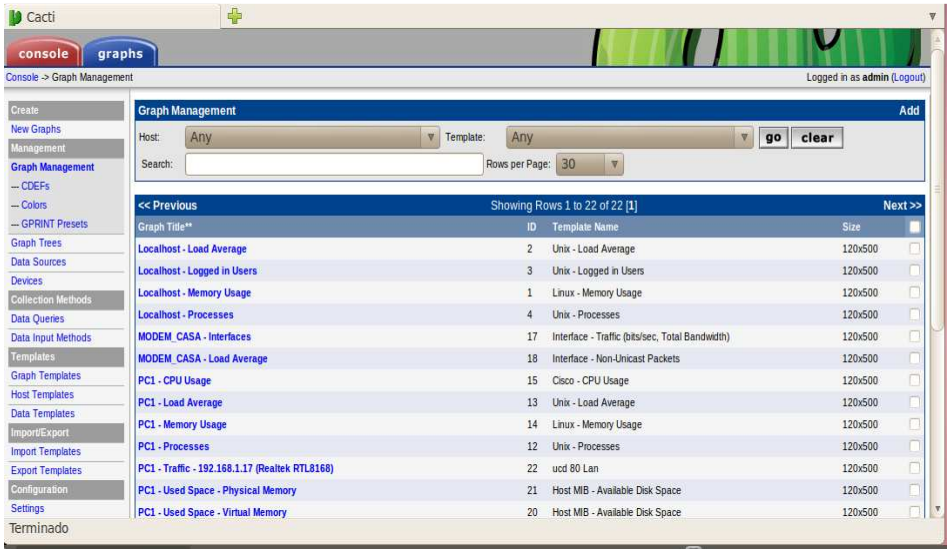


Figura III.21 : Añadiendo Gráficos – Cacti
Fuente: Investigador

Para visualizar las graficas, ubicarse bajo: Graph >> Default Tree y ahi escogemos el equipos para el cual queremos visualizar las Gráficas. Obteniendo resultados más o menos como los siguientes:

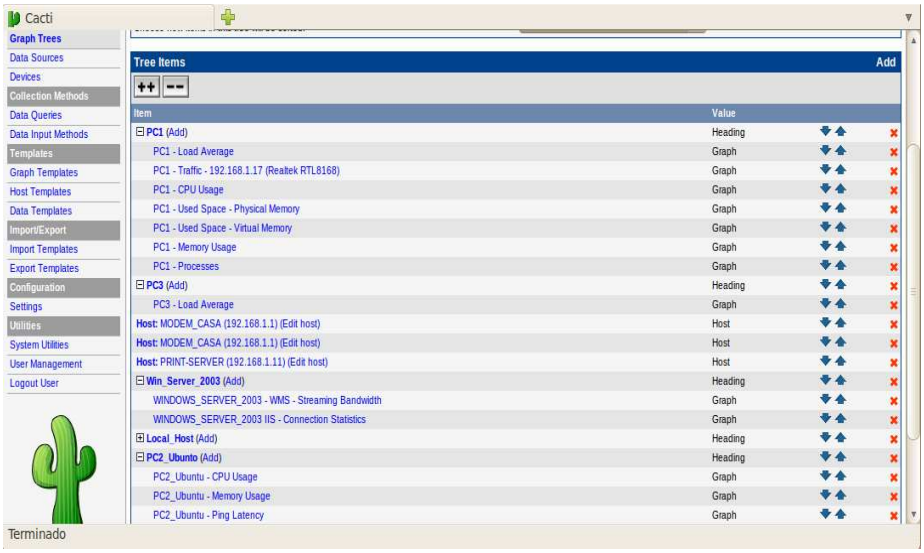


Figura III.22 : Default Tree – Cacti
Fuente: Investigador

Ahora podemos observar los gráficos que arroja de cada dispositivo configurado, a continuación se muestran las graficas de dispositivos con Windows y Linux.

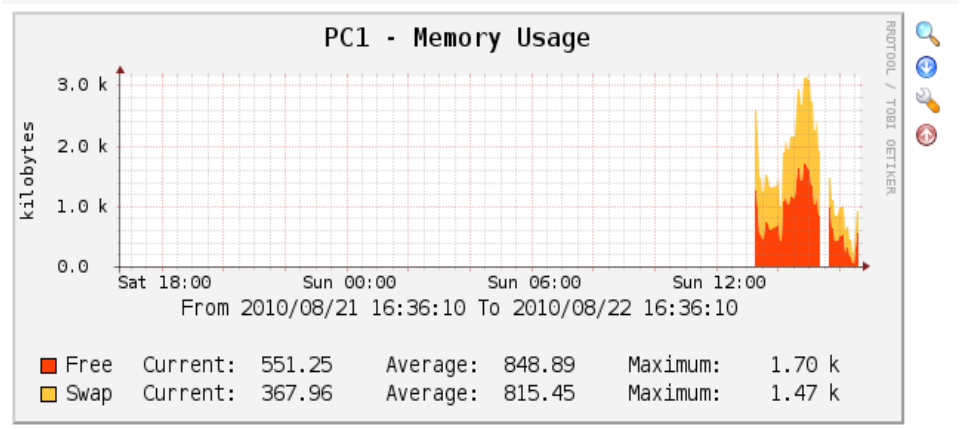


Figura III.23 : Pc1 Windows Memoria Usada – Cacti

Fuente: Investigador

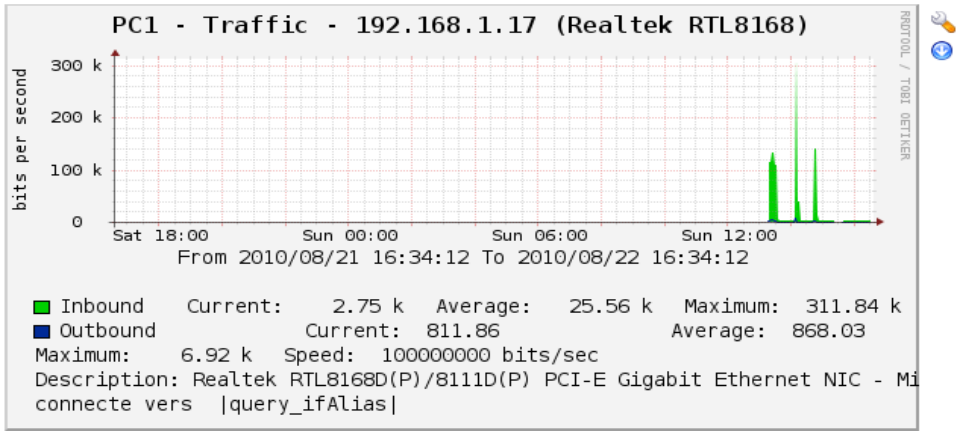


Figura III.24 : Pc1 Windows Tráfico de la Interfaz – Cacti

Fuente: Investigador

También se muestran las graficas del dispositivo con Linux, permitiendo hacer filtros de fechas.

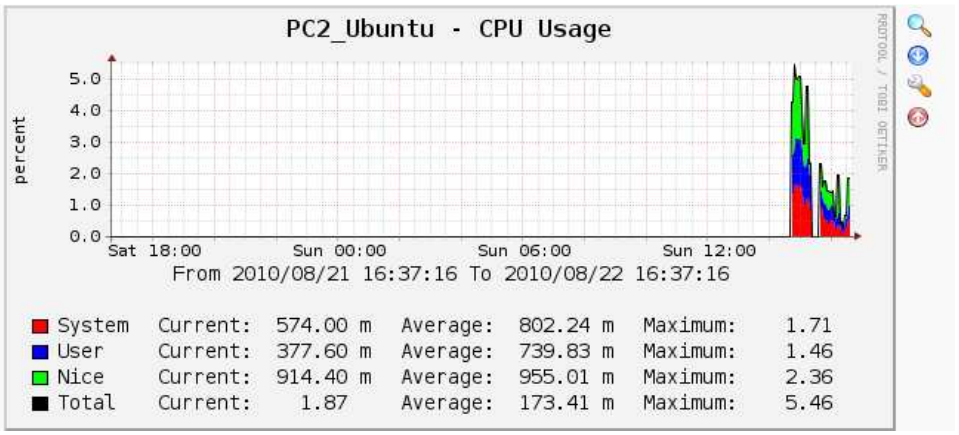


Figura III.25 : Pc2 Ubuntu Uso del CPU – Cacti
Fuente: Investigador

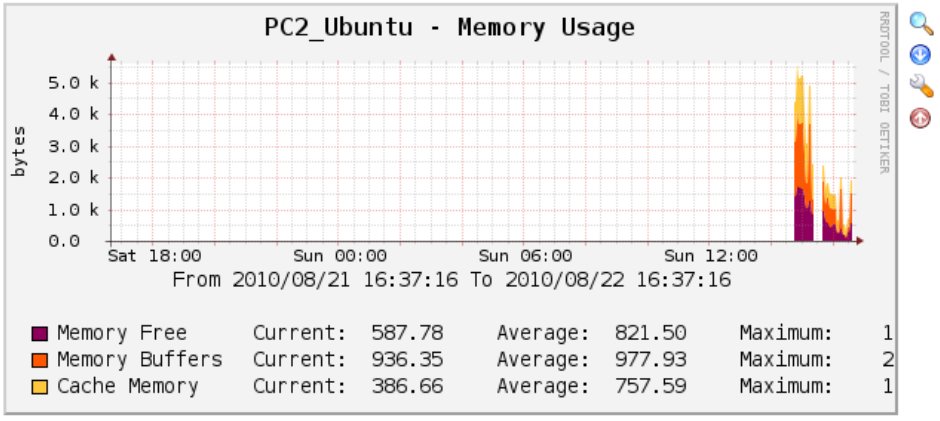


Figura III.26 : Pc2 Ubuntu Uso de Memoria – Cacti
Fuente: Investigador

3.4.2. Pruebas con la herramienta de Administración y Monitoreo ZENOSS

Abrimos un navegador web: **http://localhost/Zenoss**

Tendremos una interfaz como la siguiente:

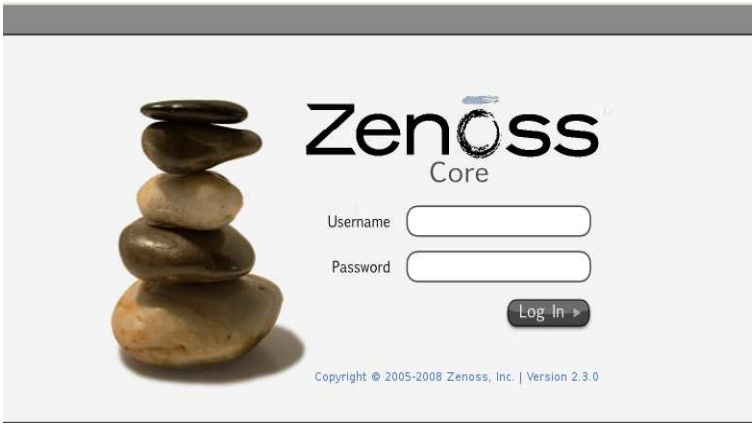


Figura III.27 : User Login – Zenoss
Fuente: Investigador

El usuario por defecto para hacer el login es admin y no tiene ninguna contraseña.

La siguiente figura muestra la interfaz principal de Zenoss, conocida como dashboard:

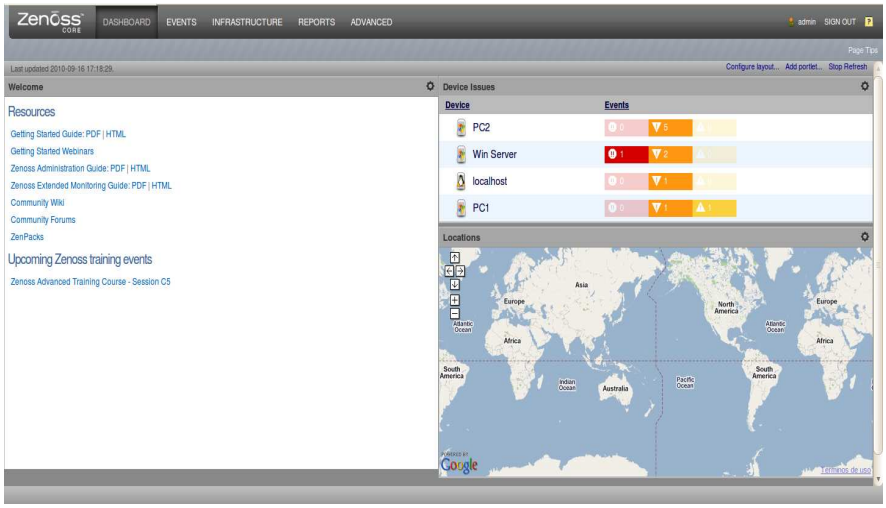


Figura III.28 : Dashboard – Zenoss
Fuente: Investigador

En la parte de Infraestructura básicamente se puede añadir dispositivos, y configurarlos de acuerdo a las necesidades, y además visualizar los componentes,

los cuales se extrae del dispositivo monitoreado, podemos observar que existe una distribución de los dispositivos dependiendo de la clase a la q pertenecen, y algunas pestañas para la navegación, como lo ilustraremos en las siguientes figuras:

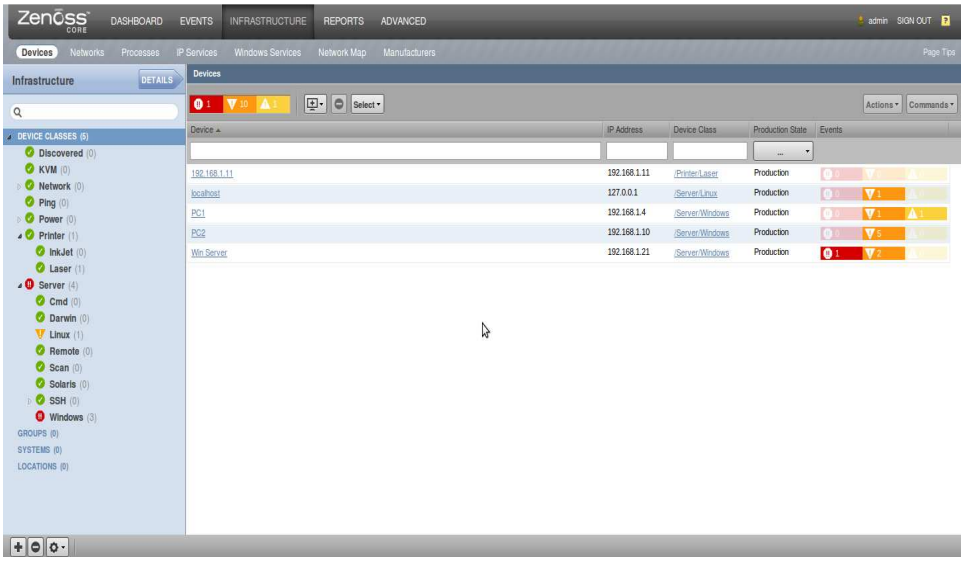


Figura III.29 : Categorización de dispositivos – Zenoss
Fuente: Investigador

Los componentes que muestra del dispositivo monitoreado son Ip services, Network Routes, File System, Procesos, Interfaz, etc, estos pueden variar dependiendo del sistema operativo del dispositivo.

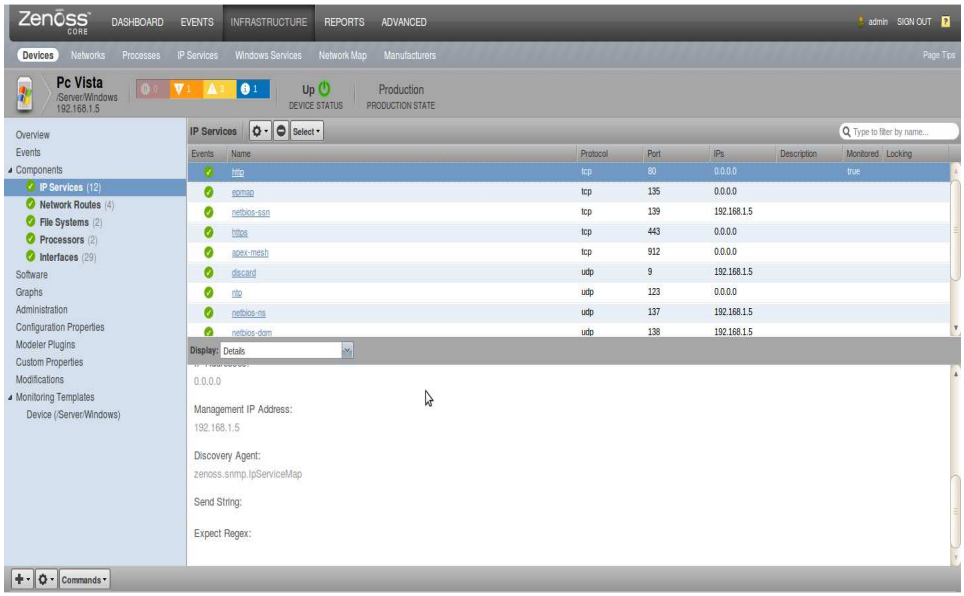


Figura III.30 : IP Service – Zenoss
Fuente: Investigador

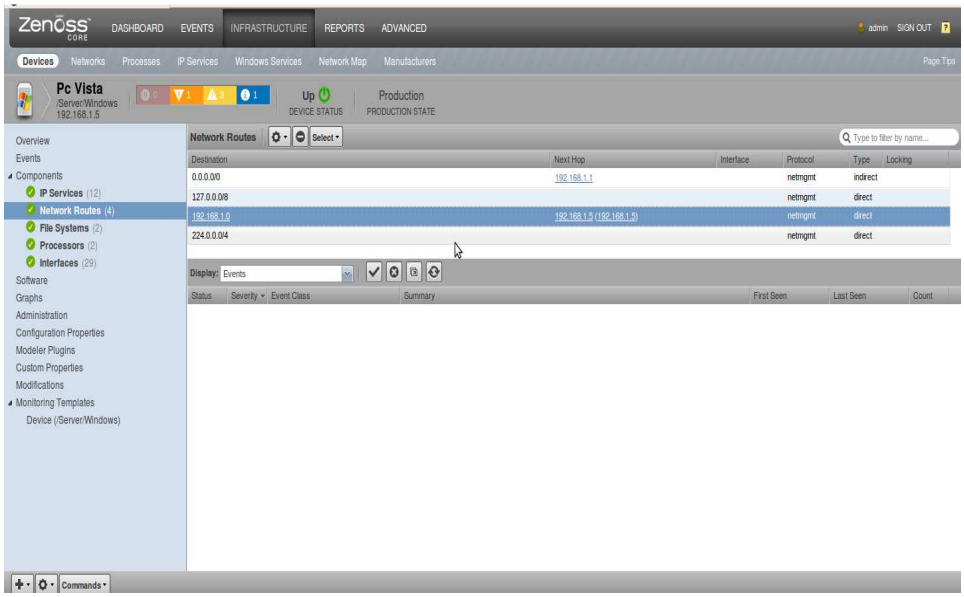


Figura III.31 : Network Routes – Zenoss
Fuente: Investigador

En esta opción muestra el número de discos o las particiones que se tiene en el dispositivo, además muestra una grafica de la utilización de los mismos.

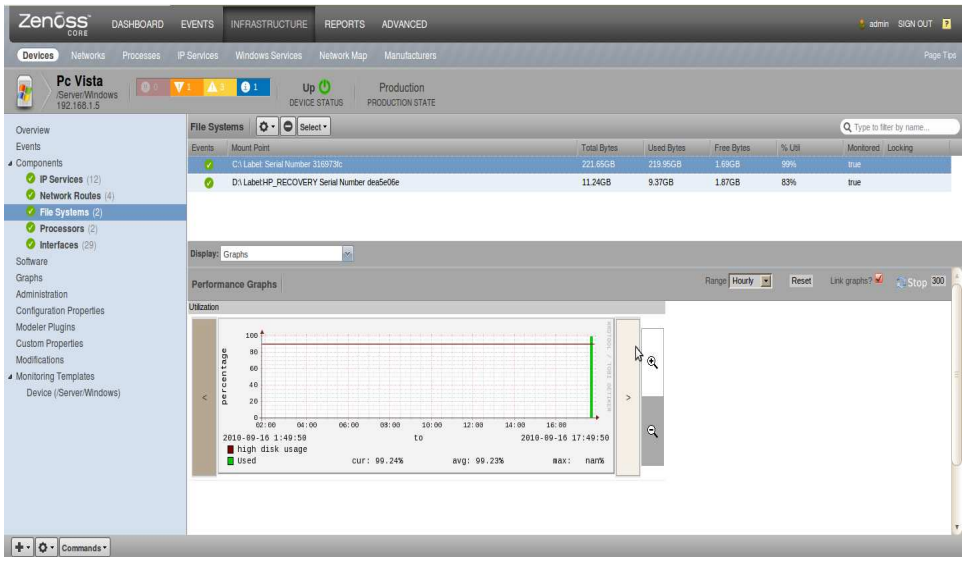


Figura III.32 : File System – Zenoss
Fuente: Investigador

En este componente se muestran todas las interfaces de red con las que cuenta el dispositivo que está siendo objeto de monitoreo, además de mostrar cuales son estas interfaces, se visualiza las graficas de througput, paquetes y errores que se producen, de todas y cada una de las interfaces.

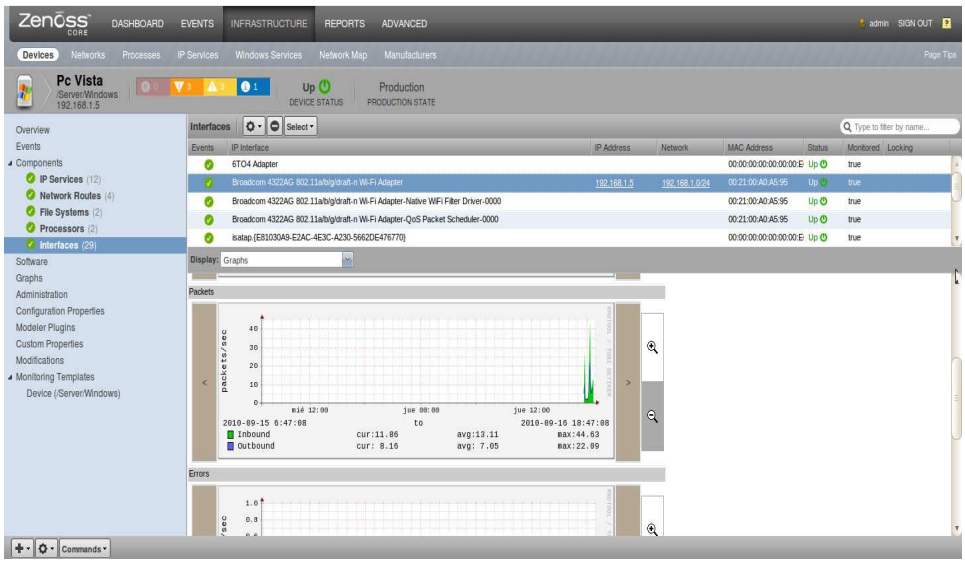


Figura III.33 : Interfaces – Zenoss
Fuente: Investigador

Esta es una característica que muestra todos los software q tiene instalados el dispositivo, incluyendo las actualizaciones de Sistema operativo, este componente solamente se activa en PC con Windows.

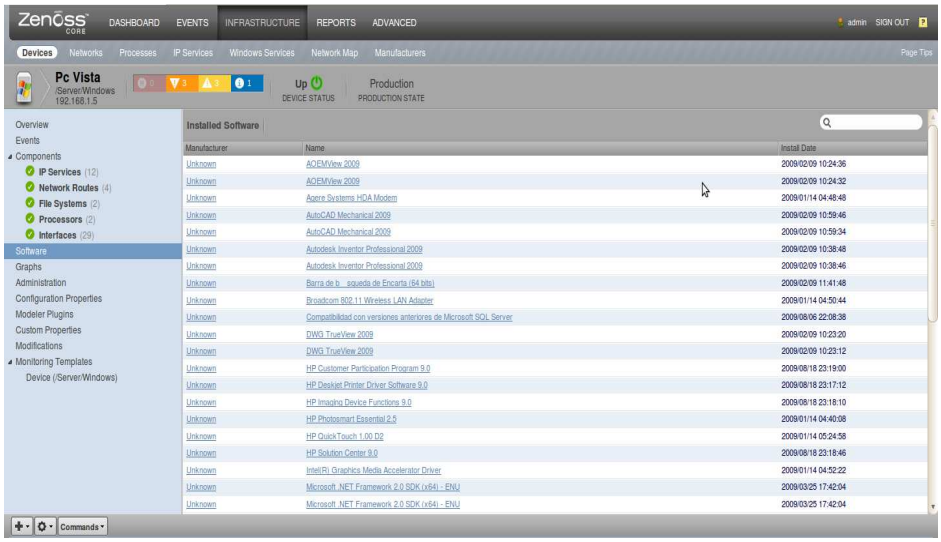


Figura III.34 : Software – Zenoss
Fuente: Investigador

En la opción de Gráficos, se puede visualizar el porcentaje de usos de los recursos del dispositivo, como memoria, cpu, paginación, para esto se usa de un agente basado en SNMP ***(Snmp-Informant).***

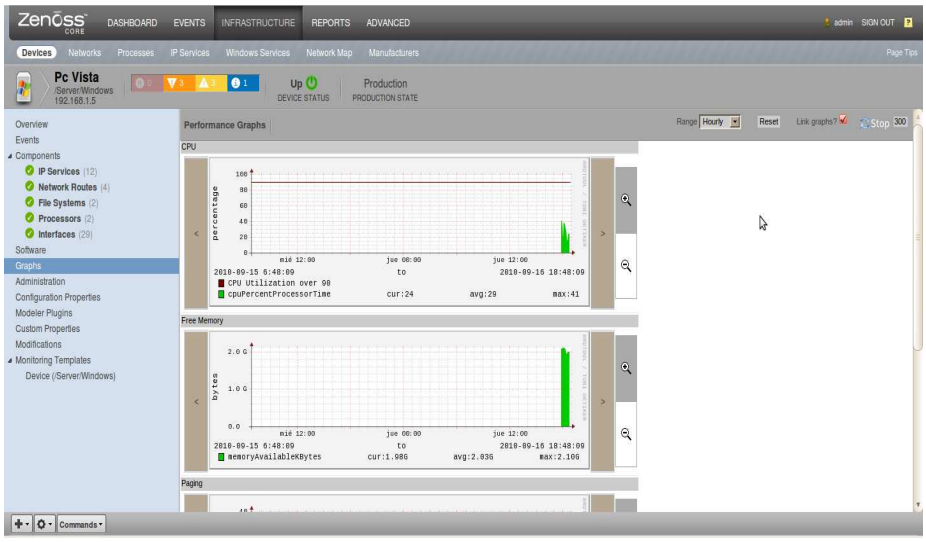


Figura III.35 : Gráficos – Zenoss
Fuente: Investigador

Además se puede correr algunos comandos desde el dispositivo, como ping, snmpwalk, etc, dependiendo de cuales se requiera.

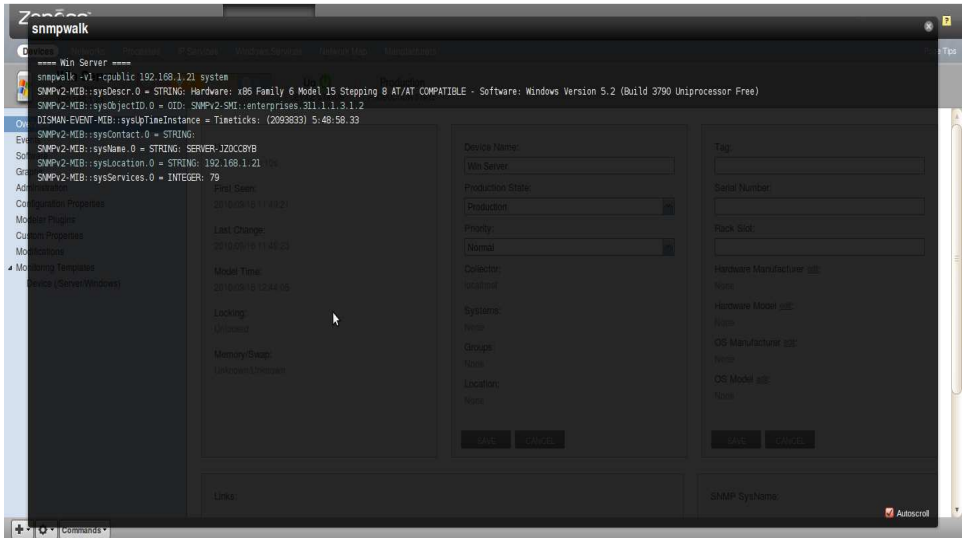


Figura III.36 : Ejecución comandos – Zenoss
Fuente: Investigador

Si bien es cierto, una de las características más llamativas e intuitiva es el Network Map, que muestra la infraestructura de los dispositivos añadidos a la herramienta, clasificándolos de acuerdo a su clase.

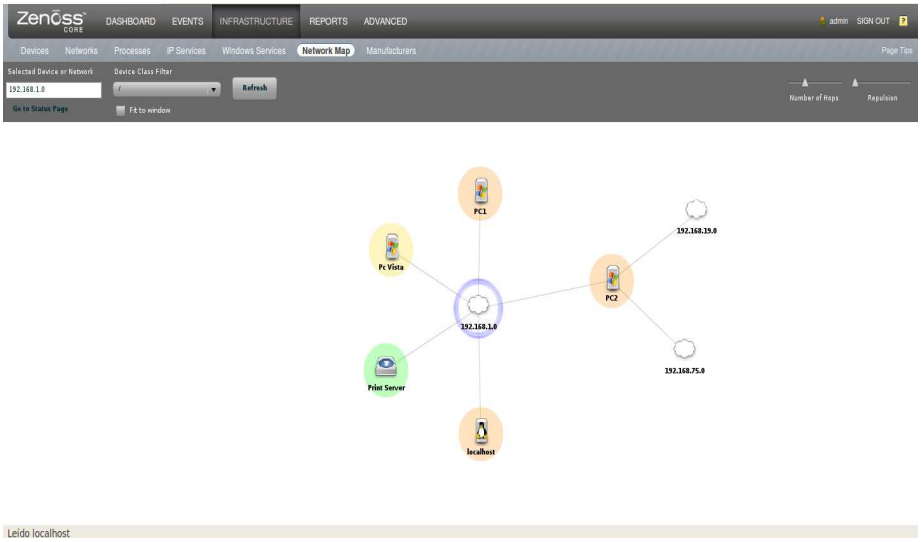


Figura III.37 : Network Map – Zenoss
Fuente: Investigador

En la pestaña de eventos nos muestra los eventos actuales que están ocurriendo en los distintos dispositivos, siendo estos, si el estado es crítico, warning, error, etc, además también nos brinda un historial de todos los eventos.

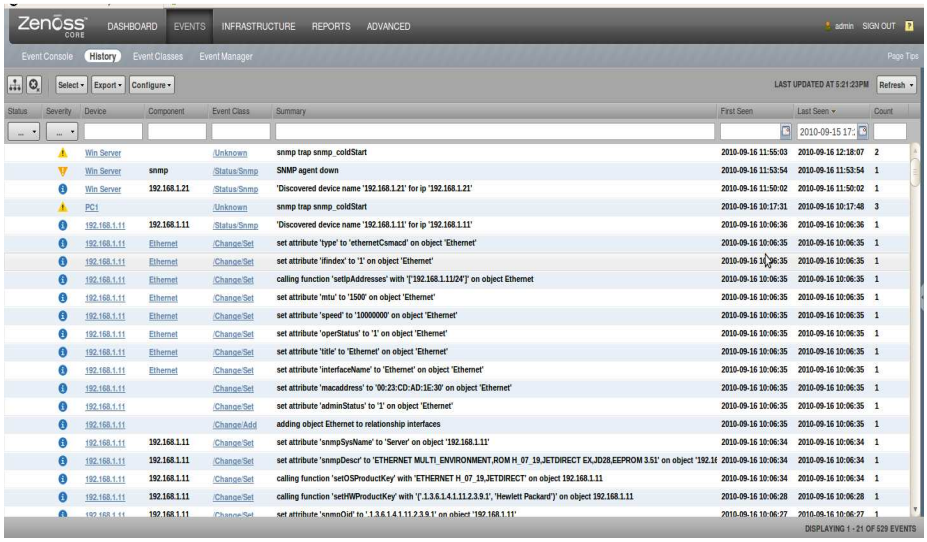


Figura III.38 : Historial de Eventos – Zenoss
Fuente: Investigador

La opción de Avanzados permite la configuración de la herramienta, administración usuarios, configuración de alarmas, etc.

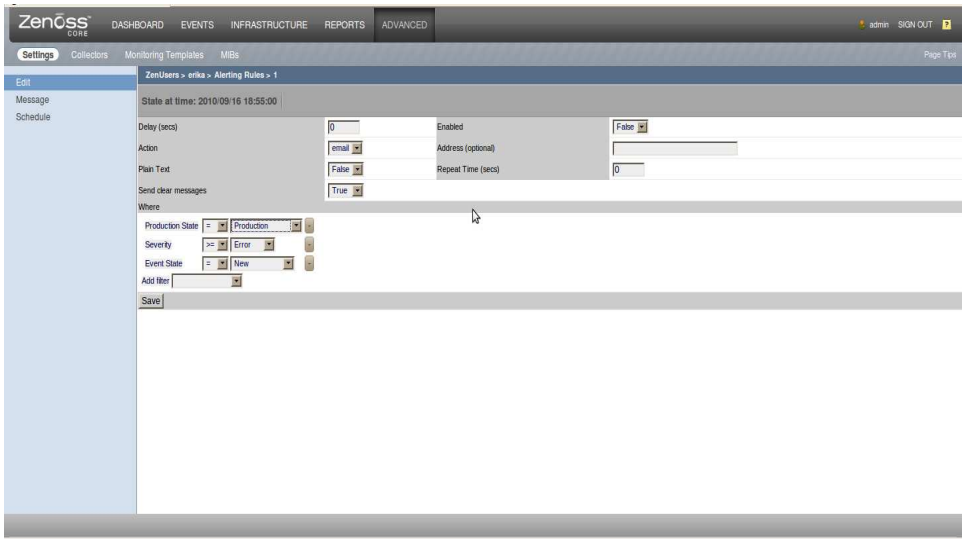


Figura III.39 : Configuración de Alarmas – Zenoss
Fuente: Investigador

Una vez configurados los dispositivos a ser monitoreados, se puede además obtener reportes de acuerdo a las necesidades del administrador o de la persona que se encuentre a cargo de esta funcion, siendo factibles la presentacion de informes de forma grafica o en forma de estadisticas, como se muestra en las figuras siguientes:

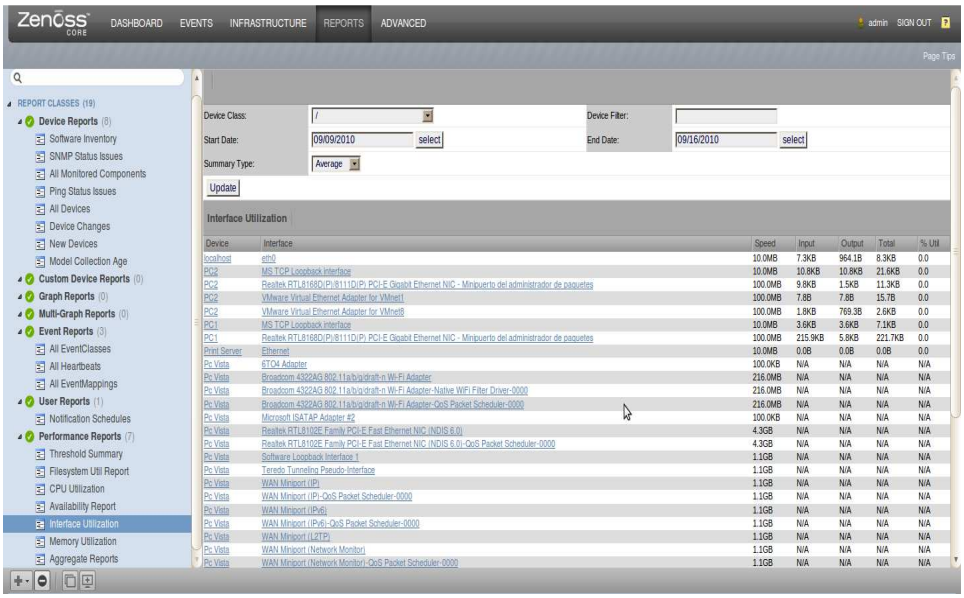


Figura III.40 : Reportes Estadísticos - Zenoss
Fuente: Investigador

3.4.3. Pruebas con la herramienta de Administración y Monitoreo ZABBIX

Abrimos un navegador web: **http://localhost/zabbix.** Tendremos una interfaz como la siguiente:

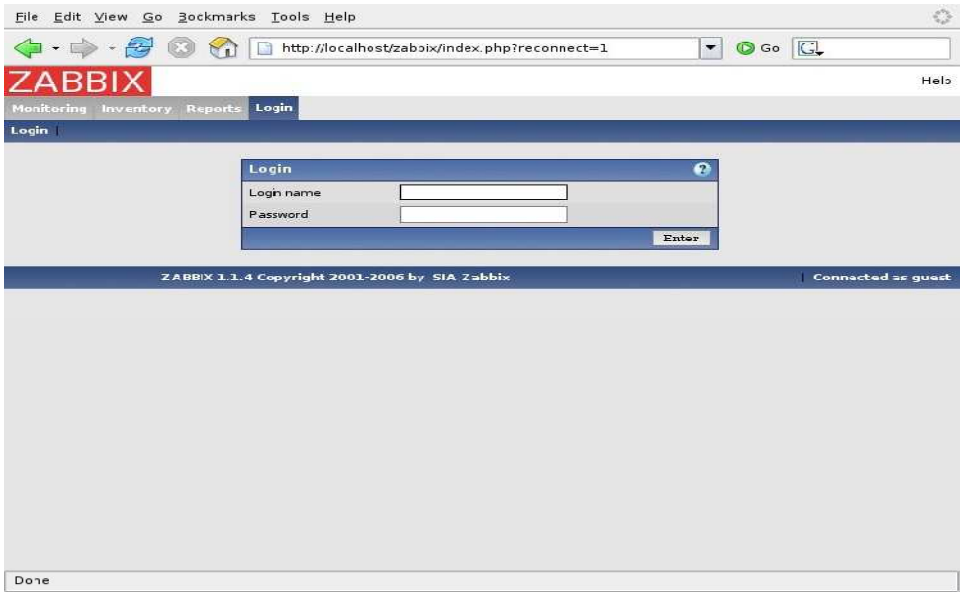


Figura III.41 : User Login – Zabbix
Fuente: Investigador

El usuario por defecto para hacer el login es admin y no tiene ninguna contraseña.

Es la interfaz inicial con la que arranca Zabbix:

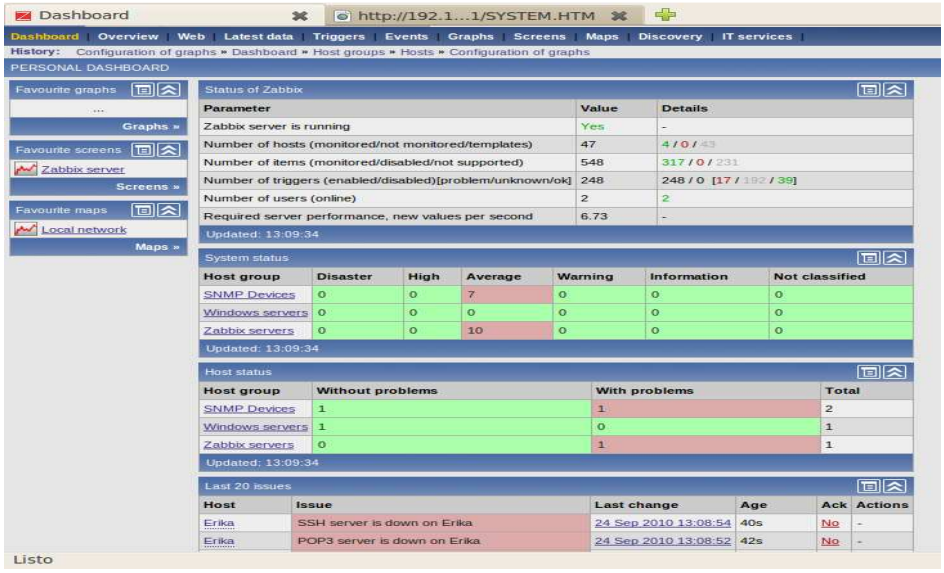


Figura III.42 : Dashboard – Zabbix
Fuente: Investigador

Para añadir un dispositivo es necesario ingresar toda la información que a continuación se muestra:

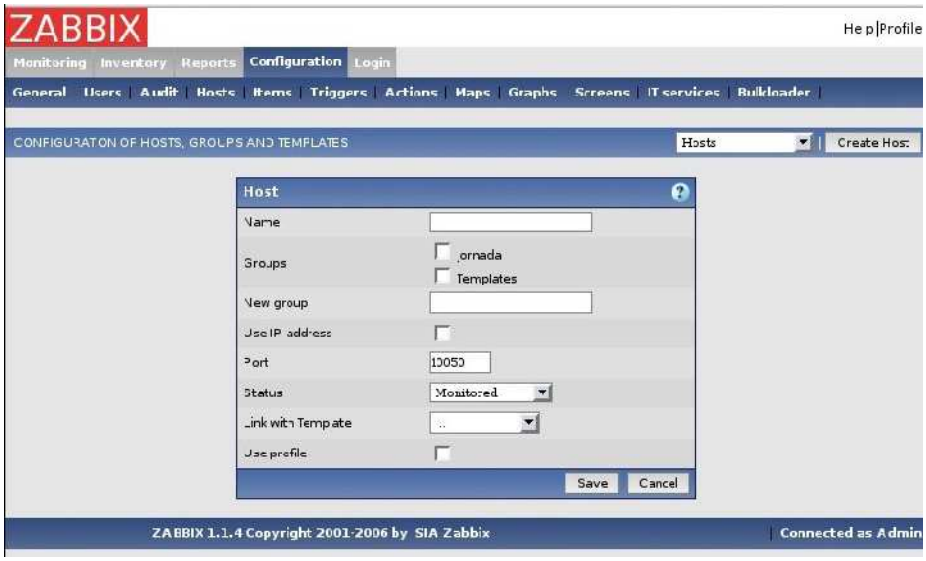


Figura III.43 : Añadiendo Host – Zabbix
Fuente: Investigador

Ahora, podemos ir a la pestaña de “Monitoring”, y visualizaremos los dispositivos añadidos y sus ítems.

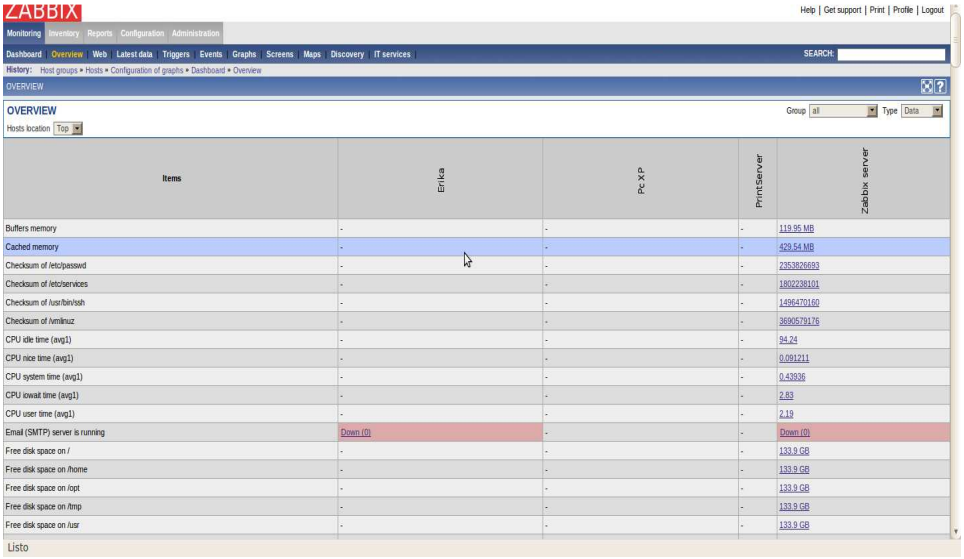


Figura III.44 : Pestaña Monitoring – Zabbix
Fuente: Investigador

Además en las opciones de "Graph" se muestra una gráfica con los resultados de un estado, como se muestran en las siguientes ilustraciones:

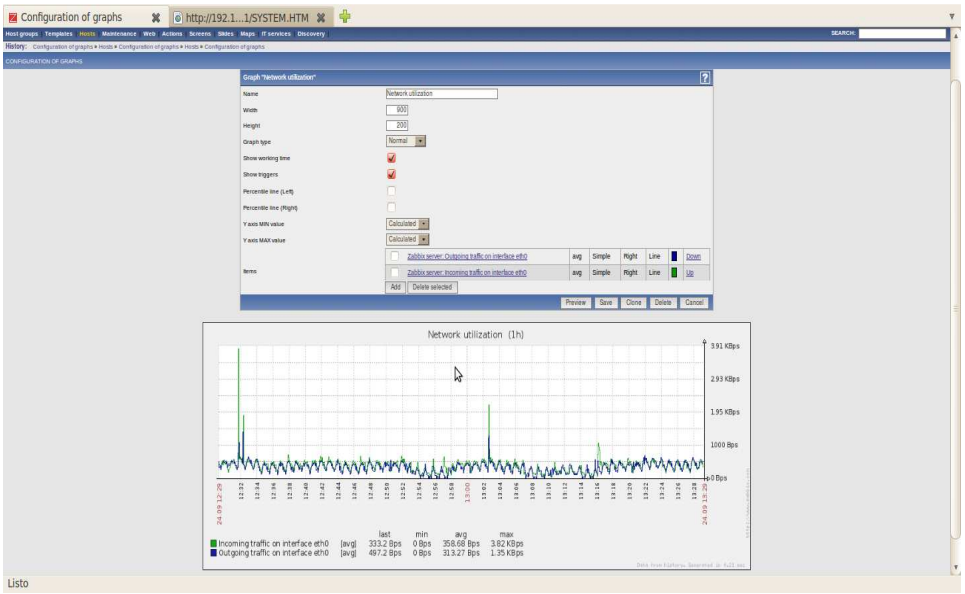


Figura III.45 : Utilización de la red – Zabbix
Fuente: Investigador

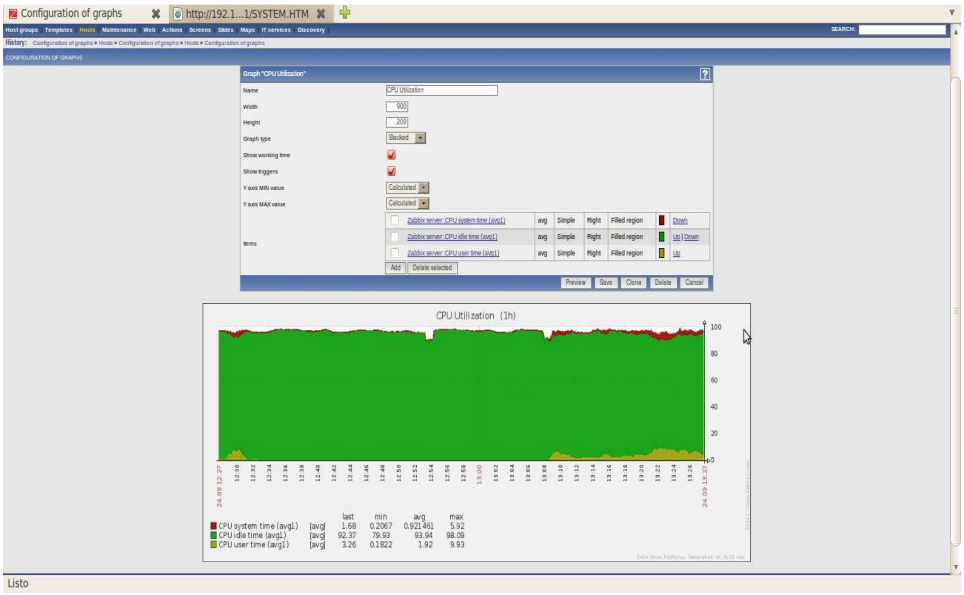


Figura III.46 : Utilización de CPU - Zabbix
Fuente: Investigador

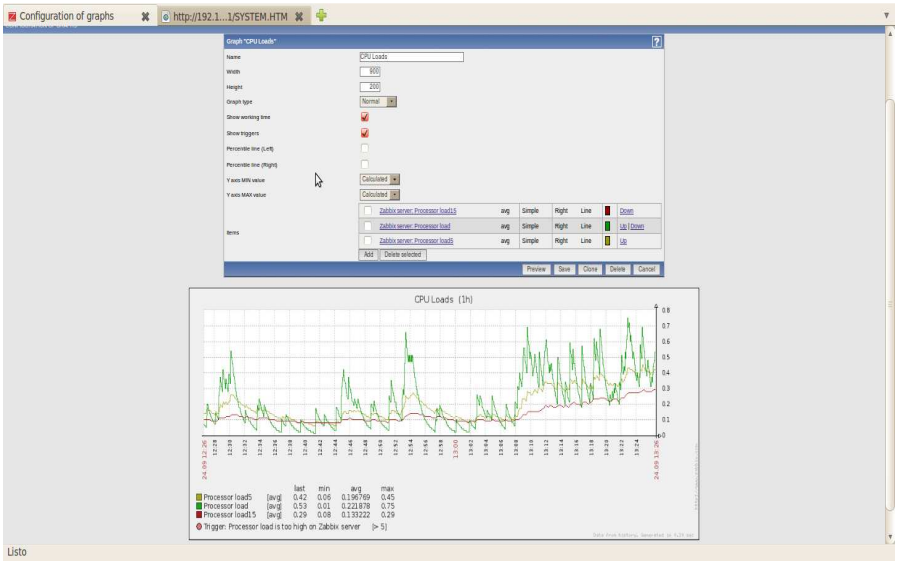


Figura III.47 : Carga CPU – Zabbix
Fuente: Investigador

En los reportes me muestra el estado de Zabbix server, el número de host monitoreados, numero usuarios, etc.

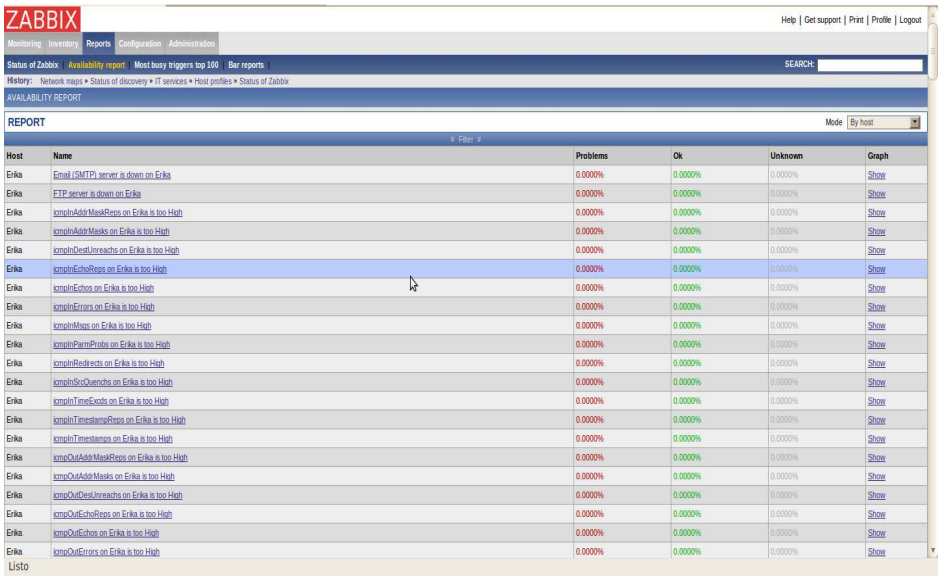


Figura III.48 : Reportes - Zabbix
Fuente: Investigador

3.5. Análisis comparativo de las herramientas de Administración y Monitoreo de Redes.

- **Usabilidad**

Herramienta de Administración	Facilidad de Uso	Intuitiva	Basado en Web	Interfaz Personalizable	Feedback a usuarios
CACTI	√	X	√	√	X
ZENOSS	√	√	√	√	√
ZABBIX	X	X	√	√	X

Herramienta de Administración	Valoración
Cacti	3
Zenoss	5
Zabbix	2

Tabla III.XV : Valoración del parámetro Usabilidad

Fuente: Investigador

- **Gestión de Usuarios**

Herramienta de Administración	Tipos de Usuario	Roles de Administración	Permisos a Usuarios	Grupos de Usuarios	Feedback a usuarios
CACTI	✓	X	✓	✓	X
ZENOSS	✓	✓	✓	✓	✓
ZABBIX	✓	✓	✓	✓	X

Herramienta de Administración	Valoración
Cacti	3
Zenoss	5
Zabbix	4

Tabla III.XVI : Valoración del parámetro Gestión de Usuarios

Fuente: Investigador

- **Recolección de Información en tiempo real**

Herramienta de Administración	5 minutos	3 minutos
CACTI	✓	X
ZENOSS	✓	X
ZABBIX	X	✓

Herramienta de Administración	Valoración
Cacti	4
Zenoss	4
Zabbix	5

Tabla III.XVII : Valoración del parámetro Recolección de información en tiempo real

Fuente: Investigador

- **Soporte**

Herramienta de Administración	Foros de Discusión	Mayor Comunidad activa	IRC	Noticias	Gratuito
CACTI	✓	**28820**	X	✓	✓
ZENOSS	✓	✓ **(75000)**	✓	✓	✓
ZABBIX	✓	**20914**	✓	✓	X

Herramienta de Administración	Valoración
Cacti	Muy Buena
Zenoss	Excelente
Zabbix	Buena

Tabla III.XVIII : Valoración del parámetro Soporte

Fuente: Investigador

- **Reportes**

Herramienta de Administración	Eventos	Históricos	Gráficos	Estadísticos	Alarmas Enviadas
CACTI	✓	X	✓	X	X
ZENOSS	✓	✓	✓	✓	✓
ZABBIX	✓	✓	✓	✓	X

Herramienta de Administración	Valoración
Cacti	2
Zenoss	5
Zabbix	4

Tabla III.XIX : Valoración del parámetro Reportes

Fuente: Investigador

- **Alertas**

Herramienta de Administración	Manejo de Eventos	Gravedad de Alerta	Umbral
CACTI	X	X	X
ZENOSS	✓	✓	✓
ZABBIX	✓	✓	✓

Herramienta de Administración	Valoración
Cacti	1
Zenoss	5
Zabbix	5

Tabla III.XX : Valoración del parámetro Alertas

Fuente: Investigador

- **Alarmas**

Herramienta de Administración	Correo Electrónico	SMS	Secuencia de Comandos	Jabber
CACTI	✓	X	X	X
ZENOSS	✓	✓	✓	✓
ZABBIX	✓	✓	✓	X

Herramienta de Administración	Valoración
Cacti	2
Zenoss	5
Zabbix	4

Tabla III.XXI : Valoración del parámetro Alarmas

Fuente: Investigador

- **Autodescubrimiento de Dispositivos**

Herramienta de Administración	Rangos IP	Redes	Autenticación (SSH, WINDOWS, SNMP)
CACTI	X	X	X
ZENOSS	✓	✓	✓
ZABBIX	✓	✓	X

Herramienta de Administración	Valoración
Cacti	1
Zenoss	5
Zabbix	4

Tabla III.XXII : Valoración del parámetro Auto-Descubrimiento de Dispositivos

Fuente: Investigador

- **Mapas**

Herramienta de Administración	Mapeo Automático de Dependencias	Estado de Dispositivos	Navegación	Visualización de Interfaces Virtuales
CACTI	X	X	X	X
ZENOSS	✓	✓	✓	✓
ZABBIX	X	✓	✓	X

Herramienta de Administración	Valoración
Cacti	1
Zenoss	5
Zabbix	3

Tabla III.XXIII : Valoración del parámetro Mapas

Fuente: Investigador

3.6. Resumen Comparativo

Con la finalidad de recopilar los resultados obtenidos en cada una de las tablas de los parámetros analizados entre las herramientas de Administración y Monitoreo de Redes se pone a consideración la siguiente tabla, de esta manera se podrá realizar la elección de una manera más clara y sencilla.

PARÁMETROS DE COMPARACIÓN	HERRAMIENTAS DE ADMINISTRACIÓN Y MONITOREO		
	Cacti	**Zenoss**	**Zabbix**
Usabilidad	3	5	2
Gestión de Usuarios	3	5	4
Recolección de Información en tiempo real	4	4	5
Soporte	Muy Bueno (4)	Excelente(5)	Bueno(3)
Reportes	2	5	4
Alertas	1	5	5
Alarmas	2	5	4
Autodescubrimiento de Dispositivos	1	5	4
Mapas	1	5	3
PROMEDIO /5	**2.33**	**4.88**	**3.77**

Tabla III.XXIV : Resumen Comparativo

Fuente: Investigador

3.7. Análisis de Resultados

Cálculo en Porcentaje de las calificaciones obtenidas

5 es el 100%

Cacti

5 100

2.33 *x*

$$\frac{2.33 \times 100}{5} = \mathbf{46.6\%}$$

Zenoss

5 100

4.88 *x*

$$\frac{4.88 \times 100}{5} = \mathbf{97.6\%}$$

Zabbix

5 100

3.77 *x*

$$\frac{3.77 \times 100}{5} = \mathbf{75.4\%}$$

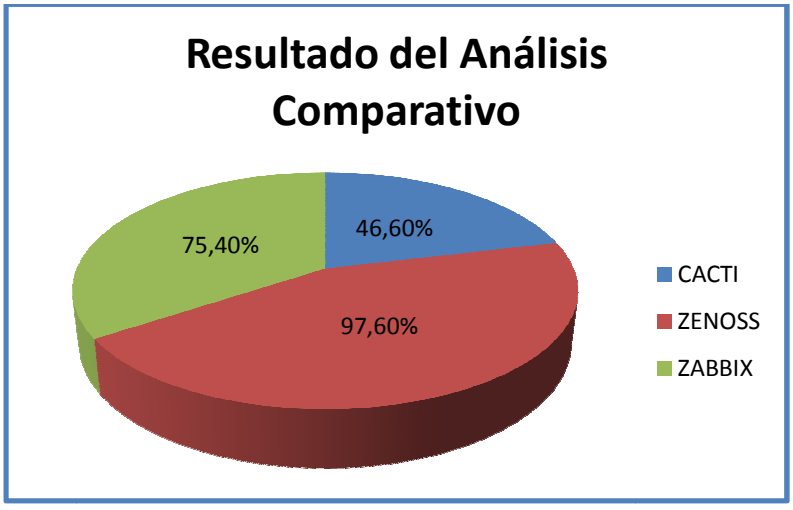


Figura III.49 : Resultado análisis comparativo

Fuente: Investigador

El resultado del análisis comparativo de Herramientas OpenSource basadas en SNMP para Administración y Monitoreo de redes: Cacti, Zenoss y Zabbix, ha arrojado como resultado que ***Zenoss*** con el ***97.6%*** es la herramienta de Administración y Monitoreo de Redes con mayores prestaciones y facilidades para implementar y dar solución a los requerimientos de la infraestructura que posee el Ilustre Municipio de Ambato.

A continuación se presentan conclusiones a las que hemos podidos llegar a través del análisis comparativo realizado:

- A pesar de que las herramientas Zenoss y Zabbix, alcanzan la mayor puntuación en el parámetro Usabilidad, ya que poseen similares características, existen diferencias indiscutibles en aspectos como manejo de interfaz, navegación, organización, en las que Zenoss es superior.

- En lo que se refiere a Gestión de Usuarios, aunque las tres herramientas analizadas poseen esta funcionalidad, hay que destacar que en Zenoss ésta función se la puede realizar de una manera más sencilla, además posee 3 tipos de usuarios con diferentes niveles de acceso.

- Al realizar las pruebas en el ambiente propuesto se puedo observar que el uso de Zenoss es más fácil, ya que no se necesitan realizar numerosas configuraciones, para obtener los resultados esperados.

- Zenoss cuenta con un extraordinario soporte, es la herramienta que cuenta con más miembros activos en su comunidad, mejorando indiscutiblemente el soporte a preguntas que se planteen en los foros, recibiendo respuestas casi inmediatas de las mismas.

- En los parámetros sobre alertas y alarmas aunque Zenoss y Zabbix poseen la característica de generar alertas cuando sobrepasen los límites de los umbrales establecidos, Zenoss realiza estas tarea de una forma superior, ya que si ocurre algún evento inesperado en la pantalla inicial de Zenoss nos va a desplegar el equipo en el cual se produjo, de una forma similar actúa en las alarmas si ocurre un evento grave este notifica inmediatamente al usuario encargado del dispositivo.

- Una de las características muy importantes es el parámetro del autodescubrimiento de los dispositivos, Zenoss facilita la tarea del administrador ya que con solo especificar el rango de la red que quiero obtener los dispositivos éste busca automáticamente, sin mayores especificaciones a diferencia de Zabbix que es la segunda herramienta en obtener mayor puntuación, que aunque posee la característica de realizar autodescubrimiento, éste no se lo realiza tan sencillo como en Zenoss.

- El parámetro de la generación de mapas de nuestra red, es un parámetro muy útil para ver la disposición de los dispositivos y que solo genera automáticamente Zenoss, por esta razón esta herramienta alcanza la mayor puntuación, a diferencia de Zabbix que es la otra herramienta que permite realizar mapas, pero con la gran diferencia que en esta herramienta el administrador debe ir generando su mapa.

CAPÍTULO IV

IMPLEMENTACIÓN DE LA HERRAMIENTA OPENSOURCE PARA LA ADMINISTRACIÓN Y MONITOREO DE RED BASADA EN SNMP, EN EL ILUSTRE MUNICIPIO DE AMBATO.

La implementación de la herramienta Zenoss se lo realizará en la plataforma Linux, distribución Ubuntu 10.04 ***(Ver Anexo 1)***.

4.1. Manipulación de la herramienta

Antes de iniciar con el proceso de monitoreo de los diferentes dispositivos, en la herramienta Zenoss, en cada uno de estos deben ser activados y configurados el protocolo SNMP ***(Ver Anexo 2).***

4.1.1. Agregar dispositivos a Zenoss

Zenoss descubre los dispositivos de las redes a las que pueda acceder con las diferentes referencias que estos le brinden, permitiendo al administrador de la red identificar y posteriormente administrarlos.

4.1.1.1. Agregar Dispositivos Manualmente

Zenoss ofrece la opción de agregar dispositivos en forma manual, permitiendo dar un formato específico y oportuno desde antes de escanear, ya que es posible incluirlo en una clase según su función, sistema operativo o fabricante e incluir plantillas a su monitoreo para obtener la información deseada de este, esta forma no suele ser la más optima ya que precisamente esos datos en ciertas ocasiones no se tienen por lo que se recurre a la opción de autodescubrimiento que explicaremos luego de hablar de esta.

1. En la barra de navegación, seleccione Infraestructura

2. Seleccione Agregar un dispositivo único 

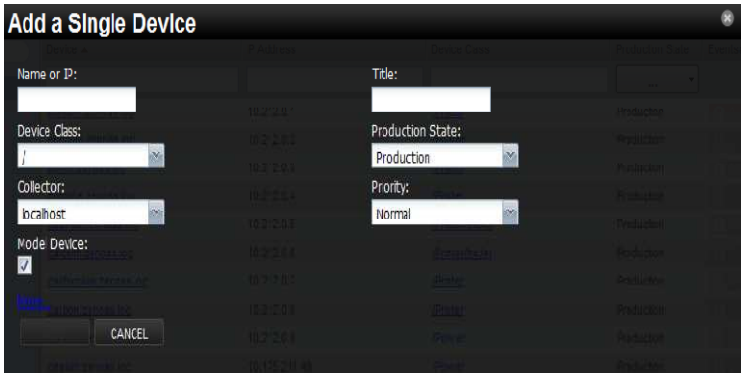


Figura IV.50 : Agregar dispositivos en Zenoss

Fuente: Investigador

3. Introduzca la información o hacer selecciones para añadir el dispositivo:

- ***Nombre o IP*** **-** Escriba la red (DNS) de nombre o la dirección IP del dispositivo.
- ***Clase de dispositivo*** - Seleccione una clase de dispositivo al que pertenece este dispositivo.

• ***Colector*** **-** Por defecto, este es el localhost.

• ***Modelo*** **-** Por defecto, esta opción está activada.

4. Opcionalmente, haga clic en **More** para mostrar campos adicionales:

• Introduzca los datos específicos del dispositivo

• Modificar la configuración de SNMP

Snmp Comunity: agregamos el password de la comunidad que el equipo tiene para entregar los datos de estado al ser monitoreado.

Snmp Port: dejamos el puerto por omisión 161.

• Establecer información de hardware y sistema operativo si se conoce

• Añadir comentarios dispositivo

5. Haga clic en Agregar.

Nota

Se puede ver el progreso de agregar dispositivos en JOBS. El Administrador de trabajo ejecuta tareas en segundo plano, como el descubrimiento de una red o la adición de un dispositivo. Cuando usted le pide al sistema llevar a cabo una de estas tareas, se agrega un trabajo a la cola.

En este punto podemos guardar los cambios y esperar a que Zenoss reconozca los datos agregados, si todo a finalizado satisfactoriamente Zenoss nos mostrará el dispositivo desde donde podremos ir al panel de manejo del dispositivo.

4.1.1.2. Añadir múltiples dispositivos

1. En la barra de navegación, seleccione Infraestructura.

2. Seleccione para agregar varios dispositivos de (Agregar dispositivos).

3. Para cada dispositivo que desea agregar, escriba el nombre de dominio completo o la dirección IP de un dispositivo de la red.

4. En el área de detalles, seleccione un tipo de dispositivo de la lista. Si el tipo de dispositivo no aparece, a continuación, utilice la opción predeterminada de selección.

5. Introduzca las credenciales adecuadas para la autenticación en el dispositivo.

6. Si desea agregar más de un dispositivo, haga clic en +.

7. Para agregar los dispositivos, haga clic en Enviar.

4.1.1.3. Descubrimiento de dispositivos

Ingresar la red o la dirección IP para que el sistema pueda descubrir los dispositivos.

1. En la barra de navegación, seleccione Infraestructura/agregar varios dispositivos

2. Seleccione la opción de detección automática los dispositivos.

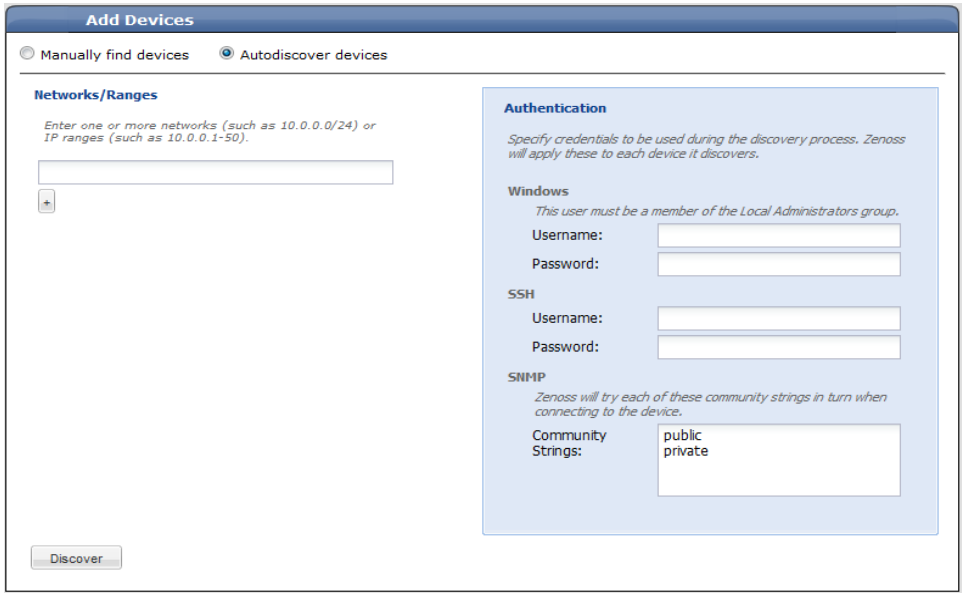


Figura IV.51 : Descubrimiento de dispositivos
Fuente: Investigador

Por ejemplo, puede introducir una dirección de red en notación CIDR: 10.175.211.0/24 o un rango de direcciones IP: 10.175.211.1-50

4.1.2. Trabajar con dispositivos

La lista de dispositivos muestra todos los dispositivos del sistema. Desde este punto de vista, puede buscar los dispositivos y realizar una amplia las tareas de gestión en todos los dispositivos.

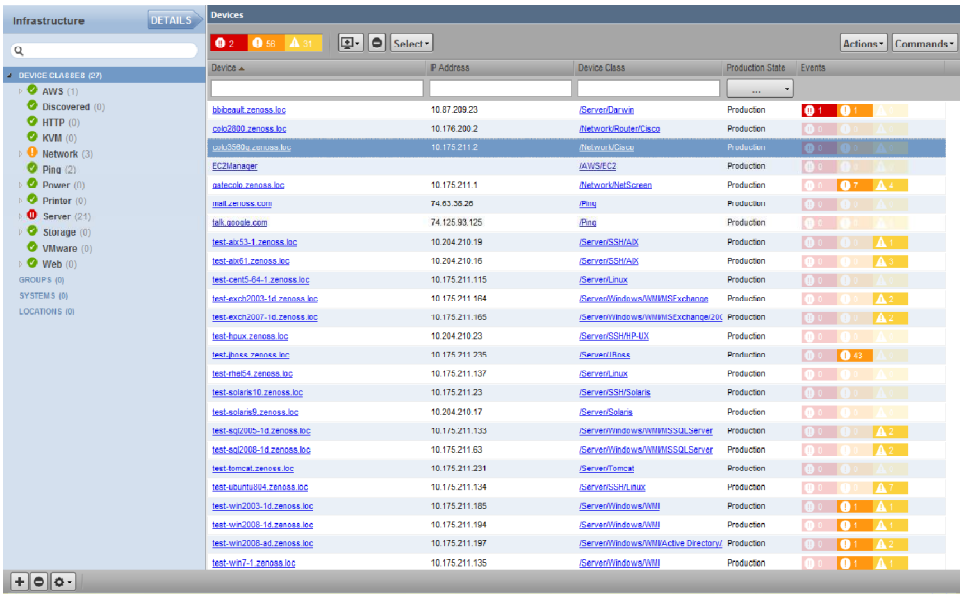


Figura IV.52 : Listado de dispositivos agregados
Fuente: Investigador

Los dispositivos se organizan en la vista de árbol por:

- Clase de dispositivo
- Grupo
- Sistema
- Ubicación

Para ver los detalles de un único dispositivo, haga clic en su nombre en la lista de dispositivos. La página de descripción de dispositivo.

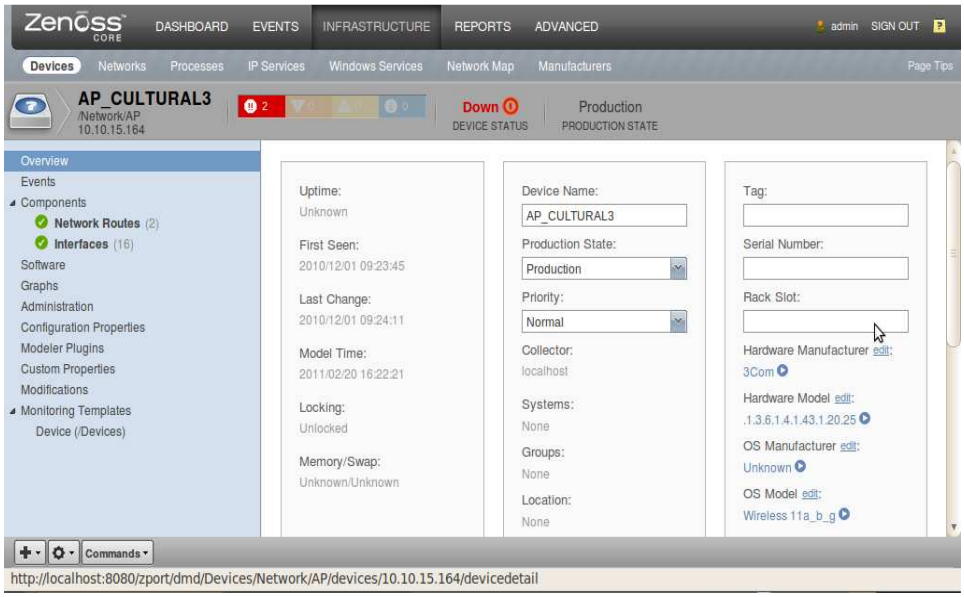


Figura IV.53 : Detalles de un único dispositivo en Zenoss
Fuente: Investigador

Estado del evento se muestra en el "arco iris de eventos" en la parte superior de la página.

Otra información clave que aparece en la parte superior de la página de resumen del dispositivo incluye:

• Nombre del dispositivo
• La dirección IP utilizada para comunicarse con el dispositivo
• Estado de dispositivo (se muestran los resultados actuales de una prueba de ping)
• Estado de producción (pre-producción, producción, prueba, mantenimiento, o se ha desechado).

El panel izquierdo de la página de descripción de dispositivo que permite acceder a otros puntos de vista de gestión de dispositivos, tales como:

4.1.2.1. Componentes

La vista de componentes proporciona información sobre los diferentes tipos de componentes del dispositivo, incluyendo:

- IPService
- WinService
- IpRouteEntry
- IpInterface
- CPU
- Sistema de archivos

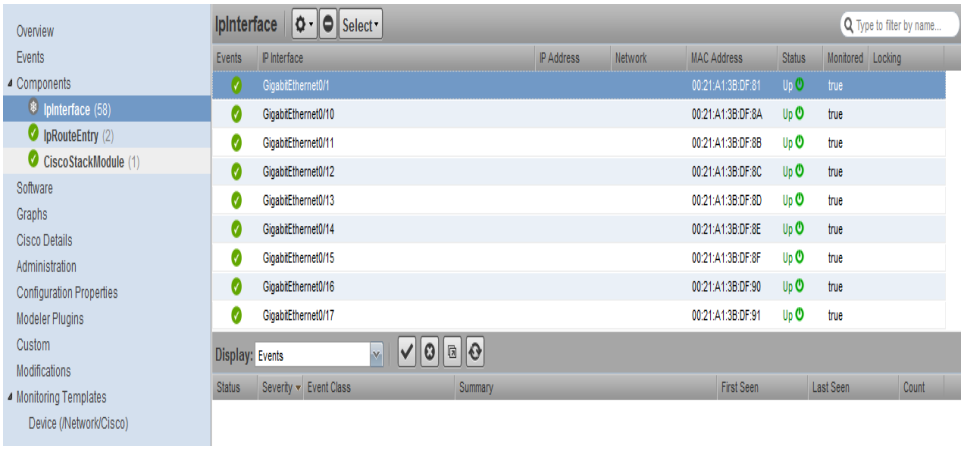


Figura IV.54 : Pestaña componentes
Fuente: Investigador

4.1.2.2. Software

Listas de software instalado en el dispositivo. Los datos facilitados en esta área dependerán del método utilizado para modelar el dispositivo. Lista de enlaces de software en el inventario del sistema de software en su infraestructura de TI.

4.1.2.3. Gráficos

Muestra los gráficos de rendimiento que se define para el dispositivo.

Figura IV.55 : Pestaña gráficos
Fuente: Investigador

Puede utilizar la tecla de flecha y los controles lupa a los lados de cada gráfico para cambiar el punto de vista gráfico, o desplazarse a través de un acercamiento o alejamiento de un gráfico.

Usted puede controlar estas opciones de gráfico de rendimiento:

Rango - Seleccione el período de tiempo que aparecen en el gráfico. Usted puede seleccionar:

- Horas - últimas 36 horas
- Diariamente - los pasados diez días.
- Semanal - últimas seis semanas
- Mensual - últimos 15 meses
- Anual - los dos últimos años

- Restablecer - Haga clic para volver a la predeterminada (vista inicial) de los gráficos.
- Vincular gráficos - Por defecto, todos los gráficos se mueven juntos.
- Stop / Start - para activar y desactivar la actualización automática de los gráficos (defecto, 300 segundos).

4.1.2.4. Administración

- Crear comandos personalizados del usuario y ejecutar comandos
- Gestión de ventanas de mantenimiento
- Determinar que tiene capacidades de administración para el dispositivo, y sus funciones.

Figura IV.56 : Pestaña administración
Fuente: Investigador

4.1.2.5. Propiedades de configuración

Puede configurar las propiedades de configuración de un dispositivo. Por otra parte, puede eliminar las propiedades locales desde un dispositivo.

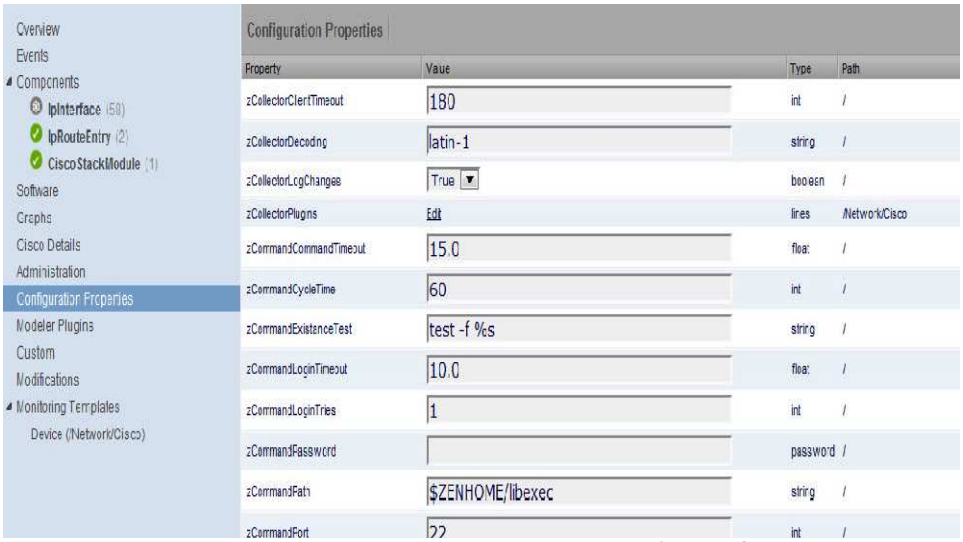


Figura IV.57 : Pestaña propiedades de configuración
Fuente: Investigador

4.1.3. Administración de dispositivos y atributos de dispositivos

4.1.3.1. Supervisión del Rendimiento

Zenoss utiliza varios métodos para controlar las estadísticas de rendimiento y componentes de los dispositivos. Estos son:

• ***ZenPerfSNMP*** - Recoge datos a través de SNMP desde cualquier dispositivo configurado correctamente para control a través de SNMP.

• ***ZenWinPerf*** (Enterprise) - ZenPack que permite la supervisión del rendimiento de los servidores de Windows.

• ***ZenCommand*** - Inicia sesión en dispositivos (mediante telnet o ssh) y ejecuta scripts para recopilar datos de rendimiento.

4.1.3.2. Información sobre la supervisión de Templates

Plantillas comprenden tres tipos de objetos:

- **Data Sources**- Especificar los puntos de datos exactos para recoger y el método a utilizar para recogerlos.
- **Thresholds**- Definir los límites previstos para los datos recogidos, y especificar los eventos que se creará si los datos no coinciden con los límites.
- **Graph Definitions**- Describir la forma de gráfico de los datos recogidos en los componentes del dispositivo.

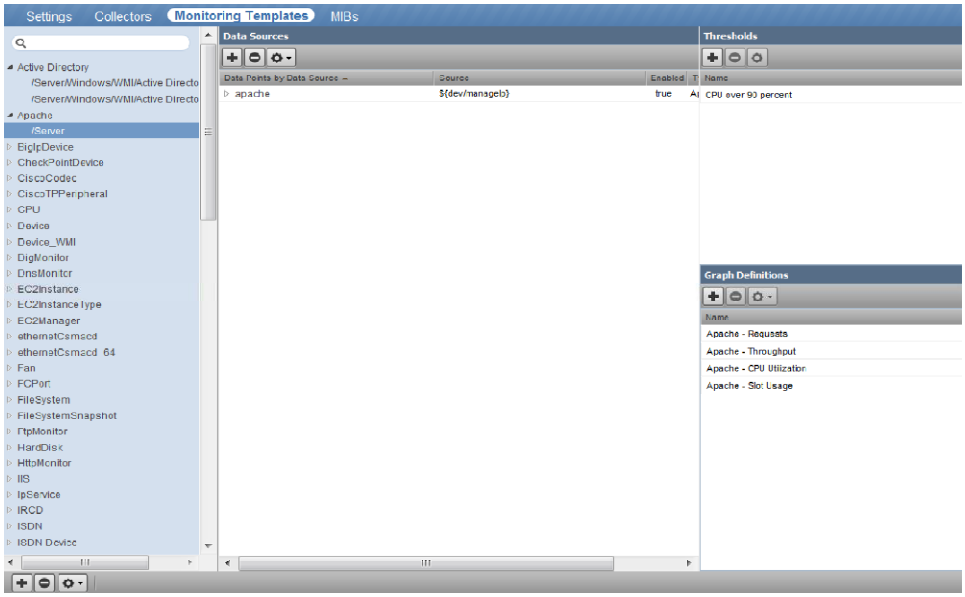


Figura IV.58 : Información sobre la supervisión de Templates
Fuente: Investigador

4.1.3.2.1. Binding Template

Antes de que el sistema pueda recopilar datos de rendimiento de un dispositivo o componente, se debe determinar qué plantillas se aplicará. Este proceso se denomina Binding Template.

Para editar las plantillas unido a un dispositivo:

1. En la barra de navegación, seleccione Infraestructura.

2. Seleccione un dispositivo en la lista de dispositivos. Seleccione ***Bind Templates* .**

3. Seleccione un template desde la lista habilitada y mueva al dispositivo

Figura IV.59 : Binding Templates
Fuente: Investigador

- **Data Sources**

Se especifican los puntos de datos para recopilar y cómo recogerlas. Cada plantilla de monitoreo comprende una o más fuentes de datos. El sistema proporciona dos tipos integrados de origen de datos: SNMP.

SNMP - Definir los datos que deben recogerse a través de SNMP por el demonio ZenPerfSNMP. Contienen un campo adicional para especificar qué OID SNMP para recolectar. (OID Muchas debe terminar en 0.0 para que funcione correctamente.) Debido a las fuentes de datos SNMP sólo especifica una métrica de rendimiento, que contienen un solo punto de datos.

Añadir un Data Source

1. Seleccione Avanzado en la barra de navegación, a continuación, seleccione Monitoring Templates.
2. En la vista de árbol, seleccione el Monitoring Template a la que desea agregar un Data Source.
3. En el área de Data Source, seleccione (Agregar origen de datos) en el menú Acción.
4. Escriba un nombre para el origen de datos y seleccionar el tipo y, a continuación, haga clic en Enviar.
5. Haga doble clic en el origen de datos en la lista.
6. Introduzca o seleccione los valores para definir el origen de datos.

- **Data Points**

Las fuentes de datos pueden devolver datos de una o más métricas de rendimiento. Cada métrica es representada por un punto de datos.

Añadir puntos de datos (Data Points)

1. Seleccione Avanzado en la barra de navegación, a continuación, seleccione Monitoring Template.
2. En el área de Data Sources, seleccione la fila que contiene un Data Sources.
3. Seleccione Agregar punto de datos en el menú Acción.
4. Escriba un nombre para el Data Point y, a continuación, haga clic en Enviar.
5. Haga doble clic en los datos que acaba de agregar. Introduzca la información o hacer selecciones para definir el punto de datos:

- **Thresholds**

Se definen los límites previstos para los Data Source. Cuando el valor devuelto por un punto de datos viola un Thresholds, el sistema crea un evento.

MinMax Thresholds

MinMax inspecciona los datos de entrada para determinar si se supera un máximo determinado o cae por debajo de un determinado mínimo. Puede utilizar un Thresholds MinMax para comprobar estos escenarios:

• El valor actual es inferior a un valor mínimo. Para ello, debe establecer sólo un valor mínimo para el Thresholds. Cualquier valor inferior a este número crea un evento de Thresholds.
• El valor actual es mayor que un valor máximo. Para ello, debe establecer sólo un valor máximo.
• El valor actual no es un número único, predefinido. Para ello, debe establecer el mínimo y máximo.

Añadir Thresholds

1. Seleccione Avanzado en la barra de navegación, a continuación, seleccione Plantillas de seguimiento.
2. En la zona de Thresholds, haga clic en (Añadir).
3. Seleccione el tipo de Thresholds y escriba un nombre y, a continuación, haga clic en Agregar.
4. Haga doble clic en el Thresholds que acaba de agregar en la lista para editar.

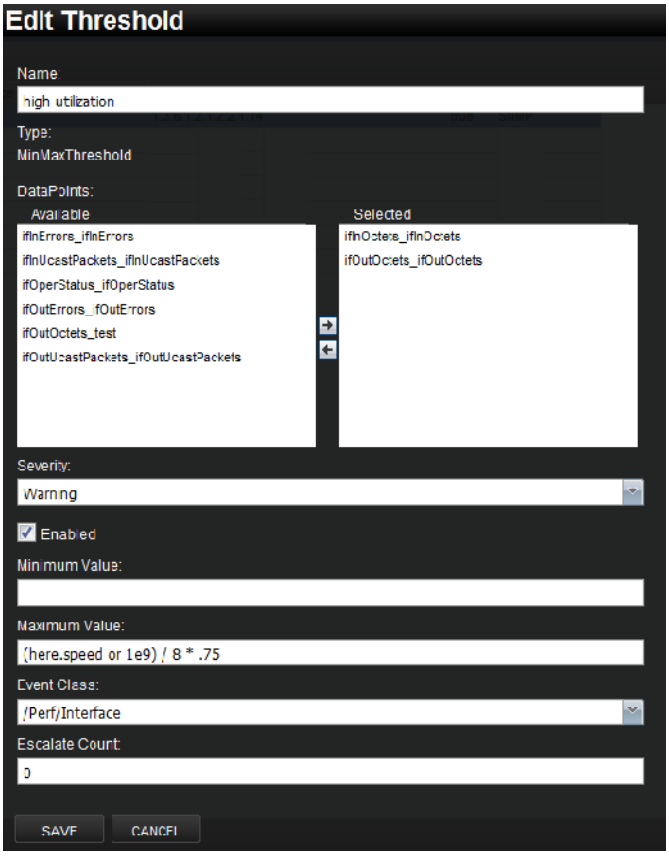


Figura IV.60 : Edición de Threshold
Fuente: Investigador

5. Introduzca o seleccione los valores para definir el Thresholds:

• *Nombre* - Muestra el valor de la ID que ha entrado en el diálogo Agregar un nuevo Thresholds.

• *Puntos de datos* - Seleccione uno o más puntos de datos a los que este Thresholds se aplicará.

• *Gravedad* - Seleccione el nivel de gravedad del primer evento desencadena cuando este Thresholds se rompe.

•*Activado* - Seleccione Verdadero para que el Thresholds se active, o Falso para desactivarlo.

• *Valor mínimo* - Si este campo contiene un valor, entonces cada vez que uno de los puntos de datos seleccione cae por debajo de este valor

se activa un evento. Este campo puede contener un número o una expresión de Python.

Cuando se utiliza una expresión Python, aquí la variable hace referencia al dispositivo o componente para el que existen datos están recogiendo. Por ejemplo, un umbral de 85% en una interfaz puede ser especificado como: here.speed * 0.85 / 8.

La división por 8 se debe a que la velocidad de interfaz con frecuencia se reporta en bits / segundo, cuando la interpretación datos bytes por segundo.

• *Valor máximo* - Si este campo contiene un valor, entonces cada vez que uno de los puntos de datos seleccionados pasa por encima este valor se activa un evento.
• *Clase de evento* - Seleccione la clase de evento del evento que se activa cuando este Thresholds se rompe.
• *Escala* - Introduzca el número de veces consecutivas este Thresholds puede romperse antes del evento la gravedad se aumenta en un paso.

- **Gráficos de rendimiento**

Puede incluir cualquiera de los Data Source o los Thresholds a partir de un Monitoring Templates en un gráfico de rendimiento.

1. Seleccione avanzado en la barra de navegación, a continuación, seleccione Monitoring Templates.
2. En el área de Grahp Definition, haga clic en (Ver gráfico).
3. Escriba un nombre para el gráfico y, a continuación, haga clic en Enviar.

4. Haga doble clic en el gráfico de la lista para editar. Introduzca la información o los valores de selección para definir el gráfico:

• ***Nombre*** - Si lo desea editar el nombre de la gráfica que ha entrado en la opción Agregar un cuadro de diálogo Nuevo gráfico. Este nombre aparece como el título de la gráfica.

• ***Altura*** - Introduzca la altura de la gráfica, en píxeles.

• ***Ancho*** - Introduzca el ancho de la gráfica, en píxeles.

• ***Unidades*** - Introduzca una etiqueta para el eje vertical del gráfico.

• ***Escala logarítmica*** - Seleccione Verdadero para indicar que la escala del eje vertical es logarítmica. Seleccione False (por defecto) para establecer la escala de lineal. Es posible que desee establecer el valor en True, por ejemplo, si los datos que se grafica crece exponencialmente. Sólo los datos positivos pueden ser graficados logarítmica.

• ***Base 1024*** - Seleccione si los datos que se gráfica se mide en múltiplos de 1024. De forma predeterminada, este el valor es False.

• ***Min Y*** - Introduzca el valor inferior para el eje vertical del gráfico.

• ***Max Y*** - Introduzca el valor superior para el eje vertical del gráfico.

•***Resumen*** - Seleccione True para mostrar un resumen de los datos actuales, la media, y valores máximos en la parte inferior de la gráfica.

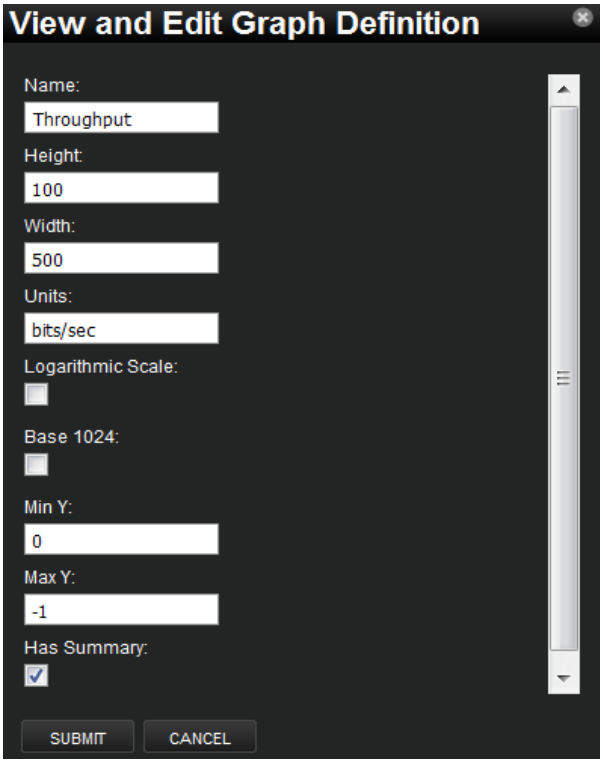


Figura IV.61 : Edición de gráficos de rendimiento
Fuente: Investigador

4.1.3.3. Comandos de usuario

Zenoss permite que los comandos se ejecuten en la interfaz de usuario basada en Web. Puede ejecutar comandos en un solo dispositivo o en un grupo de dispositivos. El sistema incluye varios comandos integrados, tales como ping y traceroute.

4.1.3.3.1. Definición de los comandos globales de usuario

Los comandos globales se encuentran en la lista de comandos de opciones en la parte superior de la página de dispositivos.

Para definir comandos globales de usuario:

1. Seleccione Opciones avanzadas
2. En el panel izquierdo, seleccione Comandos
3. En el área Definir Comandos, seleccione Agregar comando de usuario  (menú Acción).
4. Escriba un nombre para el comando y, a continuación, haga clic en Aceptar.
5. En el campo Descripción, escriba una descripción de lo que hará el comando.
6. En la sección de comandos, escriba la expresión del comando que desea ejecutar en el dispositivo.
7. Introduzca su contraseña de la cuenta del sistema de confirmación y, a continuación, haga clic en Guardar.

4.1.3.3.2. Ejecución de comandos globales del usuario

Para ejecutar un comando global de usuario, seleccionar uno o más dispositivos de la lista de dispositivos, a continuación, seleccione un comando de la lista de opciones de comandos.

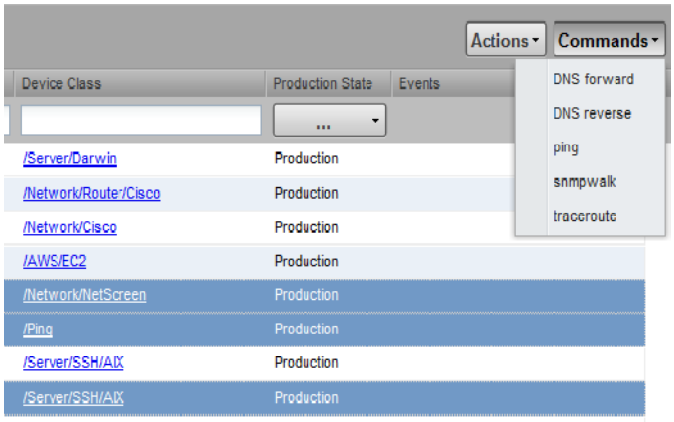


Figura IV.62 : Comandos globales de usuario
Fuente: Investigador

4.1.3.4. Administración de usuarios

Cuentas de Usuario

Cada usuario tiene un ID de usuario único, que le permite asignar permisos de grupo y las normas de alerta que son únicas para cada usuario. Identificadores únicos también ayudan a garantizar el acceso seguro al sistema.
Para crear y administrar cuentas de usuario, se debe estar registrado en la cuenta de administrador de sistema, o como un usuario con privilegios ampliados.

4.1.3.4.1. Creación de cuentas de usuario

Para crear una cuenta de usuario:

1. En la barra de navegación, seleccione Opciones avanzadas.
2. En el panel izquierdo, seleccione Usuarios.
3. Desde  (Menú Añadir), seleccione Agregar nuevo usuario.
4. En el campo Nombre de usuario, introduzca un nombre único para la cuenta.
5. En el campo Correo electrónico, escriba la dirección de correo electrónico para la cuenta de usuario. Cualquier alerta que ha configurado para este usuario será enviado a esta dirección.
6. Haga clic en Aceptar.

Después de crear la cuenta, editar la cuenta para proporcionar una contraseña y los datos de usuario adicionales.

4.1.3.4.2. Asociación de objetos con usuarios específicos

Puede asociar cualquier objeto en el sistema con un usuario en particular, para el seguimiento o informes. Una vez asociada a un usuario, a continuación, puede asignar al usuario una función específica que se aplica a sus privilegios con respecto a ese objeto.

Para crear una asociación de objetos:

1. Desde Opciones avanzadas, seleccione los objetos administrados en el panel de la izquierda.

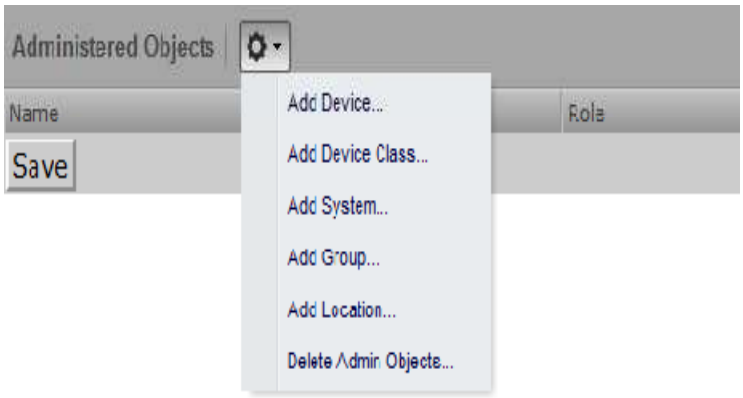


Figura IV.63 : Asociación de un objeto a un usuario
Fuente: Investigador

2. Seleccione un tipo de objeto en el menú de objetos administrados por la acción. Se puede agregar:

   • Dispositivo
   • Clase de dispositivo
   • Sistema
   • Grupo
   • Ubicación

3. Especificar el componente que desea añadir como un objeto administrado y, a continuación, haga clic en Aceptar.

4. Haga clic en Guardar para guardar los cambios.

4.1.3.4.3. Grupos de usuarios

Zenoss permite crear grupos de usuarios. Por grupo de usuarios, se puede agregar reglas y aplicarlas a través de varias cuentas de usuario.

Creación de grupos de usuarios

1. Seleccione Avanzado.
2. En el panel izquierdo, seleccione Usuarios
3. Desde el área de menú Grupos de Acción, seleccione Agregar nuevo grupo.
4. En el campo de grupo, escriba un nombre para este grupo de usuarios, a continuación, haga clic en Aceptar.
5. Haga clic en el nombre del grupo que ha creado.
6. En el menú Acción, seleccione Agregar usuario.

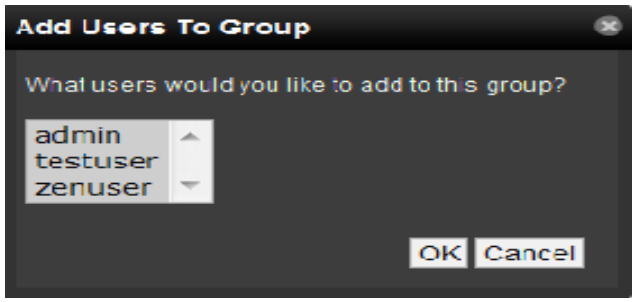


Figura IV.64 : Creación de grupos de usuarios

Fuente: Investigador

7. En la lista de las selecciones del usuario, seleccionar uno o más usuarios que desea añadir al grupo y, a continuación, haga clic en Aceptar.

El usuario o usuarios que seleccione aparecerán en la lista de usuarios para este grupo.

4.1.3.5. Configuración de alarmas

Alarmas

Este servicio es proporcionado por ZenActions, quien permite enviar mensajes de correo electrónico o páginas basadas en acontecimientos, más conocidas como SendPage.

SendMail

Como su nombre lo indica, es utilizado para generar alarmas por correo electrónico para esto, debemos tener configurado un servidor de correo. Una vez se cuente con este pre-requisito debemos ir a **Setting,** ubicado en el menú principal.

Adicionalmente Zenoss ofrece un sistema de aviso a los correos que se configuren en los diferentes usuarios agregados a Zenoss, la forma para configurarlo se explica a continuación.

1. En primer lugar debemos tener configurado un servidor de correo en la red para que podamos usarlo como almacenador de correos enviados por Zenoss o en su defecto reenvíen la petición a servidores externos, suponiendo que si poseemos el servidor de correos interno, comenzamos llenado los campos que hacen referencia a este en la pestaña “Settings” del panel izquierdo, donde se nos pide la dirección IP del servidor de correo y un nombre para

que Zenoss envíe correos a un usuario valido del servidor, (guardamos los cambios “save”).

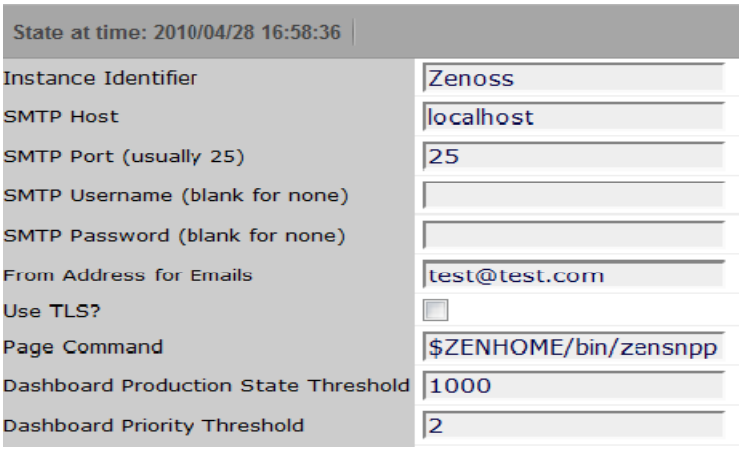


Figura IV.65 : Ingreso de datos del Servidor de Correo

Fuente: Investigador

2. En la sección “User” en esta misma interfaz entramos al usuario agregado por omisión admin, Este usuario puede cambiar según nuestra configuración de usuarios administradores.
3. Al ingresar a la consola de este usuario llenaremos el formulario según nuestras necesidades, aquí especificamos una dirección e-mail valida en el servidor de correo, a la cual le llegaran los avisos enviados por Zenoss.
4. Por último hacemos el (test) del correo para verificar que hemos hecho una adecuada configuración, dando clic en (test) y si todo ha salido bien nos saldrá un mensaje de “test send” de lo contrario saldrá “test failed” y debemos revisar los anteriores pasos.

Una vez la prueba resulte exitosa, damos clic sobre el usuario **Admin** para configurar las alarmas. Después observamos algunas pestañas para configurar la información del administrador, ver eventos y Administrar objetos. Damos click en **Alerting Rules** y posteriormente en **Add Alerting Rule**

Figura IV.66 : Adición de reglas de alerta
Fuente: Investigador

Una vez la alerta se encuentre listada, damos click sobre ella, luego encontramos tres pestañas. En la pestaña **Edit** encontramos algunos campos importantes para la configuración:

- **Enabled:** Este parámetro debe aparecer como verdadero (True)

- **Address:** En este parámetro debemos introducir el mail del administrador o persona que recibirá los mail.

- **Actions:** La acción por defecto en este caso es email, ya que la alarma que se está utilizando es la SendMail.

Luego debemos configurar algunas reglas, esta configuración es personal y va de acuerdo a las necesidades del administrador. Por último guardamos los cambios.

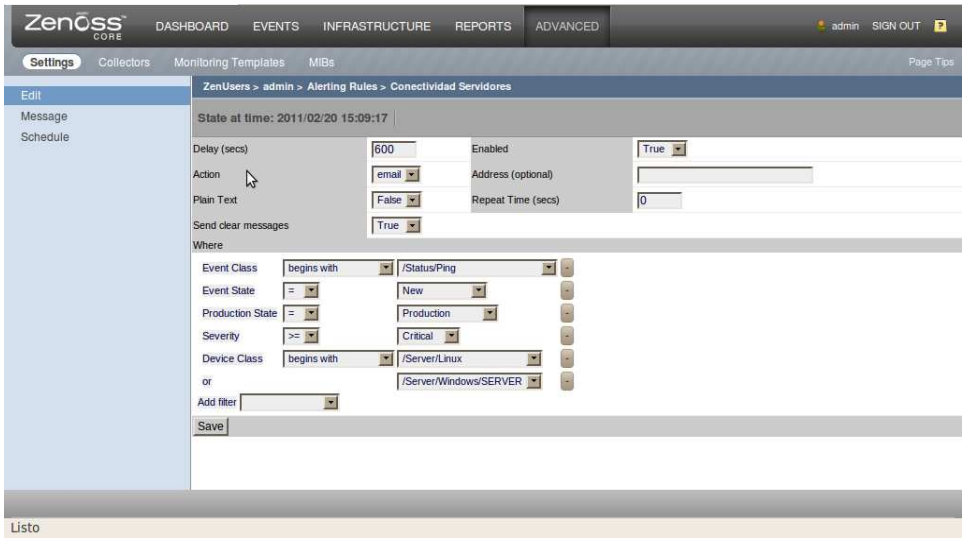


Figura IV.67 : Configuración de reglas para alarmas
Fuente: Investigador

Mensajes

Durante la edición de nuestro estado de alerta, tenemos la posibilidad de personalizar el texto del mensaje de alerta que envía Zenoss. Para ver el mensaje, haga clic en la ficha Mensaje. Los "Campos de formato del mensaje es una cadena de formato Python. Se especifican% (nombre de campo) s."

Schedule

Podemos establecer una programación para cada regla de alerta para que el sistema envíe alertas sólo durante el período especificado.

4.1.4. Reportes

El sistema proporciona una serie de opciones definidas de informes personalizados, que incluye:

- Reportes de dispositivos
- Reportes de eventos
- Reportes de rendimiento

- Reportes de usuario
- Reportes Gráficos
- Reportes personalizados de dispositivos

Para trabajar con los reportes, seleccione Reportes en la barra de navegación. La lista de los reportes aparece en la vista de árbol. Expandir un elemento de la lista para ver los reportes disponibles en esa categoría.

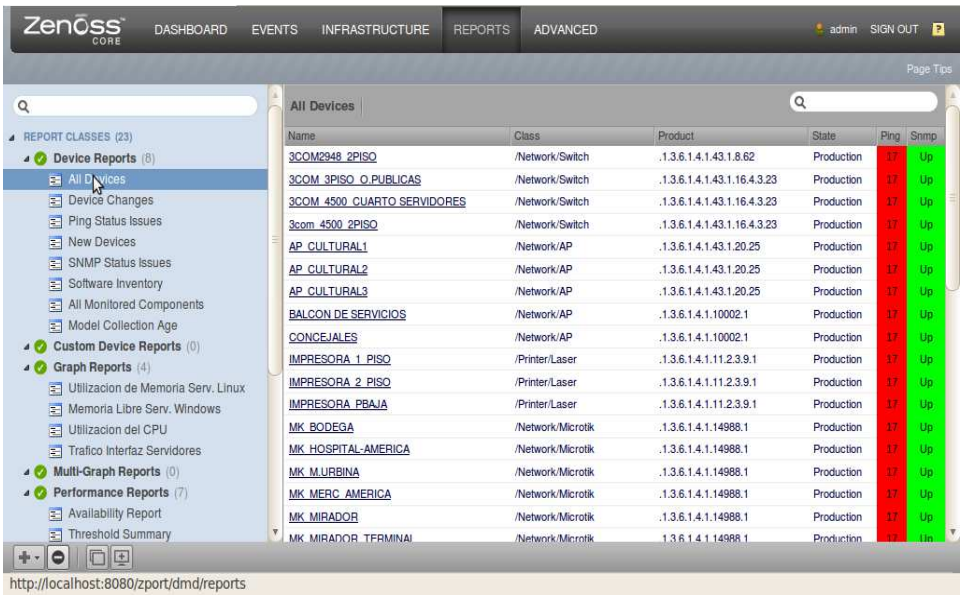


Figura IV.68 : Listado de reportes disponibles en Zenoss

Fuente: Investigador

4.1.4.1. Reporte de Dispositivos

Reporte de dispositivos agregados. Los reportes de esta categoría incluyen:

- Todos los dispositivos - Lista todos los dispositivos con el estado del ping y la información SNMP.
- Todos los componentes monitoreados - Muestra todos los componentes que actualmente se está supervisando. Esto no incluye todos los

componentes del sistema, sólo aquellos en los que el sistema está actualmente recopilando los datos de rendimiento.

- Los cambios de dispositivos - Muestra información sobre el historial de los cambios que el sistema detecta cuando se modela cada dispositivo. Si el modelo de un dispositivo tiene un estado de producción mayor que 0 y no ha sido actualizado durante 48 horas, este se presenta en el reporte.
- Dispositivos Conocidos – Lista los dispositivos que no han cambiado durante las últimas 48 horas.
- Nuevos dispositivos - Enumera los dispositivos que se han añadido recientemente.
- Estado del Ping - Enumera los dispositivos que actualmente tienen, o han tenido problemas de ping.
- Estado de SNMP - Enumera los dispositivos que actualmente tienen, o han tenido problemas de SNMP.
- Inventario de software – lista de software que se ejecutan en los dispositivos.

4.1.4.2. Reporte de Eventos

Datos agregados sobre los eventos, asignaciones de eventos y clases de eventos. Para cada clase de evento, el informe incluye el número de subclases, instancias de la clase dentro del sistema, y el número de eventos del sistema actual.

- Todas las clases de eventos - Muestra todas las clases de eventos que residen en el sistema. El informe abre estas clases por sub-clases, el número de casos de esa clase en el sistema, y el número de eventos en el sistema asociado a cada clase de evento.

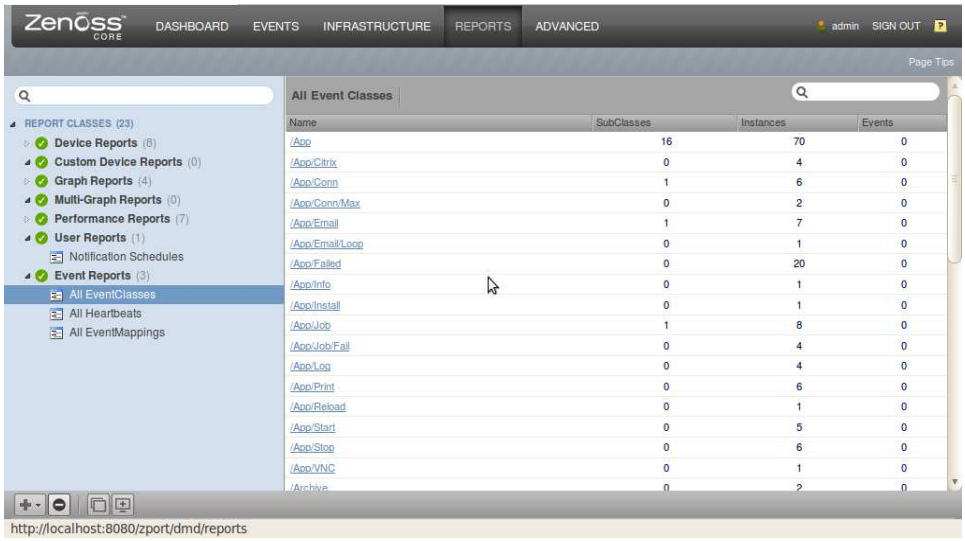


Figura IV.69 : Reportes de todas las clases de eventos – All EventClasses
Fuente: Investigador

- Heartbeats - Vigila el estado de los demonios de Zenoss, y muestra un informe de la lista de fracasos que tuvieron los dispositivos. En el informe, la columna de componentes corresponde a los demonios disponibles, tales como zenactions y zenstatus. El informe proporciona la duración de la falta de pulso en segundos.

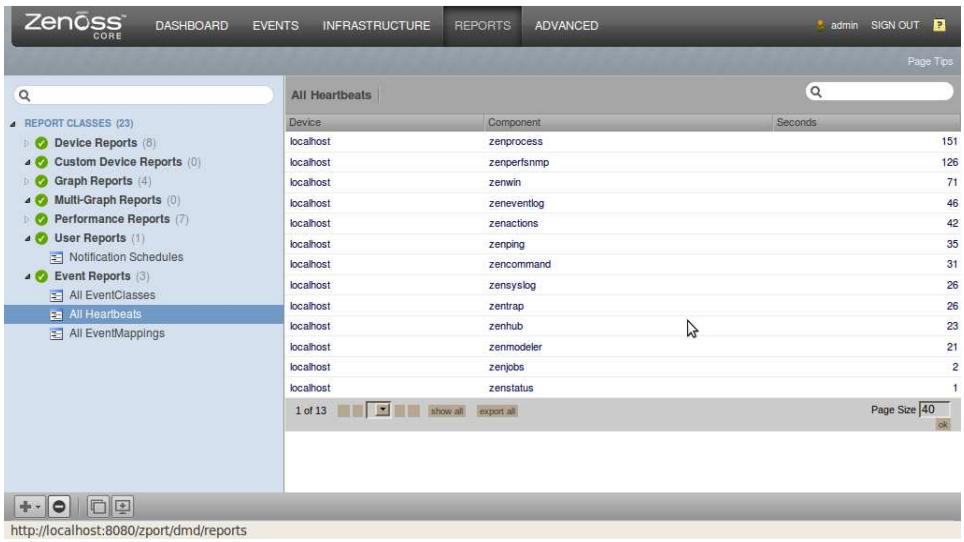


Figura IV.70 : Reportes del estado de los demonios - All Heartbeats
Fuente: Investigador

- Todas las asignaciones de eventos - Muestra todas las asignaciones de eventos definidos actualmente en el sistema de Zenoss.

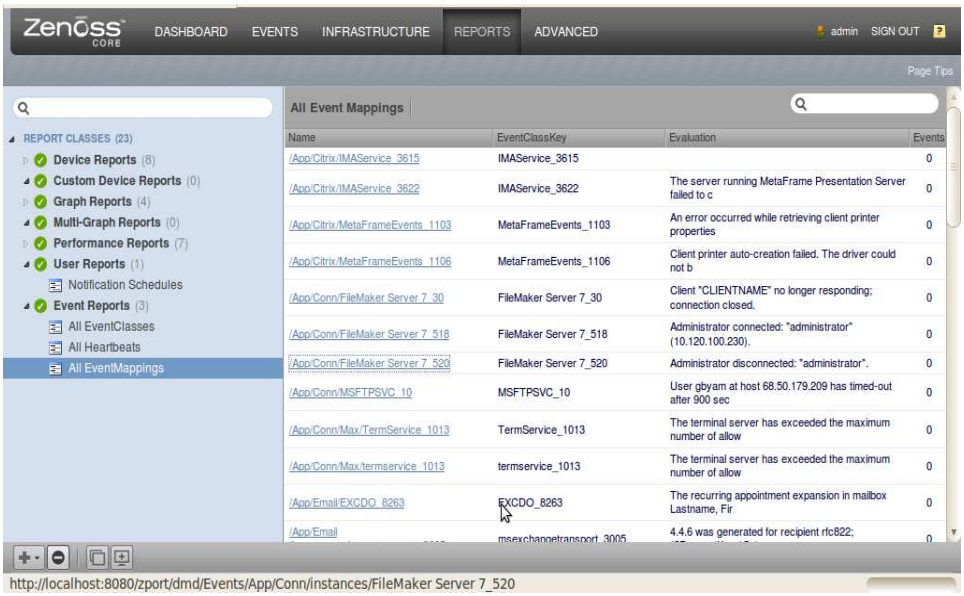


Figura IV.71 : Reportes de Asignaciones de Eventos – EventMappings

Fuente: Investigador

4.1.4.3. Reportes de Rendimiento

Los reportes de rendimiento proporcionan los datos de rendimiento en todo el sistema. Incluyen una mezcla de gráficos e informes basados en texto:

Total de Informes – Muestra los gráficos de rendimiento de los dispositivos del sistema, en formato gráfico, combinan datos de todos los dispositivos en un solo gráfico para cada medida. Comúnmente las estadísticas de rendimiento incluyen:

- El uso del CPU
- Total de memoria libre
- Total de memoria swap libre

- Tráfico de red de entrada y salida

Haga clic en la gráfica para editar los parámetros de gráfico. Usted puede:

- Cambiar los valores para la anchura, altura, Min Y, y el eje Y Max.
- Especificar los dispositivos que se agregan
- Ajustar el intervalo de tiempo de la gráfica

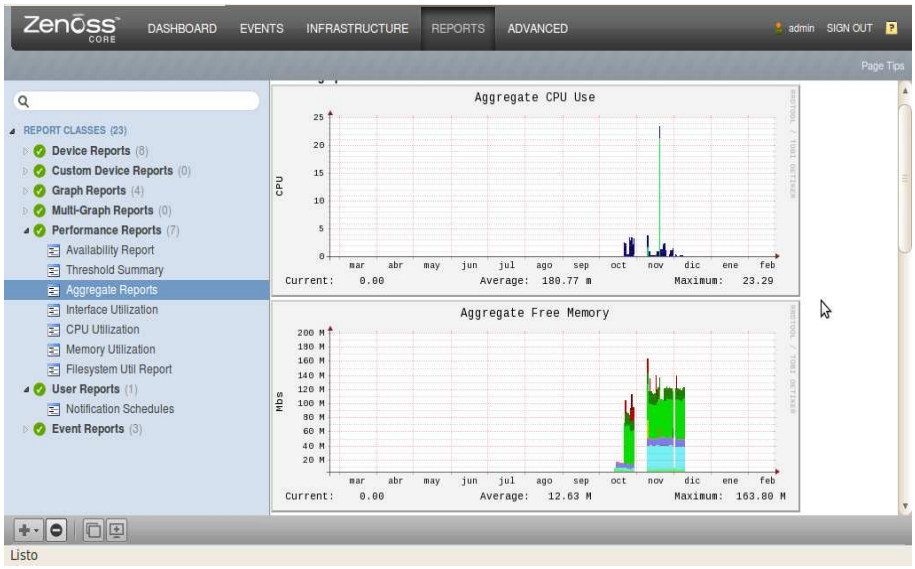


Figura IV.72 : Reportes Gráficos

Fuente: Investigador

Reporte de Disponibilidad - Muestra el porcentaje de tiempo que un dispositivo o componente se considera disponible. Se puede filtrar este informe por el dispositivo, componente, clase de evento, o la gravedad. También se puede limitar aún más los plazos de la disponibilidad.

Los reportes por defecto nos da el porcentaje de disponibilidad de los últimos siete días para la clase de evento Status/Ping con un nivel de severidad de error. Podemos cambiar los criterios de presentación de informes sobre la base de las siguientes opciones:

Filtro	Descripción
Dispositivo	Escriba un nombre de dispositivo para limitar el informe a un solo dispositivo.
Componente	Escriba un nombre de componente en la ficha del dispositivo del sistema operativo. Zenoss devuelve los dispositivos que coinciden con el componente especificado.
Fecha de Inicio	Especifique el primer día del informe.
Fecha de Finalización	Especifique el último día del informe.
Clase de Evento	Seleccione el tipo de evento para informar. Por ejemplo: / Status / SNMP.
Severidad	Seleccione la gravedad de los eventos de utilizar en el cálculo de disponibilidad

Tabla IV.XXV : Criterios de presentación de informes.
Fuente: Investigador

Después de que introduzca los criterios del reporte, puede hacer clic en el botón Actualizar para ver el nuevo informe.

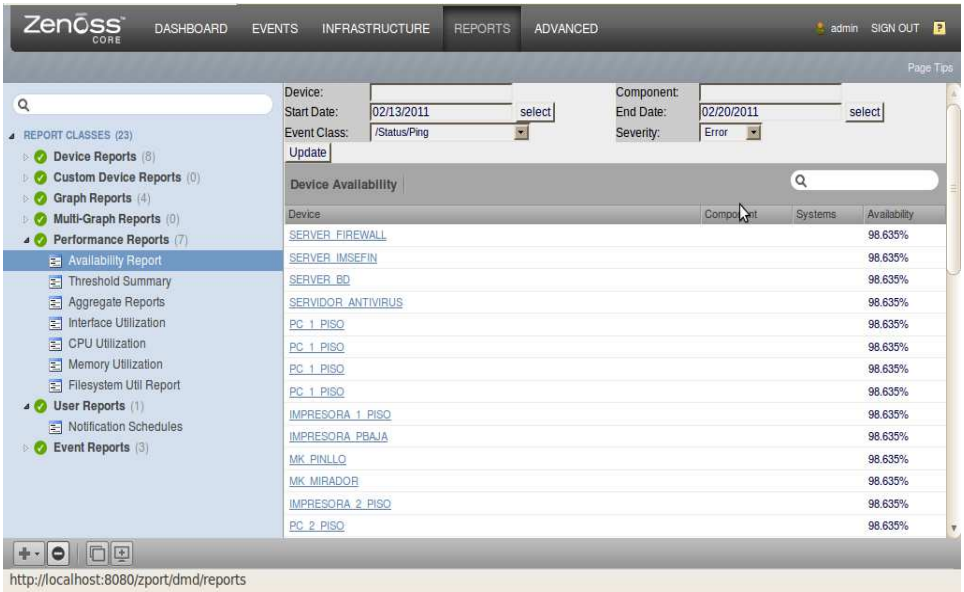


Figura IV.73 : Reporte de disponibilidad
Fuente: Investigador

Reporte de de utilización de la CPU - Proporciona el promedio de carga y el porcentaje de utilización de cada dispositivo. Si Zenoss no puede recopilar las estadísticas de rendimiento de la CPU para un dispositivo, el promedio de carga y los valores de porcentaje de utilización se muestran como "N / A". Usted puede personalizar fechas de inicio y fin, y el tipo de resumen (media o máxima).

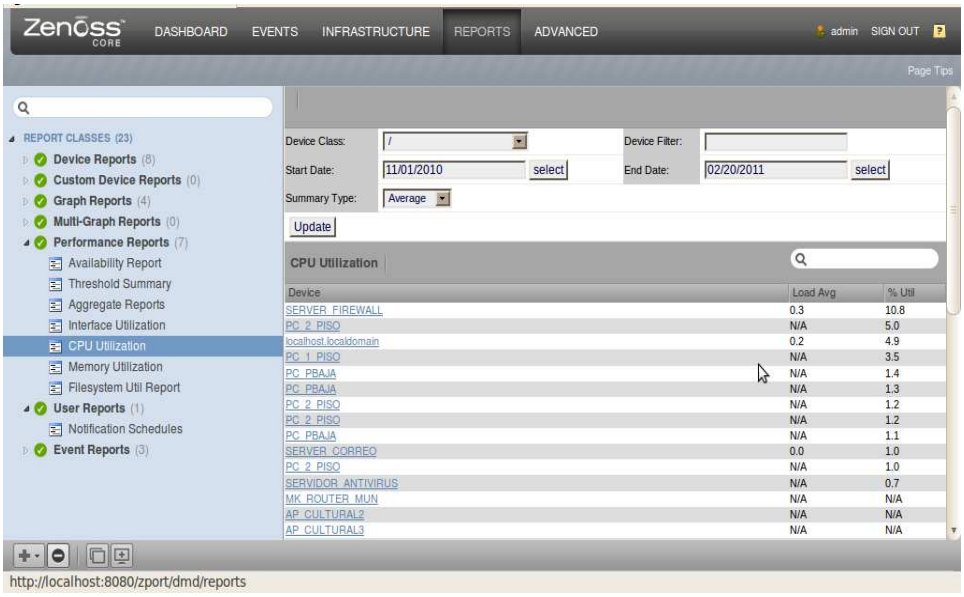


Figura IV.74 : Reporte de Utilización del CPU
Fuente: Investigador

Reporte de utilización del sistema de archivos - Para cada punto de montaje de cada sistema de archivo el reporte incluye: total de bytes, bytes utilizados, bytes libres, y el porcentaje de utilización para cada dispositivo. Puede personalizar las fechas de inicio y fin, y el tipo de resumen (media o máxima). Si Zenoss no sabe un valor, rellena el informe de los valores con "N / A".

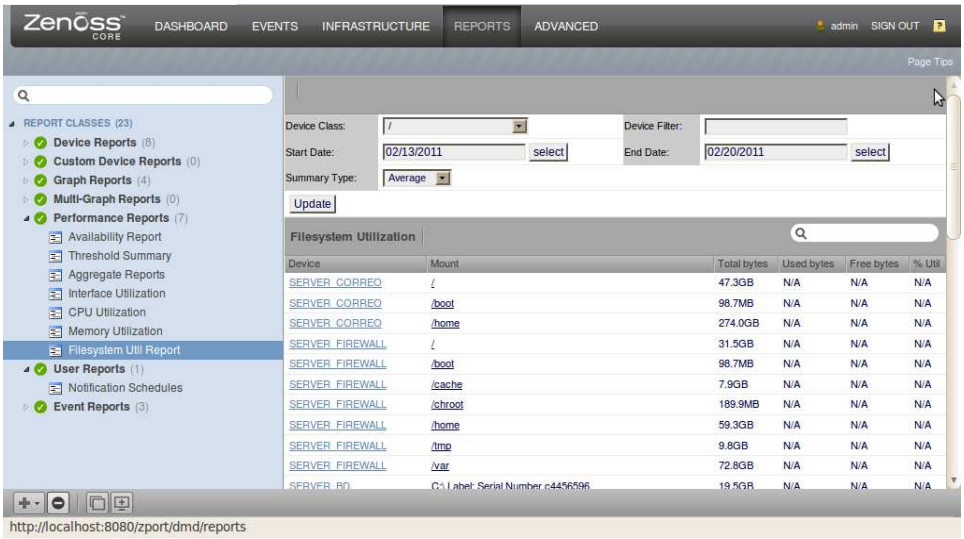


Figura IV.75 : Reporte de Utilización de los archivos del sistema
Fuente: Investigador

Utilización de la interfaz - Incluye todas las interfaces de control. Para cada interfaz, el reporte incluye el dispositivo, la velocidad, entrada, salida, el rendimiento total, y la utilización por ciento. El informe enumera "N / A" para los valores desconocidos.

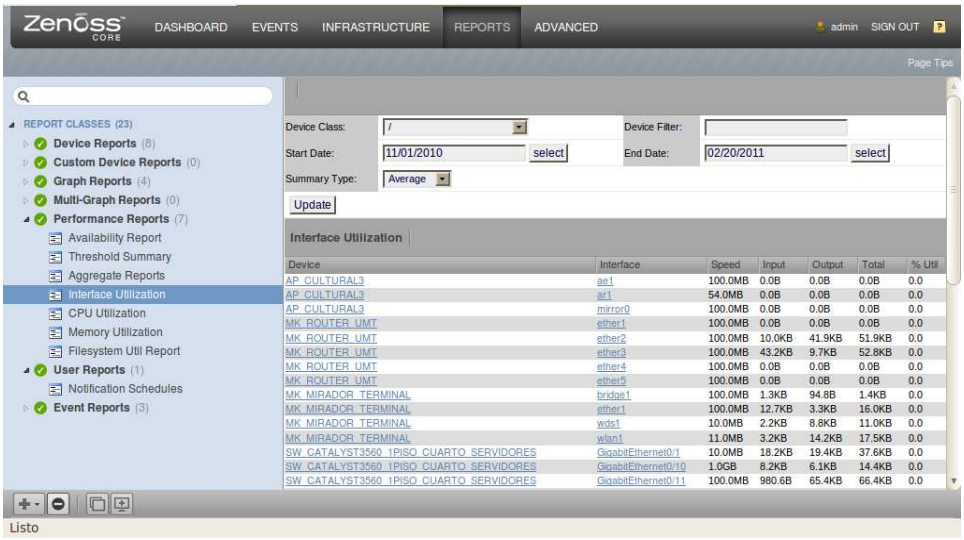


Figura IV.76 : Reporte de Utilización de la utilización de la interfaz
Fuente: Investigador

Uso de la memoria - El reporte del uso de la memoria incluye todos los dispositivos y proporciona las estadísticas de memoria: Total Disponible, caché, buffer, y el porcentaje de utilización. Al igual que varios de los informes de ejecución, se muestran los valores conocidos, mientras que "N / A" muestra los valores desconocidos.

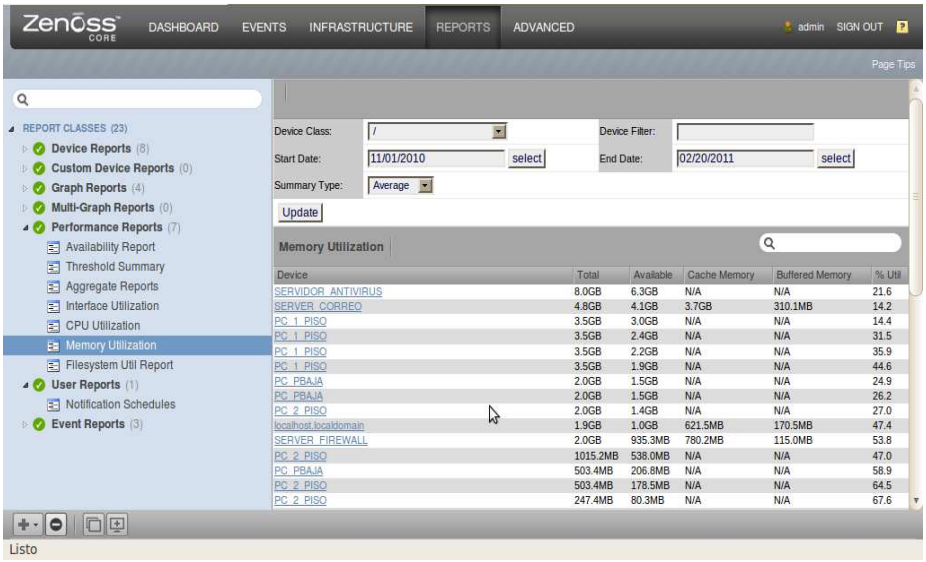


Figura IV.77 : Reporte de Uso de memoria
Fuente: Investigador

Resumen Threshold - Identifica los dispositivos que se acercan o rebasan los umbrales. Usted puede ver la unidad, el componente, la clase de evento, el recuento, la duración y porcentaje.

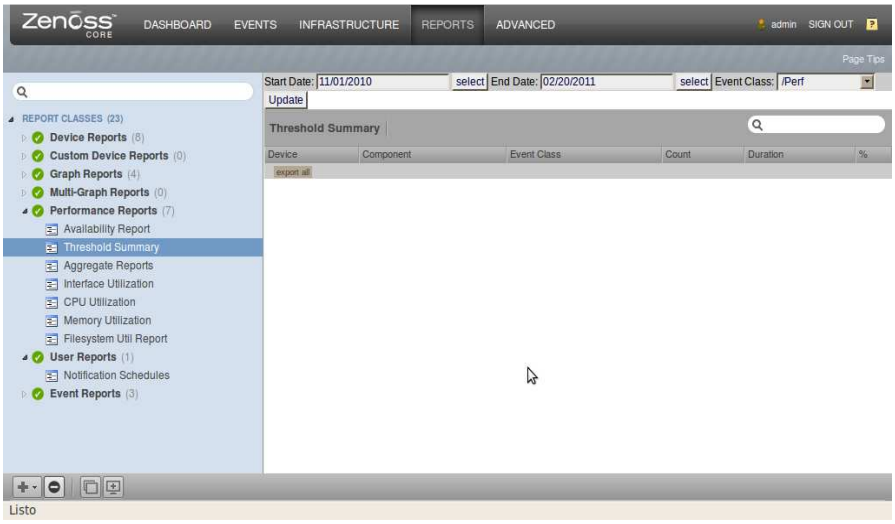


Figura IV.78 : Reporte de resumen de threshold
Fuente: Investigador

Reportes de Usuarios - Se basan en la información de cuenta de usuario y los cambios en el sistema.

Notificación de Horarios - Muestra todas las reglas de alerta y su estado de alerta por su nombre, el usuario asignado. Los otros campos en el reporte son los retrasos de alerta, estado activo, duración de alerta, y si esta activa o no. Cada alerta incluye dos filas en el informe, en la segunda fila, vemos que el real criterios de alerta.

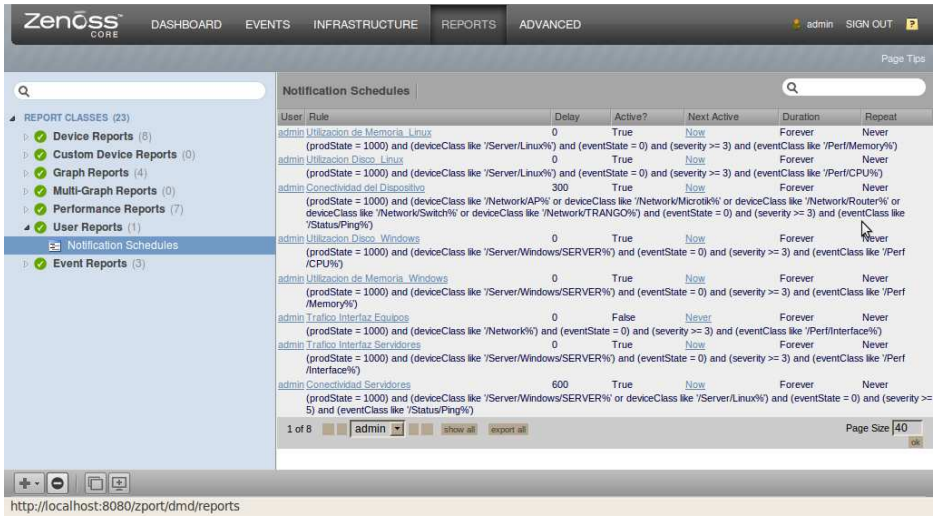


Figura IV.79 : Reporte de Notificación de horarios a usuarios
Fuente: Investigador

4.1.4.4. Reportes Gráficos

Nos permiten crear gráficos personalizados basados en los gráficos de rendimiento existente para las interfaces, procesos, sistemas de archivos, memoria y CPU.

Creando Reportes Gráficos

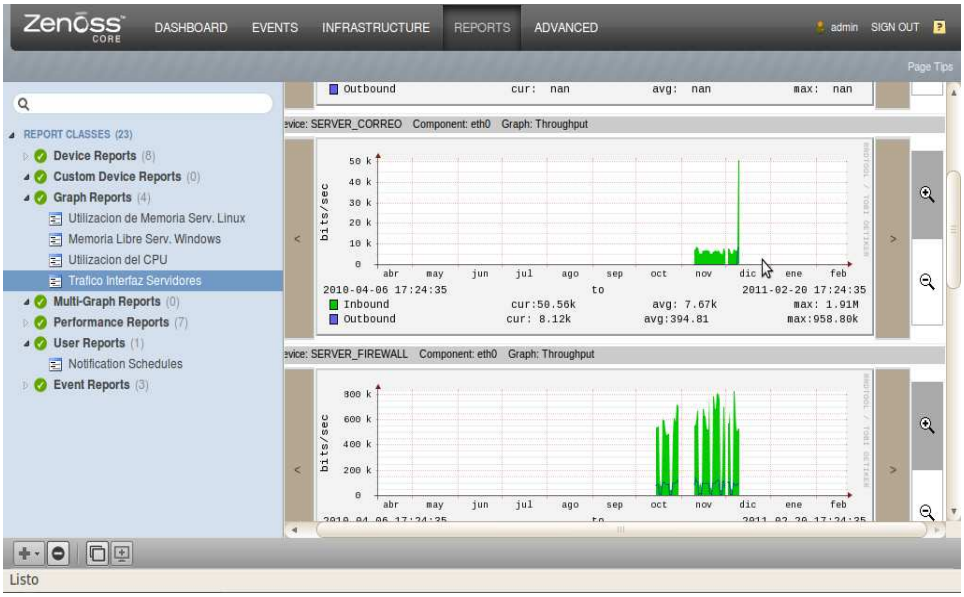


Figura IV.80 : Creación de reportes gráficos
Fuente: Investigador

1. En la vista del árbol, seleccione Añadir Reporte Gráfico de  (Menú Añadir).
2. En el cuadro de diálogo de Crear reporte Gráfico, ingrese un nombre para el reporte y click en Submit.
3. La página de edición del reporte gráfico aparece:
   Ingrese la información o haga selecciones para definir el reporte:
   - Nombre
   - Título

- Numero de Columnas
- Comentarios

4. Click en **Save** para guardar el nuevo reporte gráfico.

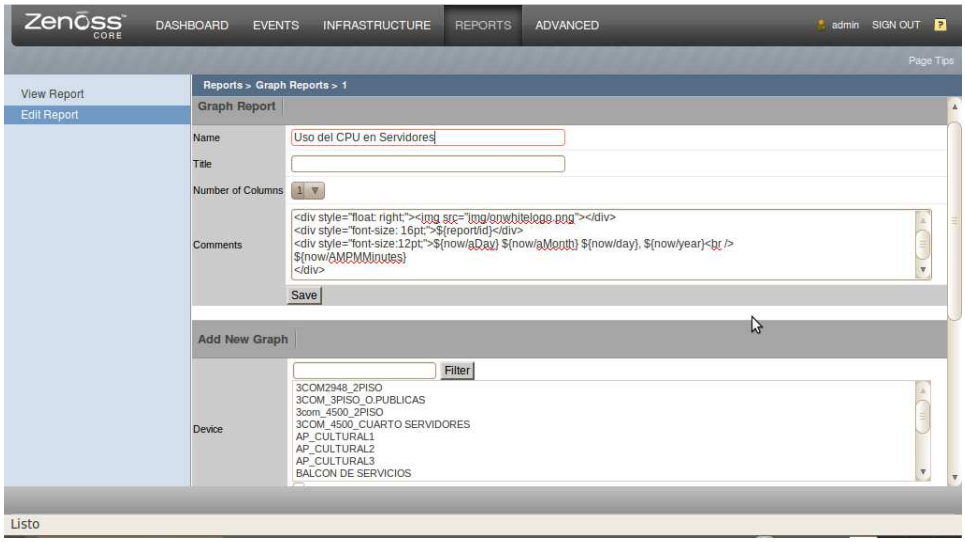


Figura IV.81 : Página de edición de reporte gráfico
Fuente: Investigador

Añadiendo Gráficos

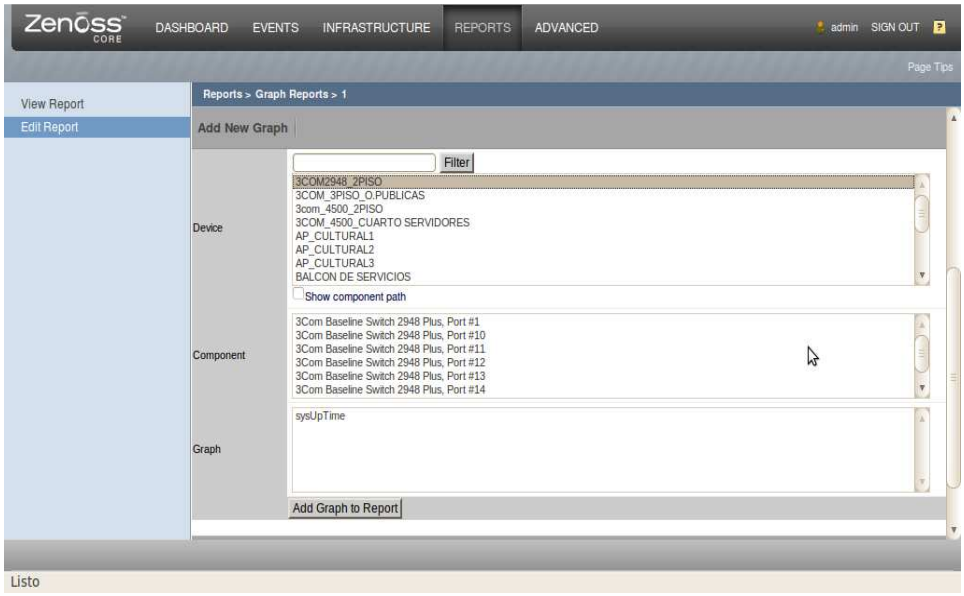


Figura IV.82 : Sección añadir nuevo gráfico a un reporte
Fuente: Investigador

La sección Añadir un nuevo gráfico de la página de edición le permite agregar uno o más gráficos para el informe. Para ello:

1. Seleccione uno o más dispositivos.
2. Opcionalmente, seleccione uno o más componentes de la lista de componentes. Esta lista despliega los nombre de todos los componentes definidos
3. Seleccione uno o más gráficos de la lista. Esta lista muestra los nombres de todos los gráficos validos para el dispositivo seleccionado, o si usted tiene uno o más componentes, los gráficos validos para los componentes.
4. Click en añadir gráfico al reporte.

4.1.5. Copia de seguridad y restauración

Zenoss proporciona dos utilidades de línea de comandos que nos permiten hacer una copia de seguridad y restauración de las piezas clave de nuestra configuración Zenoss.

4.1.5.1. Crea una copia de seguridad (Interfaz)

Para hacer copias de seguridad de la instancia del sistema de la interfaz:

1. En la barra de navegación, seleccione Opciones avanzadas.
2. En el panel izquierdo, seleccione copias de seguridad.
3. En el área Crear nueva copia de seguridad, introducir información o hacer la selección para la copia de seguridad. Las opciones disponibles son un subconjunto de los disponibles de la herramienta de línea de comandos zenbackup.
4. Haga clic en Crear copia de seguridad.

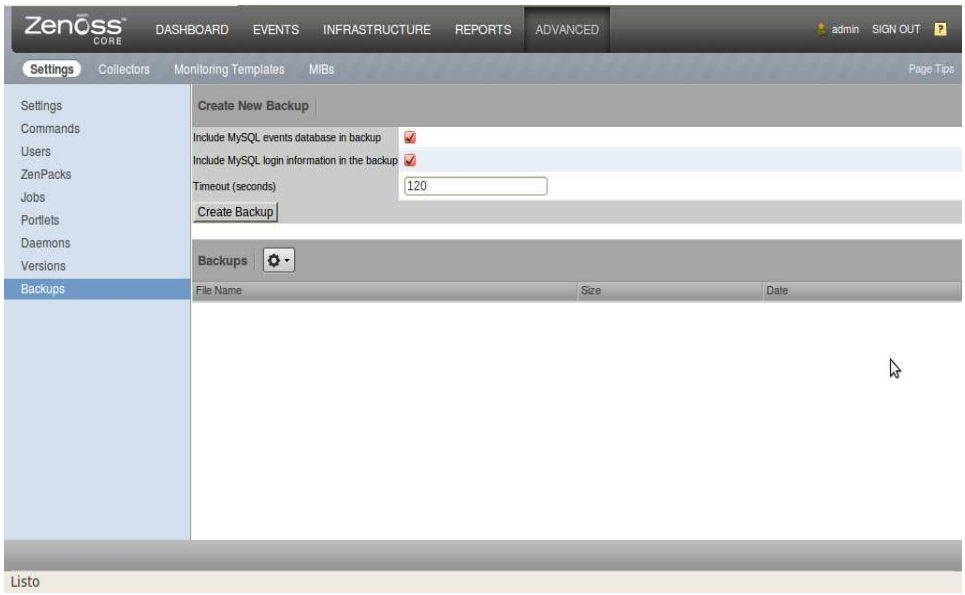


Figura IV.83 : Creación de copias de seguridad
Fuente: Investigador

4.1.5.2. Crear copia de seguridad (Comandos)

Para crear la copia de seguridad, ejecute los siguientes comandos como usuario Zenoss:

1. Detener Zenoss

service Zenoss-stack stop

2. Ejecutar

/usr/local/Zenoss/Zenoss/bin/zenbackup --save-mysql-access

3. Iniciar el servicio de Zenoss

service Zenoss-stack start

4.1.5.3. Eliminar una copia de seguridad

Para eliminar una copia de seguridad de la interfaz:

1. En la barra de navegación, seleccione Opciones avanzadas.
2. En el panel izquierdo, seleccione copias de seguridad.

3. Seleccione uno o más archivos en la lista y, a continuación, seleccione Eliminar copia de seguridad en el menú Acción.
4. Haga clic en Eliminar en el cuadro de diálogo Eliminar copia de seguridad para confirmar la acción.

4.1.5.4. Restaurar copia de seguridad (zenrestore)

Para restaurar una copia de seguridad

1. Detener Zenoss

service Zenoss-stack stop

2. Ejecutar el siguiente script para lo cual nos debemos ubicar bajo el path /usr/local/Zenoss/Zenoss/bin/ y ejecutar

zenrestore --file=BACKUPFILEPATH

3. Iniciar Zenoss

#service Zenoss-stack start

4.2. Monitorización de dispositivos de networking en la herramienta

El monitoreo de Dispositivos que nos ofrece Zenoss, es un monitoreo esencial, donde podemos encontrar la utilización del CPU, la cantidad de procesos, la memoria que se está consumiendo, entre otros.

4.2.1. Ítems monitorizados

- SysUptime
- CPU
- Memoria libre
- Memoria Utilizada

- Paginación
- Longitud de cola de Disco
- Paquetes enviados y recibidos
- Errores
- Utilización
- Espacio en el Disco
- Bytes de entrada y Salida
- Estado del Ping
- Estado de SNMP
- Nivel de Tóner
- Número de páginas impresas

4.2.2. Resultados obtenidos

Una vez introducidos y categorizados los equipos que conforman la infraestructura de red del IMA en la herramienta de administración y monitoreo ZENOSS, procedemos a realizar la monitorización. En esta parte debemos acotar que para todos los equipos monitoreados se contará con las opciones de Overview, Events, Components, Software, Graphs, Administration, Configuration Properties, Modeler Plugins, Custom Properties, Modifications, Monitoring Templates.

En las pestañas Componentes, Gráficos, Monitoring Templates, los parámetros presentados dependerán del tipo de equipo que se esté monitorizando por lo cual las opciones mostradas serán diferentes.

4.2.2.1. Monitorización de Servidores Windows y Linux

Servidores bajo Windows

Zenoss cuenta con un demonio llamado ZenWin cuya interacción le permite integrarse con el equipo Windows monitoreado para recolectar datos, solo queda identificar cada uno de los eventos para su posterior gestión.

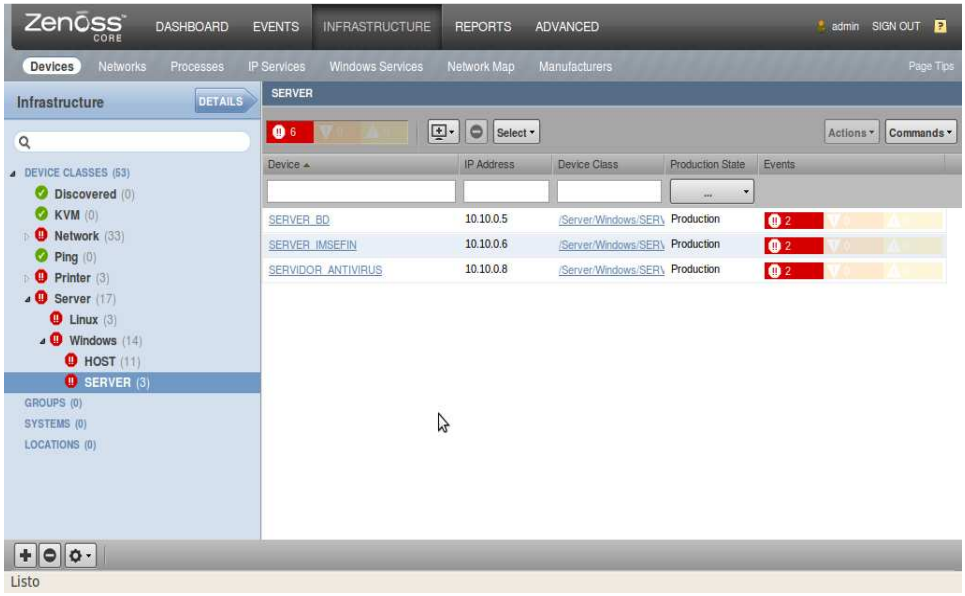


Figura IV.84 : Servidores Windows
Fuente: Investigador

Para iniciar con el monitoreo de los servidores Windows, se debe asegurar que el protocolo SNMP y el agente SNMP Informant estén corriendo exitosamente, para lo cual es necesario se debe ayudar del Software AJPD-Soft ***(Ver Anexo 3)***, el cual permite conocer si el equipo está devolviendo valores SNMP, una vez corroborado esto se debe proceder a agregar el dispositivo en la jerarquía devices/Server/Windows/Server, obteniendo la siguiente información.

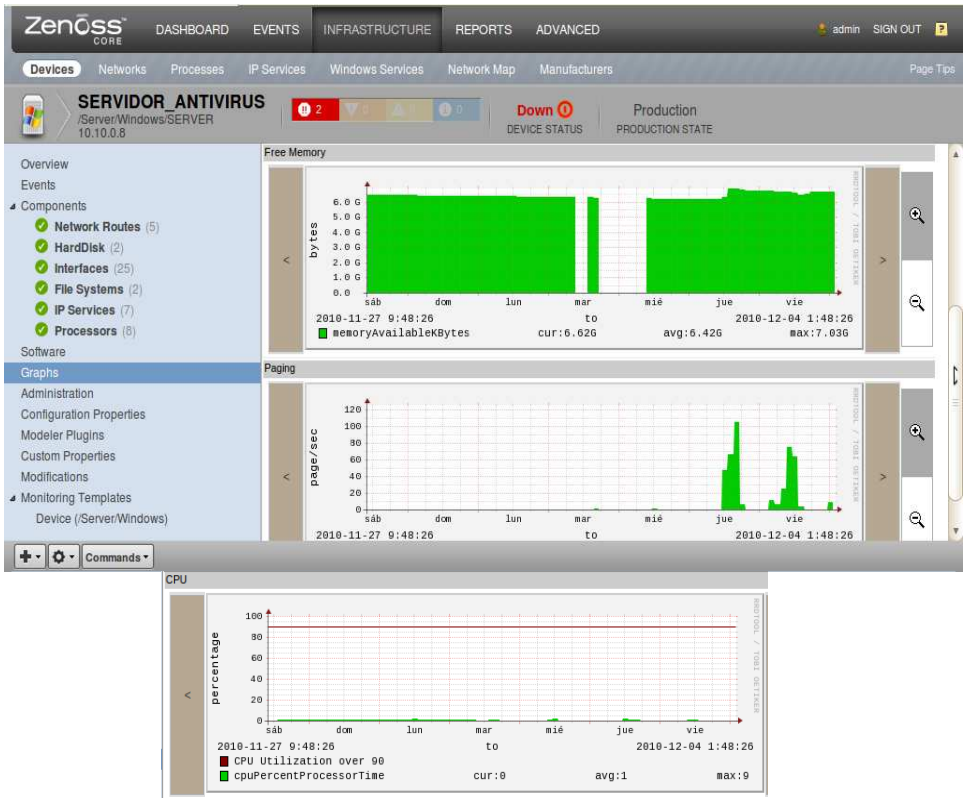


Figura IV.85 : Graphs de Memoria Libre – Servidor Antivirus
Fuente: Investigador

En la grafica anterior se visualiza que el servidor en donde se encuentra alojado los Antivirus Nod32 y Kaspersky que son los que manejan dentro de la red, cuenta con el suficiente espacio en memoria libre, ya que en este servidor únicamente se generan las actualizaciones del antivirus y se actualizan los clientes.

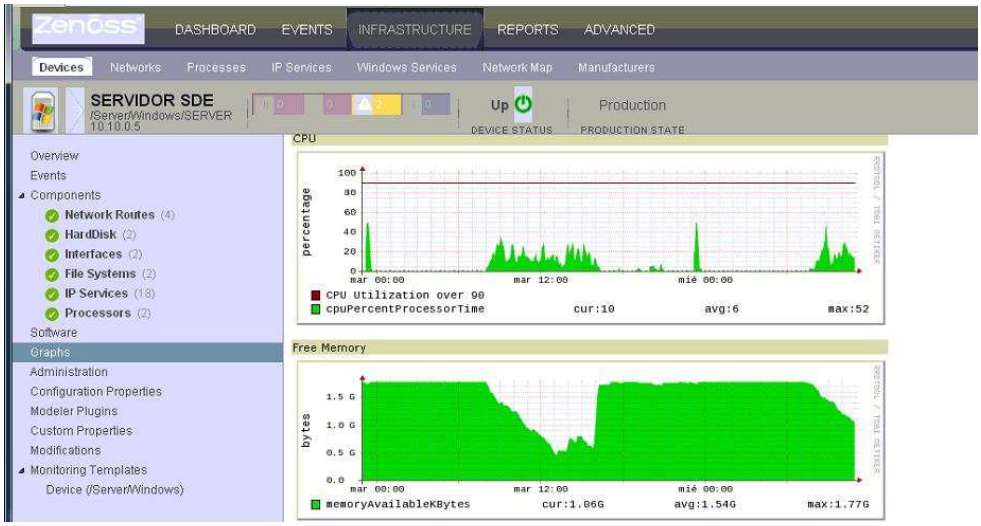


Figura IV.86 : Graphs de Memoria Libre – Servidor Base de Datos
Fuente: Investigador

En los gráficos correspondientes al uso del CPU, Memoria Libre y Paginación de los servidores de Antivirus, Base de Datos se pudo observar que en el primer servidor se tenía un uso del CPU muy bajo a diferencia del servidor de base de Datos, el cual tiene almacenado la base de datos gráfica de catastros, este servidor recibe diariamente múltiples peticiones ya que hacen uso los departamentos de Avalúos, Catastros, Planificación, Balcón de Servicios, en el gráfico se puede apreciar que en ciertos intervalos de tiempo tenía un gran uso del CPU, esto se debía a que estos departamentos realizan atención al cliente atendiendo peticiones de actualización de datos, generación de mapas viales, direcciones de un lugar específico, etc.

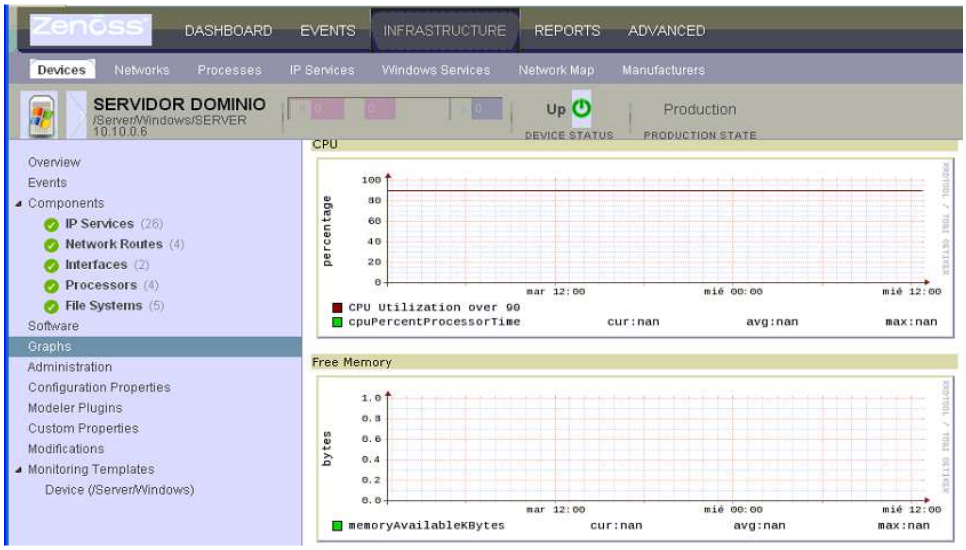


Figura IV.87 : Graphs– Servidor de Dominio
Fuente: Investigador

En el Servidor de Dominio en el mismo que se alojan diferentes aplicaciones, se detecto problemas, ya que al momento de recolectar la información SNMP necesaria para realizar las graficas de memoria, cpu y paginación, no se pudo obtener debido a que se encontraron falencias en el hardware como por ejemplo: el disco no se encuentra trabajando correctamente, por tal motivo se sugirió migrar este servidor al servidor blade.

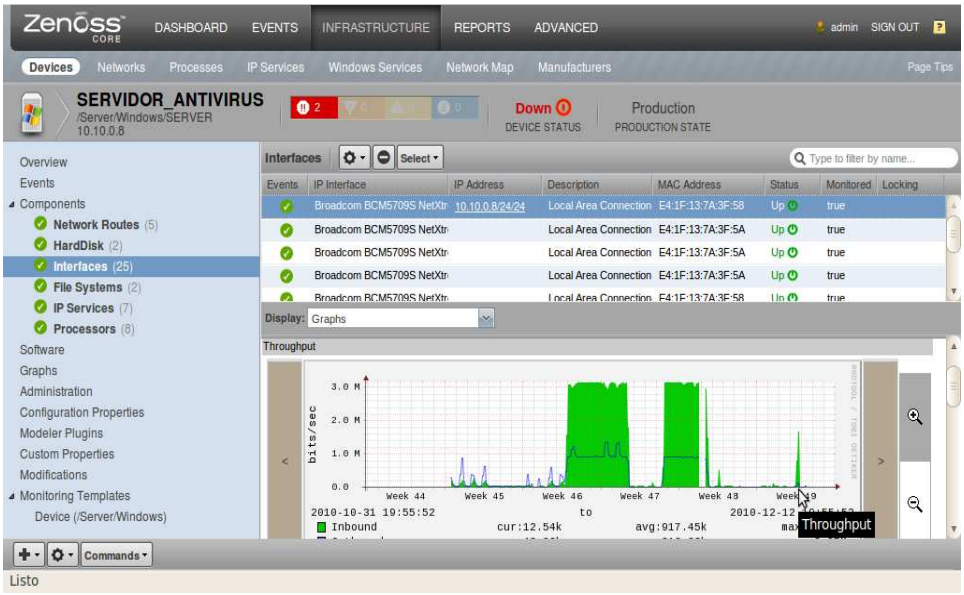


Figura IV.88 : Interfaces de Servidor Antivirus

Fuente: Investigador

Podemos visualizar el throughput que está pasando por la interfaz del servidor, observamos que existe la presencia de cantidad considerable de bits/sec, esto sucedió porque las peticiones de entrada al servidor son altas cuando los clientes están actualizando su cliente antivirus, una vez terminado el proceso de actualización de firmas de virus, se estabiliza el tráfico generado.

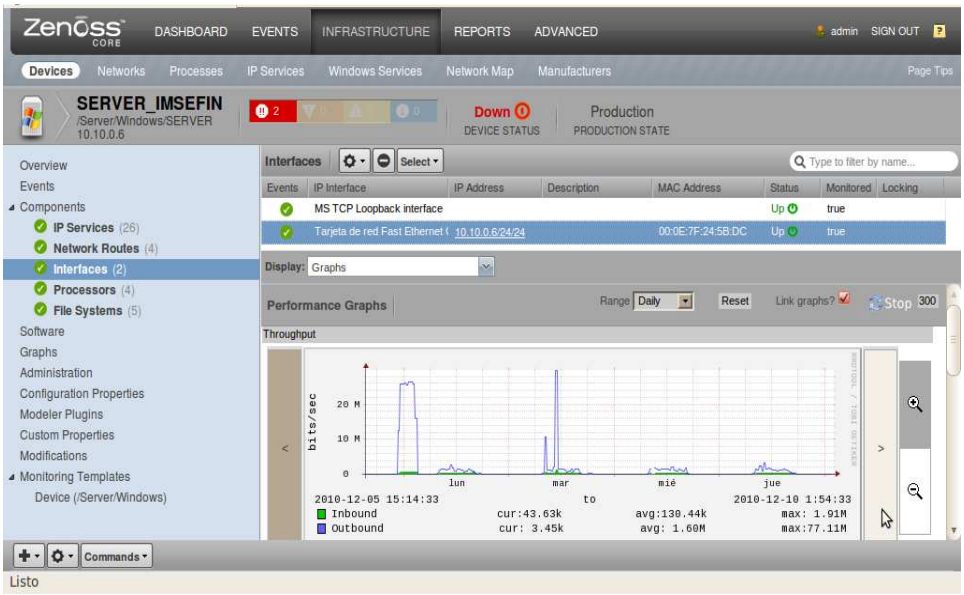


Figura IV.89 : Interfaces de Servidor de Aplicaciones

Fuente: Investigador

El acceso a la interfaz de este servidor tenía muchas variaciones sin necesidad de que el acceso se lo haga dentro o fuera de las horas pico, ya que esas son las horas en las cuales los usuarios realizan mas peticiones debido a que en este servidor están las aplicaciones con las que trabaja el IMA, es por eso que se sospechó la presencia de algún virus que hace que el servidor no trabaje en completa normalidad, sugiriéndose de tal modo se realice un escaneo profundo para la detección y reparación del mismo.

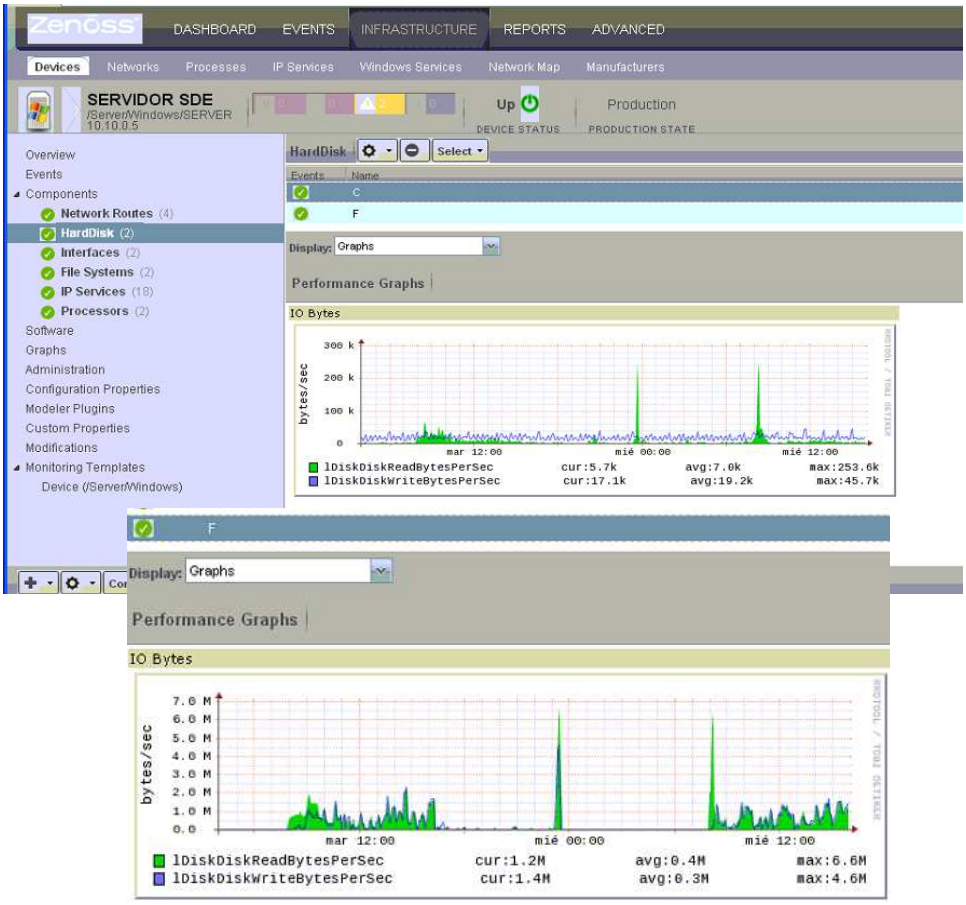


Figura IV.90 : Hard Disk de Servidor Base de Datos

Fuente: Investigador

En cuanto se refiere a la opción de partición de discos, se puede observar que en el servidor de Base de Datos cuenta con dos particiones en el disco duro, visualizando que el uso de la partición **C:/** y **F:/** existe la presencia de picos altos cuando los usuarios que acceden necesitan extraer información de la base, además en horas como las 00:00 el disco se encuentra trabajando ya que existen tareas programadas para realizar backups de las bases de datos a una hora determinada, a diferencia de la escritura en el disco que está representada por la línea azul en las graficas, es normal a medida que la información se va almacenando en las bases de datos. En

cuanto a los dos servidores de Antivirus y de Dominio, las particiones no tienen ningún punto relevante, trabajan bajo normalidad.

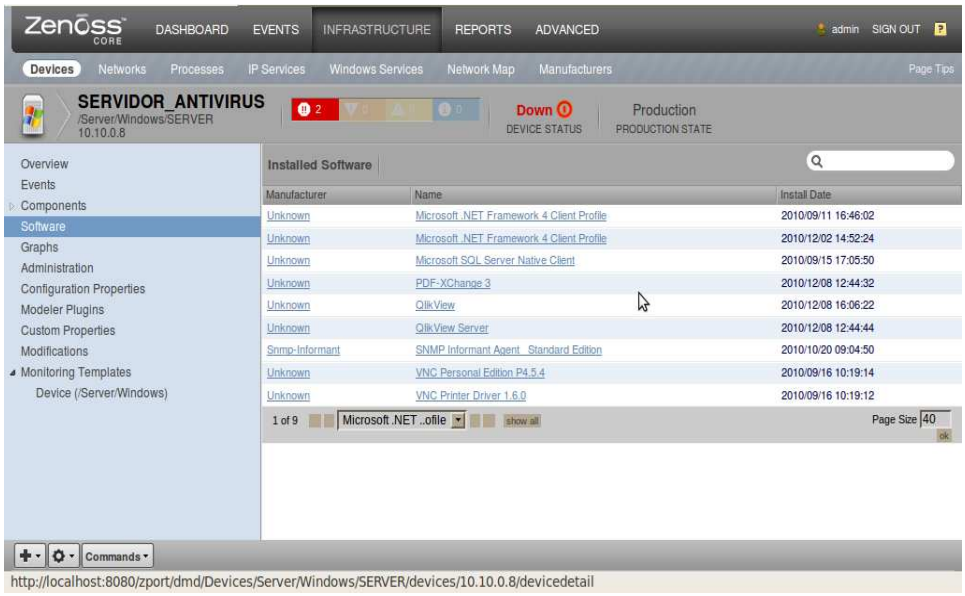


Figura IV.91 : Software de Servidor Antivirus

Fuente: Investigador

Ciertamente es muy beneficioso observar la lista de software que se tiene instalado en cada uno de los servidores para de esta manera tener un seguimiento de los mismos, así como la fecha de instalación, si en la herramienta se encuentra registrado su fabricante también será asociado al software correspondiente.

Servidores bajo Linux

En esta categoría se encuentran distribuidos los equipos que cuentan con el sistema Operativo Linux, están ubicadas bajo ***Server/Linux.***

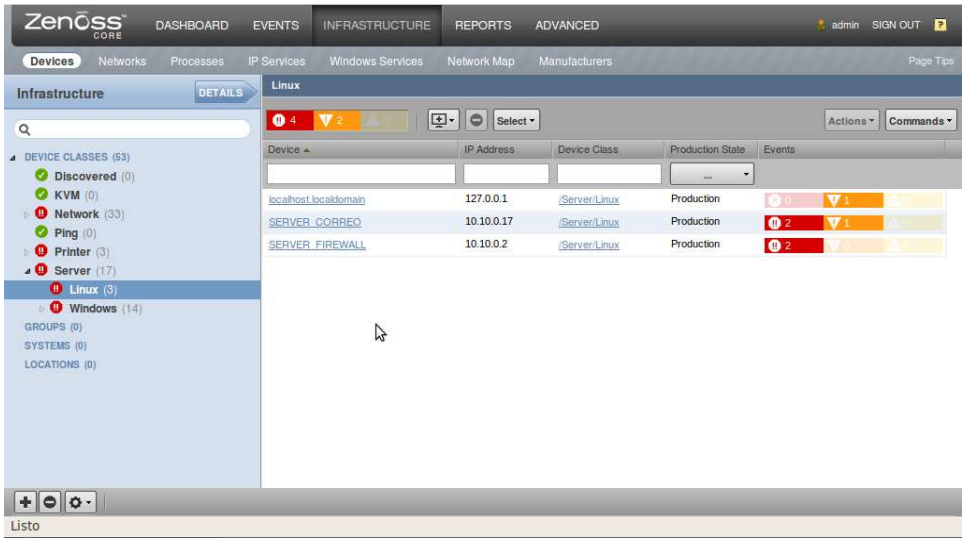


Figura IV.92 : Servidores Linux

Fuente: Investigador

La detección de un dispositivo con el agente snmp instalado arroja desde el momento de la detección por parte de Zenoss la información relevante para su clasificación por clases. Al agregar el dispositivo a la clase "/Server/Linux" podemos comenzar a testear su estado según nuestros requerimientos. En esta categoría tenemos los Servidores de Correo y Servidor de Firewall.

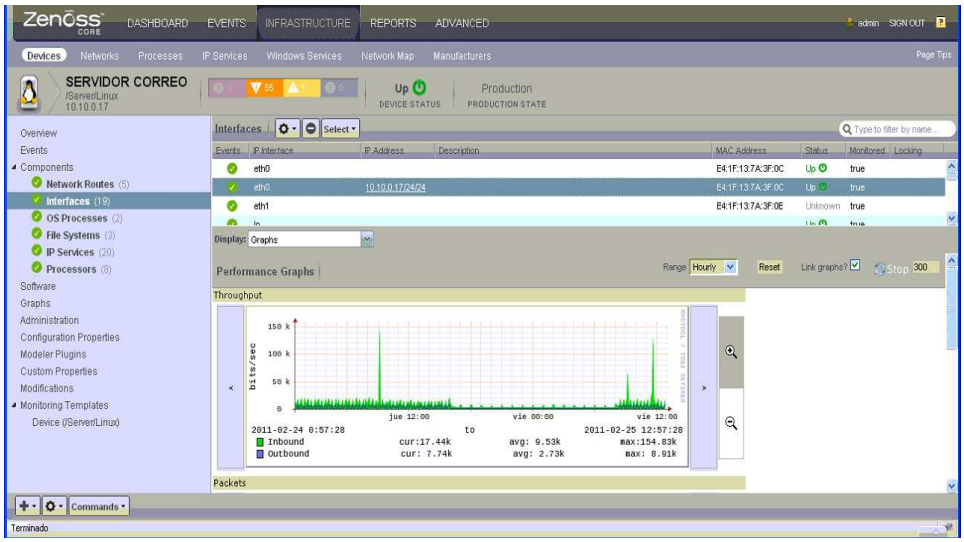


Figura IV.93 : Interfaces de red de Servidor de Correo

Fuente: Investigador

Zenoss toma las tarjetas de red de los equipos Linux como evento por omisión de la clase “/Server/Linux” pero en contraste con los equipos Windows, esta no toma los procesos de los servicios y aplicaciones que ocupan los diferentes Zokets en el sistema, por lo que se debe recurrir a otras utilidades como los “IPService” o ZenPacks.

En este servidor observamos que tiene más de una interfaz más aun tomando en cuenta las interfaces virtuales creadas, en la interfaz que más relevancia obtuvo el monitoreo se visualiza que en horas de la noche que son horas en las que el personal del IMA no accede a sus cuentas de correo es por eso que no se filtra trafico mediante este servidor, el throughput es casi nulo a diferencia que en las horas en las que el personal labora, los picos altos presenciados son el acceso excesivo o talvéz la presencia de virus, es por eso necesario realizar un escaneo para descartar la posibilidad del mismo.

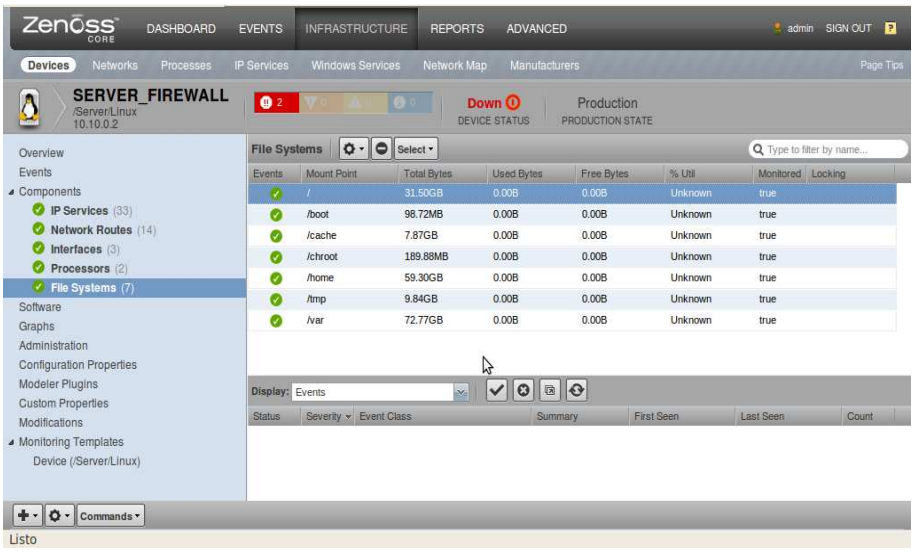


Figura IV.94 : File System de Servidor Firewall
Fuente: Investigador

Una característica de Zenoss en Linux es que se toman las particiones del sistema en el equipo y de la misma forma que en Windows, anuncia explícitamente el estado físico y datos relevantes de las mismas.

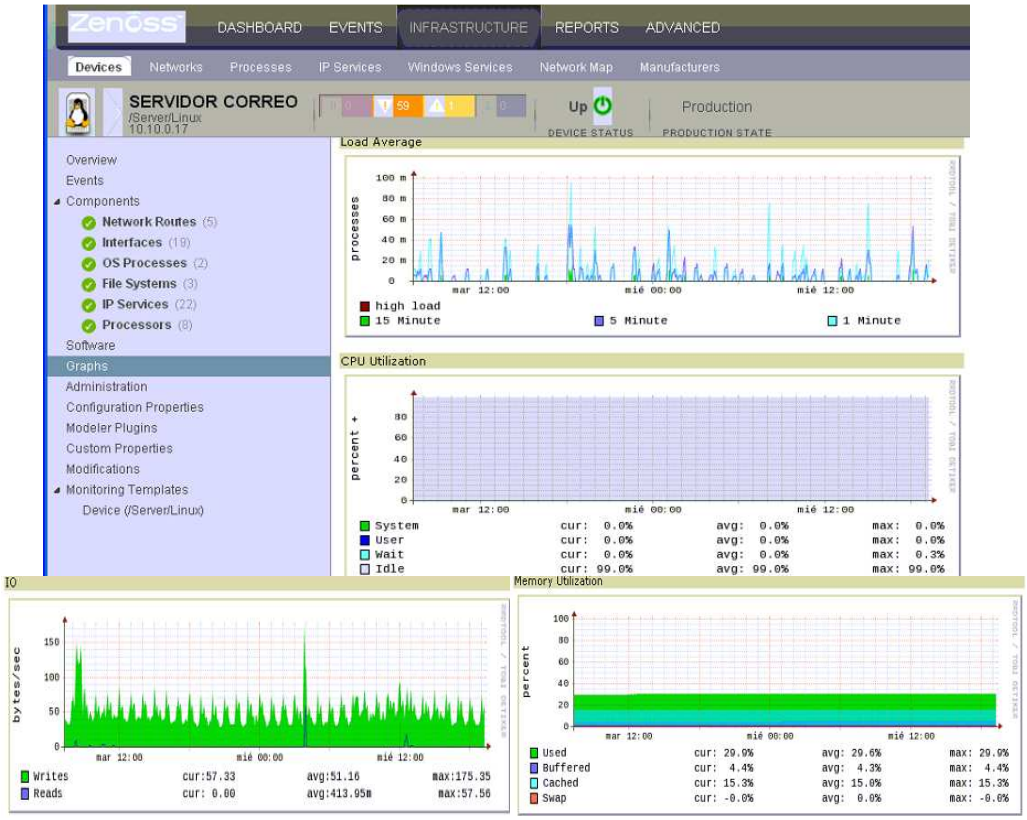


Figura IV.95 : Graphs de Servidor de Correo

Fuente: Investigador

Luego de realizar un monitoreo en el Servidor de Correo en cuanto a disponibilidad de hardware se detecto que tiene suficiente espacio en memoria para alojar mas cuentas de correo, por tal motivo el administrador no deberá tener cuidado en ese aspecto, en cuanto al uso del CPU el porcentaje de utilización es Idle que esto quiere decir que no se está realizando ningún esfuerzo, y en lo que se refiere a la carga promedio del procesador y los bytes de escritura y lecturas, tienen picos altos por el acceso que hacen los usuarios al servidor.

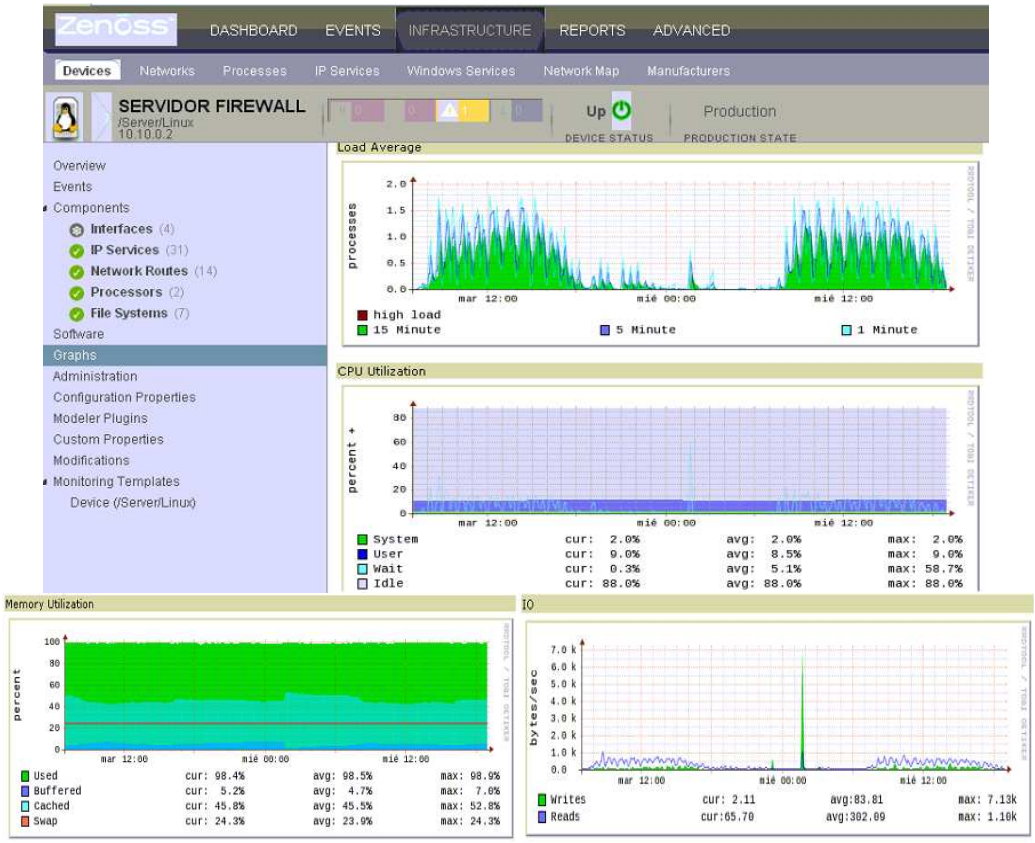


Figura IV.96 : Graphs de Servidor de Firewall

Fuente: Investigador

En este servidor se identifica que el espacio en memoria no es el suficiente para que el dispositivos trabaje al 100%, porque esta usado un promedio de 98%, del cual usa gran espacio la memoria cache con un 45%, q es un espacio considerable, es por eso recomendable liberar este memoria en cache.

4.2.2.2. Monitorización dispositivos de Red

Ahora agregamos en nuestra herramienta los dispositivos de red como Antenas (Microtick, Trango), Router, Switch, entre otros que conforman la red de networking del Ilustre Municipio de Ambato. Para ello primeramente debe estar

activo el servicio de SNMP en cada uno de los equipos, como ya se lo ha mencionado anteriormente.

De igual forma que los Servidores a los dispositivos de red se los ha distribuido dependiendo del tipo de dispositivos, teniendo de esta forma categorías como AP, Microtick, Trango, Router, y Switch, como se muestra a continuación.

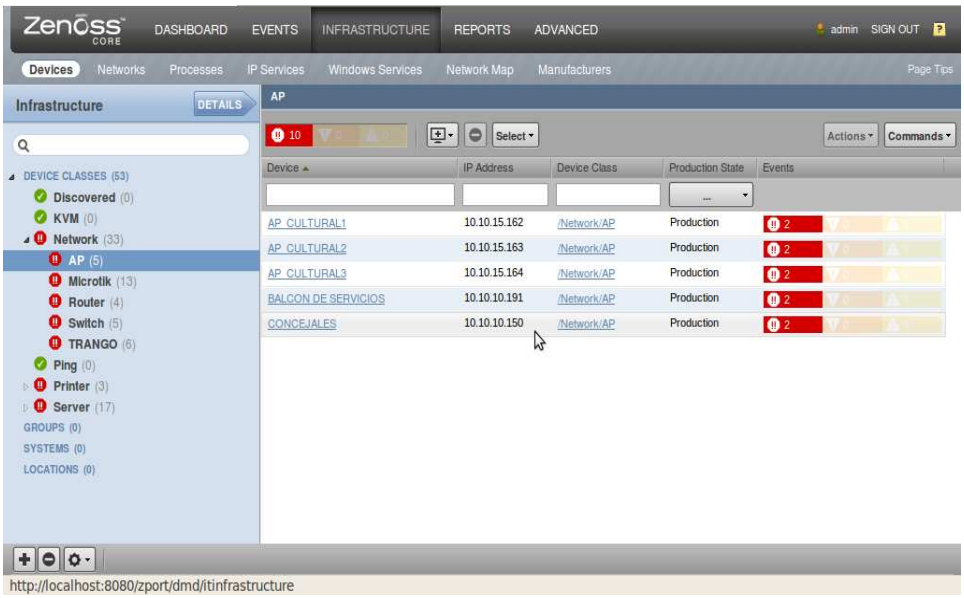


Figura IV.97 : Distribución de dispositivos de red

Fuente: Investigador

Microtick

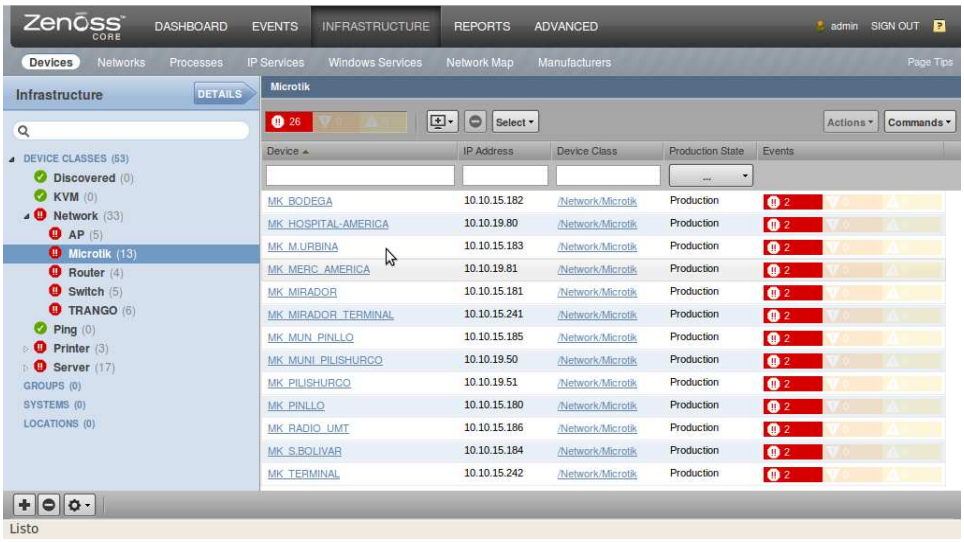


Figura IV.98 : Monitoreo de Microtick
Fuente: Investigador

En esta categoría se encuentran agrupadas las antenas de marca Microtick, tanto CPE como las Radio Bases, en esta ventana se puede observar las ip de los dispositivos, en el estado actual, el estado de producción con el que fue agregado.

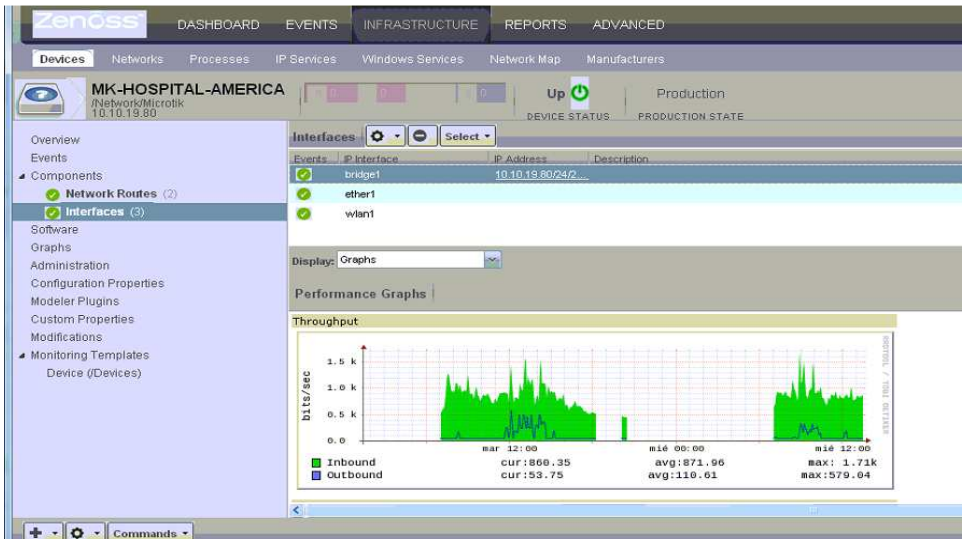


Figura IV.99 : Interfaces de Microtick enlace Hospital- América
Fuente: Investigador

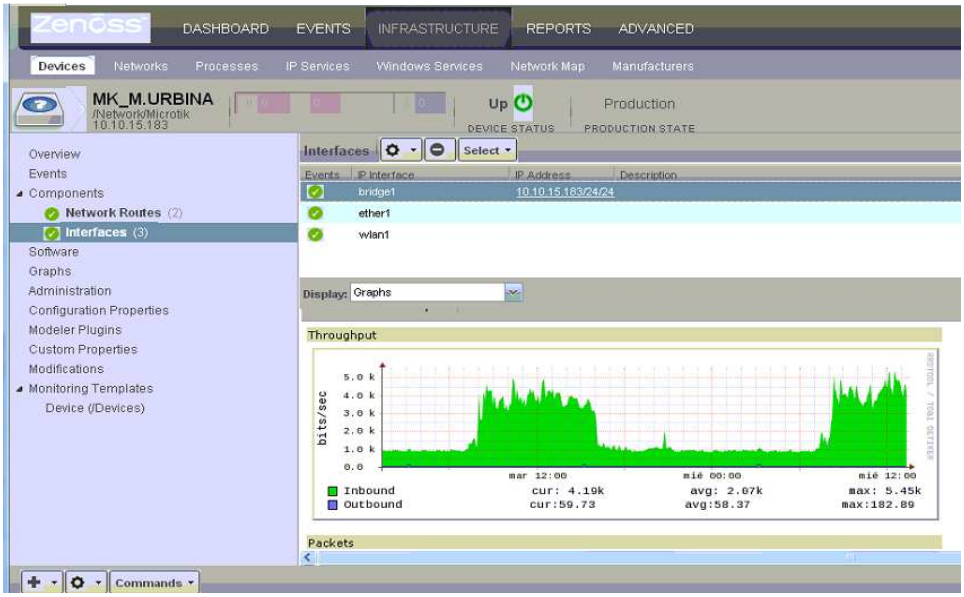
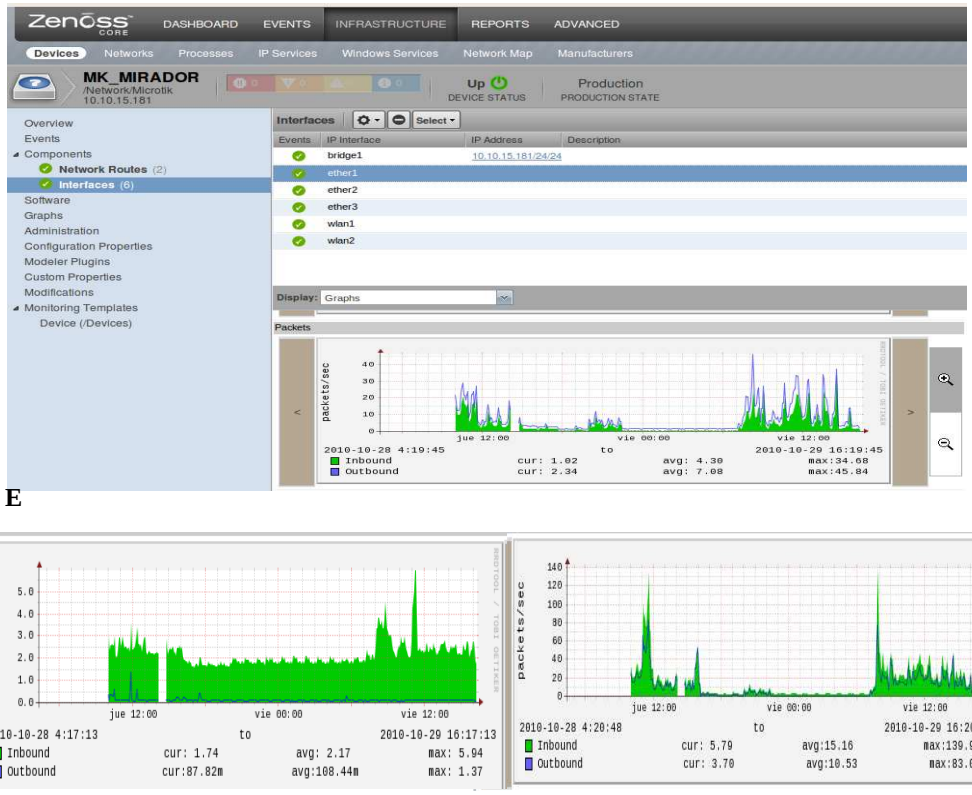


Figura IV.100 : Interfaces de Microtick Urbina

Fuente: Investigador

En las pantallas mostradas anteriormente se puede observar el tráfico que está pasando por la interfaz bridge de los equipos microtick que se encuentran ubicados en el enlace Hospital- Mercado América y Mercado Urbina, se puede apreciar que en el primer caso el throughput sobrepasa los 1 kbits/s mientras que en el equipo del Mercado Urbina el tráfico sobrepasa los 3 kbits/s, siendo estos tráficos normales en las interfaces, por lo que no se reportó ninguna anomalía en el funcionamiento de la red, se puede observar que existe una cantidad considerable de tráfico generado en las interfaces de estos dispositivos en las horas que laboran las oficinas de estas dependencias, no existe saturación en la red ya que no se registran picos tan altos que se puedan registrar como alertas de que algo anormal este sucediendo, estos picos se deben a consultas que se debieron haber generado a las aplicaciones del IMA que se manejan en estas dependencias.



E

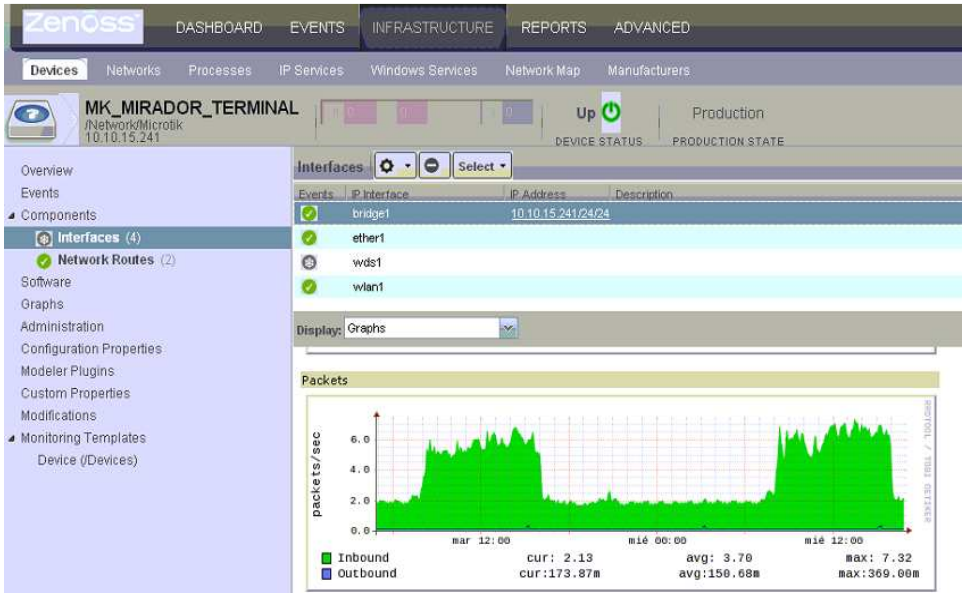
Bridge **Wlan**

Figura IV.101 : Interfaces Ethernet, Bridge, Wlan de Microtick Mirador

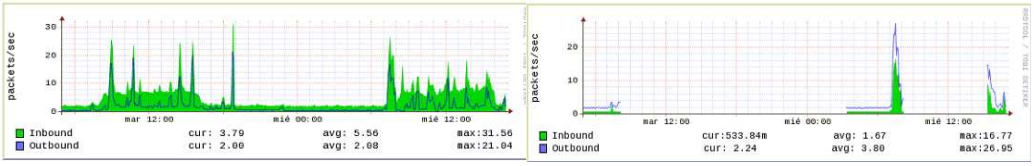
Fuente: Investigador

El tráfico analizado en el dispositivo que se encuentra ubicado en el equipo de el Mirador, se lo aprecia en las diferentes interfaces como Ethernet, wlan, y bridge que es una combinación entre las dos mencionadas anteriormente, y podemos observar que el volumen de información que fluyen en estas interfaces es constante salvo algunos picos altos que se observan en las horas de mayor concurrencia como son las horas del medio día a estas oficinas en su jornada diaria de trabajo, se puede apreciar la diferencia de tráfico de paquetes cuando no están laborando en estas oficinas.

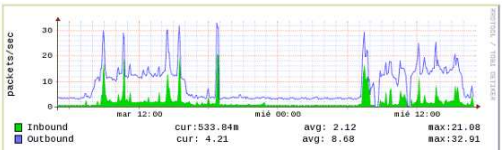
Actividades muy similares se registraron en el resto de equipos microtick en cuanto al comportamiento en cada una de sus interfaces, en lo que se refiere a throghput y envió/recepción de paquetes, por lo que no se generaron ningún tipo de alertas o alarmas, registraban un desarrollo normal en sus actividades.



Bridge



ether1 **wds1**



Wlan1

Figura IV.102 : Tráfico de paquetes en interfaces del enlace Microtick Mirador- Terminal

Fuente: Investigador

En la interfaz bridge del equipo que realiza el enlace entre el Mirador y el Terminal se puede observar que el tráfico de paquetes es el adecuado ya que el mayor número de paquetes que se está recibiendo y enviando por la interfaz ocurre en las horas laborables siendo estas de 8 am a 4 pm, no se presentan picos altos que ameriten una alerta por el exceso de tráfico en la interfaz.

En las interfaces Ethernet, wds y wlan, se registra que tanto el tráfico de paquetes de entrada como de salida son similares y no presentaron ningún inconveniente.

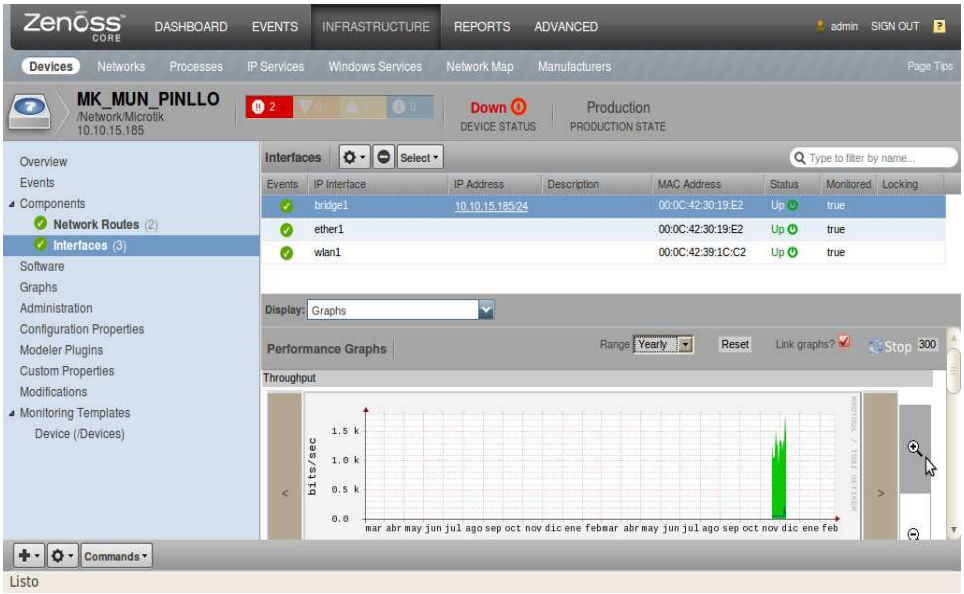
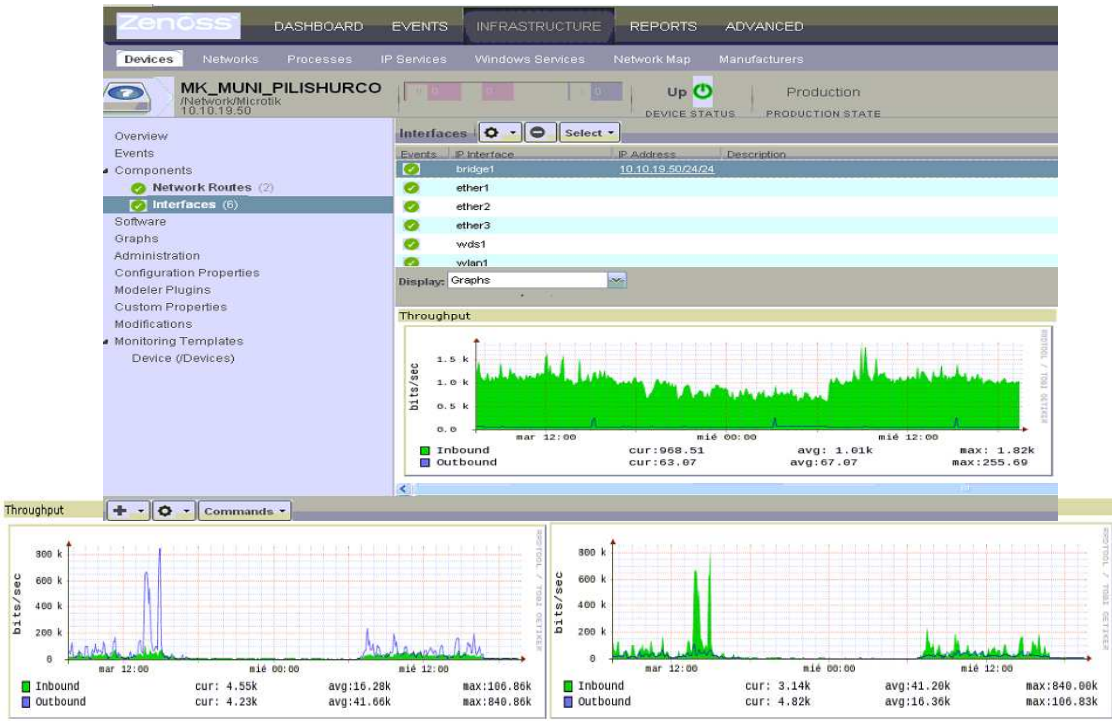


Figura IV.103 : Interfaces de enlace Microtick Municipio-Pinllo

Fuente: Investigador

En la imagen superior presentada se puede observar que el tráfico del equipo ubicado en las instalaciones del IMA enlazado con el equipo que se encuentra ubicado en Pinllo, en los meses de Noviembre y Diciembre es completamente normal ya que no se registran picos que sobrepasen los umbrales definidos para generar una alerta, los picos que se observan son generados cuando se acceden o se realizan consultas a las bases de datos, o

se están utilizando aplicaciones que funcionen en la red, el desenvolvimiento de esta interfaz y del equipo en sí ha sido normal y constante sin presentarse problemas en el mismo, salvo situaciones como cortes de energía eléctrica imprevistos en las que se perdía conectividad con el equipo.



Wlan **Ethernet**

Figura IV.104 : Interface bridge, wlan, ethernet de enlace Microtick Municipio-Pilishurco
Fuente: Investigador

En el enlace Municipio - Pilishurco, en el que el equipo se encuentra localizado físicamente en el IMA, se visualiza diferentes interfaces como Ethernet, wlan, y bridge, observamos que la fluidez del tráfico depende de los horarios en el que estén siendo utilizados, en este equipo se puede apreciar un gran tráfico en las interfaces, ya que este equipo sirve de enlace con el equipo ubicado en el Pilishurco, desde donde se distribuye la señal a algunas de las dependencias del IMA, por lo que el uso de estas interfaces es superior a las de los otros equipos de esta categoría.

Cabe recalcar que en este equipo se presentaron anomalías en los primeros días del mes de Diciembre, y gracias a la herramienta implementada se pudo detectar a tiempo el problema y conocer desde cuando se produjo errores en esta red, así también cuando se perdía conectividad, en este problema se prestó apoyo técnico para detectar cuales eran las fallas que provocaban las anomalías, detectándose que la placa del equipo debía ser reemplazada por una nueva, una vez realizado esto, se comprobó a través de la herramienta si ésta ya estaba funcionando de manera normal, hasta el momento se sigue monitoreando el equipo normalmente sin presentarse ningún inconveniente.

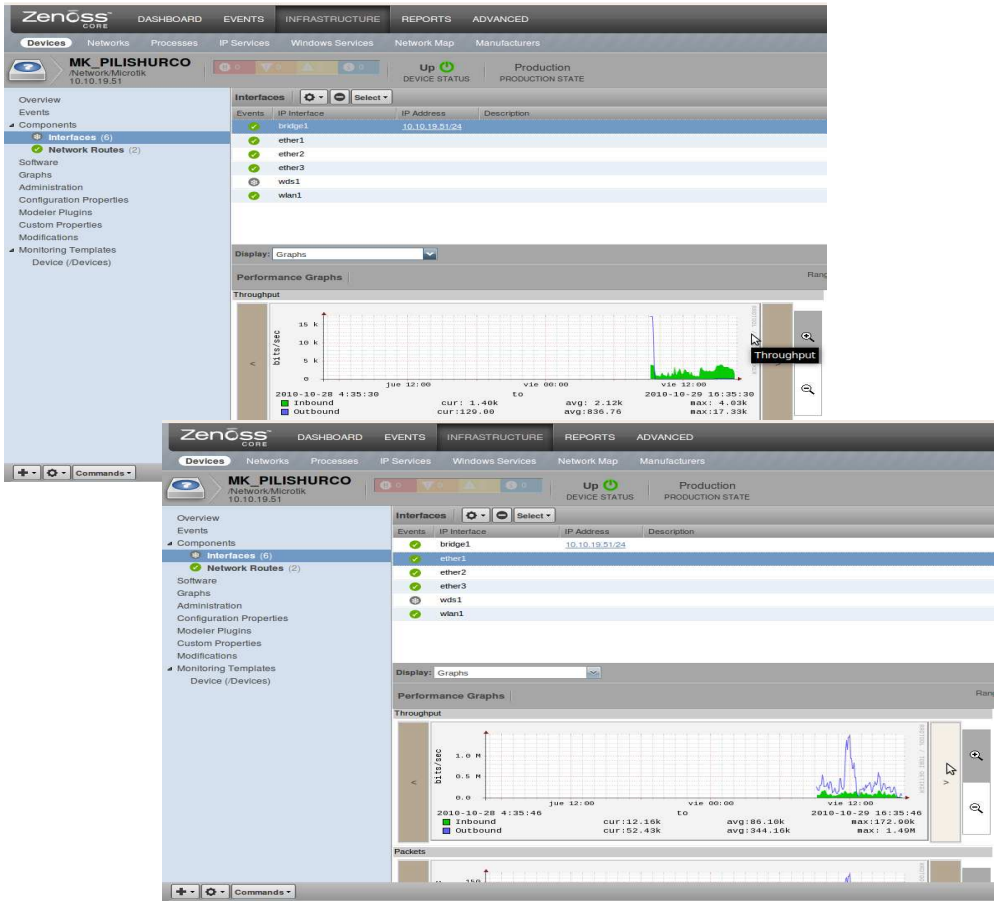


Figura IV.105 : Interface bridge, ethernet de Microtick Pilishurco

Fuente: Investigador

En las imágenes superiores podemos observar las gráfica del throughput de las interfaces Ethernet y bridge del dispositivo ubicado en el Pilishurco, evaluando el tráfico generado se concluye que va de acorde con las horas en que los usuarios hacen uso de la red, ya que son horas de trabajo y se están cargando aplicaciones y obteniendo información de las bases de datos.

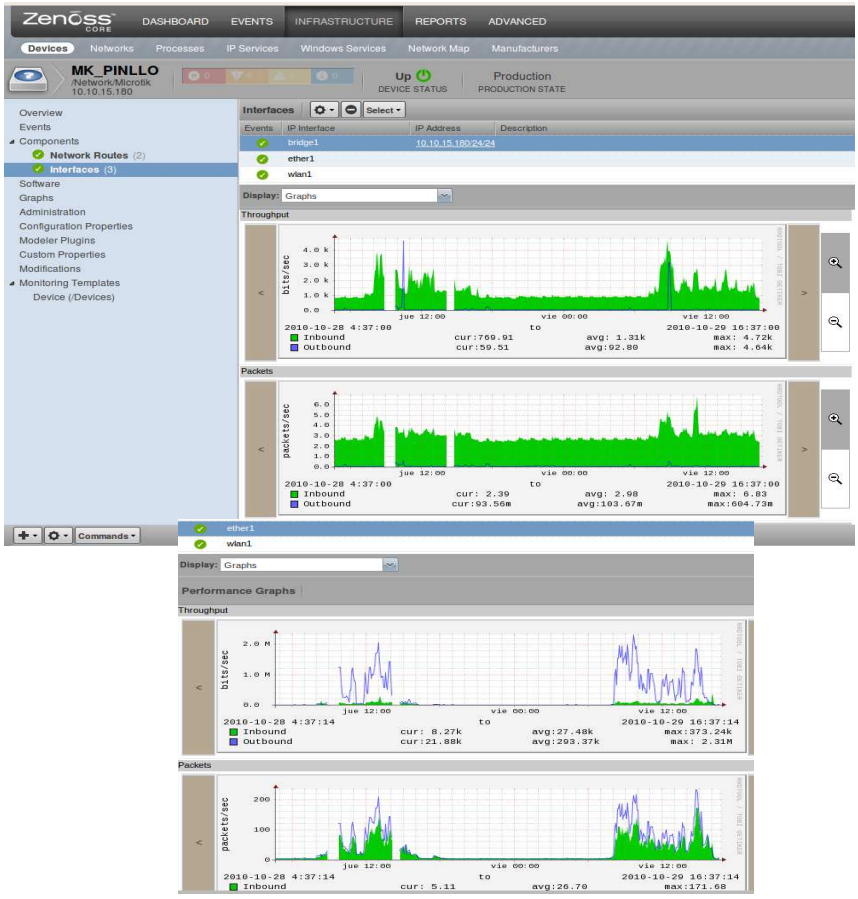


Figura IV.106 : Interfaces de Microtick Pinllo

Fuente: Investigador

Se puede apreciar el tráfico en el dispositivo localizado en el sector de Pinllo, observamos el throughput y el tráfico de los paquetes en las diferentes interfaces, en lo que se refiere al tráfico, este tiene la presencia de picos altos que son anomalías en el estado de la red, y aun más en horas pico en

las cuales los usuarios hacen más uso de la red ya que estos realizan peticiones o consultas, esto se registraba como un uso alto de la interfaz hasta que logre regular su normal funcionamiento, los sectores que se encuentran en blanco se debe a que en ese instante de tiempo el equipo estuvo caído, es decir se encuentra en estado down, por lo que no se generaba ningún tipo de tráfico y por lo tanto no se podía graficar información acerca de esto.

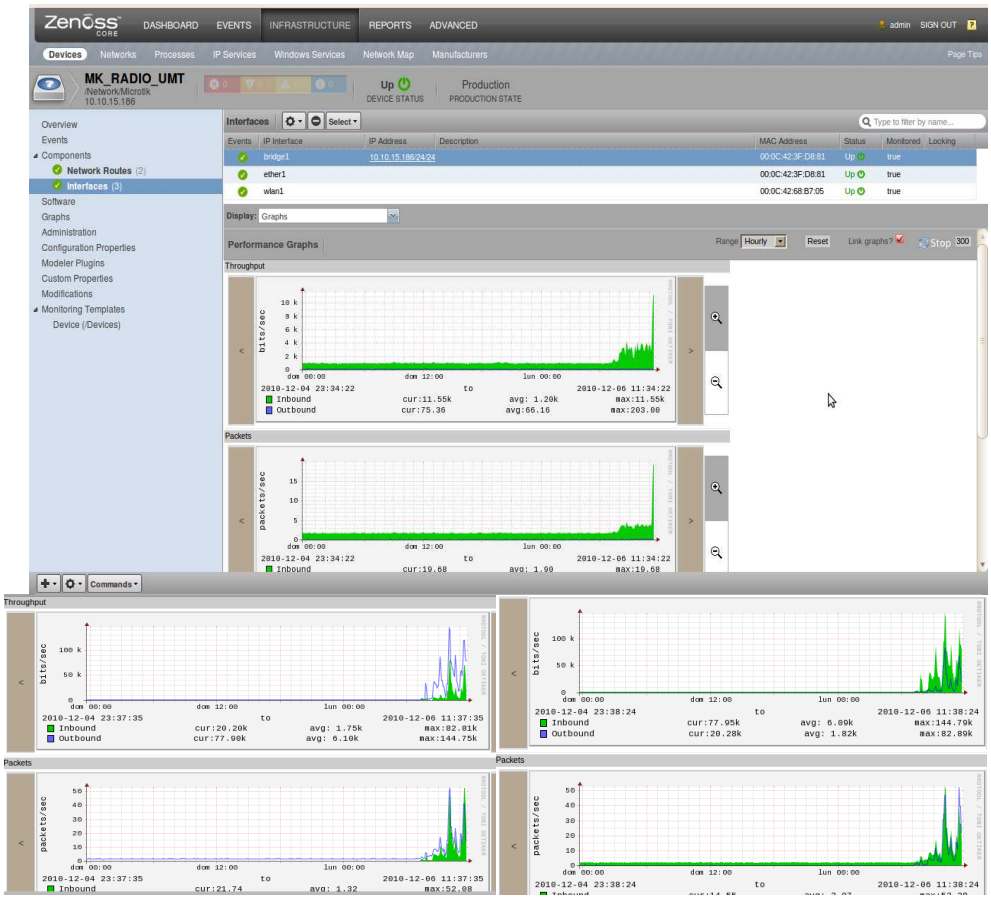


Figura IV.107 : Interfaces de Microtik UMT
Fuente: Investigador

En el equipo ubicado en la UMT no se registra mayor número de tráfico en las interfaces en el fin de semana, a lo contrario del día Lunes donde empiezan las actividades normales y en el que se puede apreciar la variación de tráfico en ciertas horas, esto sucede cuando hay afluencia de usuarios de las diferentes cooperativas que acuden a esta dependencia registrarlas o hacer actualizaciones de las mismas, es ahí donde los funcionarios realizan consultas o ingreso de información al sistema generando en ciertos momentos gran cantidad de tráfico.

Router

Los router que hacen parte de la infraestructura de networking del IMA, y se encuentran ubicados en diferentes dependencias, además en la herramienta al igual que los otros dispositivos están categorizados según su tipo, como a continuación se muestra.

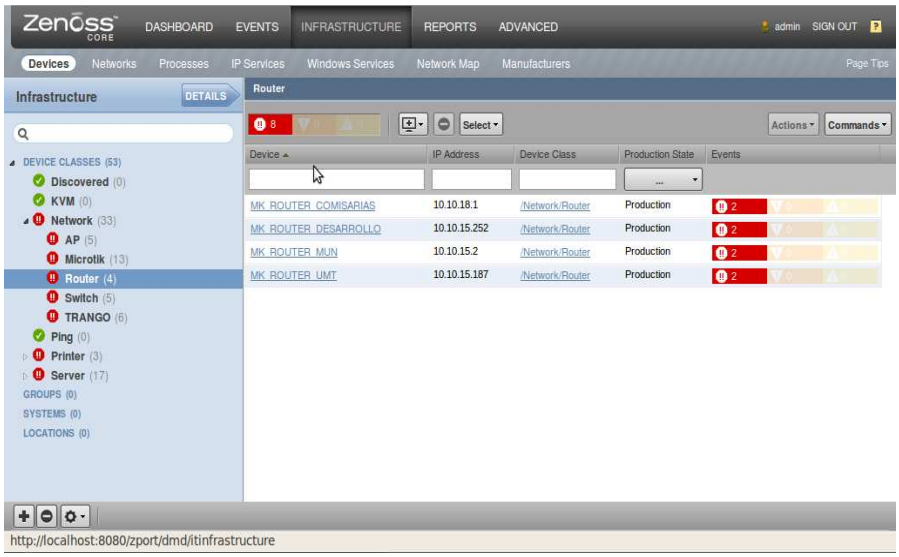


Figura IV.108 : Monitoreo de Router
Fuente: Investigador

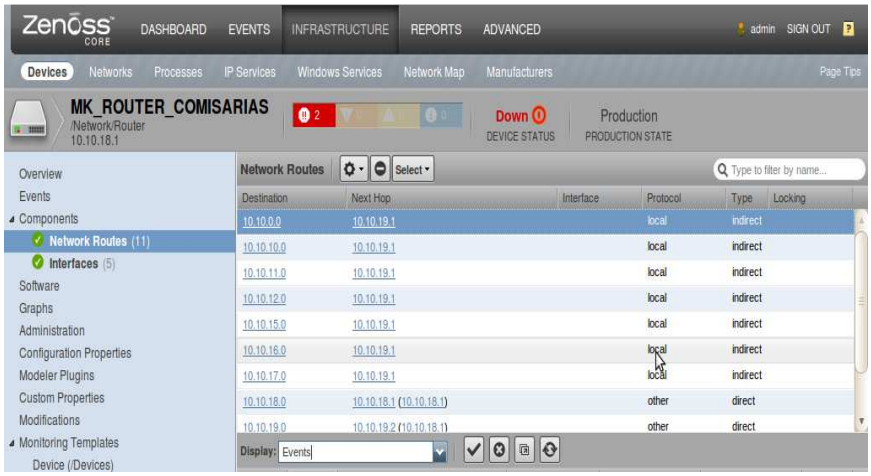


Figura IV.109 : Network Routes de Router de Comisarias
Fuente: Investigador

En los 4 Router existentes en la red de datos del IMA, localizados en el Municipio, Comisarias, UMT, y Desarrollo Social, se encuentran configuradas todas y cada una de las rutas por las cuales deben viajar los paquetes para llegar a las diferentes redes.

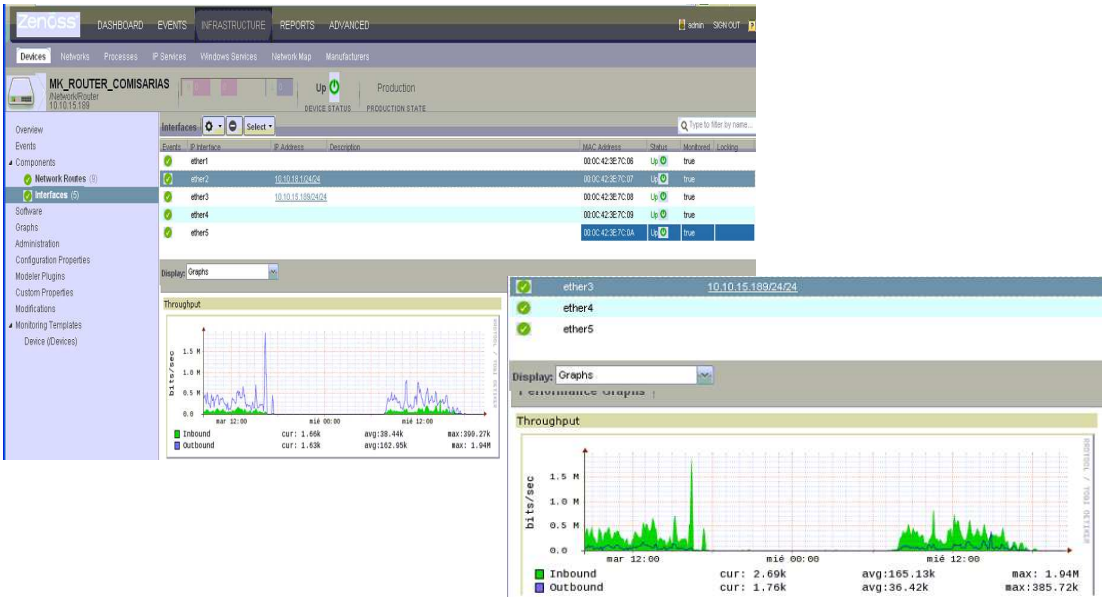


Figura IV.110 : Interfaces de Router de Comisarias
Fuente: Investigador

En los Routers podemos apreciar que generalmente están activas dos interfaz, la una que está conectada a la antena Microtik para el enlace y el otro puerto que está configurada para la LAN en cada dependencia, se observa en el router de Comisarias el tráfico en la LAN que está configurado en la eth3 es acorde la utilización de la red, ya que en esta dependencia se realizan pagos de algunos rubros y los picos más latos representas las horas en las cuales el cliente realiza los mismos, y las caídas bruscas de trafico se debe a que sucedió algún anomalía e hizo que el dispositivo se desconecte de la red y deje de funcionar, es considerable que en horas de la noche no existe presencia de trafico ya que no se está accediendo a ninguna información.

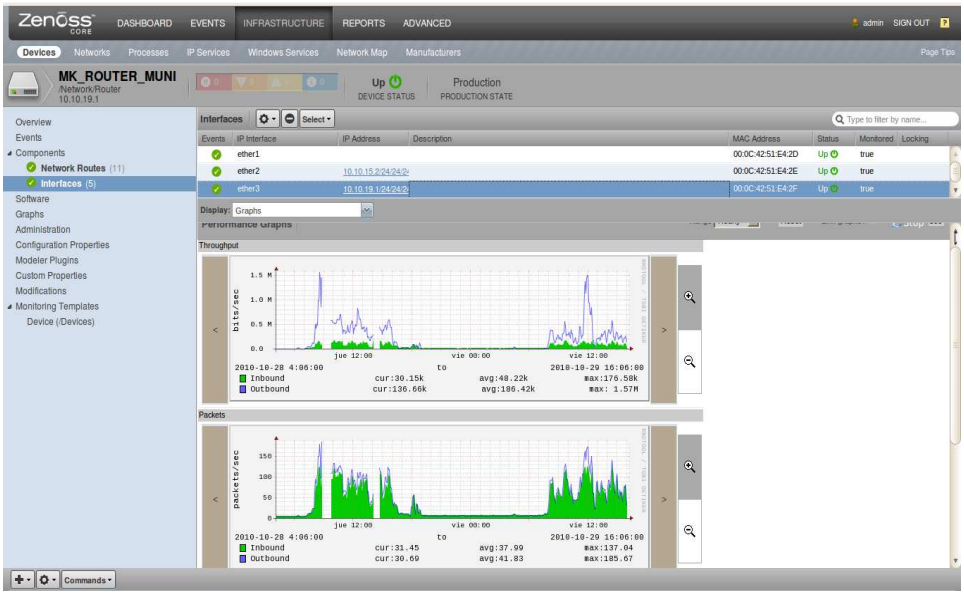


Figura IV.111 : Interfaces de Router del Municipio

Fuente: Investigador

El router que esta ubicado en el IMA, tiene la presencia de picos altos en el paso de paquetes, ya que en este router estan configuradas las rutas por las cuales llegar a las diferentes pisos que estan en otras redes, y exisiten varios departamentos que hacen uso de varias aplicaciones y a medida que los

clientes realizan peticiones el paso de paquetes se ira generando, se aprecia demás que se estabiliza el paso de paquetes cuando no se cuenta con la presencia de personal laborando.

Switch

En la infraestructura de red del IMA, existen varios switch de diferentes marcas, y modelos, se ha monitoreado todos los switch que son administrables y además que soportan el protocolo SNMP, y además se los ha organizado bajo la categoría ***SWITCH,*** siendo estos dispositivos los que continuación se presentan las graficas,

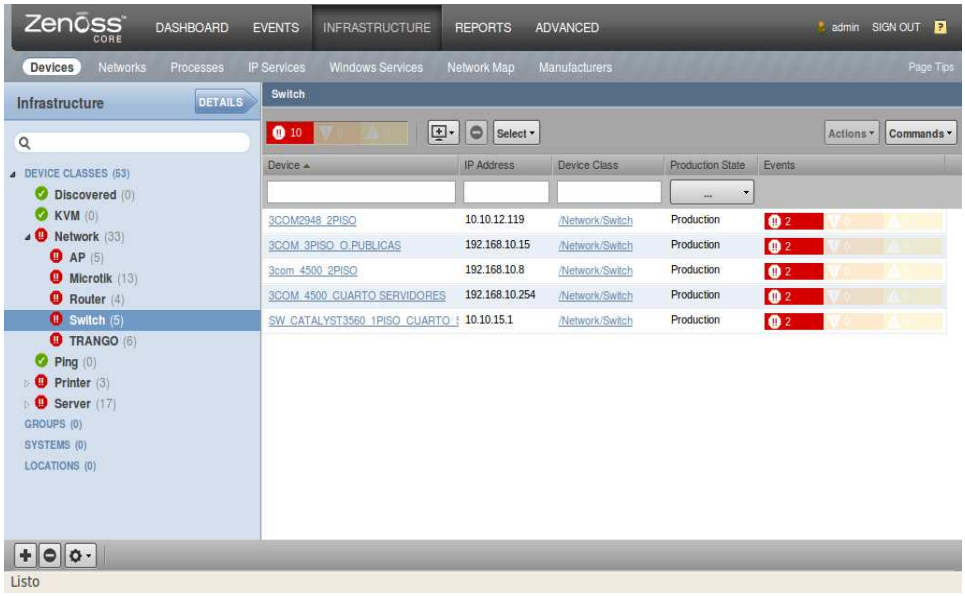


Figura IV.112 : Monitoreo de Switch

Fuente: Investigador

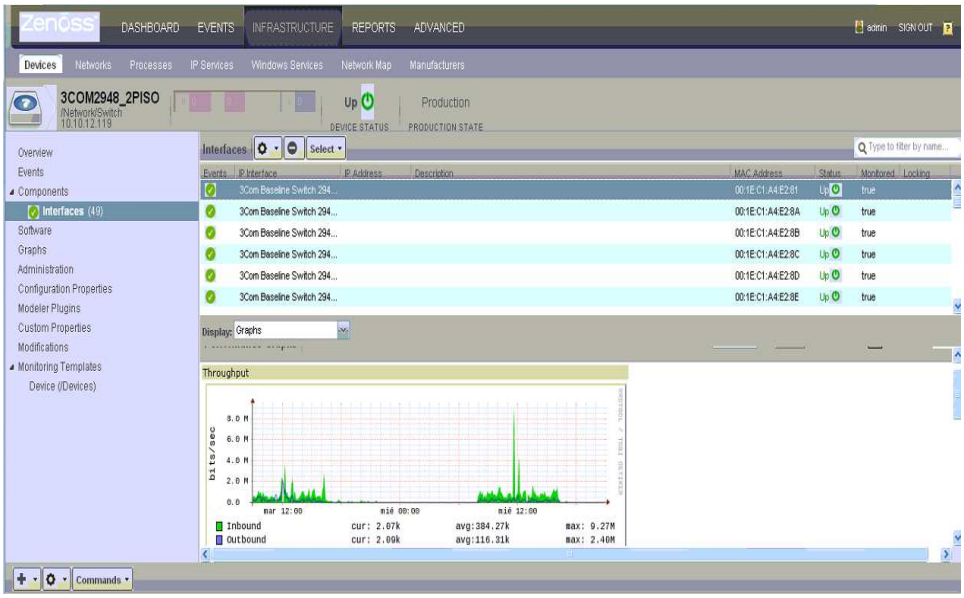


Figura IV.113 : Interface de Switch 3COM de Segundo Piso

Fuente: Investigador

En el switch 3com del segundo piso se puede observar que cuenta con 49 interfaces en la primera de sus interfaces el tráfico de entrada y salida es completamente normal, a excepción de un pico alto que sobrepasa los 8 Mbits/s, que se debe a que por ese puerto el grupo de clientes asignados realizaron numerosas peticiones o consultas a alguna aplicación del IMA.

Durante el proceso del monitoreo se detectó problemas en el Switch Catalyst 3560 que se encontraba en el cuarto de servidores, ya que están configuradas Vlan para servidores, y esto hacia que en el dispositivo exista congestión y cuellos de botella, no permitiendo que la red trabaje en completo rendimiento, es por eso que se realizó el cambio inmediato del switch a un Switch Catalyst 3560G con puertos a Gigabit.

A continuación se despliegan los resultados obtenidos, ya con el nuevo dispositivo.

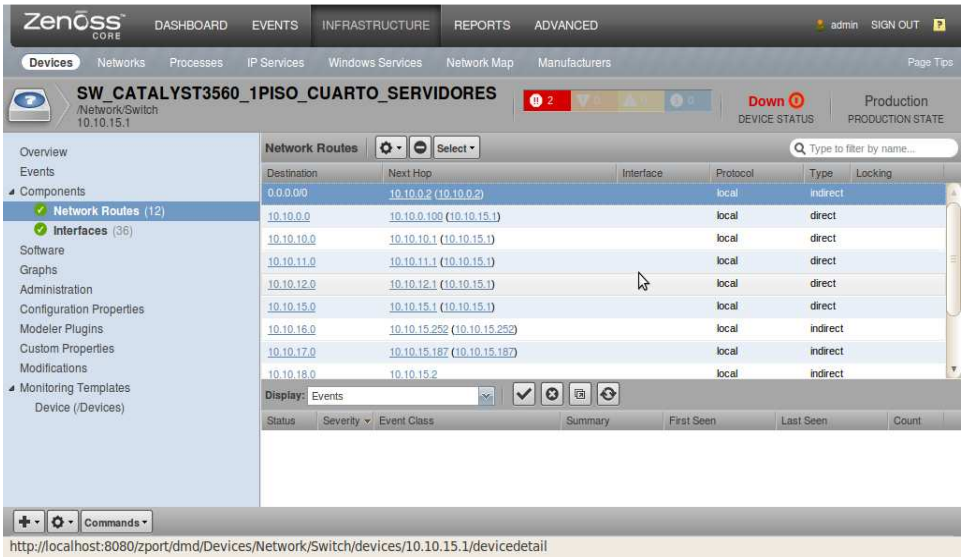


Figura IV.114 : Network Routes de Switch Catalyst 3560G Cuarto Servidores

Fuente: Investigador

Se observa el monitoreo del switch 3560G que se encuentra ubicado en el cuarto de servidores, este es un switch capa tres, en él están configuradas todas las Vlans y además las rutas para alcanzar a las diferentes redes.

En este switch se encuentra configuradas todas las vlans, por ejemplo vlan de servidores, vlan de Primer Piso, vlan de voz para conexión, Vlan de firewall, Vlan de Segundo Piso, Vlan de Tercer Piso, Vlan de Planta Baja, entre otras.

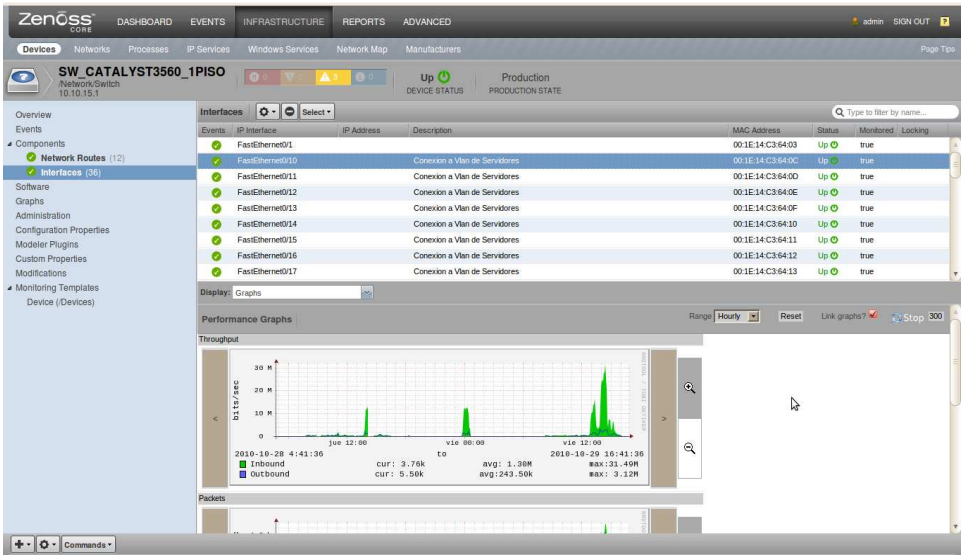


Figura IV.115 : Interface de Vlan de Servidores de Switch Catalyst 3560G

Fuente: Investigador

En la pantalla presentada se puede observar el throughput y los paquetes de entrada y salida, en las vlans configuradas en el switch 3560G, tanto los bits de entrada y salida como el tráfico de los paquetes generada, es totalmente normal, ya que no existen numerosos picos altos, que puedan afectar el rendimiento de la red. En el caso de la vlan de firewall se puede observar que el tráfico de los paquetes está dentro de los parámetros permitidos, el tráfico generado están en las horas laborables en la que el personal del IMA trabaja, los picos altos generados en paquetes de salida se debe a las múltiples peticiones atendidas a los usuarios.

Para el caso de la vlan de telefonía IP, esta se puede observar con grandes variaciones debido a que esta vlan funciona permanentemente en toda la red del IMA, es decir es una de las vlans que se encuentra operativa en todo momento ya que siempre se están atendiendo llamadas a las diferentes extensiones.

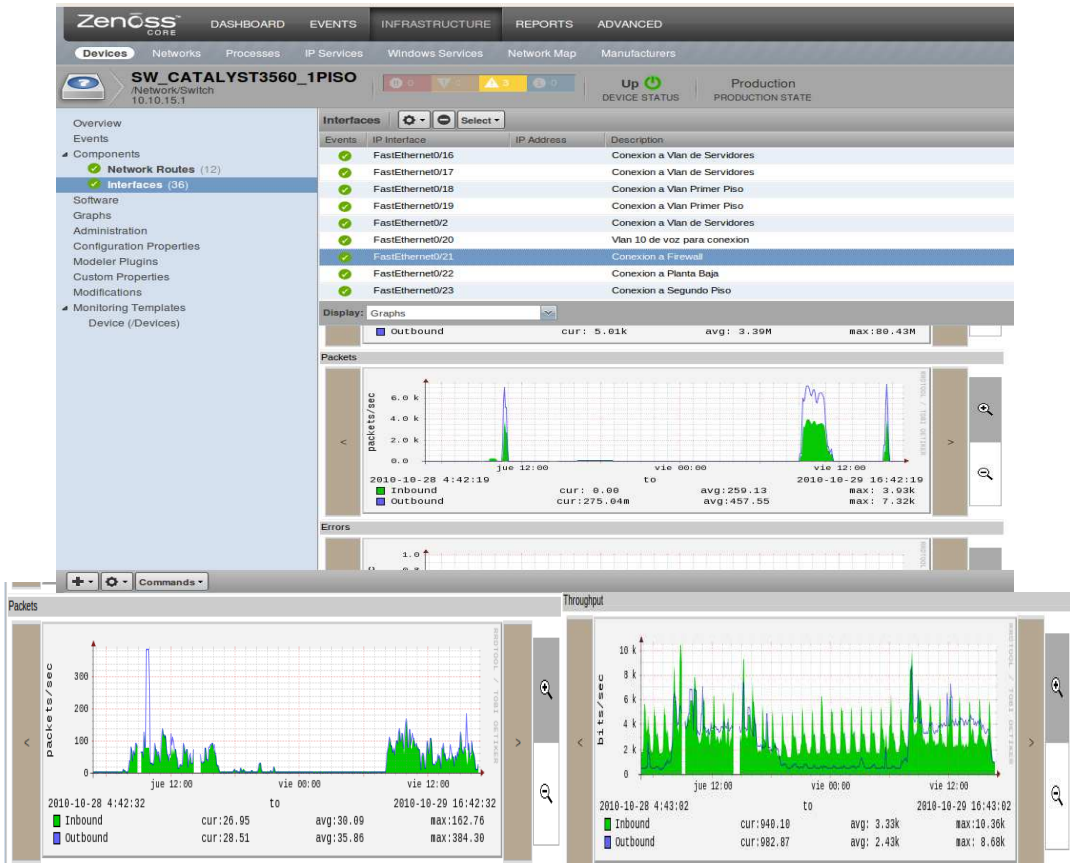


Figura IV.116 : Interface de Vlans de conexión de Firewall, Voz, de Sw Catalyst 3560G

Fuente: Investigador

Cabe recalcar el switch 3560G, tiene sus puertos a gigabit, esto es una gran ventaja ya que difícilmente van a llegar a saturarse, por lo que el funcionamiento de este ha sido completamente normal y no se han reportan anomalía alguna.

Trango

Además de las antenas microtik, en la red del IMA tenemos las antenas de marca Trango ha estos dispositivos se los hizo un tratamiento diferente a las anteriores, ya que este tipo de dispositivos no soportan el protocolo SNMP,

así que básicamente el monitoreo de estos dispositivos se lo está haciendo por PING, para ver el estado del dispositivo UP o DOWN en la red, para de esta forma detectar cual es el equipo que dejo de funcionar y en qué momento lo hizo.

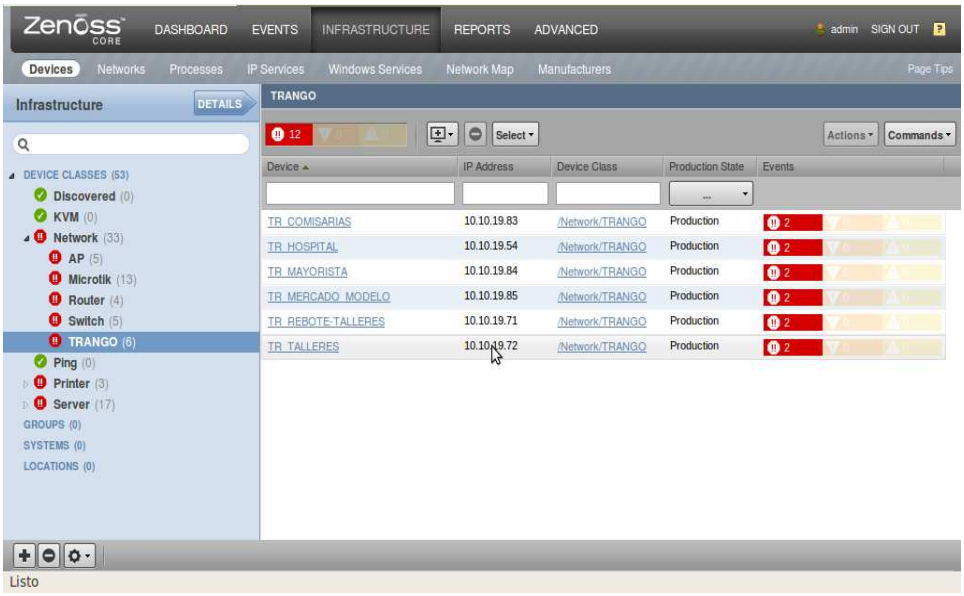


Figura IV.117 : Monitoreo de Antenas Trango

Fuente: Investigador

4.2.2.3. Monitorización Impresoras

A mas de monitorear el estado de las impresoras, se considera importante monitorear parámetros como el nivel de tóner utilizado, y el número de hojas impresas, estos parámetros se obtiene realizando un escaneo SNMP ayudado de la herramienta MIB-Browser ***(Ver Anexo 4)***, la cual devuelve las ramas MIB necesarias y las OID correspondientes, una vez obtenido esto se realiza la configuración necesaria para que empiece a graficar nuestra herramienta obteniendo los siguientes resultados.

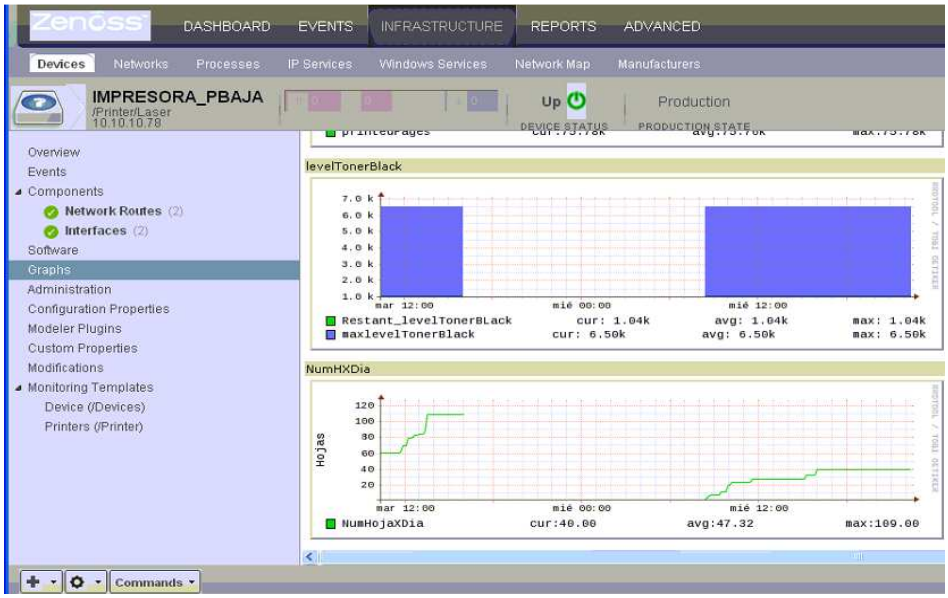


Figura IV.118 : Hojas Impresas y Nivel de tóner negro

Fuente: Investigador

Por lo general las impresoras que están siendo monitoreadas tiene el nivel de tóner sobre la mitad de uso, de esta forma el administrador se puede dar cuenta cuales necesitan ser cambiadas de tóner a tiempo y además llevar un control aproximado de cuantas hojas se imprimen, en la grafica mostrada observamos que se esa impresora realiza un aproximado de 45 hojas por dia, para de esta forma llevar un control.

4.2.2.4. Reportes

Nuestra herramienta de Administración y Monitoreo de red Zenoss, nos proporciona una serie de opciones definidas de informes personalizados, que incluye:

- Reportes de dispositivos
- Reportes de eventos
- Reportes de rendimiento
- Reportes de usuario
- Reportes Gráficos
- Reportes personalizados de dispositivos

Para trabajar con los reportes, debemos seleccionar Reportes en la barra de navegación. La lista de los reportes aparece en la vista de árbol. Expandimos un elemento de la lista para ver los reportes disponibles en esa categoría.

Reporte de Dispositivos

En esta sección, podemos apreciar un resumen en general de todos los dispositivos agregados a la herramienta Zenoss, mostrándonos por ejemplo el estado de los dispositivos en la red si están activos o no, el estado del protocolo de red SNMP en el cual están basado el monitoreo de los dispositivos, además un inventario de todos los software que están instalados en los dispositivos con sus fabricantes, etc.

Los reportes de esta categoría incluyen:

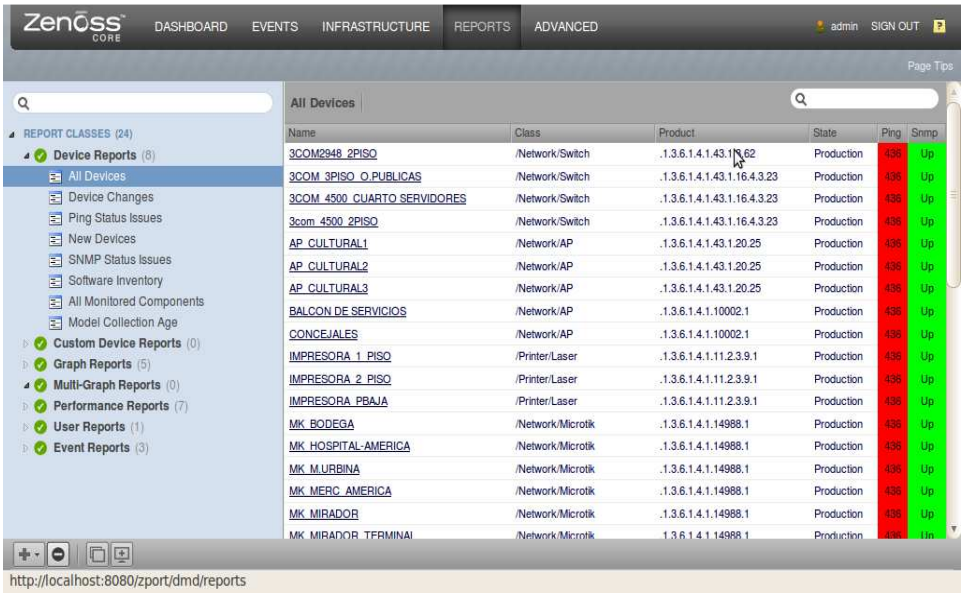


Figura IV.119 : Reporte de Dispositivos-Todos los Dispositivos

Fuente: Investigador

En este tipo de reporte se puede observar a todos los dispositivos añadidos para su monitoreo, especificado la clase a la que pertenece, la serie del producto o equipo, el estado en el que se encuentra, si se mantiene conectividad a través del Ping, y si el protocolo SNMP se encuentra Up o Down. Es un reporte en donde se muestra brevemente un resumen del estado de los equipos, esto servirá al administrador para guiarse que equipos están trabajando bien y cuáles no.

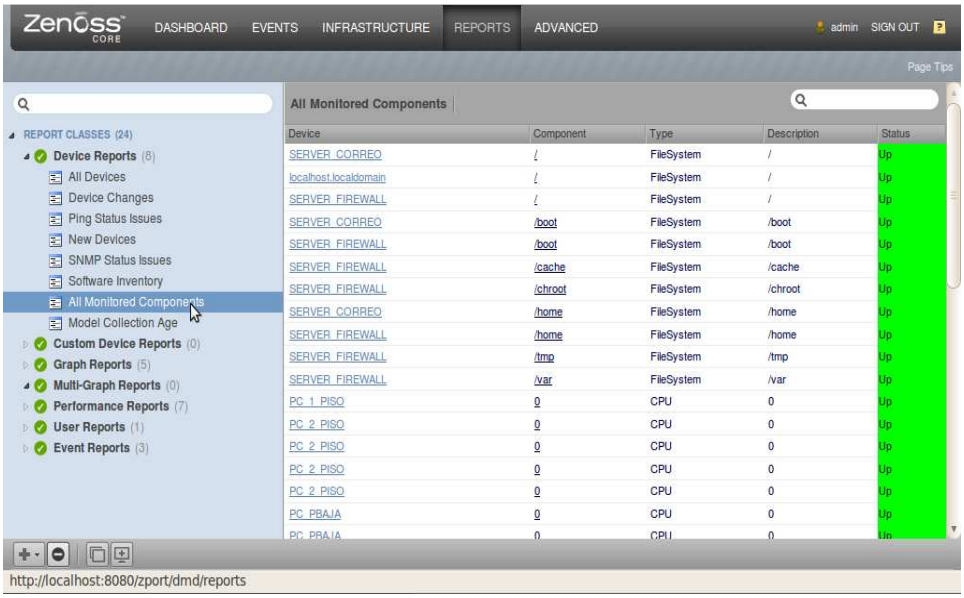


Figura IV.120 : Reporte de Dispositivos- Todos los componentes monitoreados

Fuente: Investigador

En la pantalla mostrada se puede apreciar un reporte de todos los componentes monitoreados por cada dispositivo, como Sistema de Archivos, CPU, Interfaces, Discos Duros, etc., el tipo al que corresponde cada componente, una breve descripción y el estado en el que se encuentran, si se encuentran Up o Down, mediante este reporte se podrá conocer que componente no está trabajando de manera adecuada.

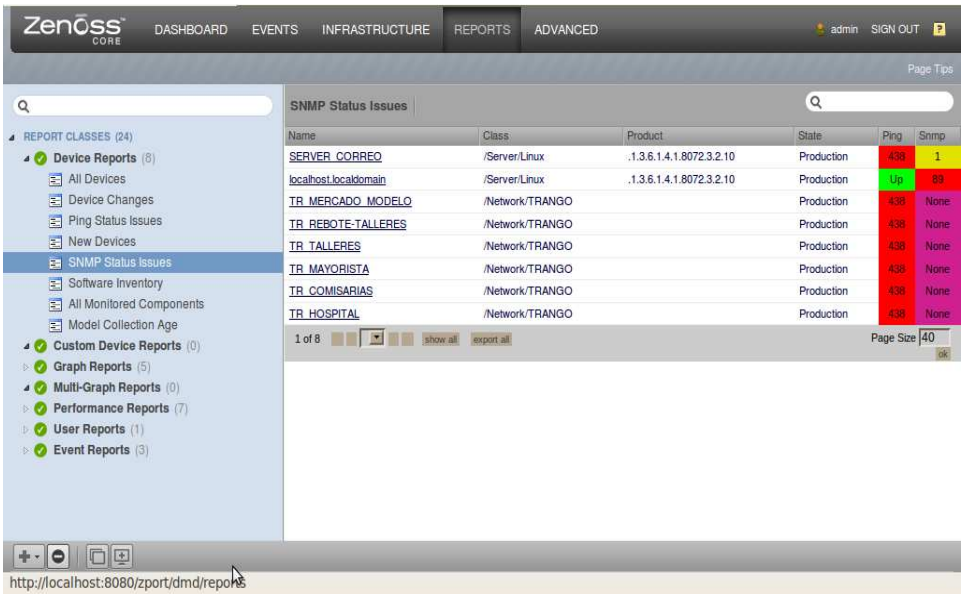


Figura IV.121 : Reporte de Dispositivos- Estado de SNMP

Fuente: Investigador

En esta clase de reporte se puede observar que una vez que el equipo por cualquier circunstancia ha perdido conectividad con el servidor donde está siendo monitoreado mostrará el número de veces que el servidor por medio de el Ping y el protocolo SNMP intenta volver a conectarse y obtener información con el dispositivo. En el caso de las antenas Trango solo se podrá observar las veces que intenta conectarse por medio del Ping, ya que estos equipos no soportan SNMP.

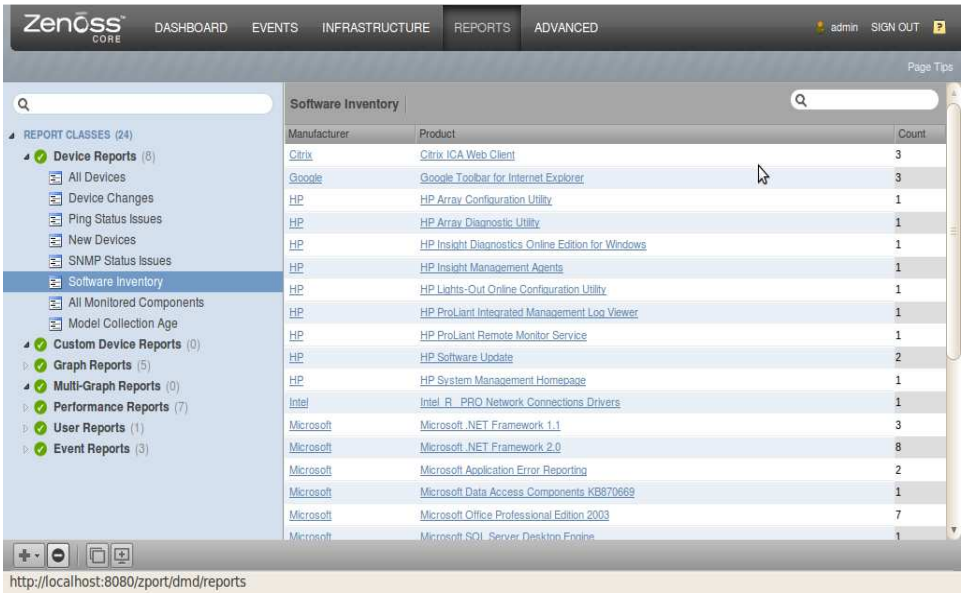


Figura IV.122 : Reporte de Dispositivos- Inventario de software

Fuente: Investigador

En la imagen se puede observar un inventario de todo el software instalado en los diferentes equipos monitoreados, el fabricante al que pertenece, la clase de producto, y el número de equipos que tienen instalado el software, por ejemplo del fabricante HP, el producto HP Software Update solo tienen instalado dos equipos.

Reportes de Rendimiento

Este tipo de reportes proporcionan los datos de rendimiento en todo el sistema. Incluyen una mezcla de gráficos e informes basados en texto, para de esta manera tener una perspectiva diferente en cuanto a porcentajes, además se pueden filtrar la presentación de información dependiendo de los requerimientos del administrador:

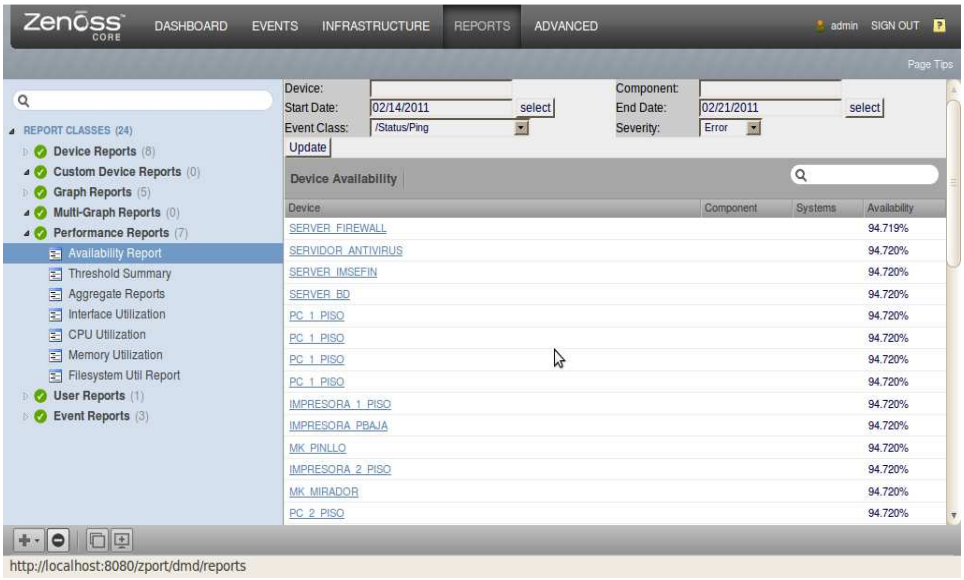


Figura IV.123 : Reporte de Rendimiento - Reporte de Disponibilidad

Fuente: Investigador

En este informe se puede conocer el porcentaje de disponibilidad de cada uno de los equipos, se puede observar que la disponibilidad de la mayor parte de dispositivos es sobre el 90%, es decir están trabajando normalmente.

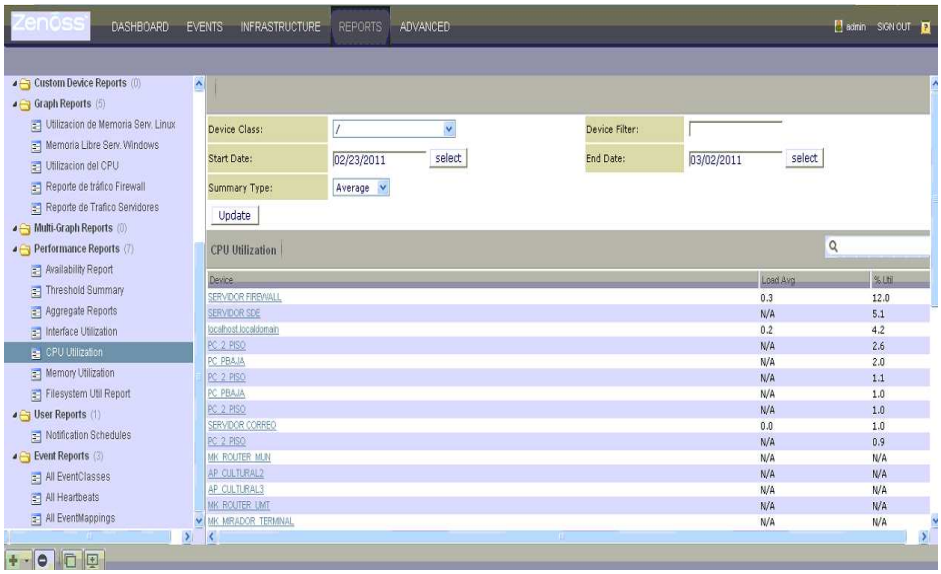


Figura IV.124 : Reporte de Rendimiento - Reporte de utilización del CPU

Fuente: Investigador

En el reporte acerca de la utilización del CPU, se puede obtener datos como el porcentaje de la carga promedio y el porcentaje de utilización del CPU, estos datos por lógica solo se pueden obtener de los servidores y host, con esta información recolectada se podrá tener una visión clara acerca del rendimiento de cada equipo.

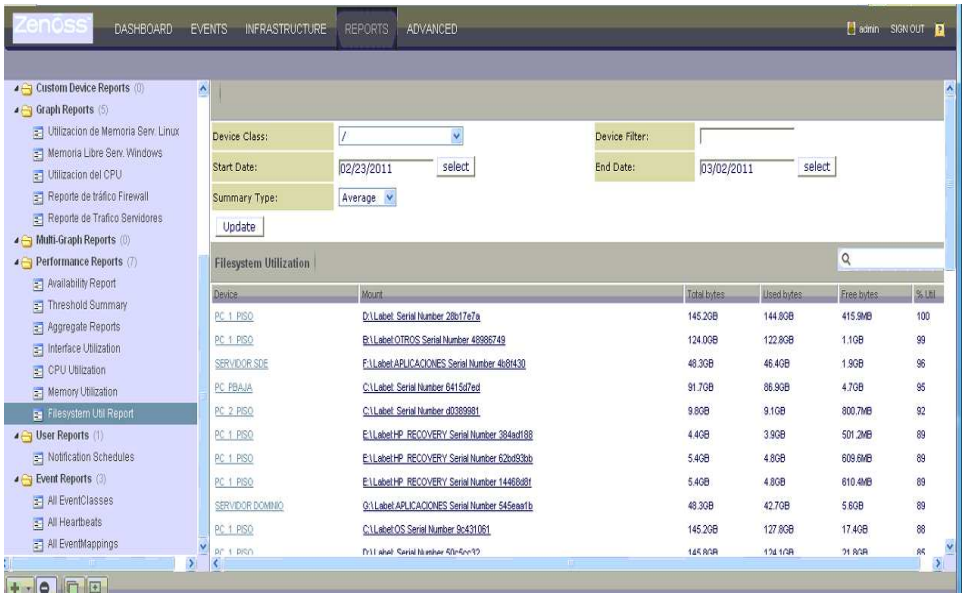


Figura IV.125 : Reporte de Rendimiento - Reporte de utilización del sistema de archivos

Fuente: Investigador

En la figura anterior se puede observar un informe completo en forma estadística acerca del uso de las interfaces de los equipos, se presentan en porcentajes el total de bytes asignados, cuanto espacio todavía se dispone libre y cuanto se ha utilizado, así como también el porcentaje de utilización de cada uno de las particiones o sistemas de archivos de los servidores y host monitoreados. En el caso del servidor de Base de Datos se puede observar que en la partición F, de los 48.3 GB asignados el 46.4 se encuentra ya utilizado, el porcentaje de utilización de esta partición es del 96%.

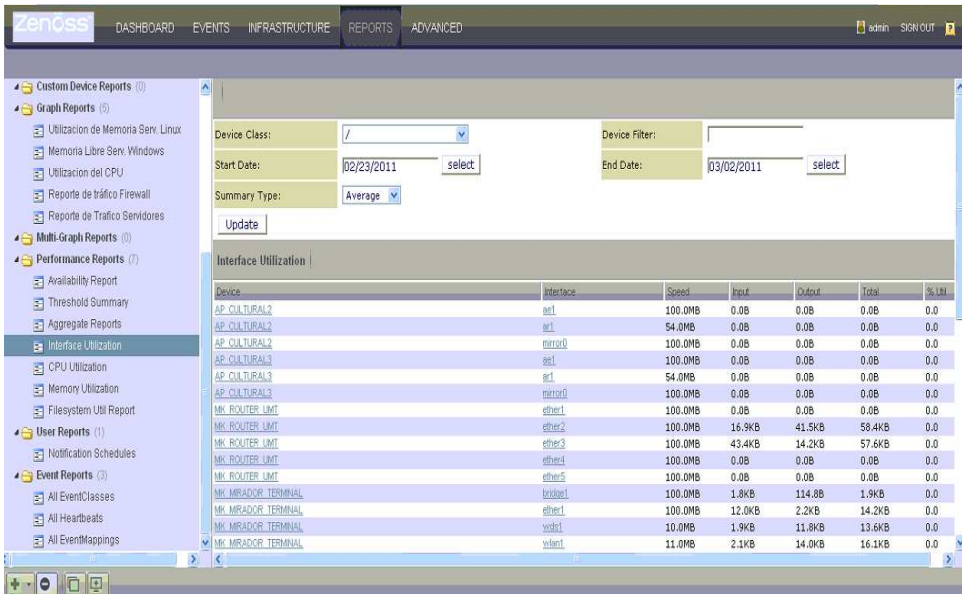


Figura IV.126 : Reporte de Rendimiento - Utilización de la interfaz

Fuente: Investigador

Otro de los reportes sumamente importantes para el administrador de la red es el reporte de la utilización de las interfaces de los dispositivos de red, gracias a este reporte se podrá obtener de manera rápida una estadística de funcionamiento de cada una de las interface de cada dispositivo, ya que nos presenta de la velocidad a la que está corriendo la interfaz, los bits de entrada y salida, y el porcentaje de utilización que tiene cada interfaz, así se podrá saber de manera rápida que interfaces están presentando anomalías en su desempeño, como toda esta información esta presentada estadísticamente será más fácil para el administrador sacar sus conclusiones.

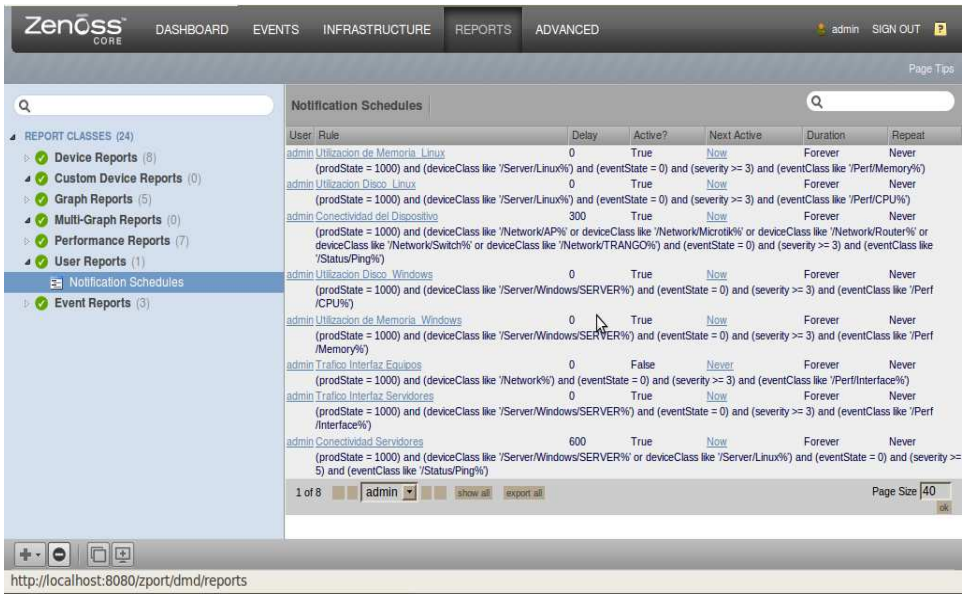


Figura IV.127 : Reportes de Notificaciones a usuarios

Fuente: Investigador

Con este reporte se puede obtener un listado de la configuración de cada una de las alarmas y a que usuario fue enviada está notificación en caso de que se activo.

Reportes Gráficos

Este tipo de reportes añade el usuario dependiendo de las necesidades, y requerimientos que se deseen visualizar, en este caso se presentan reportes graficos de la Utilización de memoria de servidores Linux, Memoria libre en servidores Windows, Utilización del CPU, Tráfico en la interfaz de los servidores, etc, resumiéndolos en un solo gráfico, para hacer fácil la interpretación de resultados.

En las ilustraciones a presentadas a continuación, podemos observar que la memoria de los servidores esta usada casi en su totalidad en un promedio de 97%, y ciertamente también está ocupando un lugar considerable la memoria

cache, este espacio insuficiente de memoria hace que el servidor trabaje presente problemas en su normal desempeño, es por eso que se recomienda liberar el espacio en memoria cache de los servidores.

Figura IV.128 : Uso de memoria en Servidor de Firewall

Fuente: Investigador

En las figuras siguientes se muestran los servidores basados en Windows, en estos al contrario de los servidores Linux se reporta la memoria libre, en este reporte mientras menos memoria libre se tenga más ocupado estará la memoria del servidor, apreciamos que tenemos suficiente espacio de memoria en el servidor de Antivirus.

Figura IV.129 : Memoria Libre en Servidor de Antivirus

Fuente: Investigador

Finalmente se requiere visualizar el tráfico en las interfaces de los servidores, dependiendo de lo que se solicite visualizar y de cuales interfaces se requiere, se puede configurar.

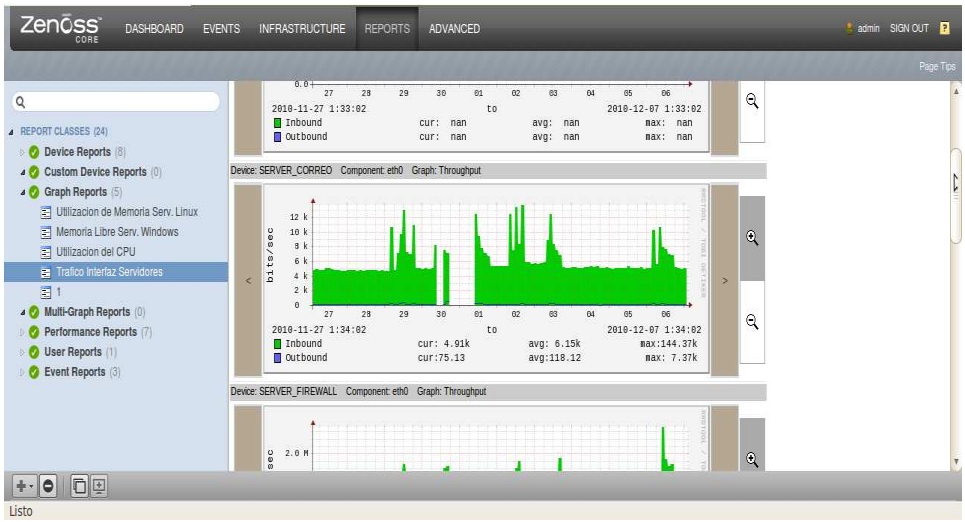


Figura IV.130 : Tráfico en Servidor de Correo

Fuente: Investigador

4.2.3. TABLA DE PROBLEMAS Y SOLUCIONES

Luego de haber realizado el monitoreo a todos y cada uno de los dispositivos existentes en la red, que soporten el protocolo SNMP, se puede resaltar los problemas que existen y las posibles soluciones que se sugiere para contrarrestar y hacer q la red trabaje en su máximo rendimientos y de esta manera brindar mejor servicios como institución.

PROBLEMA	SOLUCION
En el Servidor de Dominio se detecto problemas al instante de recolectar la información SNMP para las graficas de memoria, cpu y paginación, no se obtuvo debido a falencias en hardware.	*Se propone migrar este servidor al servidor blade, el cual se encuentra disponible en el departamento, para un mejor despeño de este servidor de vital importancia dentro de la red.*
Se sospechó la presencia de virus en el servidor de Dominio y Correo, ya que el acceso a la interfaz en estos tiene muchas variaciones inesperadas y esto hace que el servidor no trabaje en completa normalidad.	*Se sugiere realizar un escaneo profundo para la detección del virus y reparación del mismo.*
En el Servidor de Firewall se identificó el poco espacio en memoria, ya que esta usado un promedio de 98%, del cual usa gran espacio la memoria cache con un 45%, que es un espacio considerable.	*Se recomienda liberar el espacio de memoria cache, para de esta forma expandir el espacio de memoria libre.*
Se detectó problemas en el Switch Catalyst 3560 ubicado en el cuarto de servidores, ya que sus puertos trabajan a 100 Megabits, produciendo congestión y	*Se realizó el cambio inmediato del switch a un Switch Catalyst 3560G con puertos a Gigabit.*

cuellos de botella, ya que ahí están conectados los servidores de la Institución.	
En la antena MK ubicada en el IMA que hace el enlace con la radio base que se encuentra en Pillishurco se descubrió anomalías en el funcionamiento de dispositivo, ya que perdía conectividad y cuando lo tenía presentada tiempos muy altos de ping, detectándose así que el Router Board del equipo por averías eléctricas se quemó.	*Se realizó el reemplazo por una nueva Router Board, seguidamente se comprobó a través de la herramienta si ésta ya estaba funcionando de manera normal, y en la actualidad no ha presentado ningún inconveniente.*
Las antenas de marca Trango, no soportan el protocolo SNMP, este parámetro hace que se reduzca la calidad de monitoreo, ya que no se obtiene la suficiente información para detectar problemas.	*Se propone realizar el cambio de antenas por otras que sean administrables.*

Tabla IV.XXVI : Problemas y Soluciones de la red de networking del IMA

Fuente: Investigador

Luego del proceso de monitoreo e identificación de problemas y soluciones en el esquema de infraestructura de red del Ilustre Municipio de Ambato, se realizaron algunas modificaciones, las mismas que ayudarán a tener una mejor visión de la distribución de los equipos ***(Ver Anexo 7, 8)***.

4.3. COMPROBACIÓN DE LA HIPÓTESIS

4.3.1. Hipótesis

La implementación de una Herramienta OpenSource basado en SNMP para la Administración y Monitoreo de la red del Municipio de Ambato mejorará la gestión del administrador y la productividad de la red de datos.

4.3.2. Tipo de hipótesis

Hipótesis de Investigación

4.3.3. Población y Muestra

La encuesta ***(Ver Anexo 5)*** se la aplicó a todo el personal del departamento de informática del IMA, además al personal que se encuentra a cargo de la administración en las otras dependencias, siendo realizadas 10 encuestas en su totalidad.

4.3.4. Operacionalización de variables

Variable Independiente

Herramienta OpenSource basado en SNMP para la Administración y Monitoreo de la red.

Variable Dependiente

Gestión del administrador

Productividad de la red de datos.

Operacionalización Conceptual

VARIABLE	TIPO	CONCEPTO
Herramienta OpenSource basado en SNMP para la Administración y Monitoreo de la red.	Independiente	Realiza actividades de escaneo de la red, e identifica problemas que se presentan en las mismas.
Gestión del administrador	Dependiente	Encargado de realizar la supervisión, gestión y diseño de la red, seguimiento de incidencias, planificación de ampliaciones y cambios en los equipos de red.
Productividad de la red de datos.	Dependiente	Capacidad de trabajo de los recursos de la red para minimizar los tiempos que se demoran en resolver problemas.

Tabla IV.XXVII : Operacionalización Conceptual

Fuente: Investigador

Operacionalización Metodológica

VARIABLE	CATEGORÍA	INDICADORES	TÉCNICAS	FUENTE DE VERIFICACIÓN
Herramienta OpenSource basada en SNMP para la administración y monitoreo de a red	Actividad Investigación	- Usabilidad	- Revisión de documentos. - Observación directa.	- Internet
Gestión del administrador	Actividad Investigación	- Tiempo empleado para detectar un problema. - Tiempo empleado para resolver un problema. - Recursos usados.	- Observación directa.	- Departamento informática IMA.
Productividad de la red de datos.	Actividad Investigación	- Tráfico de la red. - Porcentaje de uso de los recursos de los dispositivos hardware. - Tiempos de respuesta. - Nivel de Operatividad de la red.		- Herramienta de administración y monitoreo.

Tabla IV.XXVIII : Operacionalización Metodológica
Fuente: Investigador

4.3.5. Comprobación de la hipótesis de la investigación realizada

4.3.5.1. Planteamiento de las hipótesis.

Ho: "La Implementación de una herramienta OpenSource basado en SNMP para la Administración y Monitoreo de la red del Municipio de Ambato, no mejora la gestión del administrador y la productividad de la red de datos"

Hi: "Implementación de una herramienta OpenSource basado en SNMP para la Administración y Monitoreo de la red del Municipio de Ambato, mejora la gestión del administrador y la productividad de la red de datos"

4.3.5.2. Nivel de significancia

Una vez establecida la hipótesis nula y alternativa, se debe determinar el nivel de significancia, que para el caso del presente análisis se utilizará un nivel de significación estadística de **α = 0,05,** ya que es probable que la herramienta ganadora para la implementación no se pueda usar para todos los dispositivos existentes en la red de networking del Ilustre Municipio de Ambato.

4.3.5.3. Criterio.

De acuerdo al análisis desarrollado en la presente investigación, se ha seleccionado como estadístico de prueba de hipótesis la técnica ***"chi-cuadrado".*** La fórmula que da el estadístico es la siguiente:

$$x^2 = \sum_i \frac{(observada_i - esperada_i)^2}{esperada_i}$$

Para conocer las frecuencias teóricas o esperadas, se calculan a través del producto de los totales marginales *(total del renglón x total de columna)*, dividido por el número total de casos *(gran total):*

$$fe = \frac{\textit{(total del renglón) * (total de la columna)}}{\textit{gran total}}$$

En la ***tabla*** se pueden observar los resultados de los cálculos, tanto de la frecuencia esperada, como la del valor de "$x^2_{calculado}$", luego de haber aplicado las fórmulas anteriores.

Ahora es necesario determinar el **criterio de decisión**. Entonces se acepta **Ho** cuando:
$x^2_{calculado} < x^2_{tabla}$, en caso contrario se rechaza **Ho**.

Donde el valor de x^2_{tabla} representa el valor proporcionado por la tabla de "distribución x^2", según el nivel de significación elegido y los grados de libertad.

Como se mencionó anteriormente, el nivel de significancia adoptado para esta investigación es de **α = 0,05.**

Para la determinación de los grados de libertad **(gl)** se debe aplicar la siguiente fórmula:

$$\mathbf{gl= (r - 1) * (k-1)}$$

Donde ***r*** el número de filas o renglones y ***k*** el de columnas. La investigación generó una matriz de 4r x 2k. (Ver detalle en tabla 12 del ítem "Cálculos").

Entonces:

gl = (4-1) * (2-1)

gl = (3) * (1)

gl = 3 grado de libertad

De acuerdo a la tabla estadística de distribución de chi-cuadrado, con un nivel de significancia 0,05 a 3 grado de libertad, genera un valor de $\mathbf{x^2_{tabla}}$ **= 7.815**

Degrees of Freedom	**Possibility of Chance Occurrence in Percentage (5% or Less Considered Significant)**								
	90%	**80%**	**70%**	**50%**	**30%**	**20%**	**10%**	**5%**	**1%**
1	0.016	0.064	0.148	0.455	1.074	1.642	2.706	3.841	6.635
2	0.211	0.446	0.713	1.386	2.408	3.219	4.605	5.991	9.210
3	0.584	1.005	1.424	2.366	3.665	4.642	6.251	**7.815**	11.341
4	1.064	1.649	2.195	3.357	4.878	5.989	7.779	9.488	13.277
5	1.610	2.343	3.000	4.351	6.064	7.289	9.236	11.070	15.086
6	2.204	3.070	3.828	5.348	7.231	8.558	10.645	12.592	16.812
7	2.833	3.822	4.671	6.346	8.383	9.083	12.017	14.067	18.475
8	3.490	4.594	5.527	7.344	9.524	11.030	13.362	15.507	20.090
9	4.168	5.380	6.393	8.343	10.656	12.242	17.684	16.919	21.666

Tabla IV.XXIX : Distribución de X"
Fuente: Estadística A - Distribución Chi-Cuadrado. Ing. José Manuel García.

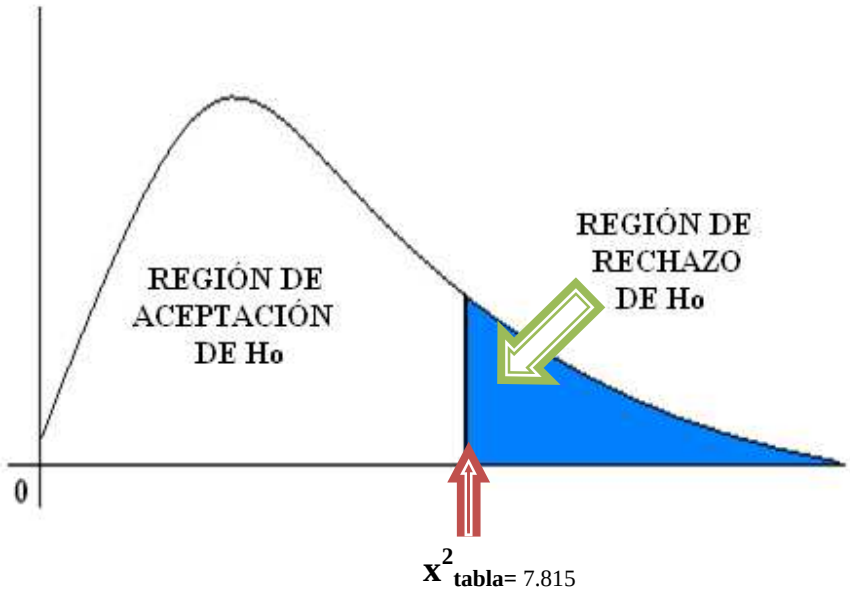


Figura IV.131 : Demostración de la Hipótesis
Fuente: Investigador

La regla de decisión es entonces: No rechazar Ho si el valor que se encuentre para x2calculado es menor que 7.815. Si el valor calculado es igual o mayor al valor crítico, se rechaza Ho y se acepta Hi.

4.3.5.4. Cálculos

Los resultados que arrojó la investigación realizada ***(Ver Anexo 6)*** se resume en las tablas mostradas a continuación:

FACTIBILIDAD		
PREGUNTAS	**MEJORA**	**NO MEJORA**
Preg.1	10	0
Preg.8	8	2
TOTAL	**18**	**2**

Tabla IV.XXX : Resultados de encuesta sobre “Factibilidad”
Fuente: Investigador

GESTION		
PREGUNTAS	**MEJORA**	**NO MEJORA**
Preg.2	6	4
Preg.3	4	6
Preg.7	8	2
TOTAL	**18**	**12**

Tabla IV.XXXI : Resultados de encuesta sobre "Gestión"
Fuente: Investigador

USABILIDAD		
PREGUNTAS	**MEJORA**	**NO MEJORA**
Preg.4	8	2
TOTAL	**8**	**2**

Tabla IV.XXXII : Resultados de encuesta sobre "Usabilidad"
Fuente: Investigador

PRODUCTIVIDAD		
PREGUNTAS	**MEJORA**	**NO MEJORA**
Preg.5	9	1
Preg.6	8	2
Preg.9	10	0
TOTAL	**27**	**3**

Tabla IV.XXXIII : Resultados de encuesta sobre "Productividad"
Fuente: Investigador

La matriz de resultados queda conformada de la siguiente manera:

Gestión del Administrador y la Productividad de la Red / **Herramienta OpenSource basado en SNMP para la Administración y Monitoreo**	**MEJORA**	**NO MEJORA**	**TOTAL**
FACTIBILIDAD	18	2	**20**
GESTION	18	12	**30**
USABILIDAD	8	2	**10**
PRODUCTIVIDAD	27	3	**30**
TOTAL	**71**	**19**	**90**

Tabla IV.XXXIV : Matriz (4r*2k) sobre resultados totales de la encuesta

Fuente: Investigador

Gestión del Administrador y la Productividad de la Red / Herramienta OpenSource basado en SNMP para la Administración y Monitoreo	MEJORA	NO MEJORA	TOTAL
FACTIBILIDAD	16	4	**20**
GESTION	24	6	**30**
USABILIDAD	8	2	**10**
PRODUCTIVIDAD	24	6	**30**
TOTAL	**72**	**18**	**90**

Tabla IV.XXXV : Valores Esperados
Fuente: Investigador

Ahora, se diseña la tabla para aplicar la fórmula de chi-cuadrado:

	fo	**fe**	**$(fo-fe)^2 /fe$**
La Herramienta OpenSource mejora la factibilidad	18	16	0.25
La Herramienta OpenSource mejora la Gestión del Administrador	18	24	1.50
La Herramienta OpenSource mejora la Usabilidad	8	8	0
La Herramienta OpenSource mejora la Productividad de la Red de Datos	27	24	0.375
La Herramienta OpenSource no mejora la factibilidad	2	4	1
La Herramienta OpenSource no mejora la Gestión del Administrador	12	6	6
La Herramienta OpenSource no mejora la Usabilidad	2	2	0
La Herramienta OpenSource no mejora la Productividad de la Red de Datos	3	6	1.5
TOTAL	**90**	**90**	**10.625**

Tabla IV.XXXVI : Frecuencias Observadas / Frecuencia Esperada
Fuente: Investigador

4.3.5.5. Decisión

Como:

$\mathbf{x^2_{calculado} = 10.625}$ y
$\mathbf{x^2_{tabla} = 7.815}$

Entonces:

$$\mathbf{x^2_{calculado} > x^2_{tabla}}$$

Lo que significa que $\mathbf{x^2_{calculado}}$, está en la zona de rechazo de la $\mathbf{H_0}$, entonces se concluye que se rechaza la hipótesis nula y se acepta la de investigación, esto es que

"La Implementación de una herramienta OpenSource basado en SNMP para la Administración y Monitoreo de la red del Municipio de Ambato, mejora la gestión del administrador y la productividad de la red de datos"

CONCLUSIONES

1. Para evaluar las herramientas seleccionadas que fueron escogidas como objeto de estudio en la presente investigación, se tomó en cuenta varios parámetros para el estudio comparativo, los mismos que fueron seleccionados cuidadosamente, resultando de esta la herramienta ganadora ZENOSS con 97.6%, ya que cumplió con la mayoría de los parámetros propuestos.

2. Con este análisis se puede concluir la importancia del protocolo SNMP para contar con un seguimiento del estado de los dispositivos que se encuentran dentro de una red y de esta forma prevenir lamentables pérdidas de la información que viaja a través de la misma.

3. El entorno gráfico que brinda Zenoss para la administración de dispositivos se considera como uno de los más agradables e intuitivos en el ambiente "opensource" convirtiendo esta herramienta en una de las principales opciones de NMS, además el constante y robusto sistema de apoyo por parte de entidades como la "comunidad Zenoss" en la elaboración y corrección de utilidades, brindan alta confiabilidad en el momento de buscar ayuda.

4. Una vez detectados los problemas presentes en la red del IMA, se los analizó todos y cada uno, como falta de memoria en servidores, presencia de virus, anomalías en los puertos de sw, caídas inesperadas de enlaces y se propuso soluciones para contrarrestar los mimos y hacer que la red trabaje bajo normalidad, teniendo pronta respuesta en varios de estas.

5. La Implementación de la herramienta Zenoss para la administración y monitoreo de la red del Municipio de Ambato, resultó de gran utilidad ya que se optimizó la gestión del administrador en cuanto a detección y solución de problemas

presentados en la red, reduciendo de esta forma tiempo hombre y recursos, que se usaban antes de la implementación de la herramienta, además la productividad de la red de datos mejoró haciendo que las aplicaciones no presenten problemas.

RECOMENDACIONES

1. Se recomienda al personal del departamento de Informática del IMA realizar actualizaciones constantes en el inventario de dispositivos dentro de la red, constando en este, las configuraciones de Ip y ubicación de los equipos, para de esta manera tener organizada la red.

2. Para que la calidad de servicio que brinda el IMA mejore, es recomendable realizar los cambios en las antenas Trango, ya que por lo general esas producen caídas de enlaces y por ende molestias a los usuarios.

3. A medida que los dispositivos se van renovando o incrementando en la red de networking es necesario ir añadiéndolos a la herramienta, para de esta forma contar con el monitoreo del estado de los dispositivos de forma centralizada.

4. Ser cuidadosos al momento de realizar las actualizaciones de versión de la herramienta y de los componentes de la misma, ya que existe una variación de uso de librerías, y hacer mal este proceso puede llevar a la caída del servidor.

RESUMEN

La investigación realizada está orientada al análisis comparativo de herramientas OpenSource para la administración y monitoreo de red basado en el Protocolo Simple de Administración de Red **(**SNMP**)**, para seleccionar la mejor en utilidad y eficiencia, y aplicarla en la intranet del Ilustre Municipio de Ambato, con el objetivo de administrar, monitorear y mantener funcionando la red con calidad, permitiendo controlar el estado de equipos y dispositivos, para conseguir la mejora en la gestión del administrador y la productividad de la red.

Para la presente investigación se utilizó los métodos Inductivo-Deductivo, Científico, Experimental y Comparativo. De acuerdo al análisis comparativo realizado mediante los parámetros: Usabilidad, Gestión de usuarios, Información en tiempo real, Soporte, Reportes, Alertas, Alarmas, Autodescubrimiento de dispositivos, Mapas de red, entre las herramientas de administración y monitoreo Cacti, Zenoss y Zabbix, se pudo concluir que Zenoss con el 97.6% es la mejor opción para cumplir con los objetivos de la investigación y requisitos de la infraestructura de networking en la cual se llevó a cabo la implementación.

La implementación de Zenoss se lo realizó sobre la distribución de Linux Ubuntu 10.04, se utilizó el archivo zenoss-stack-3.0.2-linux.bin, y las librerias: python-dev, libmysqlclient15-dev, mysql-server, build-essential, binutils, make, swig, autoconf, necesarias para construir el módulo de Zenoss, ésta se alimenta de información **(**SNMP**)**, el mismo que fue instalado y configurado en cada uno de los equipos monitoreados.

La implantación de esta herramienta, facilitó el trabajo del administrador en cuanto a gestionar la red, uso de tiempo y recursos, además permite tomar medidas preventivas y correctivas frente a problemas que puedan presentarse en la red del IMA.

En la actualidad es recomendable usar herramientas de administración y monitoreo de red, para así poder tomar medidas preventivas en cuanto a solucionar o controlar problemas en la misma.

SUMMARY

The investigation is oriented to the comparative analysis of tools OpenSource for the network monitoring based on the Simple Protocol Network Administration (SNMP) to select the best one in service and efficiency and apply in the intranet of Ambato Municipality to manage, monitor keep on functioning the network with quality, permitting to control the equipment and device condition to attain an improvement in management of the administrator and the network productivity. For the present investigation, the inductive-deductive, scientific, experimental and comparative method was used. According to the comparative analysis carried out through the parameters, usability, user management, information in real time, support, reports, warnings, alarms, device self-discovery, network maps, among the administration and monitoring tools Cati, Zenoss and Zabbix, it was possible to conclude that Zenoss with 97.6% is the best option to accomplish the investigation objects and the infrastructure requirements of networking in which the implementation was carried out. The Zennos implementation was carried out on the Linux Ubuntu 10.04 distribution. The Zenoss-stack-3.0.2-linux.bin file and the, python-dev, libmysqlclient15-dev, mysql-server, build-essential, binutils, make, swing, autoconf libraries necessary to construct the Zenoss module are used. It is fed on information (SNMP), which was installed and set in each monitored equipment. This tool implantation facilitated the administrator work as to managing the network, time and resource use; moreover it permits to take preventive an corrective measures against problems to rise in the IMA network. At the moment, it is recommended to use the network administration and monitoring tools to take preventive measures to control and solve its problems.

GLOSARIO DE TÉRMINOS

Alerta	Por correo electrónico o página que envíe como resultado de un evento.
Propiedad de configuración	Se define en una clase de dispositivo o evento. Las Propiedades de configuración son cómo la supervisión se lleva a cabo. La configuración se basa en la herencia.
Data Point-Punto de datos	Los datos devueltos desde un origen de datos. En muchos casos, sólo hay un punto de datos de un origen de datos (por ejemplo, en SNMP), pero también puede haber muchos puntos de datos de un origen de datos (por ejemplo, cuando se produce un comando en la salida de varias variables).
Data Source-Origen de Datos	Método utilizado por el sistema de recogida de información de monitoreo. Ejemplo de fuentes de datos incluyen OID SNMP, comandos SSH, y los caminos perfmon.
Dispositivo	Objeto de supervisión primaria. Por lo general, un dispositivo es la combinación de hardware y un sistema operativo.
Clase de Dispositivo	Tipo especial de organizador para administrar la forma en los modelos de sistemas y dispositivos de monitores (a través de las propiedades de configuración y control de plantillas).
Componentes de Dispositivos	Los objetos contenidos en un dispositivo. Los componentes incluyen las interfaces, los procesos del sistema operativo, los sistemas de archivos, CPU y discos duros.

Descubrimiento	Proceso por el cual la información del sistema reúne información sobre los dispositivos de la infraestructura. Los resultados de los descubrimientos se utilizan para rellenar el modelo.
Evento	Manifestación de la presencia importante dentro del sistema. Los eventos son generados internamente (por ejemplo, cuando se supera un umbral) o externa (por ejemplo, a través de un mensaje de syslog o captura de SNMP).
Clase de Eventos	Sistema de clasificación utilizado para organizar las reglas de eventos.
Reglas de Eventos	Controla cómo se manipulan los acontecimientos a medida que entran en el sistema (por ejemplo, el cambio de la severidad de un evento). Propiedades de configuración de configurar reglas de eventos.
Gráficos	Muestra uno o más puntos de datos, los umbrales, o ambos.
Gestión de Recursos	Servidores, redes y otros dispositivos en el entorno de TI.
Monitoring Templated	Descripción de lo que pueda supervisar de un componente del dispositivo o dispositivo. Seguimiento de plantillas incluyen cuatro elementos principales: las fuentes de datos, puntos de datos, los umbrales, y gráficos.
Organizadores	Jerárquica del sistema utilizado para describir los lugares y grupos. También incluye organizadores especiales, que son las clases que la configuración del sistema de control.
Componentes de	Interfaces de recursos de componentes, servicios y procesos, y el

Recursos	software instalado en el entorno de TI.
Threshold / Umbrales	Define un valor más allá del cual un punto de datos no debe ir. Cuando se alcanza un umbral, el sistema genera un evento. Por lo general, los eventos de umbral utilizar la clase/Perf evento.

ANEXOS

ANEXO 1.

PASOS PARA LA INSTALACIÓN DE LA HERRAMIENTA ZENOSS

INSTALACIÓN DE DEPENDENCIAS

Para poder instalar Zenoss Core, es necesario cumplir con las siguientes dependencias:

a. python-dev.- herramientas del lenguaje de programación para que este sistema sea capaz de entender y ejecutar programas desarrollados en python
b. libmysqlclient15-dev.- dependencias para agentes clientes de la base de datos MYSQL
c. mysql-server.- agente servidor de la base de datos
d. build-essential.- Lista informativa de paquetes esenciales para poder compilar
e. binutils
f. make
g. swig
h. autoconf

Librerías necesarias para construir el modulo de Zenoss según los requerimientos del equipo y el sistema operativo propio.
Abrimos una ventana de consola y añadimos las siguientes líneas:

#apt-get install python-dev libmysqlclient15-dev y así cada uno de los anteriormente mencionados.

Luego Miramos el status de mysql y si no está corriendo lo iniciamos.

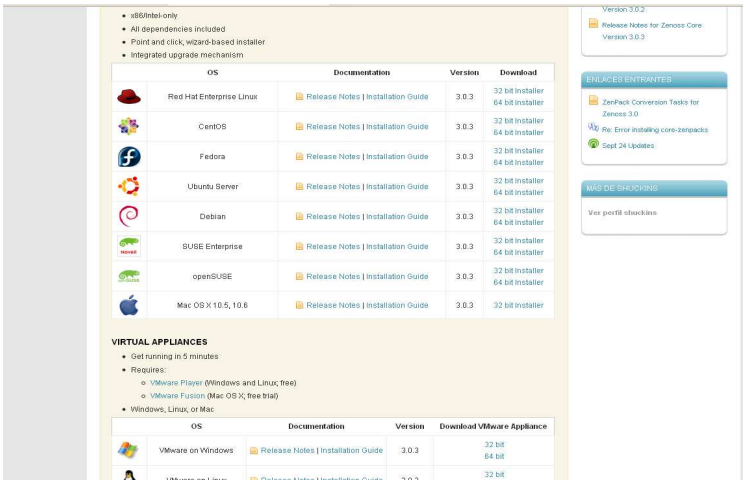
/etc/init.d/mysql status

DESCARGA DEL PAQUETE ZENOSS.BIN

Ahora ingresamos a la siguiente dirección http://www.Zenoss.com/download, nos trasladará a la página donde se podrá descargar Zenoss Core.

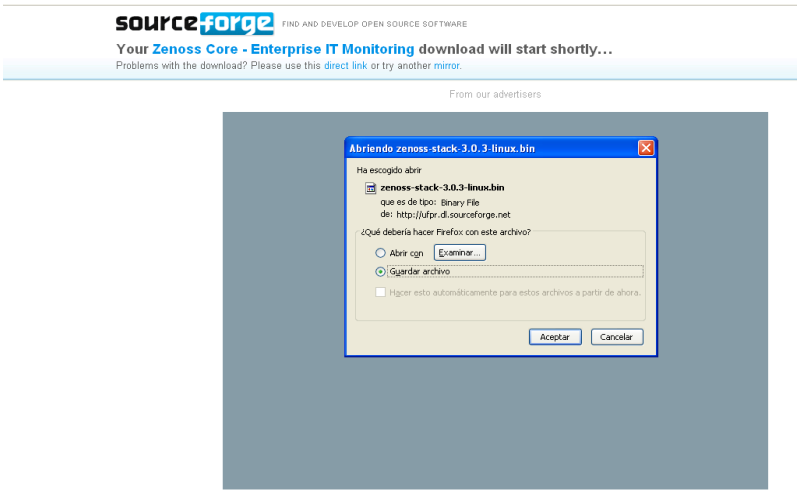
Una vez ubicados en la página, ingresamos lo datos y pulsamos el botón Register&Download.

Nos conducirá a la pantalla en donde se seleccionará el sistema para cual se instalará Zenoss en este caso Ubuntu.



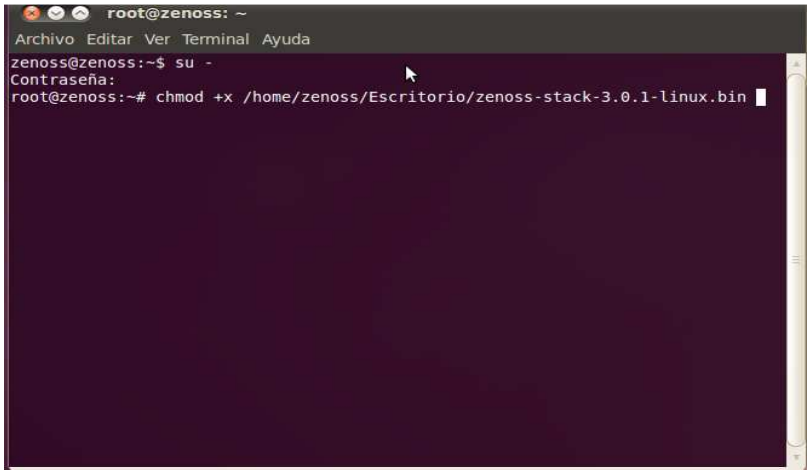
Al encontrarlo se selecciona la versión de 32 bits y se le da clic derecho “Copy Link Location” o copiar ruta del enlace.

O a su vez, dar click y se empieza a descargar el archivo.



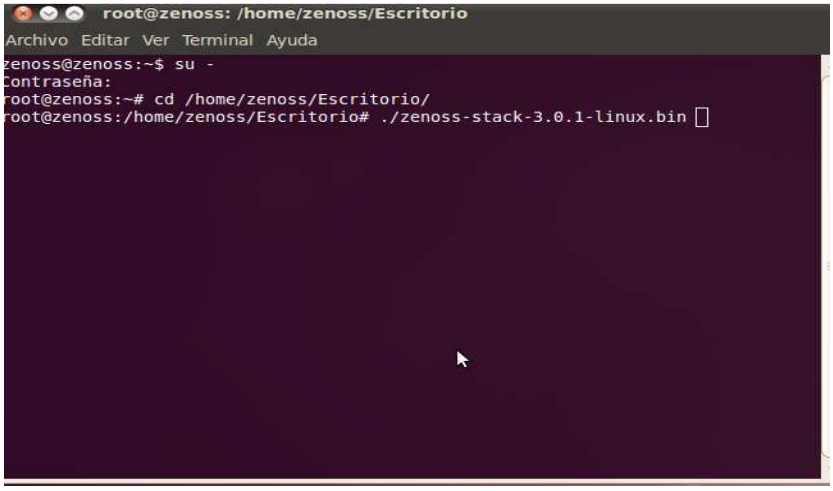
Una vez descargado procedemos a la instalación, primeramente hay que darle permisos de ejecución al archivo .bin (como usuario root):

chmod +x Zenoss-stack-2.3.0-linux.bin



Luego lo ejecutamos:

./Zenoss-stack-2.3.0-linux.bin



Al ejecutar se abre la siguiente ventana:

Pulsamos adelante y llegando al punto donde pedirá el directorio donde se va a instalar Zenoss (se puede dejar el valor por defecto es decir /usr/local/Zenoss):

Luego pedirá un password para MySQL, se recomienda dar uno que recuerde fácilmente, verificación y Adelante.

y comienza la instalación:

Ahora se espera a que la instalación finalice:

Espera que cargue la base de datos en MySQL proceso que puede durar varios segundos y al terminar muestra lo siguiente:

Se deja la casilla de verificación “Launch Zenoss” activada y le damos Finish, abrimos un navegador (en este caso Firefox) y lo abrimos con http://localhost:8080.

CONFIGURACIÓN DE SNMP

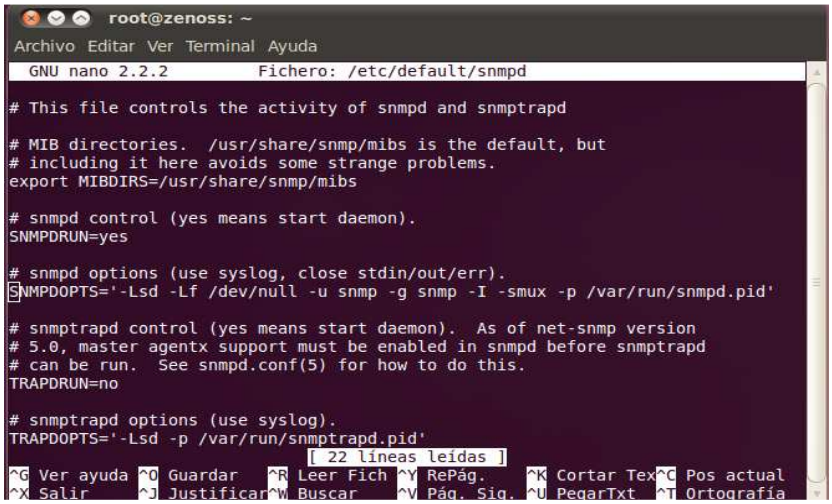
Primeramente se debe modificar algunas líneas al archivo de configuración del demonio snmpd en la siguiente ruta: **nano /etc/default/snmpd**

Buscamos la siguiente línea:

SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -I -smux -p /var/run/snmpd.pid 127.0.0.1'

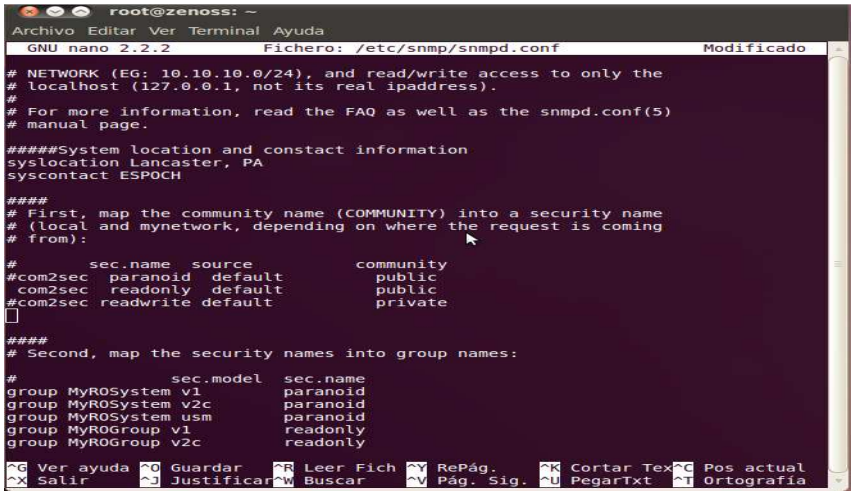
y procedemos a borrar la dirección del localhost así:

SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -I -smux -p /var/run/snmpd.pid'



Después de haber hecho esto se modifica el siguiente archivo:

#nano /etc/snmp/snmpd.conf



Modificando si es necesario el sysLocation, y sysContact, además se establece la comunidad de solo lectura. Se guardan los cambios y se reinicia el demonio del snmp:

 # /etc/init.d/snmpd restart

ADMINISTRACIÓN GRÁFICA

El usuario y password por defecto son admin (username) Zenoss (password) ingresamos estos datos y damos clic en login y nos lleva al index de administración del Zenoss.

ANEXO 2.

INSTALACIÓN DE SNMP COMO AGENTE DE MONITOREO

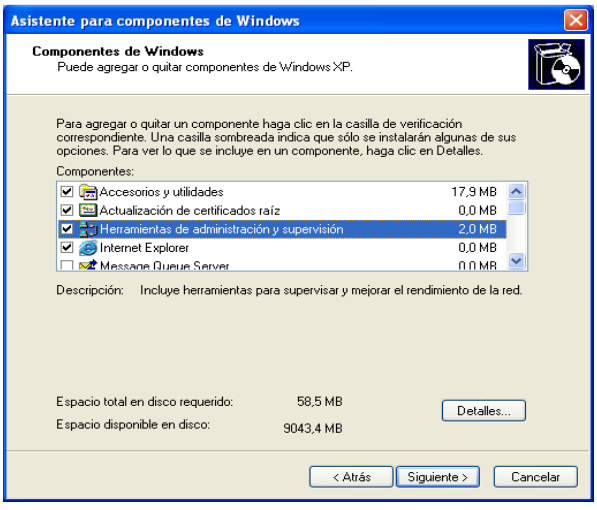
Un agente es una interface de usuario que proporciona acceso al equipo para conocer su estado y proceder tanto a labores de gestión como mantenimiento o instalación.

Un agente posee conocimiento local de información de administración (memoria libre, número de paquetes IP recibidos, rutas, etc.), la cual es traducida a un formato compatible con SNMP y organizada en jerarquías.

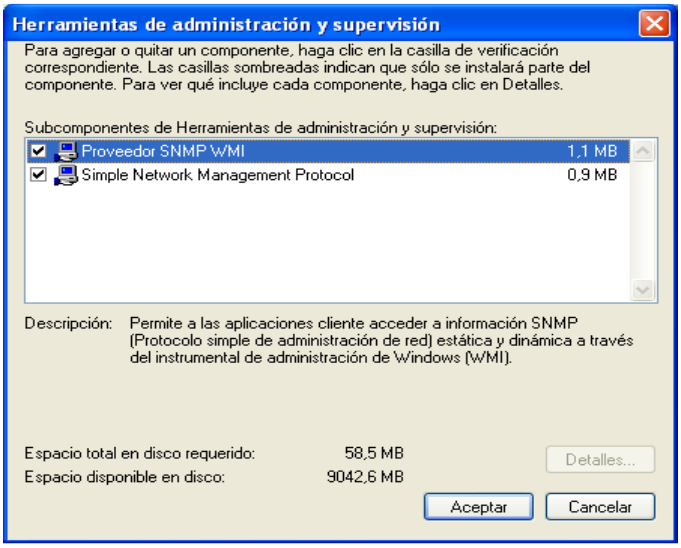
En conclusión el agente esta en el dispositivo administrado, por lo cual su correcta configuración es la que emite toda clase de información de atributos de este dispositivo hacia el nms puesto que los NMS's proporcionan el volumen de recursos de procesamiento y memoria requeridos para la administración de la red.

Agente SNMP en Windows XP

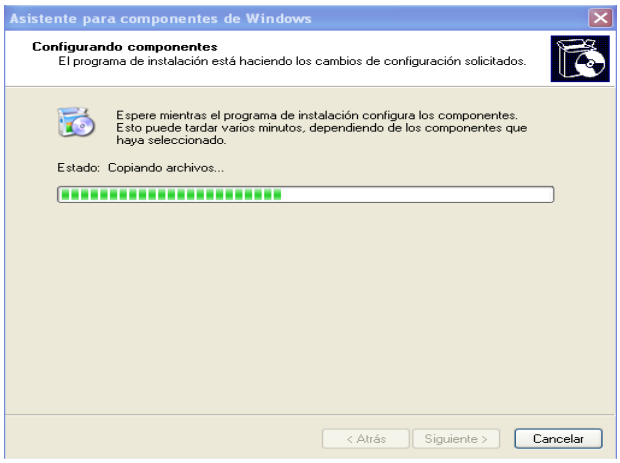
Nos ubicamos en ***Inicio/Panel de control/agregar o quitar programas/agregar o quitar componentes de Windows.***

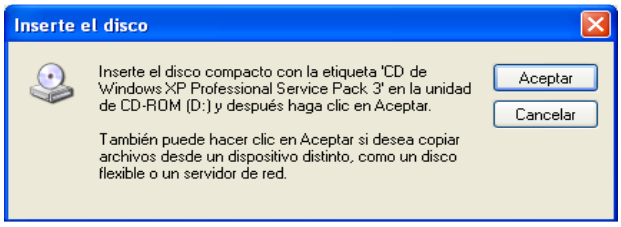


Damos click sobre herramientas de administración y supervisión y click en Detalles, tarjamos las dos pestañas donde se encuentra el protocolo simple de administración de red y el SNMP WMI que es un instrumento administrativo de Windows; es un API (Interfaz de Programación de Aplicaciones) del sistema operativo Windows para controlar, monitorear y administrar los equipos en una red.



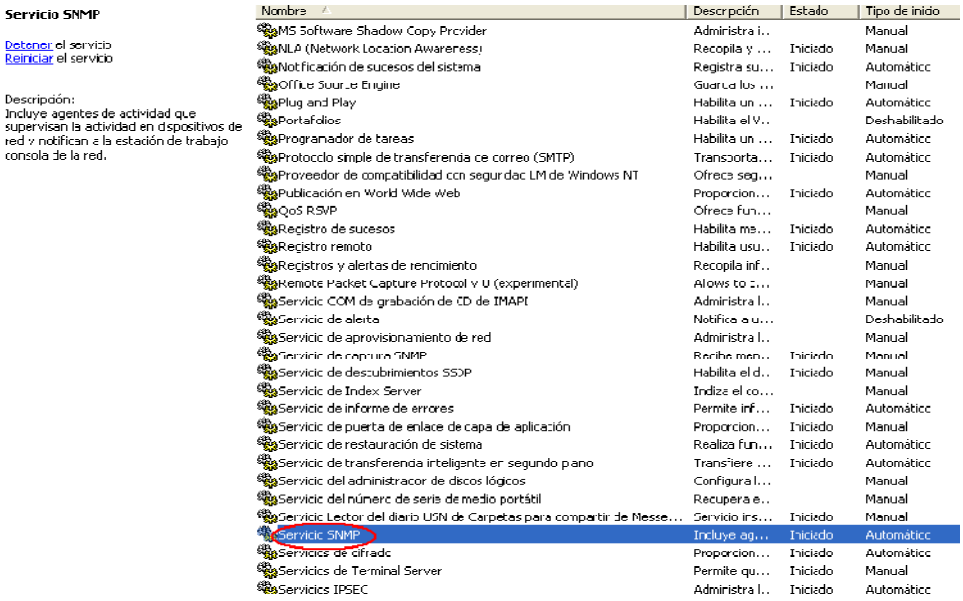
Después esta consola nos muestra que esta extrayendo los archivos necesarios y por ello nos pide el CD-ROM para este cometido, lo único que debe de hacer es introducirlo y listo.



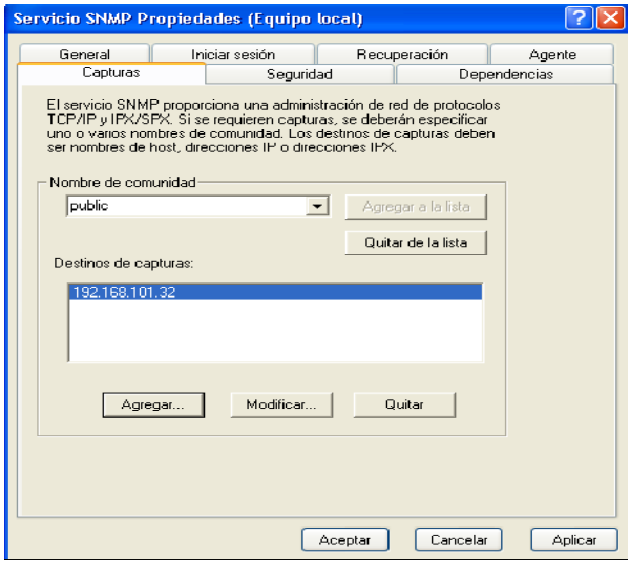


Seguido de este paso nos avisa que finalizó la instalación de este protocolo.

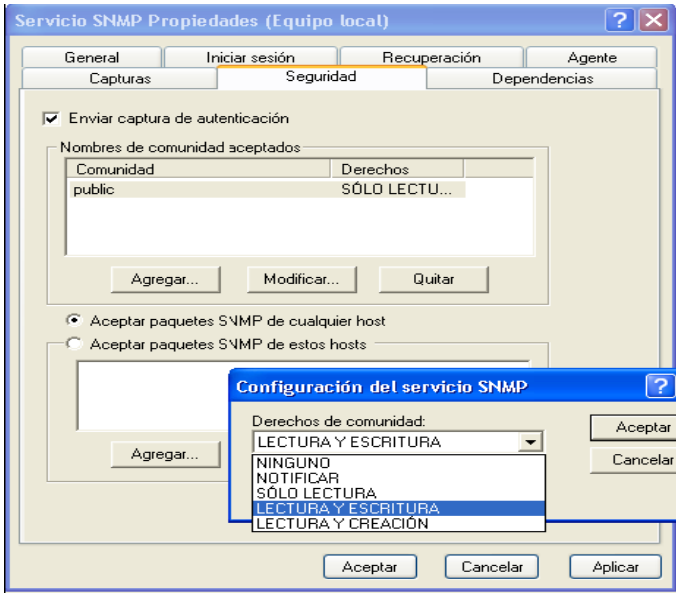
Una vez concluida la instalación, nos ubicamos en Administración de Equipos/Servicios y Aplicaciones/Servicios/servicio Smnp, y damos click derecho Propiedades.



Luego de estar en propiedades nos vamos a la pestaña Capturas ponemos la comunidad por defecto podremos public y la IP de a la cual queremos llegar, esto es para comunicarnos con la red.



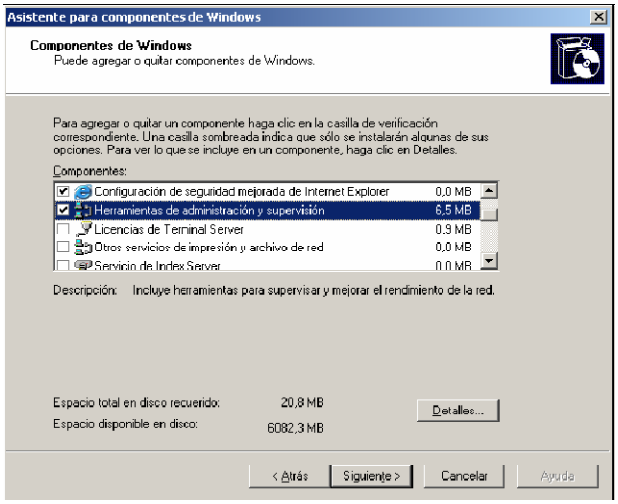
Luego se debe dar permisos de lectura y escritura para eso nos vamos a la pestaña Seguridad.



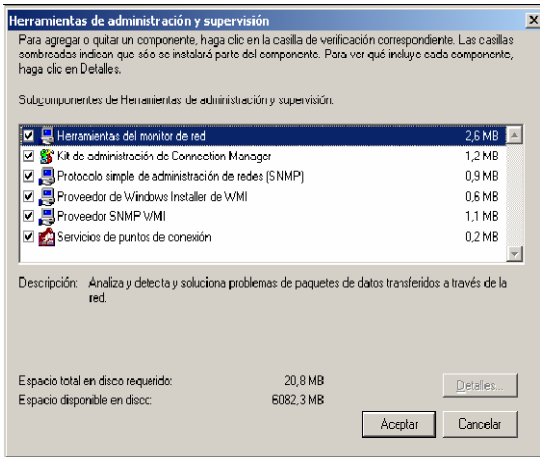
AGENTE SNMP EN WINDOWS SERVER

Ingresamos por ***Inicio/Panel de control/Agregar o quitar programas/Agregar o quitar componentes de Windows*** y buscamos dentro de las opciones

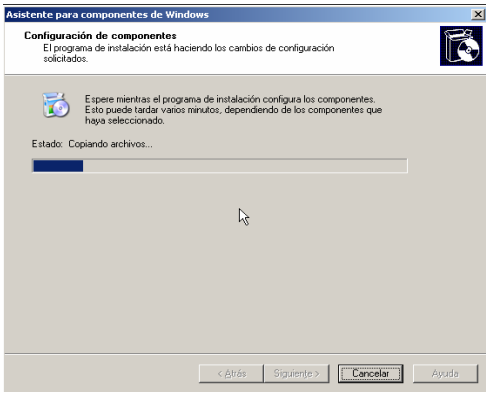
herramientas de administración y supervisión; donde debemos activar la casilla y pulsamos en ***Detalles.***

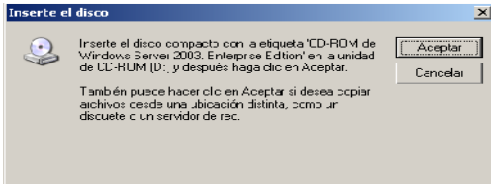


En ella nos muestra los componentes



Después esta consola nos muestra que esta extrayendo los archivos necesarios y por ello nos pide el CD-ROM para este cometido, lo único que debe de hacer es introducirlo y listo.

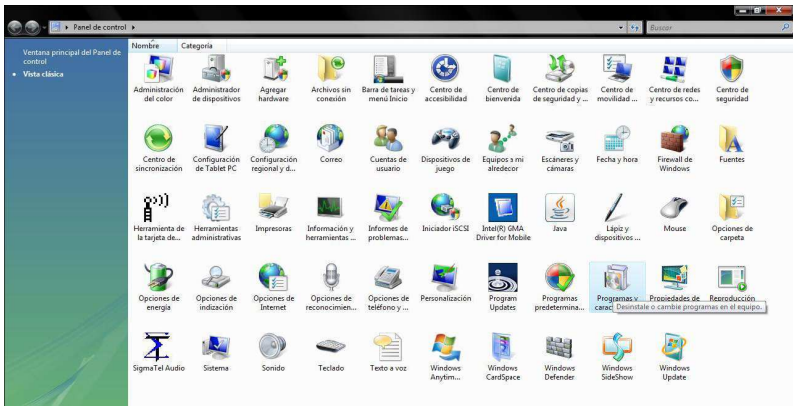




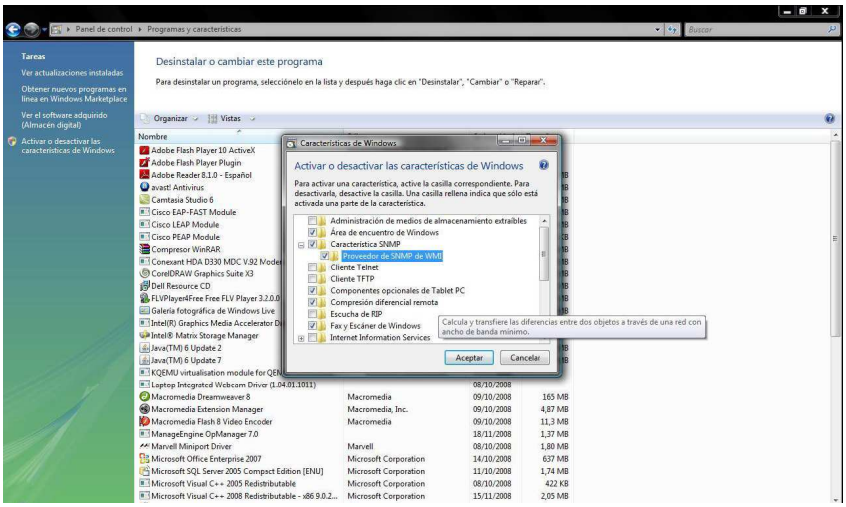
Y ya instalamos los componentes que necesitamos para que este equipo pueda abrir el puerto 25 para que se pueda comunicar con nuestro servidor de monitoreo.

AGENTE SNMP EN WINDOWS VISTA

Nos ubicamos bajo ***Inicio/Panel de Control/Programas y características,*** luego vamos a ***Activar o desactivar características de Windows.***



Encontraremos varias carpetas, buscamos la que dice Características SNMP la chequeamos la desplegamos y también chequeamos la carpeta que nos desplegó que dice Proveedor de SNMP de WMI y damos en Aceptar.



Aquí comenzara a configurarse y debemos tener un poco de paciencia porque es un poco demorado.

Luego damos click en ***Reiniciar ahora*** y listo, para aplicar los cambios. Ya quedo configurado el agente SNMP en Windows Vista.

Agente SNMP en Linux

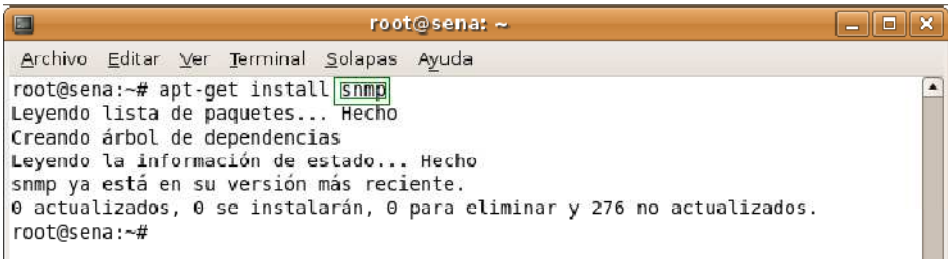
Con SNMP se nos facilita el intercambio de información de administración entre dispositivos de red. Cada intercambio es una transacción independiente entre el gestor y el agente, por esto es de suma importancia la buena configuración de este protocolo para que nuestro equipo pueda ser monitoreado por otras máquinas en la red, debemos complementariamente instalar SNMP y luego configurarlo:

1.- Descargamos el paquete del demonio “snmpd” desde los repositorios

#apt-get install snmpd

2.- Descargamos el paquete cliente de snmp para hacer pruebas internas de monitoreo.

#apt-get install snmp

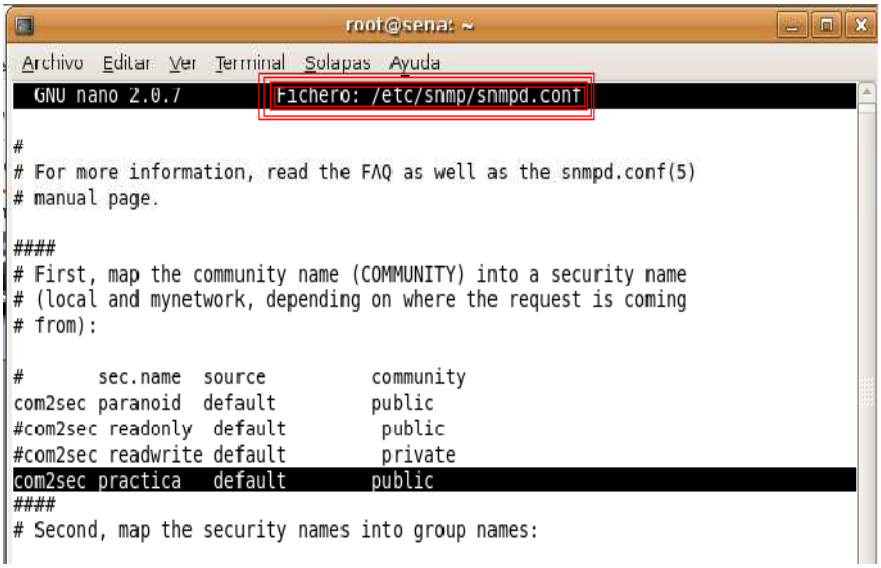


Las comunidades son grupos de atributos que el agente “SNMP” crea para definir las posibles funciones que puede ejecutar un agente cliente que se conecte a él para pedir información del estado del equipo. La comunidad requiere un password para poder hacer las peticiones de la información del equipo y a este se le conoce como comunidad, variando entre la comunidad pública para peticiones de lectura y privada para peticiones de administración en el equipo.

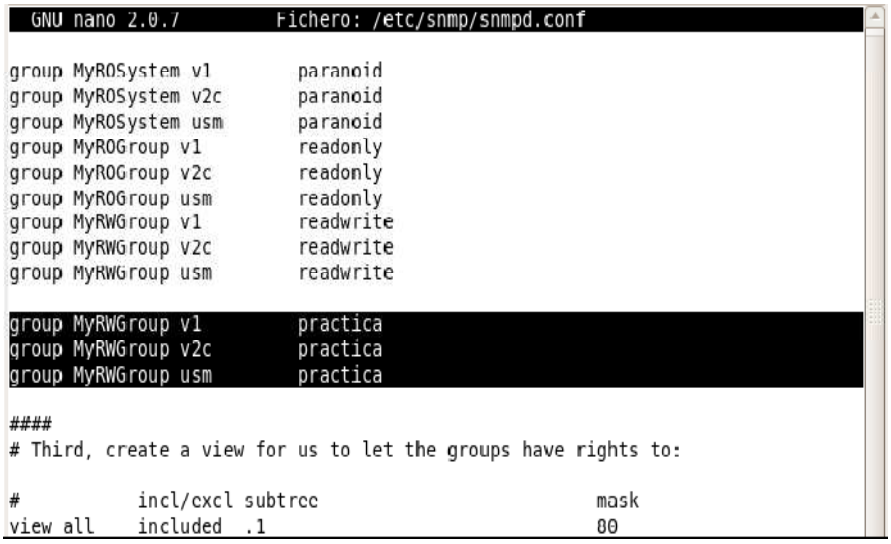
3.- Creamos una comunidad con permisos de lectura y escritura para permitir el escaneo completo del equipo en el que nos encontramos y poder realizar diferentes pruebas.

Nos logueamos como root y editamos el archivo snmpd.conf, luego agregamos la nueva comunidad a la cual llamaremos practica.

#su root
#nano /etc/snmp/snmp.conf



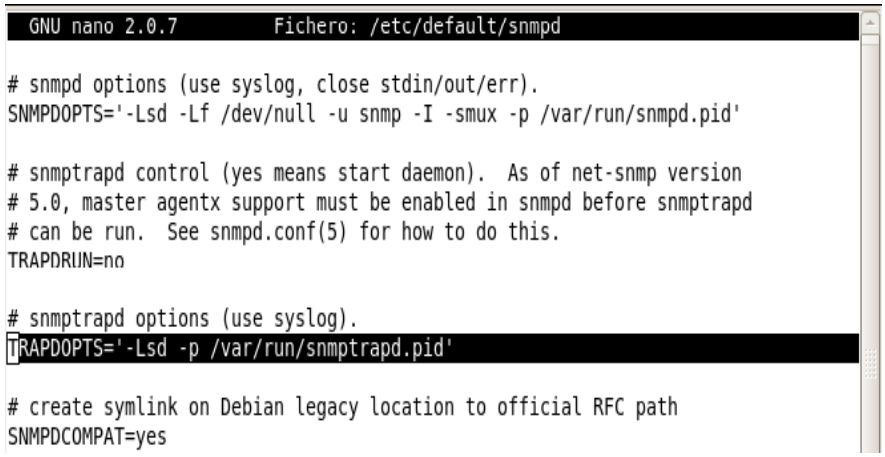
En el mismo archivo agregamos las variables para los permisos de lectura y escritura de “practica” que tendrán los agentes snmp que requieran información en el equipo y posean la comunidad especificada.



En el archivo snmpd en default especificaremos que el equipo recibirá peticiones snmp de cualquier rango de ip´s en la red.

#nano /etc/default/snmpd

Borramos a la línea seleccionada la IP de localhost y deberá verse como la presentada aquí, guardamos y salimos del archivo.



Reiniciamos el demonio para retomar los cambios efectuados

4.- Para probar que el agente snmp esta correctamente configurado, utilizamos el comando snmpwalk especificando la versión, la comunidad y la IP del equipo a monitorear, en este caso el propio.

snmpwalk –c public –v2c 127.0.0.1

DISPOSITIVOS CISCO ROUTER - SWITCH

Dispositivos cisco viene con el SNMP ya instalado. Sin embargo, debemos configurar el SNMP en cada dispositivo para que estén en la misma comunidad que el resto de su red. Como también el envío de traps y las determinadas ordenes sobre la consola para su gestión remota:

R(config)# snmp-server comunity public ro
R(config)# snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
R(config)# snmp-server enable traps tty
R(config)# snmp-server enable traps envmon
R(config)# snmp-server enable traps config
R(config)# snmp-server enable traps dsp card-status
R(config)# snmp-server enable traps dsp oper-state
R(config)# snmp-server enable traps entity
R(config)# snmp-server enable traps fru-ctrl
R(config)# snmp-server enable traps frame-relay
R(config)# snmp-server enable traps hsrp
R(config)# snmp-server enable traps syslog

```
R(config)#  snmp-server enable traps vtp
R(config)#  snmp-server host X.X.X.X community public snmpv1/v2c
```

* Donde X.X.X.X, es la Direcciòn IP del Servidor donde se encuentra instalado Zenoss.

ANEXO 3.

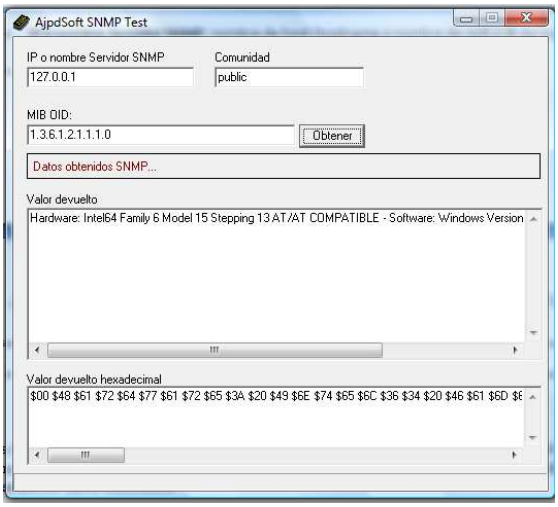
AJPDSOFT SNMP TEST

AjpdSoft SNMP Test permite obtener información de un servidor con el servicio SNMP activo. Obtiene la información a partir de la MIB indicada.

Abriremos AjpdSoft SNMP Test e introduciremos los siguientes datos:

- **IP o nombre Servidor SNMP**: nombre de host (hostname o nombre de red) o IP del equipo con el servicio SNMP activo.
- **Comunidad**: escribiremos "public"
- **MIB OID**: escribiremos el nombre de la rama de la que queramos obtener la información. Por ejemplo, para obtener el tipo de procesador del equipo introduciremos: *1.3.6.1.2.1.1.1.0*

Tras introducir los datos pulsaremos "Obtener", si todo es correcto y el equipo desde el que hemos ejecutado la aplicación AjpdSoft SNMP Test tiene permisos en el servidor SNMP obtendrá los datos solicitados.



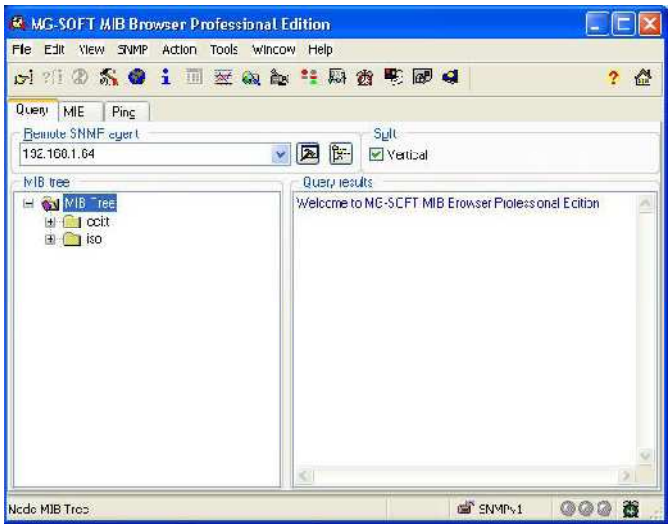
ANEXO 4.

MG-SOFT MIB Browser

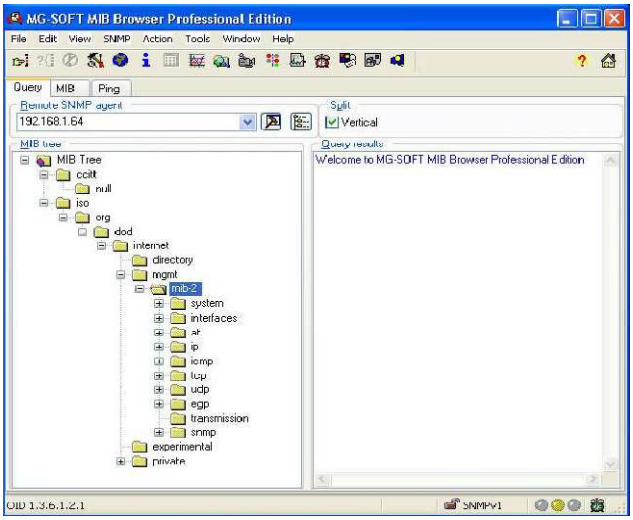
El Navegador MIB le permite ver la jerarquía de las variables SNMP MIB en forma de un árbol y le provee información adicional sobre cada nodo.

Con el Navegador MIB se puede fácilmente cargar (compilar) archivos estándares y propietarios del MIB, ver y manipular datos que están disponibles en un agente SNMP.
El Navegador MIB puede generar solicitudes SNMP Get y Get_Next permitiéndole a usted chequear las propiedades y los valores actuales de los contadores de un agente SNMP específico.

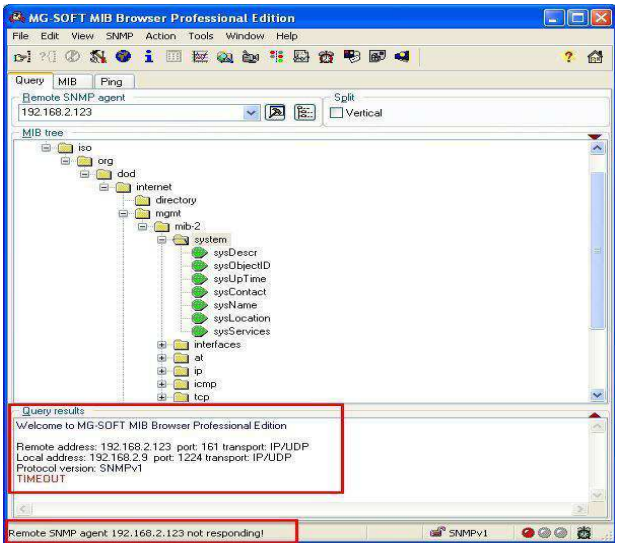
1. Abra la aplicación MG-Soft MIB Browser, haga clic en el botón Continue y cierre la ventana que muestra el tip del día. Observe que la dirección del agente remoto SNMP es la IP de la máquina asignada, en la que está trabajando.



2. Expanda la jerarquía desde la carpeta iso hasta llegar a mib-2



3. Expanda los nodos dependiendo la información que desea observar.



ANEXO 5

ENCUESTA

ESPOCH

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA EN SISTEMAS

OBJETIVO: Determinar si la gestión del administrador y la productividad de la red del Ilustre Municipio de Ambato, mejoró con la implementación de la herramienta de administración y monitoreo de red basad en SNMP ZENOSS

CUESTIONARIO

1. ¿Cree usted que la gestión y monitoreo de redes es útil en la infraestructura de networking del IMA?

SI___ NO___

2. ¿Cuándo se presentaba un error en la infraestructura de networking en el Ilustre Municipio de Ambato sabía usted donde se generaba el problema?

SI___ NO___

3. ¿Cuando existía un problema en la red de datos, indique el tiempo aproximado que le tomaba determinar el origen del mismo?

1 - 15 min ___
15 – 30 min ___
30 – 45 min ___
45 – 60 min ___
Más ___

4. Cómo calificaría ud. la manipulación y gestión de la herramienta de administración y monitoreo implementada para supervisar la red del IMA?

FACIL____ POCO DIFÍCIL ___ DIFÍCIL___

5. ¿Con la implementación de la herramienta de Administración y Monitoreo ZENOSS cree usted que se ha podido controlar los cambios y actualizaciones en la red del IMA, garantizando así el menor número de interrupciones en el servicio?

SI___ NO___

6. Considera usted que con la implementación de la herramienta ZENOSS se ha logrado mejorar el manejo de los recursos?

SI___ NO___

7. Piensa ud que el tener la administración y monitoreo de la red de forma centralizada, favorece de alguna manera la tarea del administrador de networking?

MUCHO___ POCO___ NADA___

8. La herramienta implementada permite obtener información detallada y a tiempo real del estado actual de los dispositivos que conforman la red?

SIEMPRE _____ CASI SIEMPRE_____ NUNCA_____

9. ¿Cree usted que la implementación de esta herramienta ayudará al desarrollo de la Infraestructura del IMA?

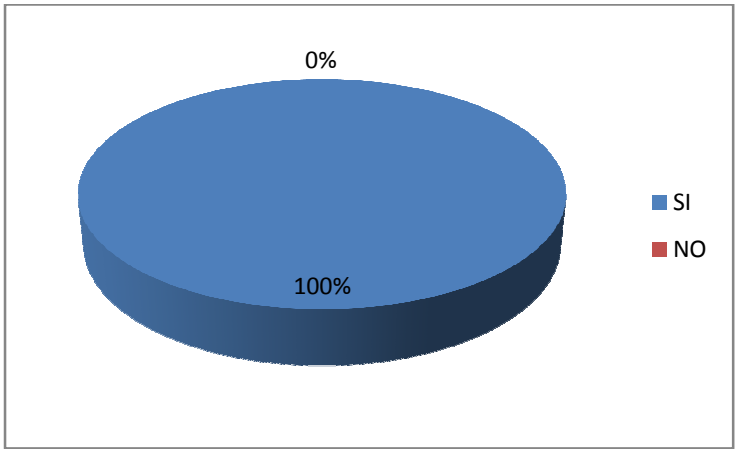
SI___ NO___

GRACIAS POR SU COLABORACIÓN

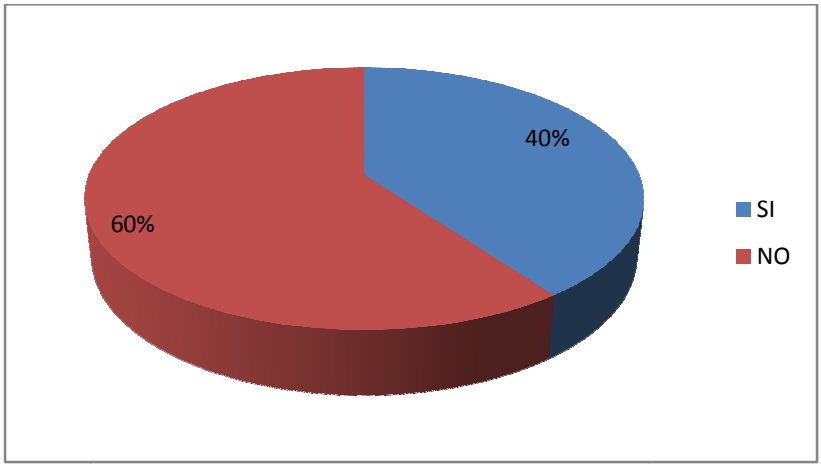
ANEXO 6

TABULACIÓN DE LA ENCUESTA

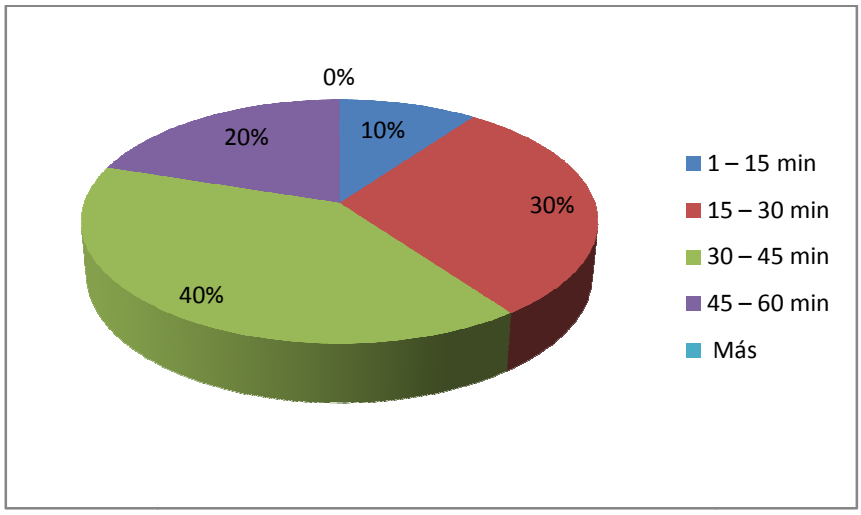
1. ¿Cree usted que la gestión y monitoreo de redes es útil en la infraestructura de networking del IMA?



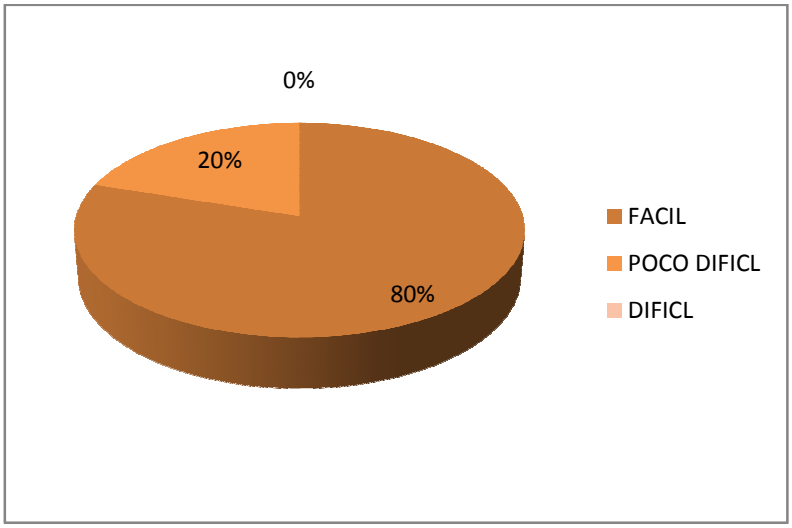
2. ¿Cuándo se presentaba un error en la infraestructura de networking en el Ilustre Municipio de Ambato sabía usted donde se generaba el problema?



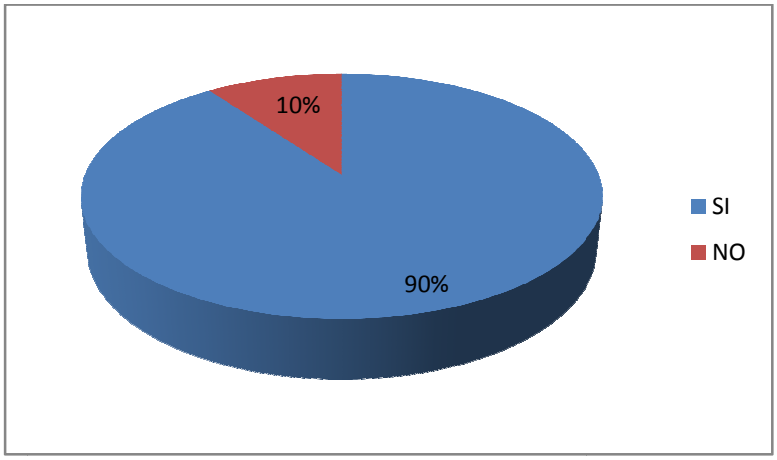
3. ¿Cuando existía un problema en la red de datos, indique el tiempo aproximado que le tomaba determinar el origen del mismo?



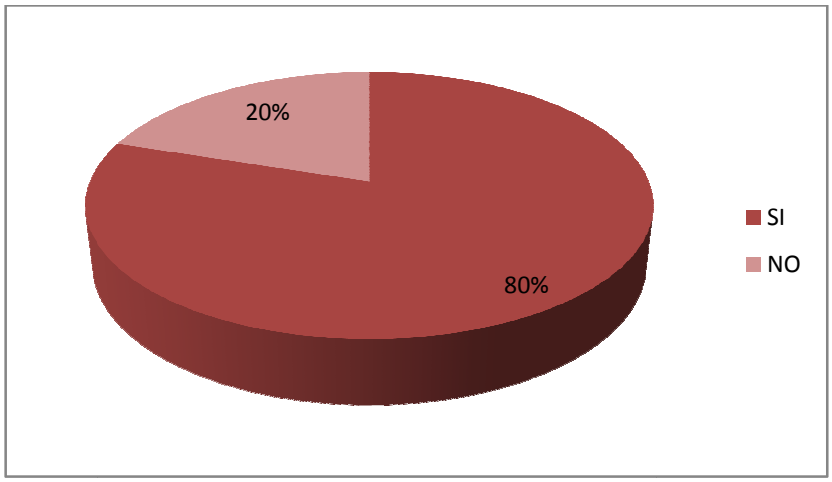
4. Cómo calificaría ud. la manipulación y gestión de la herramienta de administración y monitoreo implementada para supervisar la red del IMA?



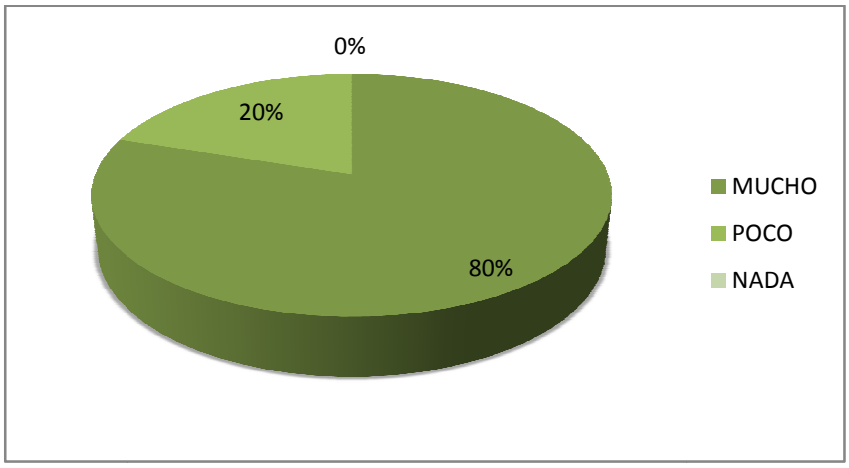
5. ¿Con la implementación de la herramienta de Administración y Monitoreo ZENOSS cree usted que se ha podido controlar los cambios y actualizaciones en la red del IMA, garantizando así el menor número de interrupciones en el servicio?



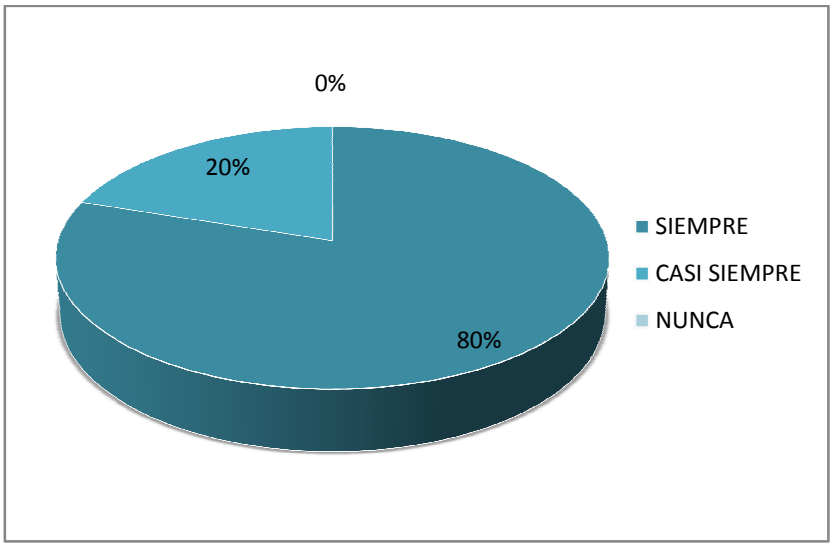
6. Considera usted que con la implementación de la herramienta ZENOSS se ha logrado mejorar el manejo de los recursos?



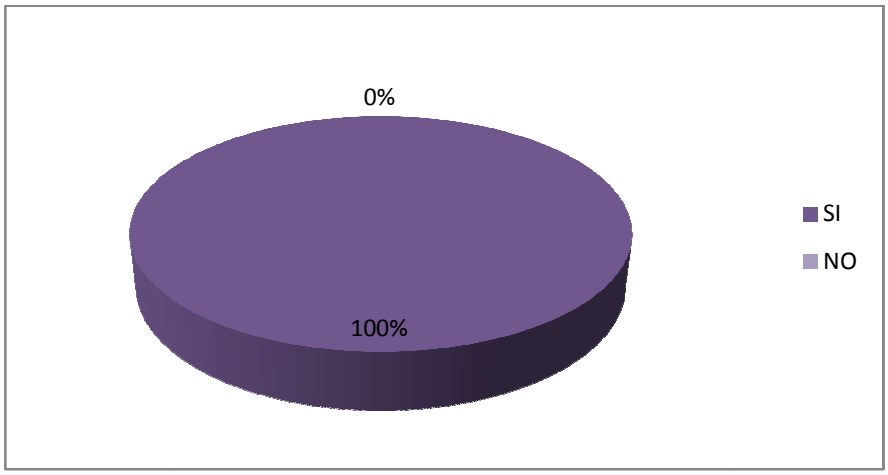
7. Piensa ud que el tener la administración y monitoreo de la red de forma centralizada, favorece de alguna manera la tarea del administrador de networking?



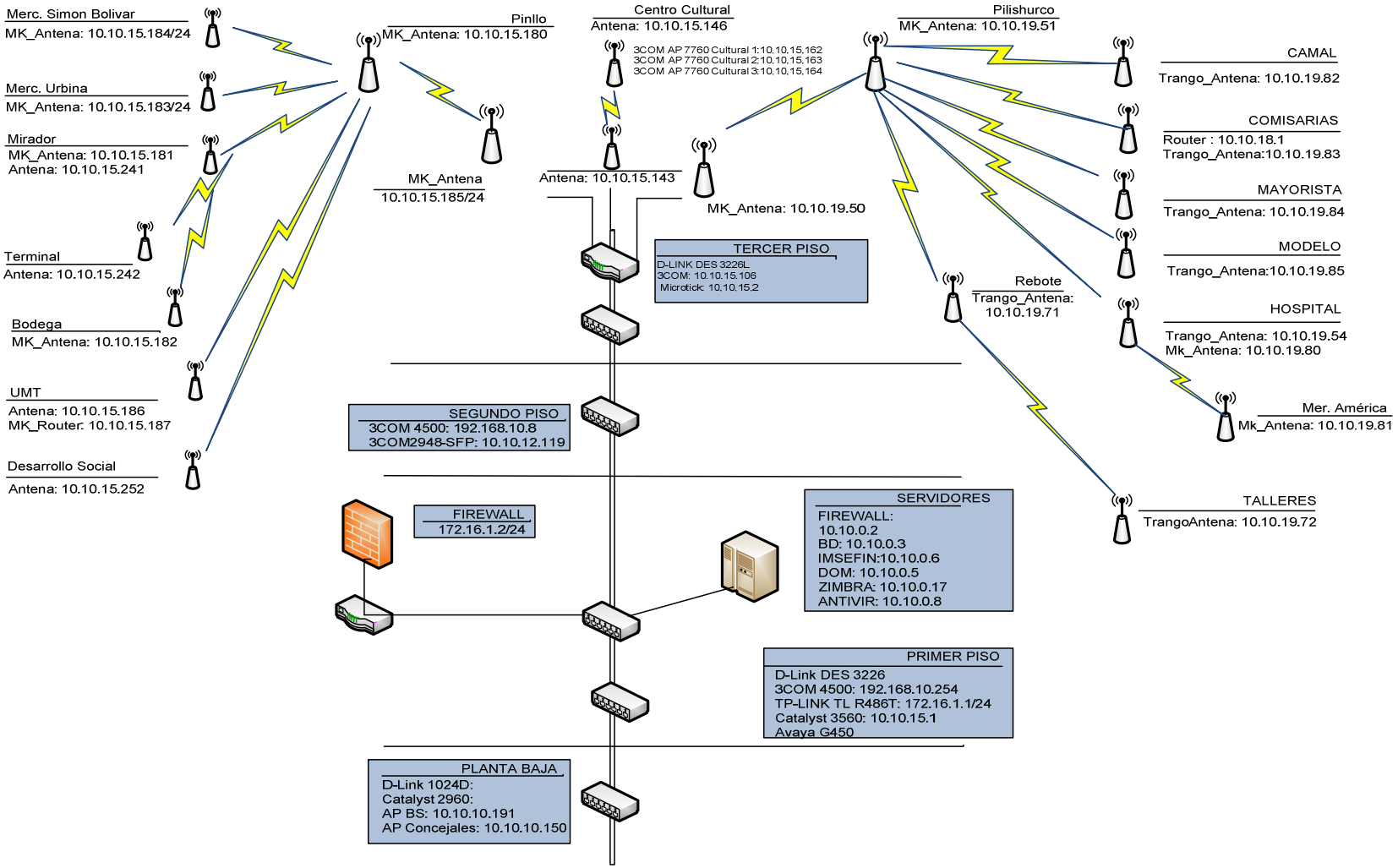
8. La herramienta implementada permite obtener información detallada y a tiempo real del estado actual de los dispositivos que conforman la red?



9. ¿Cree usted que la implementación de esta herramienta ayudará al desarrollo de la Infraestructura del IMA?



ANEXO 7. INFRAESTRUCTURA ACTUAL DE NETWORKING IMA



ANEXO 8.

Informe final entregado al departamento del IMA sobre la distribución de equipos que forman parte de su red de datos.

Al realizar un escaneo de las IP utilizadas por cada red, se obtuvieron las siguientes direcciones las mismas que están siendo usadas, a varias de estas direcciones se las ha resaltado de diferentes colores, con el objetivo de identificarlas por dispositivo, siendo así:

Servidores

Switch

AP

Radios_Microtick

Router_Microtick

Trango_Dispositivos

Al resto de direcciones IP que no se las ha resaltado, forman parte resto de dispositivos que hacen parte de la red como host, impresoras, teléfonos, etc.

10.10.0.X

10.10.0.2 Servidor Firewall-Internet
10.10.0.3
10.10.0.5 Servidor BD
10.10.0.6 aplicserver-IMSEFIN
10.10.0.7 Servidor zimbra(Virtual-Blade)
10.10.0.9
10.10.0.10
10.10.0.8 Servidor Antivirus-Blade
10.10.0.11 Blade
10.10.0.15 IMSEDB

10.10.0.14 serverwin1.municipio.ambato.gov.ec
10.10.0.17 Modulo Blade-Zimbra
10.10.0.30 IMBANCOS
10.10.0.31 Servidor ZENOSS

10.10.10.X

10.10.10.9 STORAGE03
10.10.10.150 AP_Balcón de Servicios

10.10.10.191 AP_Concejales

10.10.11.X

10.10.11.1
10.10.11.19 FX-469605
10.10.11.26
10.10.11.93
10.10.11.94
10.10.11.92
10.10.11.201 FX-46979E
10.10.11.222
10.10.11.251

10.10.12.X

10.10.12.119 3COM_2948_2PISO

10.10.13.X

10.10.13.4
10.10.13.6
10.10.13.29

10.10.15.X

10.10.15.1 SW_CISCO_3560G_Cuarto_Servidores
10.10.15.2 MK_Router_Muni_Planificacion
10.10.15.164 AP_Cultura3
10.10.15.163 AP_Cultura2
10.10.15.162 AP_Cultura1
10.10.15.186 MK_Radio_UMT
10.10.15.180 MK_Pinllo

10.10.15.185 MK_Mun-Pinllo
10.10.15.181 MK_Mirador
10.10.15.183 MK_M.Urbina
10.10.15.182 MK_Bodega
10.10.15.187 MK_Router_UMT
10.10.15.184 MK_S.Bolivar
10.10.15.241 MK_Mirador-Terminal
10.10.15.242 MK_Terminal
10.10.15.252 MK_Router_Desarrollo

10.10.16.X

10.10.16.1
10.10.16.50
10.10.16.51
10.10.16.52
10.10.16.54 Impresora
10.10.16.181 DS00SC01
10.10.16.187 si00si04.municipio.ambato.gov.ec
10.10.16.198 as00as8.municipio.ambato.gov.ec
10.10.16.199 as00as02.municipio.ambato.gov.ec
10.10.16.191 as00as04.municipio.ambato.gov.ec
10.10.16.200

10.10.17.X

10.10.17.1
10.10.17.84 umtserver.municipio.ambato.gov.ec
10.10.17.96
10.10.17.130 im02av16.municipio.ambato.gov.ec
10.10.17.131 co03cf07.municipio.ambato.gov.ec
10.10.17.200
10.10.17.201
10.10.17.222 CLIRSEN12

10.10.18.X

10.10.18.1 MK_Router_Comisarias

10.10.19.X

10.10.19.1 Interfaz_MK_Router_Municipio
10.10.19.2 Interfaz_MK_Router_Comisarias
10.10.19.50 MK_Muni-Pilishurco
10.10.19.51 MK_Pilishurco
10.10.19.54 TR_Hospital
10.10.19.71 TR_Rebote -Talleres
10.10.19.72 TR_Talleres
10.10.19.80 MK_Hospital-América
10.10.19.81 MK_Merc.América
10.10.19.82 TR_Camal
10.10.19.83 TR_Comisarias
10.10.19.84 TR_Mayorista
10.10.19.85 TR_Merc.Modelo

192.168.10.X

192.168.10.8 3com_2PISO
192.168.10.15 3com_3piso_O.Publicas
192.168.10.254 3COM_4500_1PISO

PASSWORD

Se estandarizaron los user y password de los dispositivos administrables en la red, los mismos que se describen a continuación:

SERVIDORES

- **Zimbra:** 10.10.0.17

  user: root

  passw: linuximamail

- **BD:** 10.10.0.5

  user: ADMINISTRADOR

  passw: ima32??admin232008

- **Dominio:** 10.10.0.6

user: administrador

passw: ima32??admin232008

-Antivirus: 10.10.0.8

user: Administrator

passw: admsys2010.

SWITCH

SW_CISCO: 10.10.15.1

passw: muniambato2010

3com

user: admin

passw: en blanco (default)

AP

user: admin

passw: muniambato2010

RADIOS Y ROUTER MICROTIK

passw: muniambato2010

DISPOSITIVOS TRANGO

passw: trango

- ***Excepción:***

Camal: 10.10.0.49

passw: 123456

ANEXO 9.

BIBLIOGRAFÍA

- **ADMINISTRACIÓN Y MONITOREO DE REDES**

  - Análisis y Monitoreo de Redes

    URL:http://www.integracion-de-sistemas.com/analisis-y-monitoreo-de-redes/index.html.

    [Consulta : 15-07-2010]

  - Arquitectura de la Administración de Redes

    URL: http://html.rincondelvago.com/arquitectura-de-la-administracion-de -

    redes.html

    [Consulta : 15-07-2010]

  - Diseño e Implementación de un Ambiente de Administración Distribuida Compatible con el Protocolo SNMP.

    URL: http://www.criptored.upm.es/guiateoria/gt_m123c.htm

    [Consulta : 15-07-2010]

  - Manual FULL MDS Proyecto Grupo1

    URL: http://www.scribd.com/doc/8751704/Manual-FULL-MDS-Proyecto-

    [Consulta : 18-07-2010]

  - Manual de Seguridad en Redes

    URL: http://www.scribd.com/doc/2926302/Manual-de-Seguirdad-en-Redes

    [Consulta : 5-08-2010]

- Administración de redes utilizando Protocolo Snmp (Simple Network Management Protocol)

  URL:
  http://www.digital.unal.edu.co/dspace/bitstream/10245/1106/1/9910555_2009.pdf

  [Consulta : 8-08-2010]

- SNMP: PROTOCOLO SIMPLE DE ADMINISTRACION

  URL:http://www.apuntux.com/2009/08/06/snmp-protocolo-simple-de-administracion-de-red-todo-lo- que-quizo-saber-y-no-se-atrevia-a-preguntar/
  [Consulta : 8-08-2010]

- Características clave de la administración y monitoreo de redes

  URL: http://support.gfi.com/manuals/es/nsm7/nsm7manual_es-1-03.html

  [Consulta : 13-08-2010]

- Introducción a la Administración de Redes

  URL:http://www.slideshare.net/radiocomunicaciones_utpl/introduccin-a-la administracin-de-redes

  [Consulta : 13-08-2010]

- Administración de redes

  URL: http://www.monografias.com/trabajos27/redes-mom/redes-mom.shtml

  [Consulta : 15-08-2010]

- Gestión y Monitoreo de Redes

  URL:
  http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/solano_v_h/capitulo1.pdf

[Consulta :15-08-2010]

- Informe de Monitoreo de la Red

  URL: http://www.scribd.com/doc/24548465/Informe-Monitoreo-de-la-Red

  [Consulta : 16-08-2010]

- Importancia del monitoreo proactivo de las redes

  URL:http://www.gbm.net/bt/bt44/tendencias/importancia_del_monitoreo_proactivo_de_las_redes.php

  [Consulta : 16-08-2010]

- Redes Seguras

  URL: http://delta.cs.cinvestav.mx/~fraga/Cursos/Seguridad/redes_seguras.pdf

  [Consulta : 16-08-2010]

- Administración de redes

  URL:http://www.pucp.edu.pe/biblioteca/docs/elibros_pucp/alcocer_carlos/23_Alcocer2000_Redes_Cap_23.pdf

  [Consulta :16-08-2010]

- Como administrar redes

  URL: http://www.aprendaredes.com/downloads/Como_Administrar_Redes.pdf

  [Consulta :16-01-2011]

- Monitoreo

  URL: http://www.seguridad.unam.mx/eventos/admin-unam/Monitoreo.pdf

[Consulta : 10-01-2011]

- Operaciones de la Administración de Red.

  URL: http://www.monografias.com/trabajos43/administracionredes/administracion-redes2.shtml
  [Consulta : 23-01-2011]

- **HERRAMIENTAS DE ADMINISTRACIÓN Y MONITOREO DE REDES**

  - **CACTI**

    - Cómo instalar Cacti en Ubuntu 10.04 (Lucid Lynx) | Base Conocimientos JM

      URL: http://www.soportejm.com.sv/kb/index.php/article/cacti

      [Consulta : 3-09-2010]

    - Monitorización de recursos de red con SNMP y Cacti

      URL:http://www.victornuno.com/2008/11/18/monitorizacion-de-recursos-de- red-con-snmp-y-cacti/

      [Consulta : 3-09-2010]

    - Cacti

      URL: http://es.wikipedia.org/wiki/Cacti

      [Consulta : 3-09-2010]

- Cacti

  URL:http://www.codigolibre.org/index.php?option=com_content&view=article&id=5387:cacti&catid=36:gnu-cat&Itemid=31

  [Consulta : 3-09-2010]

- Instalar Cacti

  URL: http://www.solusan.com/wp-content/2007/07/instalar_cacti.pdf

  [Consulta : 6-09-2010]

- Página Oficial Cacti

  URL: www.cacti.com

  [Consulta : 6-09-2010]

- **ZENOSS**

  - Manual Sistema de Monitoreo Zenoss en Ubuntu 8

    URL: http://www.scribd.com/doc/8751797/Manualsistema-de-Monitoreo-Zenoss-en-Ubuntu-8

    [Consulta : 13-09-2010]

  - Zenoss

    URL: http://www.scribd.com/doc/8113441/zenoss

    [Consulta : 13-09-2010]

  - Guía de Administración de Zenoss

URL: http://docs.huihoo.com/zenoss/admin-guide/2.1.1/ch07s05.html,

[Consulta : 13-09-2010]

- Zenoss

  URL: http://www.scribd.com/doc/8113441/zenoss

  [Consulta : 13-09-2010]

- Monitoreando la red con Zenoss

  URL: http://www.zenoss.com/product/network-monitoring

  [Consulta : 11-10-2010]

- Ayuda Ubuntu

  URL: https://help.ubuntu.com/community/Zenoss

  [Consulta : 18-10-2010]

- Comunidad Ubuntu

  URL: https://help.ubuntu.com/community/Servers

  [Consulta : 18-10-2010]

- Página Oficial Zenoss

  URL: www.zenoss.com

  [Consulta : 1-12-2010]

- **ZABBIX**

  - Zabbix vs Zenoss

    URL:http://www.lastcombat.com/videos.php?one=Zenoss&two=Zabbix&f=Za
    bbix_vs_Zenoss

    [Consulta : 20-09-2010]

  - Zabbix en debian 503 lenny

    URL:http://www.cdbarra.com/monitorizacion/zabbix-18-en-debian-503-lenny- instalacion.html

    [Consulta : 20-09-2010]

  - Blog Zabbix

    URL:http://informaticareal.spaces.live.com/?_c11_BlogPart_BlogPart=blogview&_c=BlogPart&partqs=cat%3DZabbix
    [Consulta :23-09-2010]

  - Instalar agente Zabbix en Windows

    URL:http://www.rubenortiz.es/2009/05/26/instalar-agente-zabbix-en windows/

    [Consulta : 24-09-2010]

  - Blog Zabbix

    URL: http://zabbix-es.blogspot.com/2009_02_01_archive.html

    [Consulta :24-09-2010]

- Página Oficial Zabbix

  URL: www.zabbix.com

  [Consulta : 25-09-2010]