UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS

ELECTRÓNICA E INDUSTRIAL

Carrera de Ingeniería en Electrónica y Comunicaciones

TEMA:

HERRAMIENTA OPENSOURCE DE ADMINISTRACIÓN Y MONITOREO BASADO EN SNMP PARA EL MEJORAMIENTO DEL FUNCIONAMIENTO DE LA RED EN SPEEDY COM CIA LTDA.

Proyecto de Trabajo de Graduación. Modalidad: TEMI. Trabajo Estructurado de Manera Independiente, presentado previo la obtención del título de Ingeniero en Electrónica y Comunicaciones.

SUBLÍNEA DE INVESTIGACIÓN: Administración de Redes.

AUTOR: José Iván Freire Bonilla

PROFESOR REVISOR: Ing. Marco Antonio Jurado Lozada, Mg.

Ambato - Ecuador

Abril 2013

APROBACIÓN DEL TUTOR

En mi calidad de tutor del trabajo de investigación sobre el tema: "Herramienta opensource de administración y monitoreo basado en snmp para el mejoramiento del funcionamiento de la red en Speedy COM CIA LTDA.", del señor Freire Bonilla José Iván, estudiante de la Carrera de Ingeniería en Electrónica y Comunicaciones, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, considero que el informe investigativo reúne los requisitos suficientes para que continúe con los trámites y consiguiente aprobación de conformidad con el Art. 16 del Capítulo II, del Reglamento de Graduación para obtener el título terminal de tercer nivel de la Universidad Técnica de Ambato.

Ambato Abril 26, 2013

EL TUTOR

Ing. Marco Antonio Jurado Lozada, Mg.

AUTORÍA

El presente trabajo de investigación titulado: “Herramienta opensource de administración y Monitoreo basado en snmp para el mejoramiento del funcionamiento de la red en SPEEDY COM CIA LTDA.”. Es absolutamente original, auténtico y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato Abril 26, 2013

José Iván Freire Bonilla

CC: 180452903-8

APROBACIÓN DE LA COMISIÓN CALIFICADORA

La Comisión Calificadora del presente trabajo conformada por los señores docentes: Ing. Edison Homero Álvarez Mayorga, Mg., Ing. Mario Geovanni García Carrillo, Mg. e Ing. Geovanni Danilo Brito Moncayo, Mg. revisó y aprobó el Informe Final del trabajo de graduación titulado "Herramienta opensource de administración y Monitoreo basado en snmp para el mejoramiento del funcionamiento de la red en SPEEDY COM CIA LTDA.", presentado por el señor José Iván Freire Bonilla, de acuerdo al Art. 18 del Reglamento de Graduación para obtener el título Terminal de tercer nivel de la Universidad Técnica de Ambato.

…….

Ing. Edison Homero Álvarez Mayorga, Mg.

PRESIDENTE DEL TRIBUNAL

……..

Ing. Mario Geovanni García Carrillo, Mg.

DOCENTE CALIFICADOR

……...

Ing. Giovanni Danilo Brito Moncayo, Mg.

DOCENTE CALIFICADOR

DEDICATORIA:

A Dios, que fue el creador de todas las cosas, el que me ha dado fortaleza para continuar cuando a punto de caer he estado.

A mis Padres, a quien les debo toda mi vida, les agradezco el cariño y su comprensión, a ustedes quienes han sabido formarme con buenos sentimientos, hábitos y valores, lo cual me ha ayudado a salir adelante buscando siempre el mejor camino.

A mis hermanos por estar a mi lado en los buenos y malos momentos y para quienes quiero ser un modelo a seguir.

A mis abuelitos, por su apoyo y la confianza que siempre me han brindado.

José Freire.

AGRADECIMIENTO:

A Dios, por estar conmigo en cada paso que doy, por fortalecer mi corazón e iluminar mi mente y por haber puesto en mi camino a aquellas personas que han sido mi soporte y compañía durante todo el periodo de estudio.

A mis padres, hermanos y demás familiares ya que me brindan el apoyo, la alegría y me dan la fortaleza necesaria para seguir adelante.

A la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, por abrirme las puertas y permitirme seguir adelante en mi vida profesional.

Al Ingeniero Marco Jurado, por su tiempo, colaboración, paciencia, apoyo en la realización del presente proyecto y sobre todo por esa gran amistad que me brindó y me brinda, por escucharme y aconsejarme siempre.

A todo el personal de la empresa Speedy Com., en especial al Ing. Juan Salcedo por la apertura y colaboración prestada para la elaboración del presente proyecto.

José Freire.

INDICE

Contenido Página

INDICE DE TABLAS

INDICE DE FIGURAS

RESUMEN EJECUTIVO

El propósito del presente proyecto está enfocado al monitoreo y administración de red de la empresa SPEDY COM.

El contenido de la investigación esta detallada en 6 capítulos descritos a continuación:

En el Capítulo I, se detalla todo lo referente a la problemática que presenta la empresa, y se enmarcan los objetivos que se piensa alcanzar con la investigación.

En el Capítulo II, se investiga y recopila toda la información necesaria y relevante con la cual se pudo adquirir conocimientos fundamentales de los sistemas y herramientas para la administración y monitoreo de la red.

En el capítulo III, se detalla la metodología que se utilizó para la recopilación de información necesaria de la empresa y de los procesos involucrados, con el fin de desarrollar el proyecto.

En el Capítulo IV, se interpreta y analiza la información obtenida de la empresa y del monitoreo constante de la red, en base a las observaciones realizadas.

En el Capítulo V, se detallan las conclusiones y recomendaciones obtenidas durante todo el proceso de observación y análisis de la empresa, tomando muy en cuenta datos relevantes.

Finalmente en el Capítulo VI, se desarrolla y diseña la propuesta de la Herramienta opensource de administración y Monitoreo basado en snmp para el mejoramiento del funcionamiento de la red en SPEEDY COM CIA LTDA.; además se implementa el proyecto tomando en cuenta cada uno de los requerimientos del mismo y utilizando la tecnología actual disponible en el país

INTRODUCCIÓN

En la actualidad las redes de datos se vuelven cada vez más extensas, 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.

Capítulo I

El Problema de Investigación

1.1. Tema de investigación

Herramienta opensource de administración y Monitoreo basado en snmp para el mejoramiento del funcionamiento de la red en SPEEDY COM CIA LTDA.

1.2. Planteamiento del problema

1.2.1. Contextualización

Actualmente las redes de datos de las empresas son cada vez más complejas y diversas, la necesidad y exigencia de su correcta operación es cada vez más crítica para el éxito en funcionamiento de las mismas. Con el avance de la tecnología las redes soportan mucho más aplicaciones y servicios que facilitan la vida diaria del ser humano y su comunicación a nivel mundial, haciendo así que el monitoreo y correcta administración de la misma sea una necesidad y no solo una opción.

En Ecuador las redes 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 en el país, 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.

En Ambato, la empresa SPEEDY COM CIA LTDA al ser una compañía proveedora del servicio de internet necesita de una manera inmediata el monitoreo de toda su red, además de sus equipos, ya que por su deficiente monitoreo de red se producen cortes de servicio, causando molestias a sus usuarios y demorando en detectar el daño causado en la red, lo que conlleva a que la empresa tenga pérdidas económicas considerables y perdidas de usuarios.

Por lo que se ha decidido la utilización de un sistema para poder tener la información por día y meses del estado y funcionamiento de los mismos obteniendo así información importante del actual funcionamiento de la red y poder mejorar el servicio, dando así un servicio transparente, que va a satisfacer las necesidades del usuario.

1.2.1.1. Árbol del Problema

En la figura 1.1 se detalla los efectos y causas en un árbol del problema.

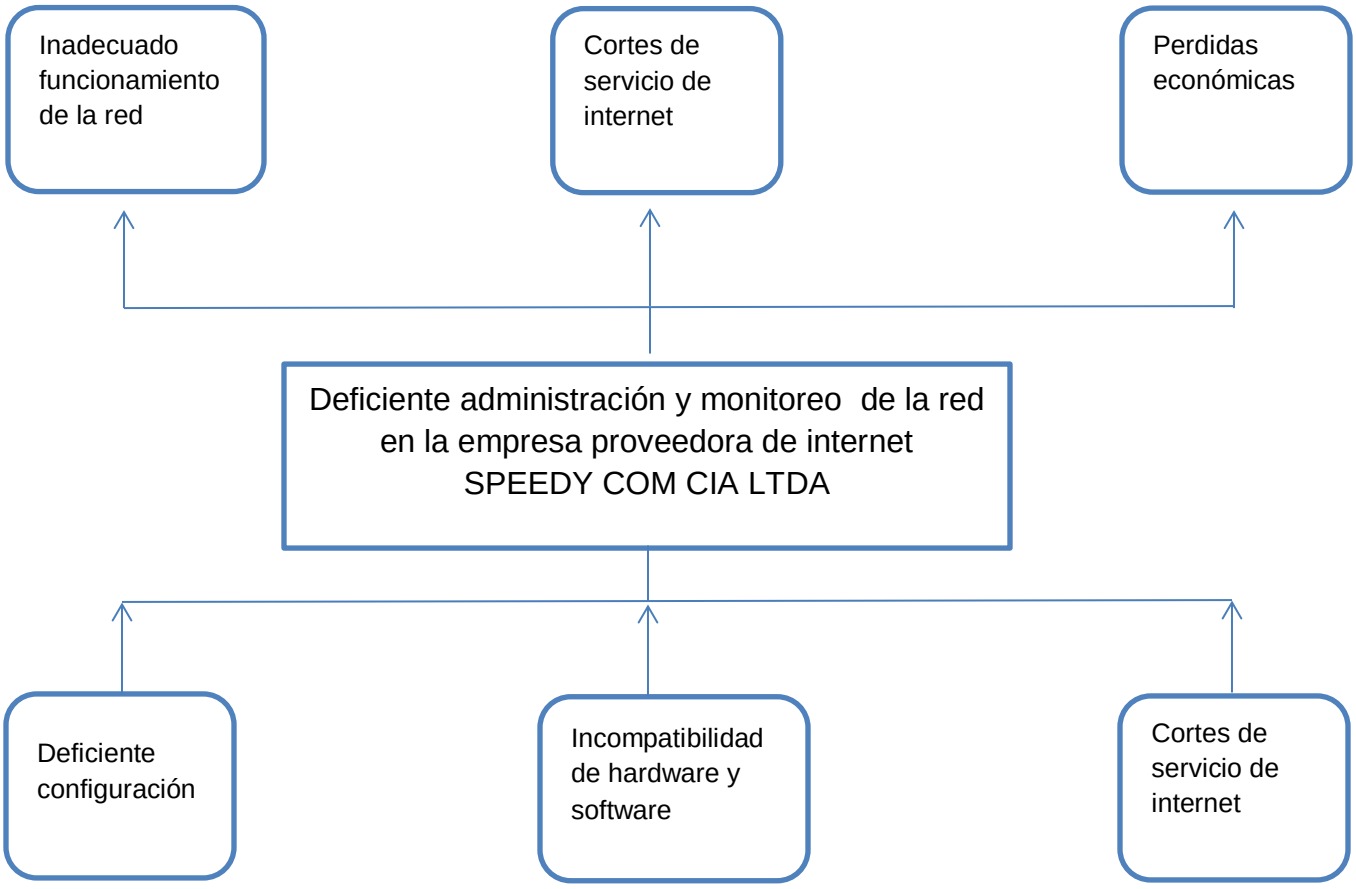


Figura 1.1. Árbol de Problemas

Elaborado por: El Investigador

1.2.2. Análisis Critico

El área de administración y monitoreo de la red de la empresa proveedora del servicio de internet no cuenta con un sistema adecuado de monitoreo de red a la falta de una configuración adecuada, cuyas limitaciones provocan un inadecuado

control de la red lo que puede generar el colapso de la misma provocando así molestias para la empresa y sus usuarios.

La incompatibilidad de hardware y software en el ISP, permite un monitoreo deficiente y pobre, además de cortes de servicio de internet en la misma empresa y a todos sus usuarios lo que genera una desconformidad en los usuarios, haciendo que varios usuarios presenten un sin número de quejas.

Los molestos cortes de servicio que se dan, provocan que los clientes de la empresa que son el sostén de la empresa se sientan inconformes con el servicio hasta llegar al punto que no desean más de los servicios que presta la empresa Speedy provocando así pérdidas económicas para la empresa.

1.2.3. Prognosis

Si determinadas circunstancias impidieran resolver el problema del monitoreo de la red sería imposible minimizar los costos en cuanto a pérdidas del servicio de internet a más de daños de los equipos, cuya solución conllevaría a mayores gastos producidos por la compra de equipos y actualización de nuevo software.

1.2.4. Formulación del problema

¿Cómo influye la deficiente administración y monitoreo en el funcionamiento de la red?

1.2.5. Preguntas directrices

¿Cuáles son los niveles y procesos de monitoreo y administración de la red en la empresa proveedora de internet SPEEDY COM CIA LTDA?

¿Es adecuado el funcionamiento de la red?

¿Se puede plantear una propuesta para el mejoramiento del funcionamiento de la red de la empresa SPEEDY COM CIA LTDA.?

1.2.6. Delimitación

- Área: Programación y redes.
- Línea de investigación: Programación y redes.
- Sublínea de investigación: Administración de Redes.
- Campo: Ingeniería Electrónica y Comunicaciones.
- Aspecto: Administración y control de la red.
- Delimitación Espacial: El presente trabajo de investigación se lo realizo en la ciudad de Ambato, provincia de Tungurahua, Empresa Speedy com ubicado en las calles Víctor Hugo Y Av. Atahualpa junto a Talleres de Andinamotors.
- Delimitación Temporal: El tiempo utilizado para realizar el presente trabajo de investigación fue de seis meses a partir de su aprobación del presente TEMI, por el Honorable Consejo Directivo de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

1.3. Justificación

El trabajo realizado fue de importancia ya que ayudo a que se tenga constante monitoreo de la red en la empresa SPEEDY COM CIA LTDA, ayudando así a su control y correcto funcionamiento en todas sus aplicaciones y servicios, beneficiando así a todos sus usuarios y a la misma empresa, para que puedan seguir gozando de la utilización óptima de la red con todas sus aplicaciones y servicios, sin ningún problema, cortes del servicio y molestias.

El proyecto realizado es factible ya que no es de un gran costo, ayudando así cada vez más al mejoramiento de la empresa y por medio de esta a sus numerosos usuarios que usan este servicio.

Los beneficiarios con este proyecto será la empresa y como parte de esta sus numerosos usuarios ya que tendrán un servicio de mejor calidad las 24 horas del día.

1.4. Objetivos

1.4.1. General

- Analizar cómo influye la deficiente administración y monitoreo en el funcionamiento la red de la empresa proveedora de internet SPEEDY COM CIA LTDA.

1.4.2. Específicos

- Identificar los niveles y procesos de monitoreo y administración de la red en la empresa proveedora de internet SPEEDY COM CIA LTDA.

- Determinar los parámetros que influyen en el funcionamiento de la red en la empresa proveedora de internet SPEEDY COM CIA LTDA.

- Proponer una herramienta opensource de administración y monitoreo basados en SNMP que permita mejorar el funcionamiento de la red en la empresa proveedora de internet SPEEDY COM CIA LTDA.

Capítulo II

Marco teórico

2.1. Antecedentes Investigativos

Dentro de los registros bibliográficos que posee la Biblioteca de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato, no se logró encontrar un tema similar al planteado. Sin embargo en la Universidad de Sevilla España se encontró el siguiente tema:

"Sistema de monitorización – Estado del arte" Realizado por: Luis Caballero Cruz, Año 2010.

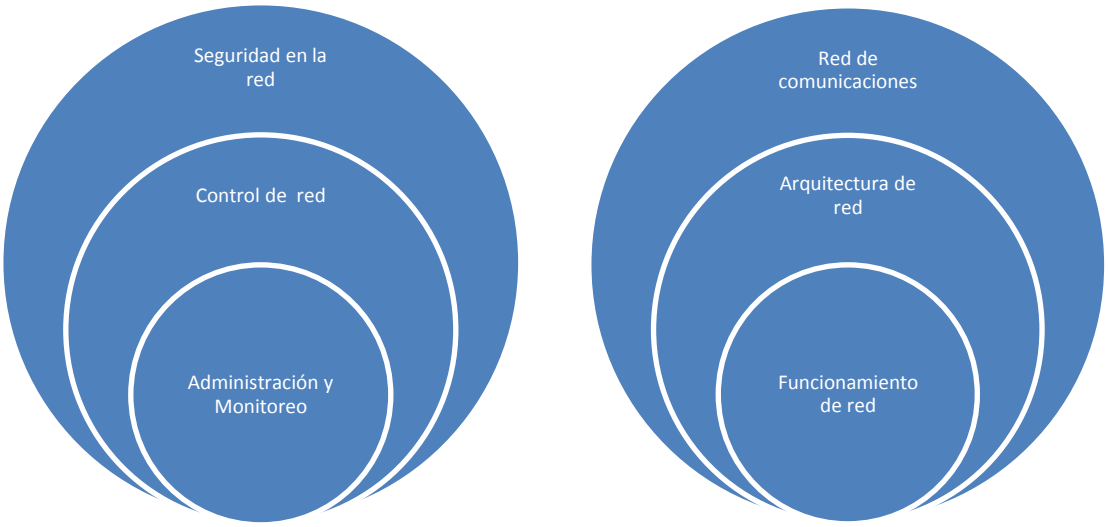
La conclusión del mencionado trabajo de investigación permitirá tener una visión más amplia de la administración y monitoreo bajo las herramientas opensource ya que es necesario conocer a las herramientas para obtener información del procedimiento que se debe seguir para su óptima utilización.

2.2. Fundamentación Legal

El presente trabajo de investigación, se basó en la Ley Especial de Telecomunicaciones y su reforma, Ley de Compañías, así como los estatutos y reglamentos internos de la empresa Speedy COM CIA LTDA, también se regirá al reglamento de graduación para obtener el título terminal de tercer nivel de la Universidad Técnica de Ambato.

2.3. Categorías Fundamentales

El presente proyecto de investigación se basó en dos variables que a continuación se detallan en la figura 2.1 permitiendo observar cómo están interrelacionadas**:**



Variable Independiente:

Administración y Monitoreo.

Variable Dependiente:

Funcionamiento de red

Figura 2.1. Inclusión Interrelacionadas de las Variables

Elaborado por: Investigador

2.3.1. Constelación de Ideas de la Variable Independiente

En la Figura 2.2 se explica la variable dependiente por medio de una constelación.

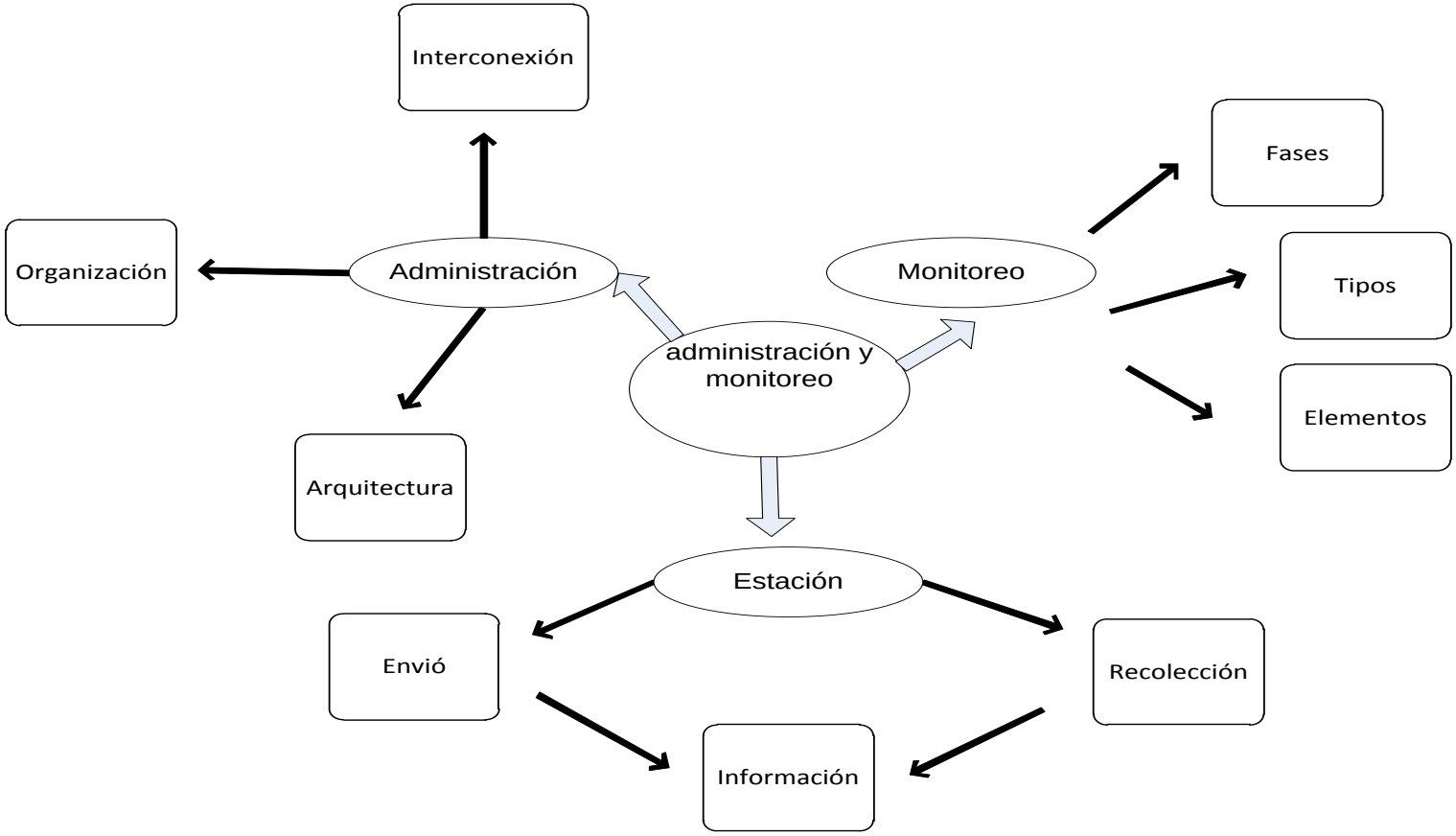


Figura 2.2. Constelación de Variable Dependiente

Elaborado por: Investigador

2.3.2. Constelación de Ideas de la Variable Dependiente

En la Figura 2.3 se explica la variable independiente por medio de una constelación.

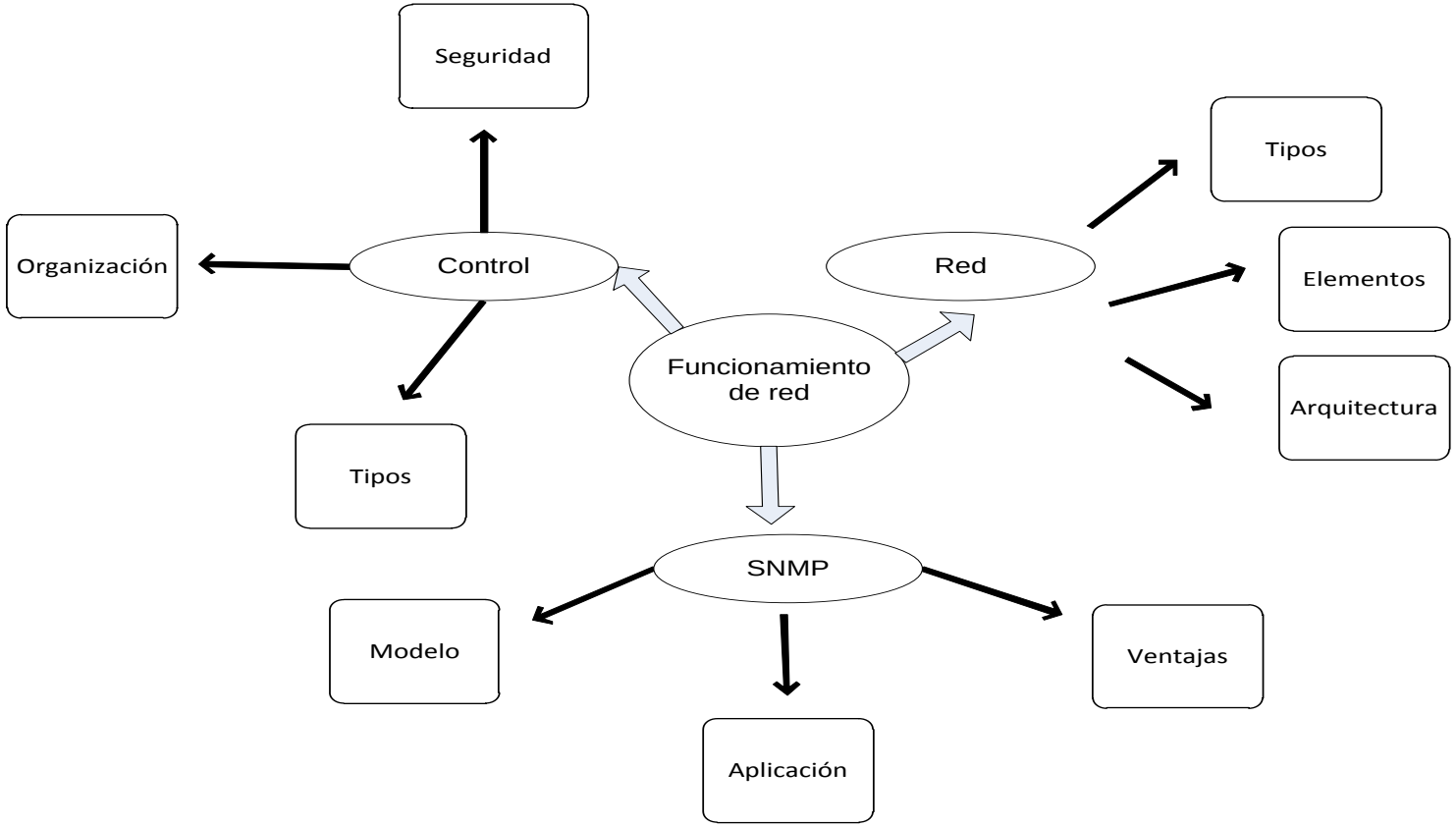


Figura 2.3. Constelación de Variable Independiente

Elaborado por: Investigador

Categorías fundamentales

2.3.3. Red

Una Red es un sistema de comunicación que se da entre distintos equipos para poder realizar una comunicación eficiente, rápida y precisa, para la transmisión de datos de un ordenador a otro, realizando entonces un Intercambio de Información y compartiendo también Recursos disponibles en el equipo.

La red tiene que estar conformada indefectiblemente por un Terminal o un Nodo que permita la conexión, y esencialmente el Medio de Transmisión, que es definido esencialmente por la conexión que es llevada a cabo entre dichos equipos.

Esta conexión puede ser realizada en forma directa, utilizando Cables de todo tipo, o bien mediante Ondas Electromagnéticas, presentes en las tecnologías inalámbricas, que requieren un adaptador específico para esta comunicación, que puede ser incluido en el equipo o conectado al equipo.

Cuando esta Red se da entre dos o más nodos que se encuentran lo suficientemente distantes entre sí, se habla de una Subred, que tiene la misión simplemente de servir como nexo o puente entre ellos, actuando como si fuera un Nodo Intermedio, pero no por ello afectando la comunicación, alterándola o impidiendo que llegue exactamente la misma información.

Entre los distintos tipos de Redes encontramos los siguientes tipos de redes, diferenciados lógicamente por el tamaño, la cantidad de terminales que abarcan:

- LAN – Red de Área Local: En inglés Local Área Network, se trata de redes pequeñas (hogareñas o empresariales) en donde cada equipo está conectado al resto.

- MAN – Red de Área Metropolitana: En inglés Metropolitan Área Network, en este tipo de redes la extensión es mucho mayor, abarcando una ciudad o una pequeña población determinada.
- WAN – Red de Área Extensa: En inglés Wide Área Network, en este caso las redes se dan entre países enteros o inclusive pueden alcanzar una extensión continental.

2.3.4. 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. 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.

2.3.5. Administración de redes

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 comprenden 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.

2.3.6. Dimensiones de la Administración de Redes.

La administración de redes, tiene 3 dimensiones que son las siguientes.

- Dimensión Funcional.- Se refiere a la asignación de tareas de administración por medio de áreas funcionales.
- Dimensión Temporal.- Se refiere a dividir el proceso de administración en diferentes fases cíclicas, incluyendo las fases de planeación, implementación y operación.
- 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. ”
  http://www.buenastareas.com/ensayos/Dimenciones-De-La-Administracion-De-Redes/2636377.html”

2.3.7. Objetivos de la Administración de Redes

Los objetivos de la Administración de Redes son los siguientes:

- 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.

2.3.8. 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 sistema de administración de red moderna es la de ser un sistema abierto, capaz de manejar varios protocolos y trabajar con varias arquitecturas de red, esto quiere decir: soporte para los protocolos de red más importantes. http://www.buenastareas.com/ensayos/Dimenciones-De-La-Administracion-De-Redes/2636377.html

2.3.9. 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, que son las siguientes:

1. Definición de la información de administración que se monitorea.
2. Acceso a la información.
3. Diseño de políticas de administración.
4. Procesamiento de la información.

Los tipos de monitoreo son:

- Local.- Cuando se realiza un monitoreo de área local dentro de la red interna del usuario
- Remoto.- Cuando se realiza el monitoreo desde un lugar remoto a la red como puede ser desde una estación remota que este a varios kilómetros de la red.
- Automático.- Cuando un dispositivo se encarga de monitorear y comunicar el estado en que se encuentra.
- Manual.- Cuando la persona monitora personalmente y comunica su estado.

Los elementos monitoreados pueden ser:

- En su totalidad.- Cuando se monitorea todo de manera global como por ejemplo toda una red.
- En Segmentos.- Cuando se monitorea por secciones de acuerdo a la necesidad de los dispositivos a ser monitoreados.

El monitoreo puede ser realizado en forma:

- Continua.- Cuando se realiza un monitoreo constante de los dispositivos.
- Eventual.- Cuando se realiza un monitoreo cuando el momento lo amerita.

2.3.10. Objetivos del Monitoreo

Los objetivos de realizar un monitoreo son los siguientes:

- 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. “http://www.integracion-de-sistemas.com/analisis-y-monitoreo-de-redes/index.html”

2.3.11. 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.

A continuación en la figura 2.4 se muestra cómo está constituida la arquitectura de la Administración de Redes.

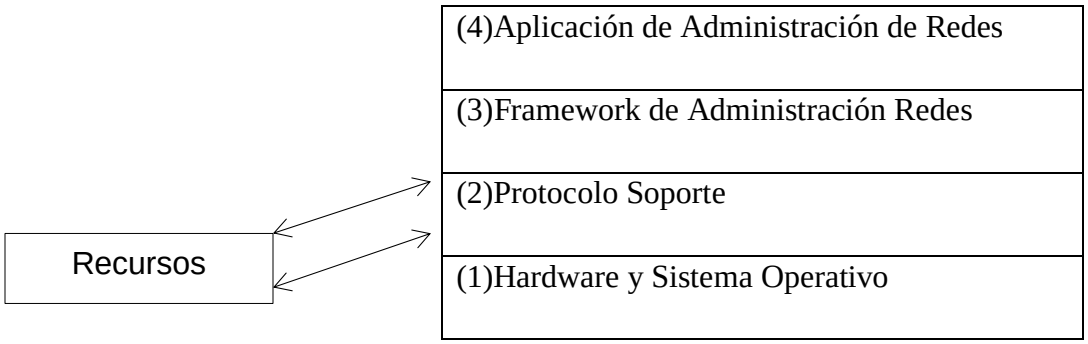


Figura 2.4. Arquitectura de la Administración de Redes

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 orientados 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.
   "http://www.geocities.ws/abianchi04/textoredes/snmp.pdf"

2.3.12. 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.

A continuación se muestra algunos de los componentes de hardware a ser administrados:

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.

El software típico que se incluye en la administración son:

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.

En la siguiente figura 2.5 se puede observar los elementos involucrados en la Administración y Monitoreo de Redes.

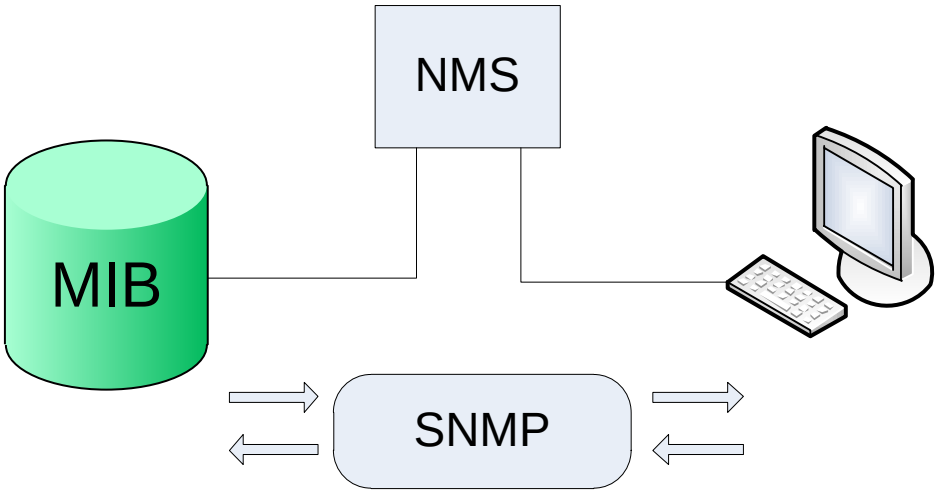


Figura 2.5: Componentes de la Administración y Monitoreo de Red

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

En donde:

MIB (Base de Información Gestionada o del Ingles Management Information Base) es un tipo de base de datos que contiene información jerárquica, estructurada en forma de árbol, de todos los dispositivos gestionados en una red de comunicaciones

NMS (sistema de gestión de red o del Ingles network management system) que es una combinación de hardware y software utilizado para controlar y administrar una red de ordenadores o redes.

SNMP o Protocolo Simple de Administración de Red o (del inglés Simple Network Management Protocol) es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Permite a los administradores supervisar el funcionamiento de la red, buscar y resolver sus problemas, y planear su crecimiento.

http://es.wikibooks.org/wiki/Mejores_pr%C3%A1cticas_para_redes_de_datos/Introducci%C3%B3n_a_la_administracion_de_redes

2.3.13. Control de acceso a red

El control de acceso a red es un concepto de ordenador en red y conjunto de protocolos usados para definir como asegurar los nodos de la red antes de que estos accedan a la red. NAC puede integrar el proceso de remedio automático (corrigiendo nodos que no cumplen las normativas antes de permitirles acceso) en el sistema de red, permitiendo a la infraestructura de red como routers, switches y firewalls trabajar en conjunto con el back office y el equipamiento informático del usuario final para asegurar que el sistema de información está operando de manera segura antes de permitir el acceso a la red.

El objetivo del control de acceso a red es realizar exactamente lo que su nombre implica: control de acceso a la red con políticas, incluyendo pre-admisión, chequeo de políticas de seguridad en el usuario final y controles post-admisión sobre los recursos a los que pueden acceder en la red los usuarios y dispositivos y que pueden hacer en ella.

2.3.14. Objetivos del control de acceso a red

El control de acceso a red (NAC) representa una categoría emergente en productos de seguridad, su definición es controvertida y está en constante evolución. Los objetivos principales de este concepto se pueden resumir en:

Mitigar ataques de día cero:

El propósito clave de una solución NAC es la habilidad de prevenir en los equipos finales la falta de antivirus, parches, o software de prevención de intrusión de hosts y acceder así a la red poniendo en riesgo a otros equipos de contaminación y expansión de gusanos informáticos.

Refuerzo de políticas:

Las soluciones NAC permiten a los operadores de red definir políticas, tales como tipos de ordenadores o roles de usuarios con acceso permitido a ciertas áreas de la red, y forzarlos en switches y routers.

Administración de acceso e identidad:

Donde las redes IPs convencionales refuerzan las políticas de acceso con base en direcciones IP, los dispositivos NAC lo realizan basándose en identidades de usuarios autenticados, al menos para usuarios finales de equipos portátiles y sobremesa.

2.3.15. Seguridad en la red

El activo más importante en las organizaciones públicas, privadas y de cualquier índole, es la información que tienen. Entre más grande es la organización más grande es el interés de mantener la seguridad en la red, por lo tanto, es de suma importancia el asegurar la seguridad de la información.

La seguridad no es solamente el implementar usuarios y contraseñas, es el implementar políticas que garanticen la seguridad tanto física como lógica de la información.

Dentro del entorno de la red se debe asegurar la privacidad de la información y de proteger las operaciones de daños no intencionados como deliberados.

Dentro de las redes inalámbricas el sentido de seguridad es más sentido debido a la naturaleza de las mismas. En sus inicios la seguridad en este tipo de redes era muy deficiente y algunas personas de daban a la tarea de encontrar redes inalámbricas para acceder a ellas desde las calles.

Este documento pretende dar una idea general sobre este tema y poder tener una idea clara de la importancia que esto tiene.

2.3.16. Planificación de seguridad en redes

La planificación de la seguridad en el diseño de la red es de suma importancia, pues de esto depende el buen desempeño de la red y evita trabajo posterior, pérdida de datos y posibles daños a la red.

En ocasiones se considera el tema de seguridad fuera de tiempo lo cual trae consecuencias de retrabado, gastos excesivos y posibles pérdidas de información.

Algunos puntos que debemos tomar en cuenta para una correcta planificación de seguridad en la red son:

- Accesos no autorizados.
- Daño intencionado y no intencionado.
- Uso indebido de información (robo de información).

El nivel de seguridad de la red dependerá de su tamaño e importancia de la información. Un banco deberá de tener un nivel muy alto de seguridad por las transacciones que maneja, una red casera no tendrá la misma importancia, solo se orientará a los accesos de los familiares a ciertos puntos de las computadoras que la formen.

En este momento se definen las políticas referentes a los usuarios y contraseñas, los métodos de acceso a los servidores y a los sistemas. Se definen la complejidad que debe reunir las contraseñas y su validación dentro de la red, el tiempo de trabajo de las estaciones de trabajo, áreas de acceso por cada usuario, etc. "http://docs.oracle.com/cd/E19253-01/821-0596/gdpgj/index.html"

2.3.17. Arquitecturas de las redes de comunicaciones

Las redes de comunicación se diseñan y se construyen en arquitecturas que pretenden servir a sus objetivos de uso. Por ejemplo, existen necesidades de intercambio de información entre usuarios que obligan a mantener un flujo continuo

de información, o al menos que la información llegue sin retardos apreciables para el usuario y sin desordenar, pues de lo contrario se altera su significado. Este es el caso de la voz o, en muchos casos, del vídeo.

También es posible utilizar arquitecturas que se basan en un flujo discontinuo de información formado por "paquetes" separados de datos. Estas arquitecturas son típicas de sistemas donde la información es discontinua de forma natural (como por ejemplo en el uso del correo electrónico), pero también se puede utilizar en aquellos sistemas que requieren un flujo continuo de información, siempre y cuando se garantice que la red de comunicaciones entrega la información sin un retardo apreciable para los usuarios y sin desordenar los paquetes de datos en los que se ha descompuesto el flujo de información.

Para que la información enviada por un terminal, sea recibida en el otro extremo, las redes y las arquitecturas mediante las que se implementan establecen un camino entre los extremos por el que viaja la información. Como las redes de comunicaciones no unen directamente a todos los usuarios con el resto, sino que tienen una estructura jerárquica, es necesario contar con un procedimiento de conmutación o encaminamiento que dirija la información hacia su destinatario.

Siguiendo con esta lógica, existen dos tipos básicos de arquitecturas de redes de comunicación: conmutación de circuitos y conmutación de paquetes.

En la conmutación de circuitos, el camino llamado circuito entre los extremos del proceso de comunicación se mantiene de forma permanente mientras dura la comunicación, de forma que es posible mantener un flujo continuo de información entre dichos extremos. Este es el caso de la telefonía convencional. Su ventaja principal radica en que una vez establecido el circuito su disponibilidad es muy alta, puesto que se garantiza este camino entre ambos extremos independientemente del flujo de información.

En la conmutación de paquetes, no existe un circuito permanente entre los extremos y, la red, simplemente, se dedica a encaminar paquete a paquete la información entre los usuarios. En la práctica esto significa que los paquetes en los que se ha

dividido la información pueden seguir caminos diferentes. Su principal ventaja es que únicamente consume recursos del sistema cuando se envía o se recibe un paquete, quedando el sistema libre para manejar otros paquetes con otra información o de otros usuarios.

Por tanto, la conmutación de paquetes permite inherentemente la compartición de recursos entre usuarios y entre informaciones de tipo y origen distinto. Este es caso de Internet, su inconveniente reside en las dificultades en el manejo de informaciones de tiempo real, como la voz, es decir, que requieren que los paquetes de datos que la componen lleguen con un retardo apropiado y en el orden requerido. Evidentemente las redes de conmutación de paquetes son capaces de manejar informaciones de tiempo real, pero lo hacen a costa de aumentar su complejidad y sus capacidades. “http://docs.oracle.com/cd/E19253-01/821-0596/gdpgj/index.html”

2.3.18. Protocolo Simple de Administración de Redes (SNMP)

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

Los nodos administradores pueden ser enrutadores, host, puentes, impresoras u otros dispositivos capaces de comunicar información de estado al mundo exterior, como se puede observar en la figura 2.6.

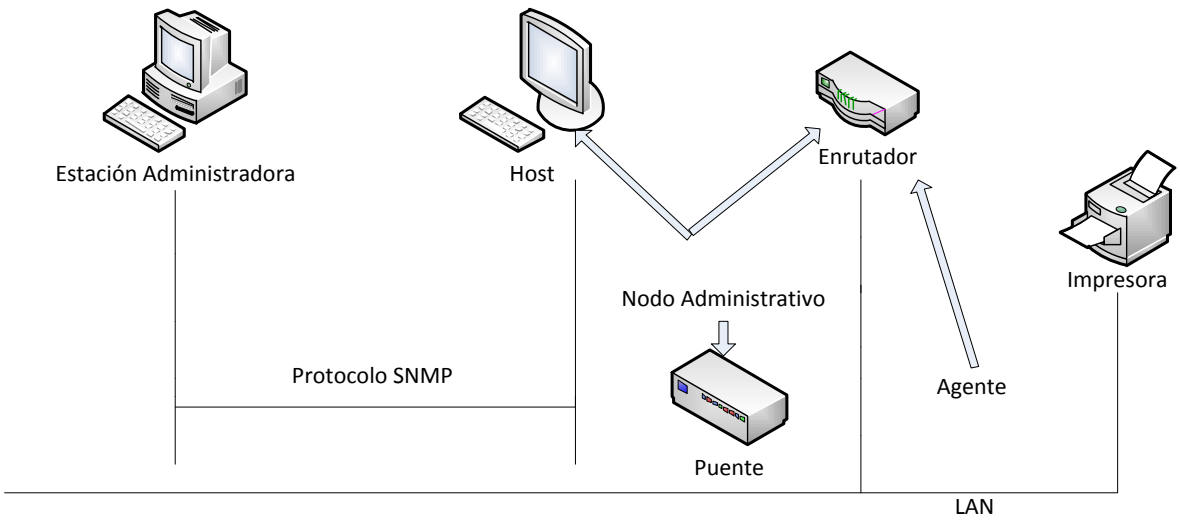


Figura 2.6: Proceso de Administración

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

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 se hace referencia 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 módulo 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 se utilice se puede 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. “http://support.microsoft.com/kb/172879/es.”

2.3.19. Arquitectura de un modelo SNMP

En la figura 2.7 se puede observar el modelo de arquitectura en la que se encuentra conformado el protocolo SNMP.

En donde la información obtenida de las MIB de los dispositivos se transmite a una Estación de gestión de red principal a través del protocolo SNMP un mejor control y gestión de la red.

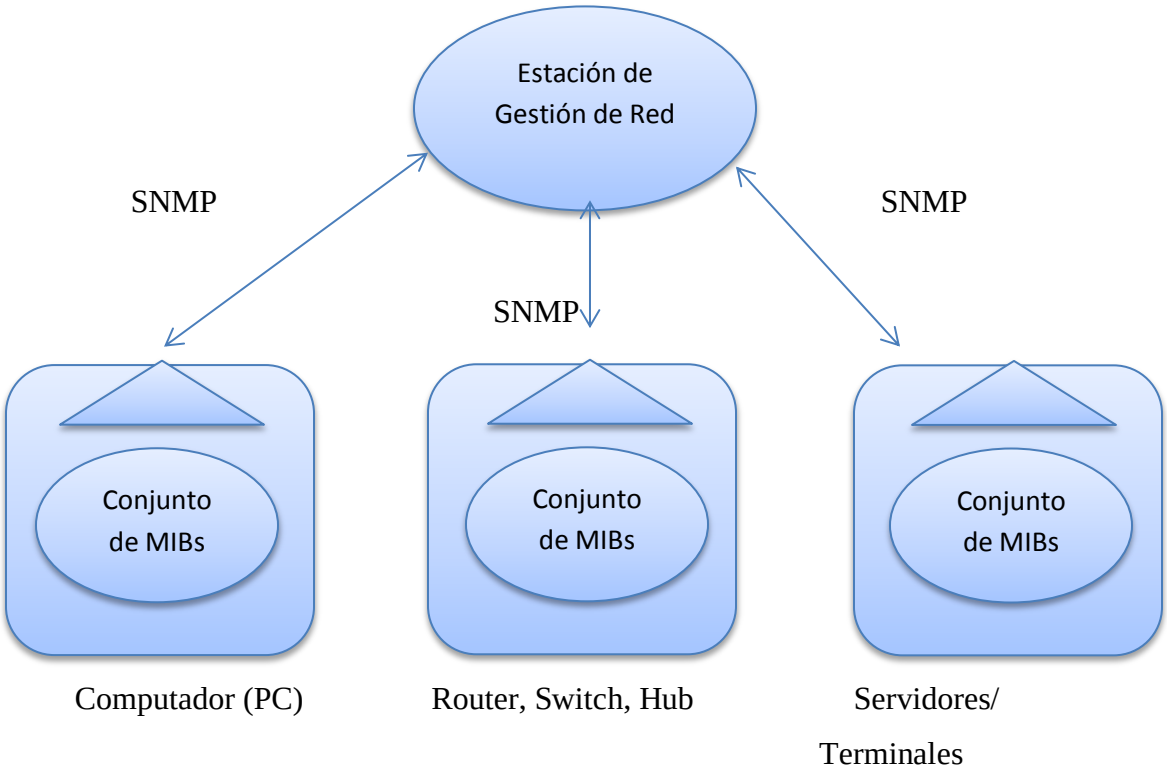


Figura 2.7: Arquitectura de un modelo SNMP

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.

2.3.20. Ventajas y Desventajas de SNMP

Ventajas de SNMP

La ventaja de SNMP es la siguiente:

1. 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 más 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.

Desventajas de SNMP

Las desventajas de SNMP son las siguientes:

1. 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.

2. 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.

2.3.21. 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

Las ventajas de SNMP v1 son:

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

Desventajas

Las desventajas de SNMP v1 son:

- 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 SNMP v1, ha mejorado en los tipos de datos y operaciones, pero sigue quedando corto en cuanto a seguridad.

Ventajas:

Las ventajas de SNMP v2 son:

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

Desventaja

La desventaja de SNMP v2 es:

- 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.

Ventaja:

La ventaja de SNMP v3 es:

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

Desventaja:

La desventaja de SNMP v3 es:

- Aún no es muy conocido y poco implementado.

2.3.22. Proceso de envió de un Mensaje SNMP

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

Transmisión

El proceso que realiza el agente SNMP al momento de la transmisión es el siguiente:

1. Se construye UDP
2. Se involucra el servicio de autenticación con la dirección de transporte.
3. Se construye el mensaje SNMP
4. Se codifica

Recepción

El proceso que realiza el agente SNMP al momento de la recepción es el siguiente:

1. Comprobación sintáctica
2. Verificación de la versión utilizada
3. Autentificación, Verifica si falla
4. Proceso de petición

Mensaje SNMP

- Mensaje SNMP <---------->Datagrama UDP.- El agente SNMP trabaja con el protocolo UDP por medio de datagramas para un envió rápido de los datos.
- Disminuye el procesado de mensajes y complejidad del agente.

2.3.23. Mensajes enviados por SNMP

Algunos de los mensajes enviados por SNMP para petición de solicitudes son los siguientes:

Get Request: Solicita uno a más 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).

En la figura 2.8 se puede observar la estructura del mensaje SNMP y el proceso de su envió.

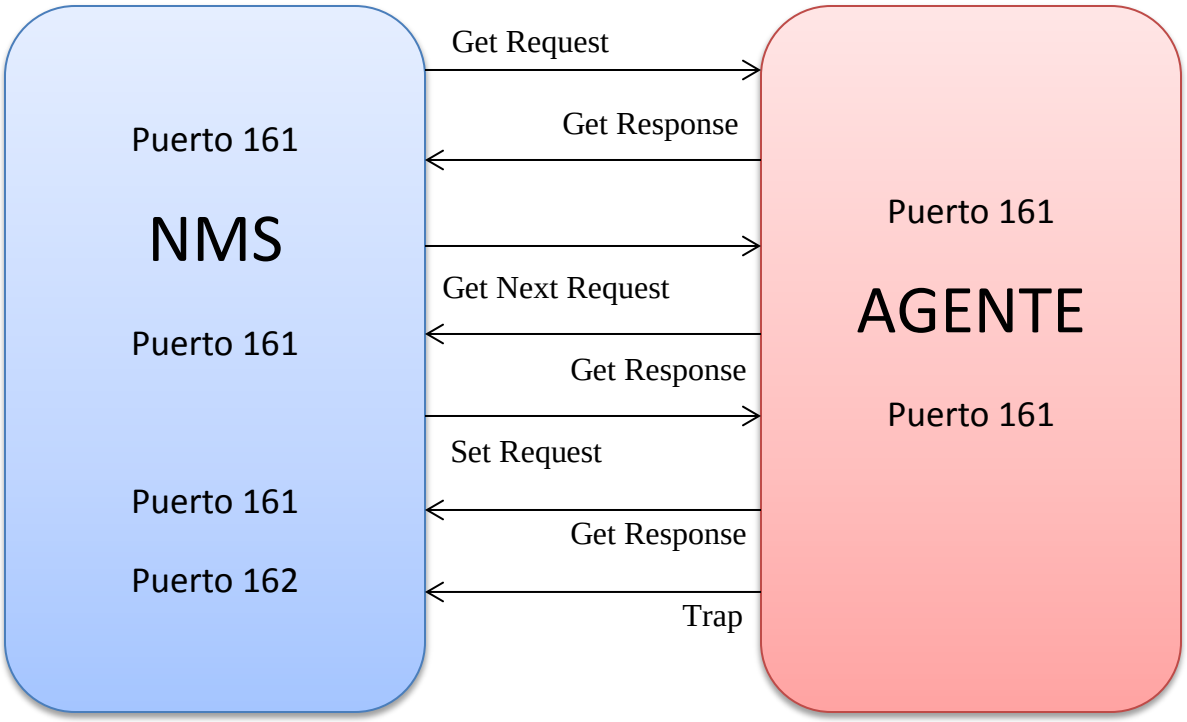


Figura 2.8: Estructura del mensaje SNMP

Fuente: http://es.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.
http://www.uazuay.edu.ec/estudios/sistemas/teleproceso/apuntes_1/snmp.htm

2.3.24. 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.

El control de fallas tiene 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.

La Administración de cambios comprende la planeación, la programación de eventos e instalación.

Administración del comportamiento.

La 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.

Los Servicios de contabilidad proveen 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.

El 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.

2.3.25. 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.

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.

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)

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.

Técnicas de monitoreo pasivo.

Solicitudes remotas

Las solicitudes remontas son solicitudes que se las puede hacer a distancia por lo que no necesita una presencia obligatoria, las solicitudes remotas se las puede realizar de las siguientes maneras:

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).

2.3.26. 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.

Aspectos que pueden ser monitoreados

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.

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.

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)

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.

2.3.27. Aspectos a considerar para 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 a través de la red auto 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.

2.3.28. 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.

2.3.28.1. 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.

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 gráfica 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.

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

Principios de Funcionamiento

El funcionamiento de Cacti puede ser dividido en tres tareas diferentes que se las muestra en el gráfico 2.9:

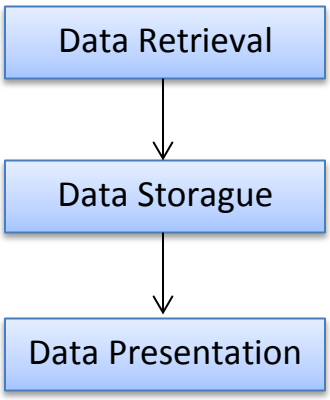


Figura 2.9: Principios de funcionamiento de Cacti
Fuente: http://www.cacti.net/downloads/docs/pdf/manual.pdf

Data Retrieval - Recuperación de Datos

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.

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 último.

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.

http://www.eurogaran.com/index.php/es/servidores-linux/monitorizacion/cacti/

Arquitectura de CACTI

Básicamente Cacti consta de los siguientes elementos que se muestran en la figura 2.10:

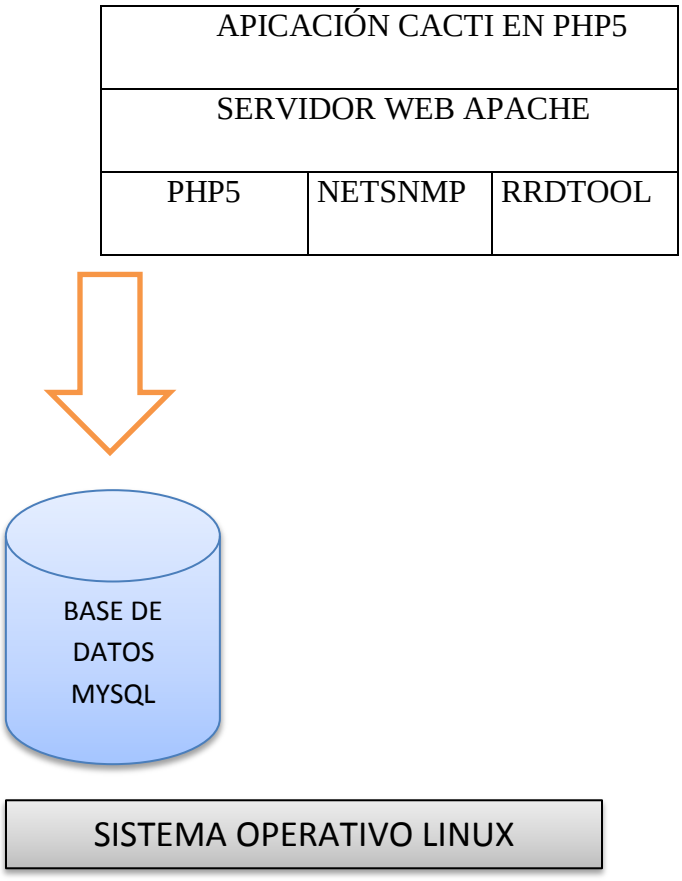


Figura 2.10: Arquitectura de Cacti sobre Linux

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

2.3.28.2. 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 él, 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.

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: gráfica y guarda registros de series temporales de datos.
- MySQL: Una base de datos de código abierto.

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 como se puede observar en la figura 2.11.

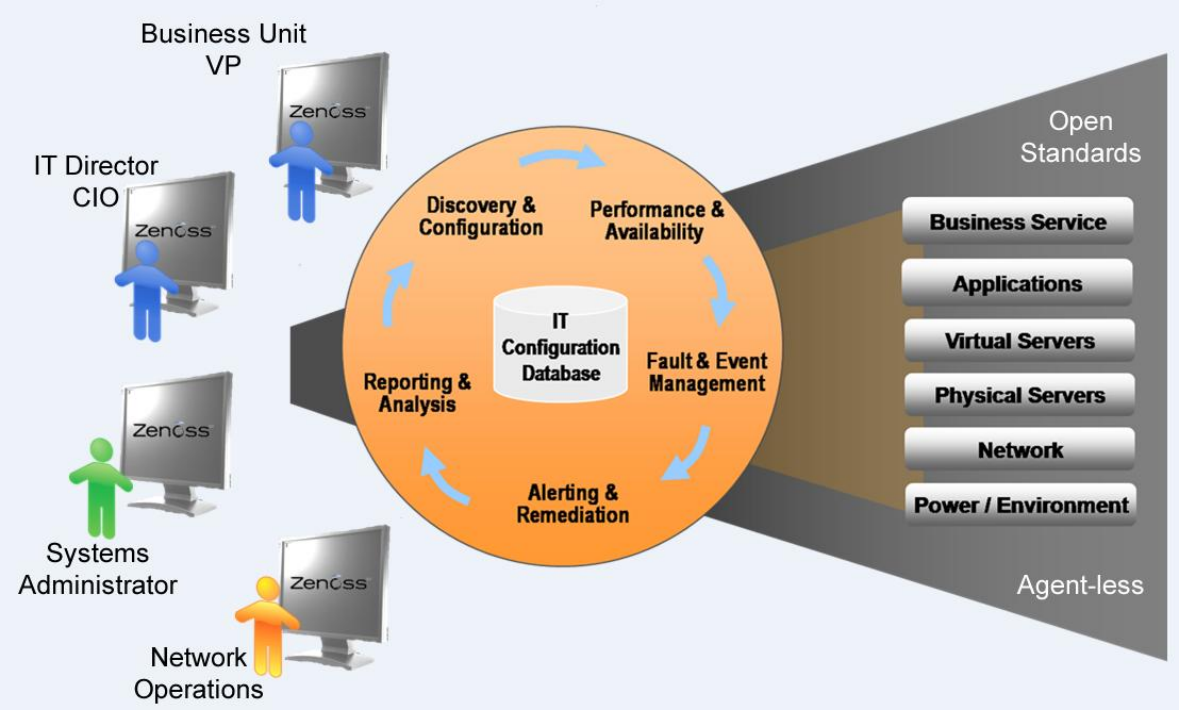


Figura 2.11: Vista de alto nivel Zenoss

Fuente: http://ufpr.dl.sourceforge.net/project/zenoss/Documentation/zenoss-3.0.xdocs/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.

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

En la figura 2.12 se muestra de manera más detallada sobre las versiones de zenoss.

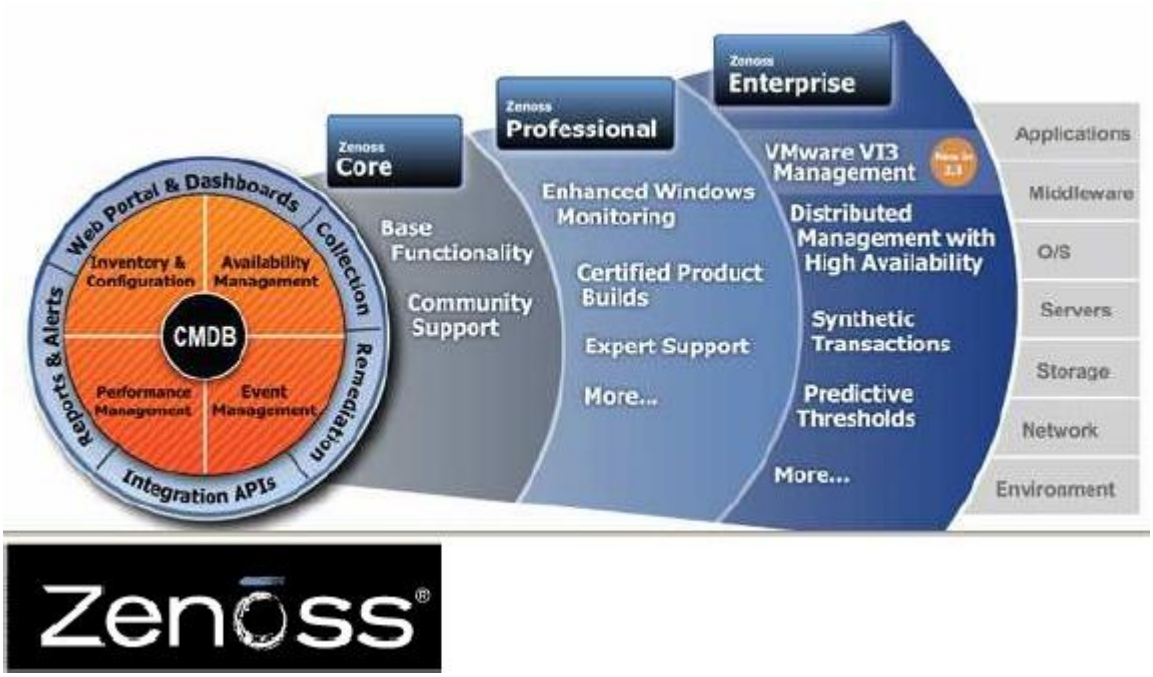


Figura 2.12: Versiones de Zenoss

Fuente: http://es.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).

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.

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 continua.

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.
En la figura 2.13 se puede observar las herramientas de localización con las q cuenta zenoss.

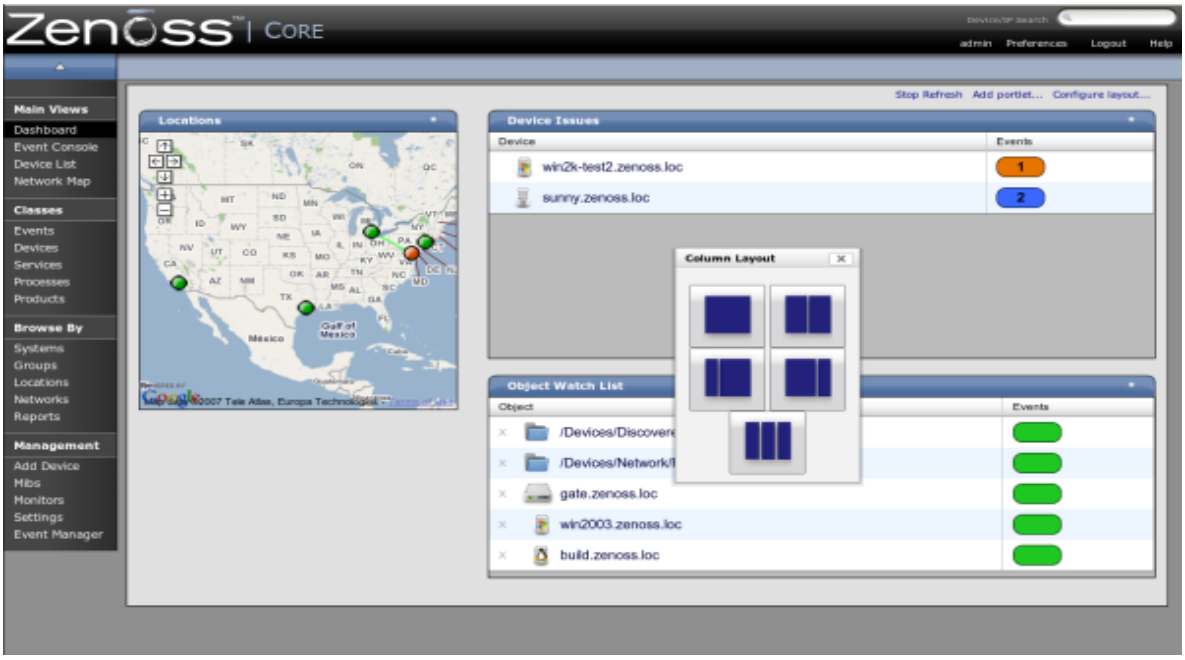


Figura 2.13: Herramientas Dashboard o de Localización

Fuente:http://www.infotechgroup.com.ar/site/index.php?option=com_content&view=article&id=23&Itemid=15

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.

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.

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.

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.

Supervisión y ejecución de Zenoss:

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

Arquitectura de Zenoss

En la figura 2.14 se ilustra la arquitectura del sistema Zenoss.

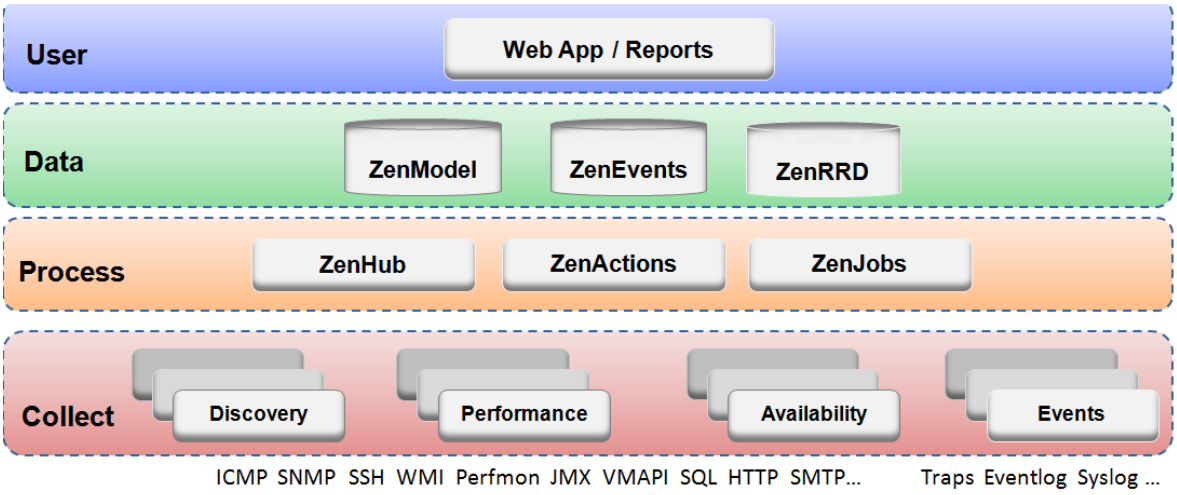


Figura 2.14: Arquitectura de Zenoss

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

En donde Zenoss es un sistema escalonado de cuatro partes principales que se les ira detallando a continuación:

- Capa de Usuario
- Capa de Datos
- Capa de Procesamiento
- Capa de Colección

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.

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

A continuación en la tabla 2.1 se muestra la base de datos con la que cuenta zenoss y sus principales características.

Tabla 2.1: Base de datos Zenoss

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.

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

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.

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:

A continuación en la tabla 2.2 se muestra la automatización de modelado de demonios y sus características.

Tabla 2.2: Automatizado de Modelado de 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

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

Disponibilidad de Modelos de demonios:

A continuación en la tabla 2.3 se muestra la disponibilidad de modelos de demonios con la que cuenta zenoss y sus características.

Tabla 2.3: Disponibilidad de Modelado 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.

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

Evento de Colección de demonios:

A continuación en la tabla 2.4 se muestra los eventos de colección de demonios con la que cuenta zenoss y sus principales carcateristicas.

Tabla 2.4: 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.

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

Monitoreo de desempeño de demonios:

A continuación en la tabla 2.5 se muestra cómo se realiza en monitoreo del desempeño de los demonios de zenoss.

Tabla 2.5: 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 plugins local o remotamente a través de SSH.

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

Respuesta automática Demonios:

A continuación en la tabla 2.6se muestra las respuestas automáticos que entregan los demonios de zenoss.

Tabla 2.6: Respuesta automática de Demonios

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

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

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 monitoreados como vienen en línea.

En la figura 2.15 se muestra una figura del flujo de trabajo con el que cuenta zenoss:

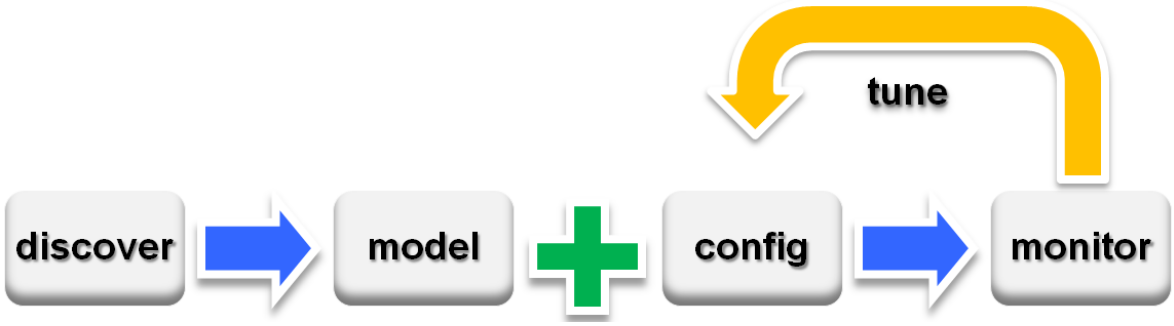


Figura 2.15: Flujo de Trabajo: Control de Model Driven

Fuente: http://ufpr.dl.sourceforge.net/project/zenoss/Documentation/zenoss-3.0.xdocs/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.

En la figura 2.16 se muestra un ejemplo del monitoreo que realiza Zenoss

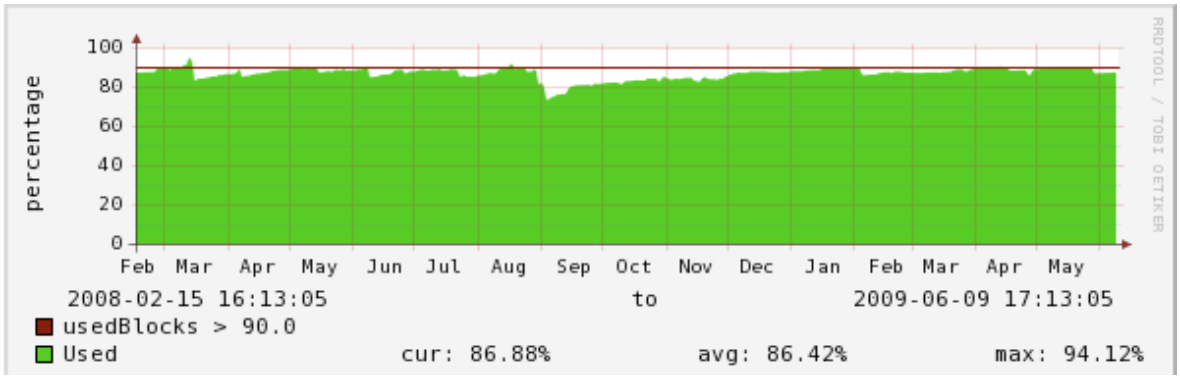


Figura 2.16: Monitoreado de archivos del sistema

Fuente: http://ufpr.dl.sourceforge.net/project/zenoss/Documentation/zenoss-3.0.xdocs/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).

"http://www.zenoss.com/"

2.3.28.3. 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 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.

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 el 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

Requisitos software

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

En la tabla 2.7 se muestra el software es necesario para ejecutar Zabbix:

Tabla 2.7: Software 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.

Fuente: http://es.opensuse.org/Zabbix

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

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.

En la figura 2.17 se puede observar la Arquitectura con la que cuenta Zabbix y sus principales características:

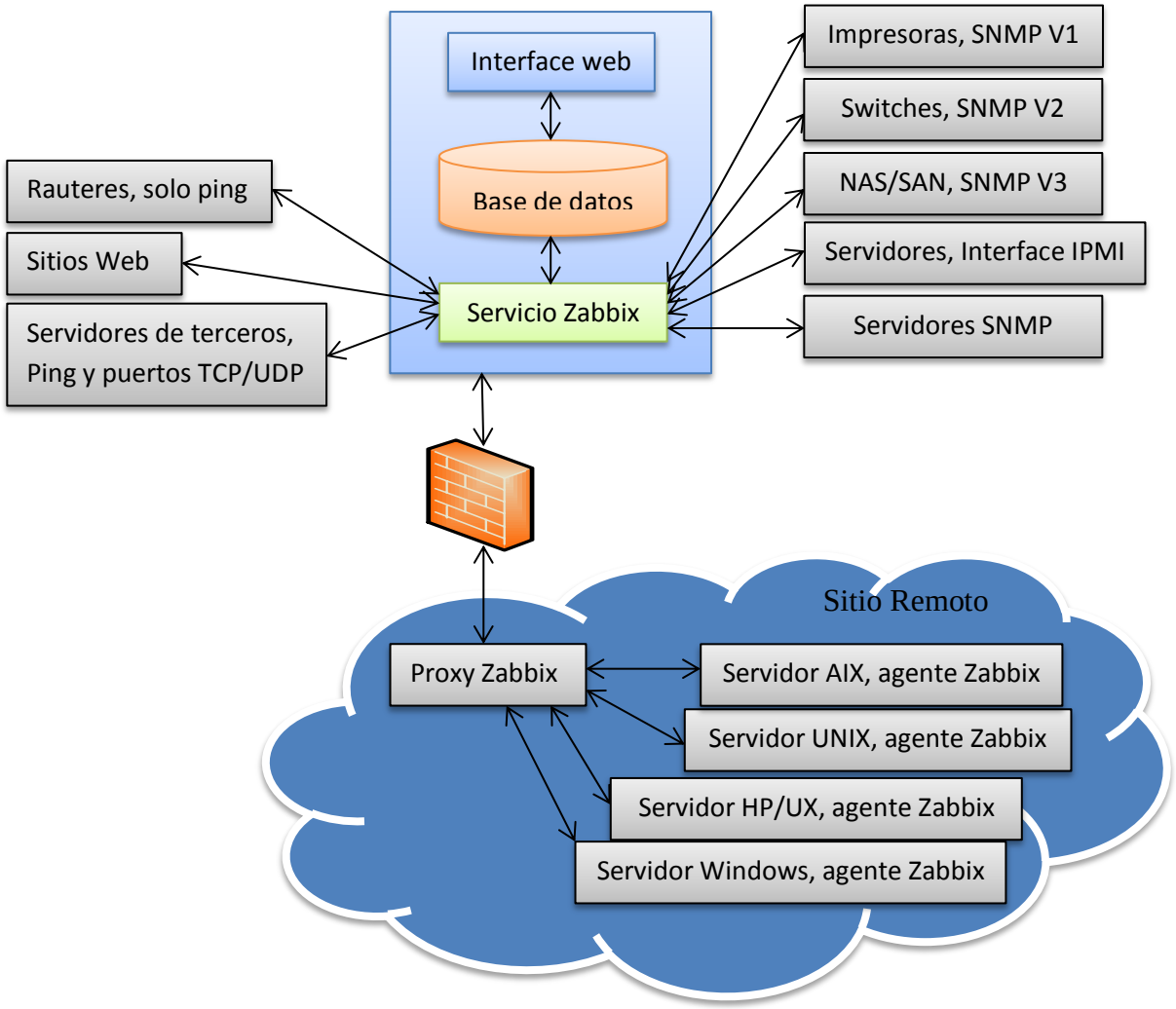


Figura 2.17: Arquitectura de Zabbix

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.
http://www.zabbix.com/

2.4. Hipótesis

¿La administración y monitoreo de la red de la empresa SPEEDY COM CIA LTDA influye en su adecuado funcionamiento?

2.5. Señalamiento de Variables de la Hipótesis

2.5.1. Variable Independiente

Administración y Monitoreo de la red

2.5.2. Variable Dependiente

Funcionamiento de red

Capítulo III
Metodología

3.1. Enfoque de la investigación

Esta investigación tuvo un enfoque cuali-cuantitativo en sus aspectos por su forma de solución del problema.

Fue cualitativa ya que permitió mejorar el rendimiento de la red, permitiendo que la empresa pueda brindar un servicio de calidad las 24 horas del día optimizando así la calidad del servicio al cliente y a la vez la conformidad del mismo con el servicio.

Fue cuantitativa porque al mantener un control en la red, esta se mantendrán en buen estado, reduciendo tiempo y a la vez costos, ya que al tener un control en la red se sabrá cuál es el problema y permitirá arreglarlo de manera inmediata, ganado así la empresa ya que se brindara un servicio de calidad asegurando así la conformidad de los clientes y una mayor demanda de estos.

3.2. Modalidad De Investigación

La presente investigación se contextualizó en la modalidad de investigación de campo y documental-bibliográfica.

De campo porque se realizó un estudio sistemático de los hechos en el lugar donde se producen los acontecimientos y documental bibliográfica porque se tuvo como

propósito detectar, profundizar y ampliar diferentes enfoques, teorías, conceptualizaciones y criterios de diversos autores, basándose en diferentes documentos, como por ejemplo diarios, revistas y otras publicaciones.

3.3. Tipos de Investigación

La investigación tuvo un nivel **exploratorio** porque permitió conocer el problema, permitiendo una visión más clara del mismo. Un nivel **descriptivo** que permitió dar pronósticos básicos, para lo cual se requirió un conocimiento suficiente de la situación. El nivel **explicativo** detectando las causas de determinados comportamientos, explicando los factores precisos de ciertos procedimientos. Por último la **asociación de variables** estuvo presente evaluando las variables de comportamiento, midiendo el grado de relación entre las mismas.

3.4. Población y muestra

En el presente Trabajo de Investigación se realizaron un promedio de 50 observaciones directas para comprobar el funcionamiento de la red de la empresa.

3.5. Técnicas e instrumentos de Investigación

La técnica que se empleó en la presente investigación fue la observación.

Observación.- Mediante la observación se detectan problemas que se encuentran en nuestro entorno, y mediante nuestros sentidos recogemos datos para su posterior análisis e interpretación que nos permita llegar a conclusiones y a la toma de decisiones.

3.6. Plan de recolección de la información

Para la recolección de información se realizó un promedio de 50 observaciones directas para comprobar el funcionamiento de la red de la empresa.

Una vez recolectada la información se procederá a su respectiva tabulación de datos.

3.7. Procedimiento y análisis de la información

Obtenido el resultado de las observaciones directas se procedió al análisis de la información para comprobar la factibilidad de la propuesta del Servidor de administración y monitoreo basado en SNMP para mejorar el control de la red en SPEEDY COM CIA LTDA., usando software de código abierto.

Capítulo IV

Análisis e Interpretación de Resultados

4.1. Introducción

El siguiente análisis, corresponde a los resultados obtenidos de la observación realizada, de 50 veces para comprobar el funcionamiento de la red de la empresa, la cual proporcionó información referente a la actual condición de la administración y monitoreo de la red.

La información obtenida fue tabulada y analizada de forma sistemática, además interpretada estadísticamente para obtener resultados precisos y confiables.

Tabla 4.1: Observación del funcionamiento de la red de la empresa Speedy

Fecha	Hora	Problema
03/09/2012	9:00	Llamadas de reclamos por parte de los usuarios, debido a problemas del nodo de Macasto y a su retraso en la reparación de este, el cual fue causado por avería en el router principal.
04/09/2012	16:00	Problemas del nodo de Pinllo debido a fallas en el router del mismo.
06/09/2012	10:00	Problemas en el servicio de internet con un cliente debido a daños en el cable de red en el sector del nodo de Horizonte.
10/09/2012	12:00	Caída de toda la red de la empresa debido a

		un corte de luz programada por la empresa eléctrica Ambato.
12/09/2012	15:00	Problema en el servicio de internet de un cliente debido a daños en la antena del usuario en el sector de Atahualpa.
13/09/2012	11:00	Problemas en el nodo de Palama debido a corte de luz en el nodo por desgaste de batería.
17/09/2012	16:00	Problemas con el proveedor de servicios de internet de alta capacidad de Speedy debido a fallos en sus sistemas.
19/09/2012	9:00	Problemas en el servicio de internet de un cliente debido a desconfiguración en su antena en el sector del Mall de los Andes.
20/09/2012	15:00	Problemas con el nodo de Nitón debido a fallos en la antena receptora ptp.
21/09/2012	10:00	Llamadas de reclamos por parte de los usuarios, debido a problemas del nodo de Palama y a su retraso en la reparación de este el cual fue causado por avería en uno de sus AP principal.
24/09/2012	9:00	Problemas con el nodo de Atahualpa debido a fallos en su router.
24/09/2012	16:00	Problemas en el servicio de internet de un cliente debido a corte en su cable de red en el sector de Techo Propio.
26/09/2012	12:00	Problema con algunos usuarios del nodo de Tropezón debido a la baja velocidad que presenta el servicio de internet.
27/09/2012	18:00	Problemas en el servicio de internet de un cliente debido a avería en su antena en el sector de Letamendi.
01/10/2012	10:00	Problemas con un cliente del nodo de Baños

		debido a que la velocidad en su servicio de internet es baja.
01/10/2012	14:00	Llamadas de reclamos por parte de los usuarios, debido a problemas del nodo de Totoras y a su retraso en la reparación de este el cual fue causado por corte de luz por agotamiento de su batería.
03/10/2012	9:00	Problemas en la red de Speedy debido a intento de ataque de Hacker desde afuera.
04/10/2012	10:00	Problemas en la red de Speedy debido a un corte de energía en la empresa causado por fallo en la red energética de la empresa.
04/10/2012	17:00	Problemas en el servicio de internet con un cliente debido a falla en la tarjeta de red del ordenador del cliente en el sector de Atahualpa.
05/10/2012	11:00	Problemas con el proveedor de servicios de internet de alta capacidad de Speedy debido a fallos en sus sistemas.
05/10/2012	10:00	Corte de servicio en el nodo de Horizonte debido a mantenimiento de la red por parte de la empresa.
08/10/2012	10:00	Corte de servicio en el nodo de Palama debido a mantenimiento de la red por parte de la empresa.
08/10/2012	15:00	Problemas con un cliente en el nodo de Tropezón debido a que la velocidad en su servicio de internet es baja
09/10/2012	10:00	Corte de servicio en el nodo de Niton debido a mantenimiento de la red por parte de la empresa.
10/10/2012	10:00	Corte de servicio en el nodo de Pinllo debido a mantenimiento de la red por parte de la

		empresa.
10/10/2012	17:00	Problemas con los usuarios debido a un problema en el servidor de DNS por parte de la empresa.
12/10/2012	9:00	Problemas en el nodo de Nitón debido a avería en su antena principal.
12/10/2012	15:00	Problemas con el servicio de un cliente debido a cambio de ubicación de la antena echo sin aviso por el usuario en el sector de Macasto.
15/10/2012	9:00	Problemas con un cliente en el Puyo debido a daños en el router del usuario.
16/10/2012	12:00	Llamada de reclamos los usuarios debido a lentitud en la velocidad del servicio de internet en el nodo de Baños.
16/10/2012	17:00	Problemas en el servicio de un cliente debido a conexión eléctrica de la antena en el sector de Pelileo.
18/10/2012	10:00	Problemas con un cliente debido a demora en la instalación del servicio por parte de la empresa en el sector de Picaihua.
18/10/2012	15:00	Problemas con un cliente debido a demora en la reinstalación del servicio por parte de la empresa en el sector de Miñarica.
19/10/2012	9:00	Problemas con el servicio de un cliente debido a robo de la entena del cliente en el sector de Izamba.
22/10/2012	9:00	Problemas en el nodo de totoras debido a corte de energía eléctrica en el nodo.
22/10/2012	12:00	Corte de servicio en el nodo de Salcedo debido a mantenimiento del mismo.
23/10/2012	11:00	Corte de servicio de la red de Speedy debido

		a corte de energía en la empresa programada por la empresa eléctrica Ambato SA.
24/10/2012	10:00	Problemas en el servicio de un cliente debido ha filtrado de agua en la antena del usuario en el sector de Izamba.
24/10/2012	16:00	Problemas en el servicio de un cliente debido a corte en su cable de red en el sector del Pisque.
25/10/2012	10:00	Problemas en el nodo de Pinllo debido a avería en su router.
29/10/2012	9:00	Problemas en el nodo de Baños debido a corte de energía en el nodo, debido a agotamiento en su batería.
29/10/2012	17:00	Problemas en el servicio de un cliente debido a desconfiguración de la antena por parte del usuario en el sector de Pelileo.
30/10/2012	11:00	Problemas en el servicio de un usuario debido a caída y daño en su antena en el sector de Pillaro.
30/10/2012	14:00	Corte de servicio en el nodo de Atahualpa debido a mantenimiento por parte de la empresa
31/10/2012	10:00	Problemas en el servicio de un cliente debido a pérdida de línea de vista debido a una construcción cerca al cliente en el sector de Pinllo.
2/11/2012	10:00	Problemas en el nodo de Nitón debido a robo de una antena sectorial.
5/11/2012	9:00	Problemas en el nodo de Nitón debido a robo de un AP en el mismo.
5/11/2012	17:00	Llamada por reclamo de un cliente debido a velocidad lenta de su servicio de internet en el nodo de Macasto.

6/11/2012	10:00	Problemas en el nodo de Pinllo debido a daño en su ap.
7/11/2012	12:00	Problemas con el servicio de un cliente debido a desconfiguración en la tarjeta de red del ordenador del cliente en el sector de Ingahurco.

Elaborado por: Investigador

4.2. Análisis e Interpretación

En base a la tabla 4.1 se puede realizar el siguiente análisis:

Una vez realizado el promedio de 50 observaciones en la red de la empresa Speedy se puede decir que la red no está libre de problemas y daños en su óptimo funcionamiento ya sea por inconvenientes causados por los equipos, la naturaleza, la empresa, robos, o los mismos usuarios del servicio de internet, dando como resultado lo siguiente:

El 70% de daños en la red de la empresa es causado por motivos de averías en los dispositivos de red debido a causas naturales.

El 20% de los daños es causado por los usuarios debido a su imprudencia y desconocimiento con respecto a los dispositivos y cuidado de los mismos.

Un 5% de los daños es por motivo de corte por parte de las empresas proveedoras de servicio internacionales que brindan su servicio a la empresa Speedy.

Un 5% es debido a corte de servicio de energía eléctrica debido a cortes programados por la empresa eléctrica o por cortes en los nodos por agotamiento de sus baterías.

Con respecto a los nodos se puede decir que, el nodo de Horizonte es el que tiene más problemas con su velocidad de internet por causa de saturación en los enlaces y por la interferencia en la frecuencia.

Se debe tener mucho cuidado en especial en el nodo de Nitón debido a los robos de los equipos causados últimamente, y en el resto de nodos debido a daños en sus sistemas y al agotamiento de las baterías que brindan electricidad a los nodos.

Por estos y otros motivos que se pueden presentar, la empresa al no contar con un monitoreo constantemente en su red para localizar de una manera más inmediata las averías causadas en la red, depende parcialmente de las llamadas de reclamos de sus usuarios para darse cuenta de estos problemas, demorando así su reparación, los mismos que causa un malestar y desconformidad en sus usuarios con el servicio.

Capítulo V
Conclusiones y Recomendaciones

5.1. Conclusiones

En base al estudio realizado y los resultados obtenidos se puede concluir lo siguiente:

1. Existen varias razones inevitables por las cuales la red se pude caer o averiar y suspender su correcto funcionamiento, ya sea por causas naturales o por culpa de intervención humana.
2. Algunos de los daños en la red de los usuarios es causado por desconocimiento e irresponsabilidad de los mismos.
3. Se tiene daños que son causados por el corte de energía eléctrica en los nodos debido al agotamiento es sus baterías de abastecimiento.
4. Hay una demora considerable en la detección y reparación en las averías causadas en la red, causando molestias y desconformidad en los usuarios.

5.2. Recomendaciones

1. Se recomienda estar al tanto de los motivos por el cual la red se puede averiar, en especial con la naturaleza, para un control y mejor administración de la misma.
2. Se recomienda dar una mejor explicación y advertencias a los usuarios del servicio, sobre el manejo, cuidado y conexiones los equipos al momento de la instalación para así no tener problemas futuros causados por estos.

3. Se recomienda llevar un cronograma de duración de las baterías de abastecimiento de energía de los nodos para así no tener el problema de que los nodos se queden sin energía y dejen de funcionar.
4. Se recomienda implementar una herramienta de administración y Monitoreo para el mejoramiento del funcionamiento de la red en SPEEDY COM CIA LTDA.

Capítulo VI
Propuesta

Tema: Herramienta opensource de administración y Monitoreo basado en snmp para el mejoramiento del funcionamiento de la red en SPEEDY COM CIA LTDA.

6.1. Datos Informativos

6.1.1. Institución Ejecutora

Universidad Técnica de Ambato. Facultad de Ingeniería en Sistemas, Electrónica e Industrial.
Nombre de la institución: "SPEEDYCOM CIA LTDA"
Tipo de organización: Privada
Departamento: Redes

6.1.2. Beneficiarios

Los beneficios de esta propuesta son:
* "SPEEDYCOM CIA LTDA"
* Trabajadores
* Y clientes de SPEEDYCOM CIA LTDA

6.1.3. Ubicación

Provincia: Tungurahua
Cantón: Ambato
Dirección: Víctor Hugo Y Av. Atahualpa junto a Talleres de Andinamotors

6.1.4. Tiempo Estimado Para La Ejecución

Inicio: julio 2012
Fin: Enero 2013

6.1.5. Equipo responsable

Investigador: José Iván Freire Bonilla
Tutor: Ing. Marco Jurado
Entidad: Universidad Técnica de Ambato (FISEI)

6.2. Antecedentes de la Propuesta

Luego de la investigación realizada, se comprobó que la empresa Speedycom CIA LTDA requiere que se implemente la Herramienta opensource de administración y Monitoreo basado en snmp para una mejor administración y monitoreo de su red, ya que la falta de este genera pérdidas en el servicio y disgusto en sus usuarios.

Actualmente la empresa no cuenta con una Herramienta de administración y monitoreo de red, lo cual implica que al momento que ocurre daños en la red los técnicos de Speedy demoren en identificar cual es la falla en la red causando molestias y pérdidas para la empresa.

Es así que con la observación y análisis realizado se notó que se puede mejorar la administración y monitoreo de la red de Speedy con la implementación de una

Herramienta opensource, y de esa manera satisfacer a las necesidades de la empresa.

6.3. Justificación

El constante desarrollo de las redes de comunicaciones y sus servicios hace que sea necesaria la implementación de una herramienta que ayude con la constante administración y monitoreo de la red ayudando así a su control y correcto funcionamiento en todas sus aplicaciones y servicios.

Con un constante monitoreo y administración de la red de Speedy se logrará mejorar el control de la red y en la de todos sus usuarios además de un aumento en la calidad de su servicio.

Uno de los principales beneficios del presente proyecto se enfoca en brindar una mejor atención y servicio a sus usuarios que son el eje principal de la empresa y así estos puedan seguir gozando de sus aplicaciones y servicios.

Otro de los beneficios de la propuesta es la ventaja con la que cuenta la propuesta es su acceso remoto que facilita a los encargados de la red acceder a los datos desde cualquier lugar reduciendo tiempo en la detección de errores y de la misma manera agilitando la resolución del problema, ganado así la empresa y los usuarios que cuentan con este servicio.

El poder monitorear y administrar la red de una manera constante da oportunidad de controlar de una manera adecuada los servicios que brinda la red, así como también nos permite observar el funcionamiento de la misma, permitiendo así una inmediata reparación al momento en que algún elemento comience a presentar fallos en la red.

6.4. Objetivos

6.4.1. Objetivo general

- Implantar una Herramienta opensource de administración y Monitoreo basado en snmp para el mejoramiento del funcionamiento de la red SPEEDY COM CIA LTDA.

6.4.2. Objetivos específicos

- Analizar las Herramientas OpenSource de Administración y Monitoreo de Redes basadas en SNMP, que permita resolver las necesidades de la empresa Speedycom CIA LTDA.

- Implantar la herramienta seleccionada para realizar la Administración y Monitoreo de la red de la empresa SPEEDY COM CIA LTDA.

- Comprobar el correcto funcionamiento de la herramienta seleccionada para la administración y monitoreo de red de la empresa SPEEDY COM CIA LTDA

6.5. Análisis de Factibilidad

6.5.1. Factibilidad Técnica

La implantación de una Herramientas OpenSource de Administración y Monitoreo de Redes basadas en SNMP, permitirá realizar esta tarea con una mayor precisión de tal forma que la calidad del servició mejorar sustancialmente.

El presente proyecto es técnicamente factible puesto que se utilizara tecnología de última generación que se lo puede obtener en el mercado Nacional, la cual cuenta con varias aplicaciones a su disposición aumentando su eficiencia y funcionamiento, además cuenta con altos niveles de seguridad para garantizar la integridad de los datos. Además será un sistema que se integrara fácilmente a las nuevas tecnologías permitiendo mejorar sus aplicaciones.

6.5.2. Factibilidad Económica

El proyecto es factible económicamente ya que la Herramienta al ser del tipo software libre se lo puede obtener de manera gratuita y la empresa cuenta con los recursos necesarios para la adquisición de hardware necesario para la implementación del miso.

6.5.3. Factibilidad Operativa

Desde el punto de vista operativo la propuesta es factible debido a que SppedyCom cuenta con una infraestructura física adecuada, además quienes conforman la empresa están de acuerdo y muy conscientes de que se va a mejorar el rendimiento de la red con la implementación de una herramienta para la adecuada administración y monitoreo de la misma.

6.5.4. Factibilidad Científica

El proyecto es factible científicamente ya que existe una cantidad considerable de información del mismo, además de foros y grupos en internet para su correcta implementación y uso.

6.6. Fundamentación

6.6.1. Análisis de la infraestructura actual de la red de la empresa proveedora de internet SPEEDY COM CIA LTDA.

SPEEDY COM cuenta con 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 soporte técnico; ante esta situación y por la necesidad de detectar caídas de servicios que se tornan vitales, para la empresa 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 solución.

En la figura 6.1 se muestra de manera simple la infraestructura actual de networking de SPEEDYCOM:

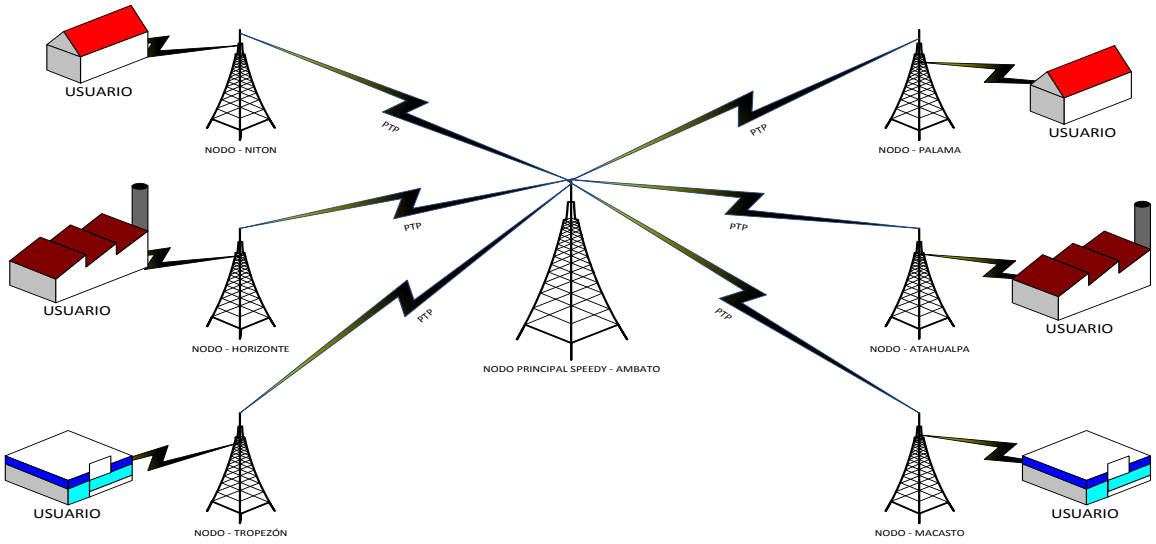


Figura 6.1: Infraestructura actual de networking SPEEDY

Elaborado por: Departamento de soporte técnico Speedy

La red de SPEEDY actualmente está conformada por un nodo principal que se encuentra ubicado en la sede de la empresa, que mediante un enlace punto a punto se distribuye desde la red principal a varios nodos ubicados en sectores específicos de la ciudad de Ambato como lo son: Nitón, Horizontes, Tropezón, Palama, Atahualpa y Macasto, los cuales cada nodo cuenta con un respectivo número de aps para así poder brindar de manera inalámbrica servicio de internet a los usuarios de lugares aledaños a los mismos.

La red al no tener un sistema que ayude con el monitoreo y administración de la misma, a veces crea algunas deficiencias en su óptimo y normal funcionamiento, causando así molestias y desconformidad en los usuarios.

6.6.2. Análisis comparativo de herramientas opensource para la Administración y Monitoreo de red basado en snmp.

En la tabla 6.1 se indica un análisis comparativo entre las herramientas de administración y monitoreo de redes: Cacti, Zenoss y Zabbix, para analizar cuál de

estas herramientas es la que mejor cumpla y se adapte con las necesidades que requiere la empresa.

Los criterios a considerarse son los siguientes:

Tabla 6.1: Parámetros de comparación

Parámetro	**Definición**
Usabilidad	Facilidad de instalación, configuración, implementación y uso
Gestión de Usuario	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	Posibilidad de colectar continuamente información y reportarla en tiempo real.
Soporte	Soporte en línea a través de blogs, foros, comunidades.
Reportes	Forma de presentar los datos obtenidos en el monitoreo para su análisis y 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.
Auto descubrimiento de	Descubrir computadores y componentes en la

dispositivos	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.

Fuente: Investigador, tomado como referencias los siguientes trabajos de investigación: http://www.info.unlp.edu.ar/uploads/docs/presentacion_testing.pdf, http://www.willydev.net/InsiteCreation/v1.0/WillyCrawler/2008.05.12.Articulo.Comparacion%20Bases%20de%20Datos%20Open%20y%20propietarias.pdf, http://churriwifi.wordpress.com/2009/12/29/11-herramientas-etl-%C2%BFque-son-para-que-valen-productos-mas-conocidos-etl%C2%B4s-open-source/

6.6.2.1. Pruebas con la herramienta de Administración y Monitoreo 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.

Para poder probar CACTI, se inicia con la instalación del mismo en el servidor.

Una vez instalado se abre un navegador web y se digita la siguiente dirección: http://localhost/cacti.

Seguido aparecerá una interfaz como se muestra en la figura 6.2:

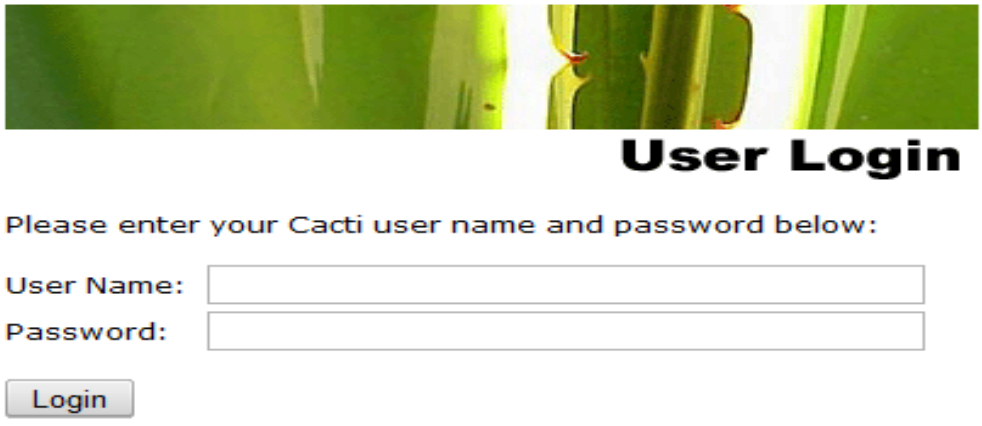


Figura 6.2: Login de Usuario Cacti

Elaborado por: Investigador

Para poder ingresar y empezar a utilizar cacti, se debe ingresar el nombre de usuario que por defecto es admin y su contraseña por defecto igual es admin, la cual se puede editar para mayor seguridad.

En la figura 6.3 se muestra la interfaz de gestión de Cacti y todos sus servicios que puede prestar:

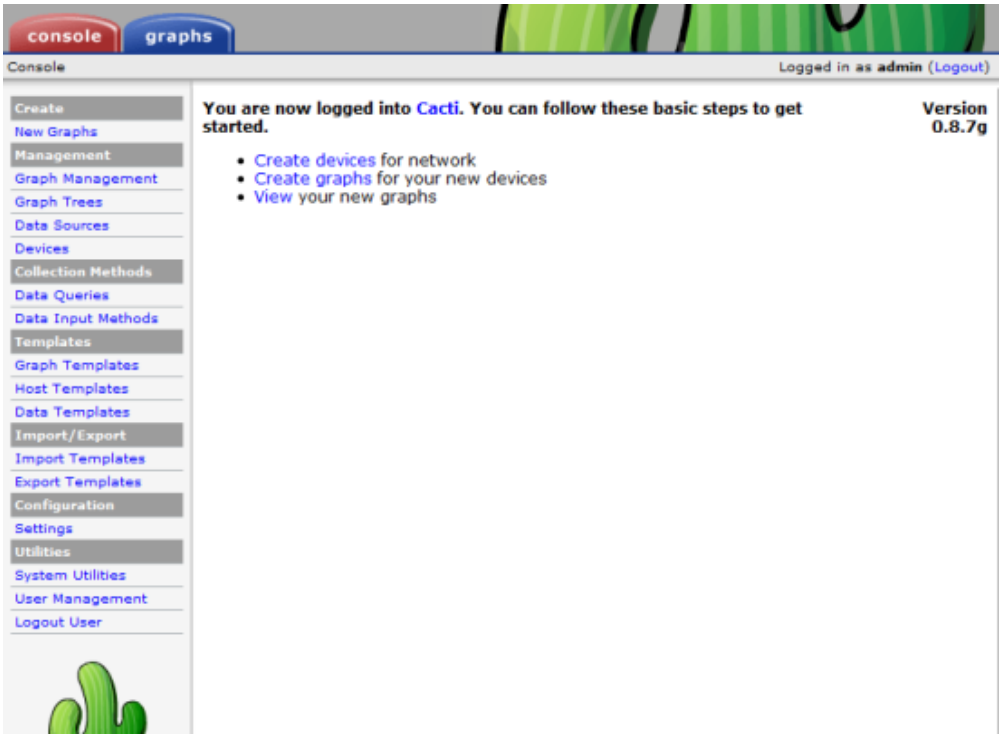


Figura 6.3: Interfaz de gestión Cacti

Elaborado por: Investigador

En la figura 6.4 se puede observar en esta pestaña todos los dispositivos que están siendo objeto de monitoreo en el cual tenemos 8 dispositivos ingresados para su monitoreo.

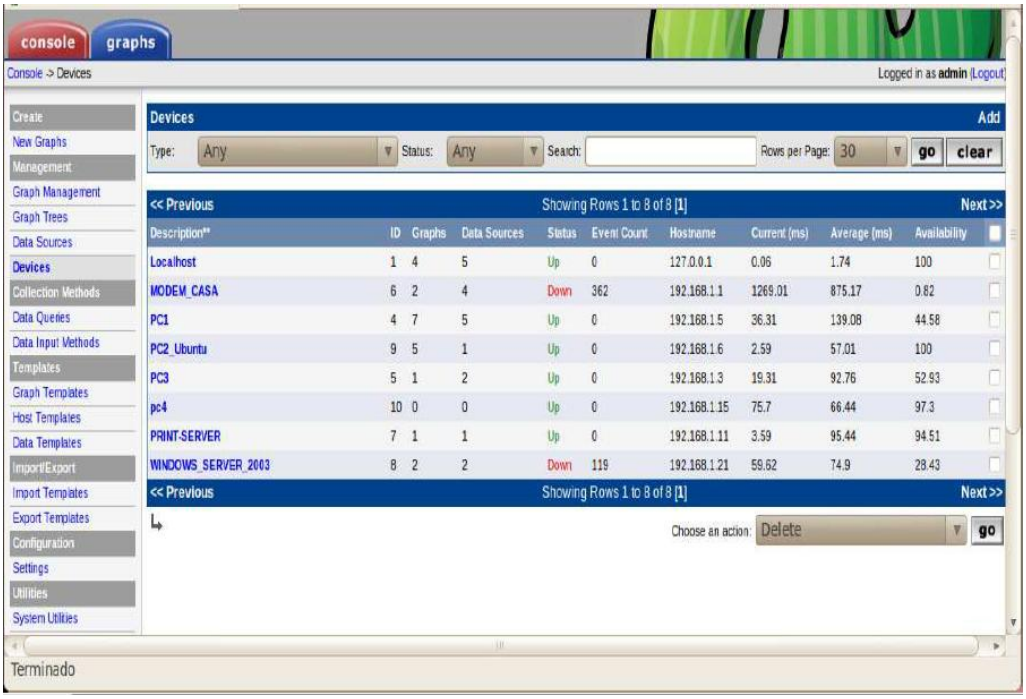


Figura 6.4: Dispositivos Monitoreados Cacti

Elaborado por: Investigador

Para crear los gráficos hacer click en la pestaña Create Graphs for this Host, en donde se podrá indicar qué gráficas se desea generar como se puede observar en la figura 6.5.

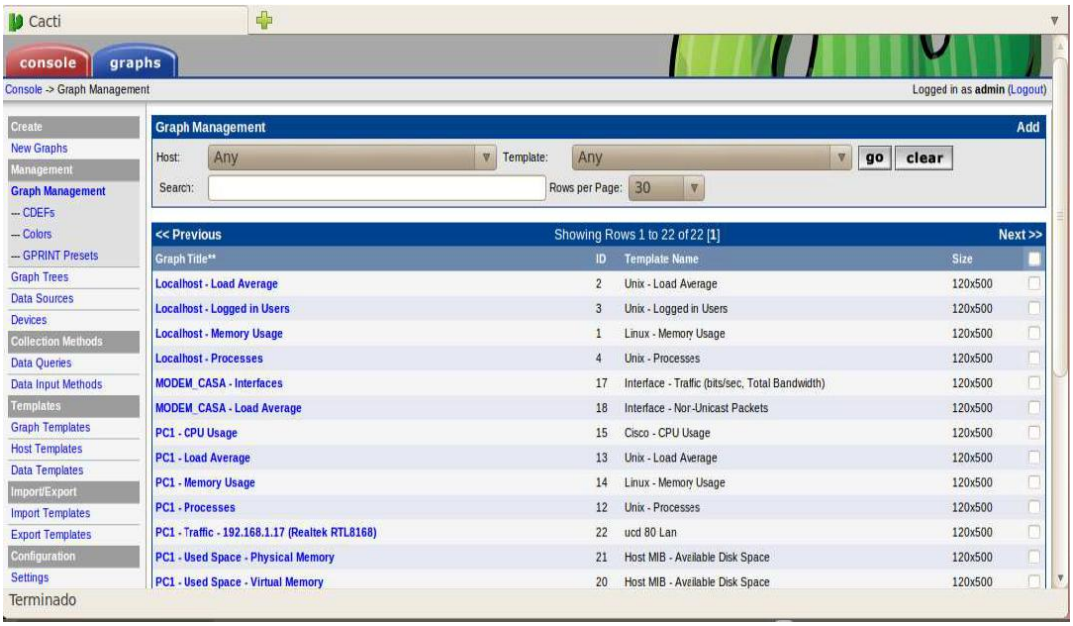


Figura 6.5: Añadiendo gráficos Cacti

Elaborado por: Investigador

Para visualizar las gráficas, se ubica bajo: Graph >> Default Tree, en donde se podrá escoger el equipo que se desea visualizar las Gráficas. Obteniendo resultados como se puede observar en la figura 6.6:

Figura 6.6: Default Tree Cacti
Elaborado por: Investigador

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

En la figura 6.7 se muestra el uso de memoria en Pc1 con sistema operativo Windows en donde cacti muestra los parámetros con sus siglas en ingles free y swap para así poder visualizar de mejor manera el uso del cpu.

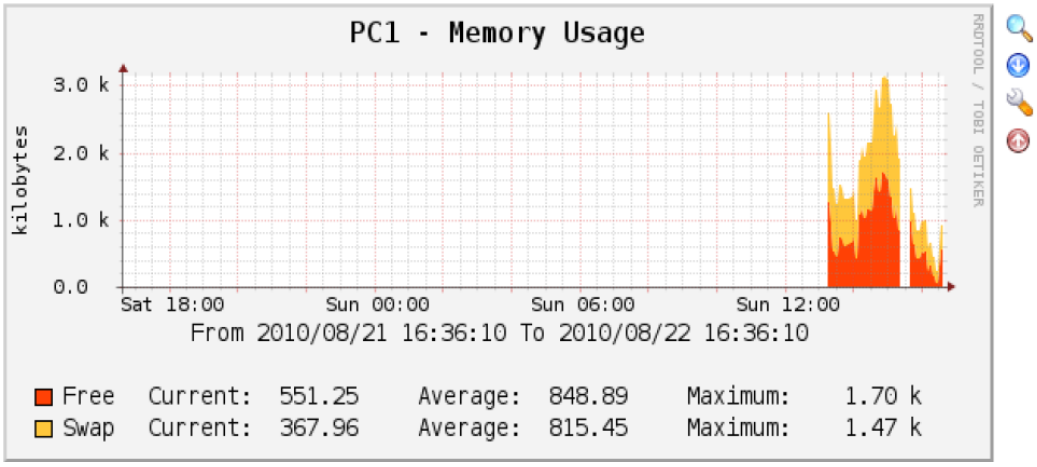


Figura 6.7: Pc1 Windows memoria usada Cacti

Elaborado por: Investigador

En la figura 6.8 se muestra el tráfico de la interfaz en Pc1 con sistema operativo Windows en el cual cacti muestra el tráfico de entrada y salida con sus siglas en ingles Inbound y Outbound respectivamente.

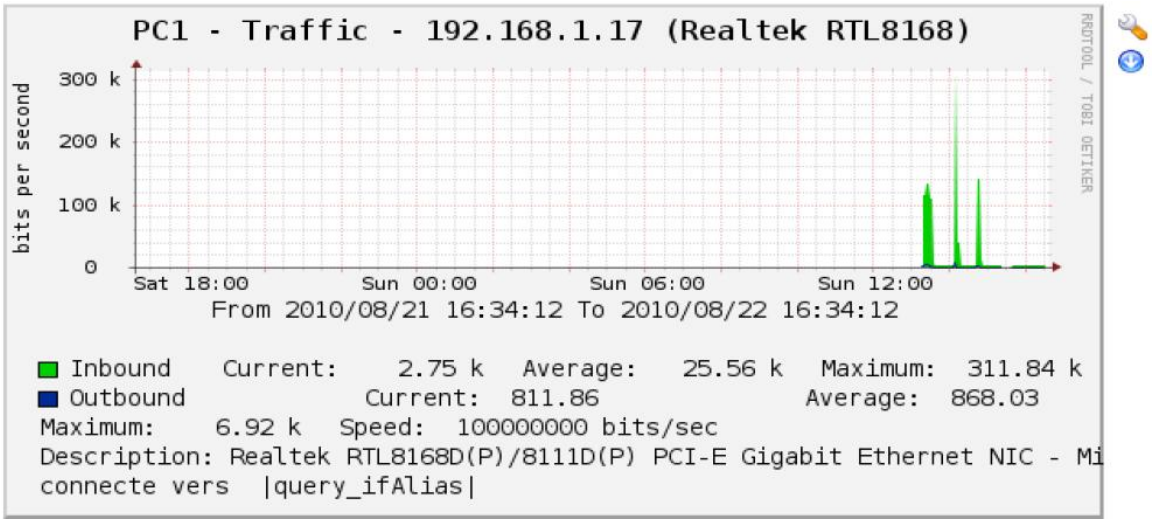


Figura 6.8: Pc1 Windows Tráfico de la interfaz Cacti

Elaborado por: Investigador

También se muestra las gráficas del dispositivo con Linux, permitiendo hacer filtros de fechas.

En la figura 6.9 se muestra es uso de CPU en Pc2 con sistema operativo Ubuntu en donde cacti brinda un gran número de parámetros como lo son con sus siglas en inglés: System, User, Nice, Total, facilitando así un monitoreo más óptimo sobre el uso del cpu

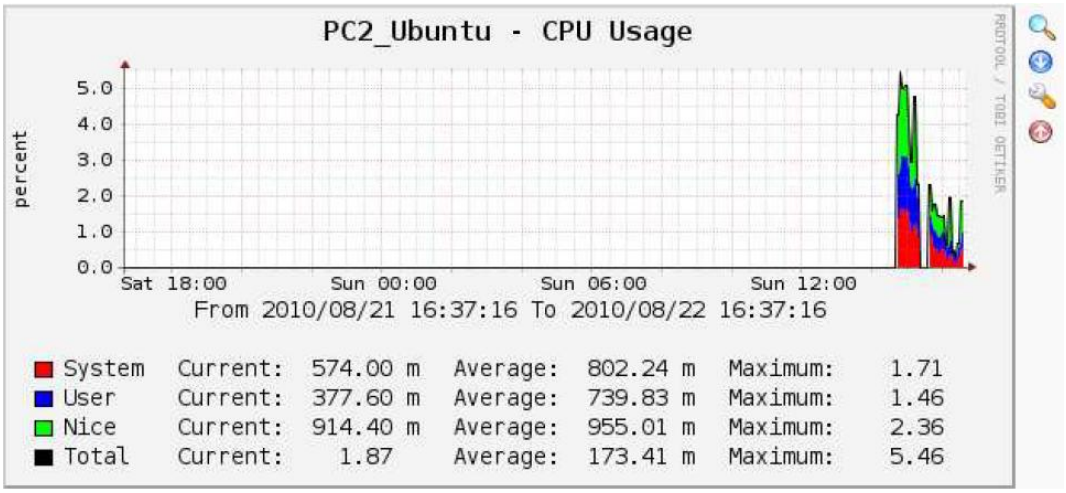


Figura 6.9: Pc2 Ubuntu uso de CPU Cacti

Elaborado por: Investigador

En la figura 6.10 se muestra es uso de Memoria en Pc2 con sistema operativo Ubuntu en donde se muestra el valor de memoria libre, memoria de buffers y memoria cache, para una mejor uso y administración de estas.

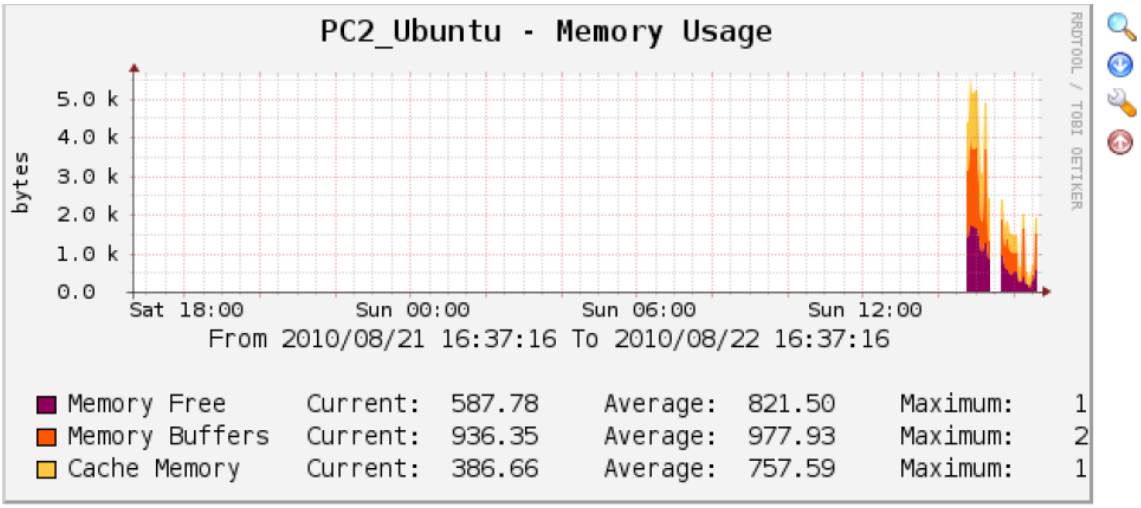


Figura 6.10: Pc2 Ubuntu uso de Memoria Cacti

Elaborado por: Investigador

6.6.2.2. Pruebas con la herramienta de Administración y Monitoreo 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.

Una vez instalado zenoss se abre un navegador web: http://localhost/Zenoss
Se tendrá una interfaz como se muestra en la figura 6.11:

Figura 6.11: Login de Usuario Zenoss

Elaborado por: Investigador

Para poder ingresar y empezar a utilizar zenoss, se debe ingresar el nombre de usuario que por defecto es admin y no tiene ninguna contraseña, la cual se puede editar para mayor seguridad.

En la figura 6.12 se muestra la interfaz principal de Zenoss, conocida como dashboard, en la cual se puede observar varios enlaces como recursos y ayuda para facilitar la utilización de esta herramienta.

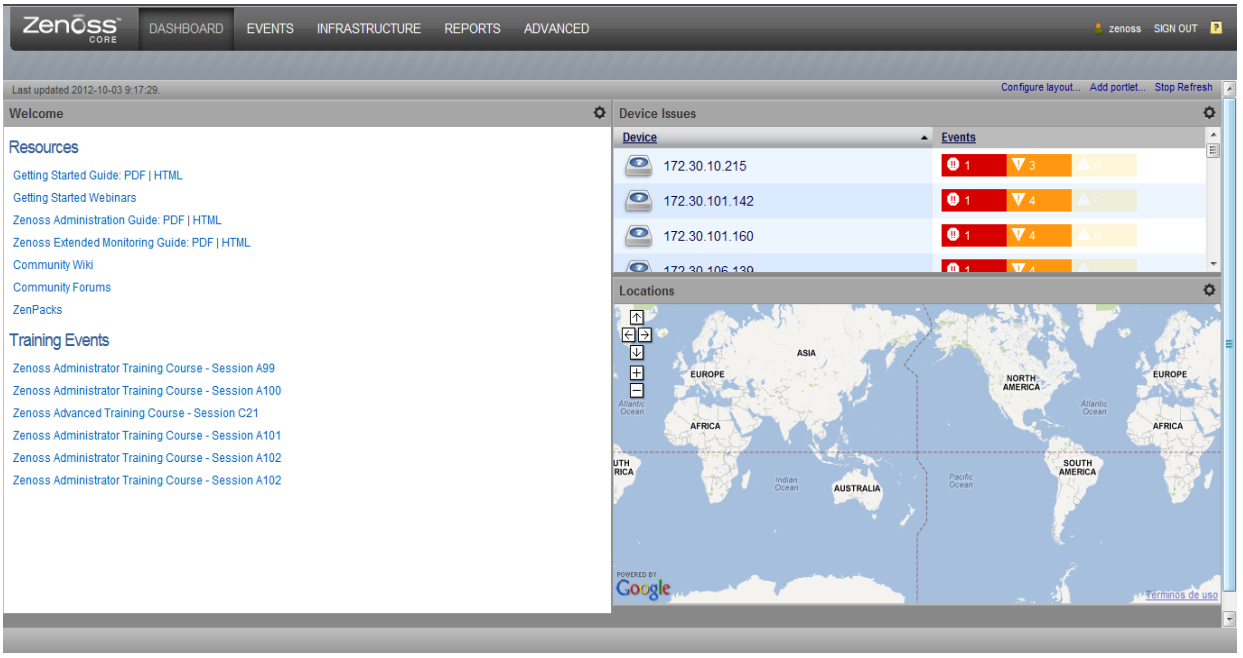


Figura 6.12: Dashboard Zenoss

Elaborado por: 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, se puede observar que existe una distribución de los dispositivos dependiendo de la clase a la que pertenecen, y algunas pestañas para la navegación, como se muestra en la figura 6.13:

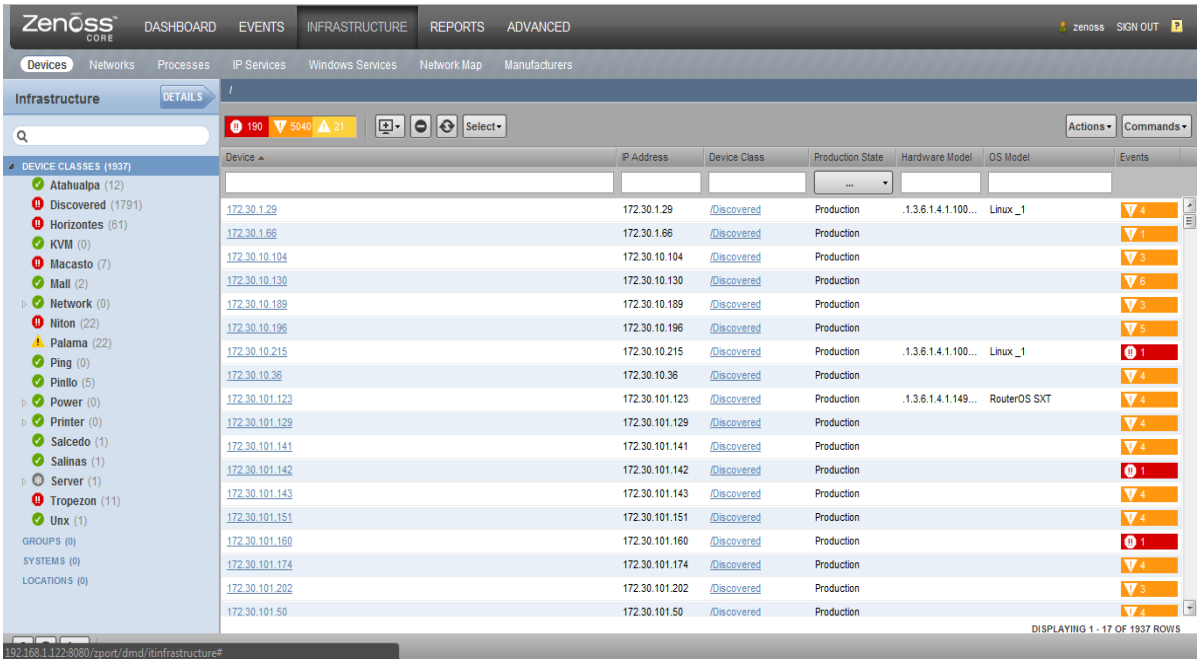


Figura 6.13: Categorización de dispositivos Zenoss

Elaborado por: 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 como se muestra en la figura 6.14.

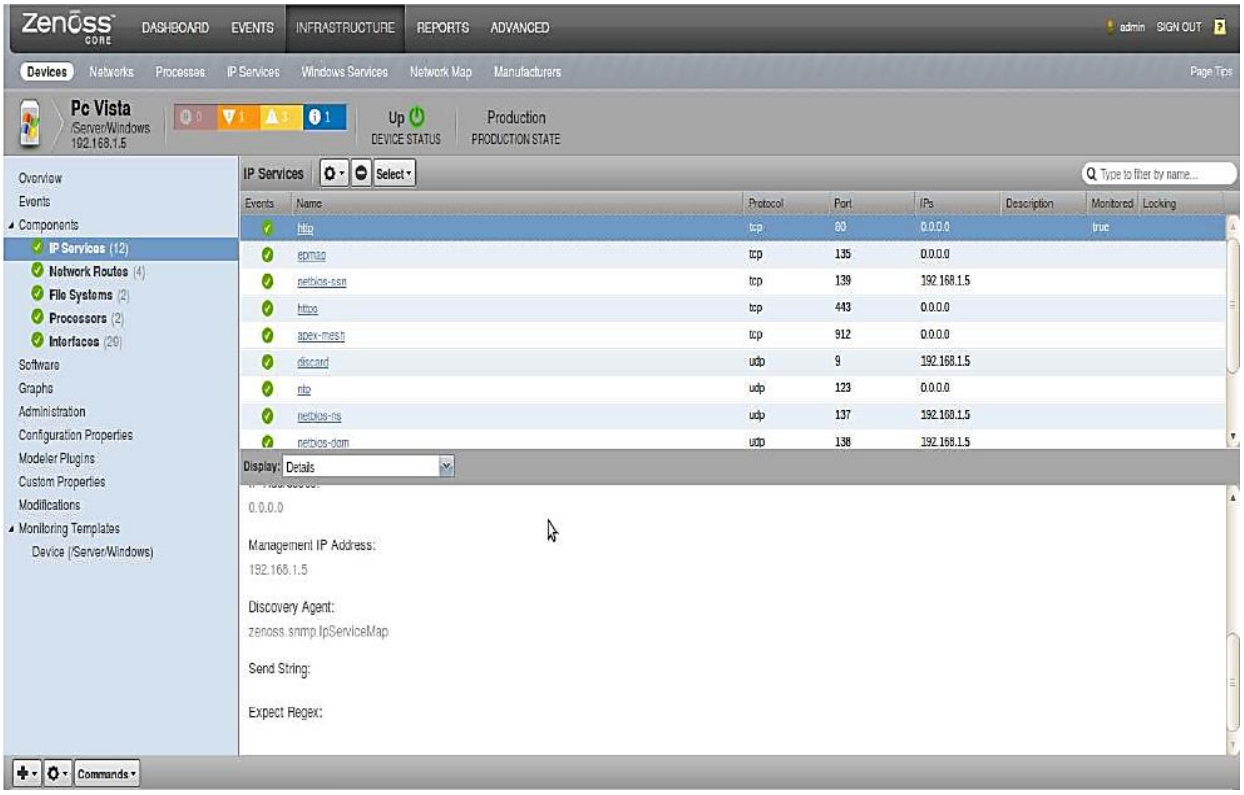


Figura 6.14: IP service Zenoss

Elaborado por: Investigador

En la figura 6.15 se muestra los dispositivos Network routers por los que tiene que pasar pc Windows, los cuales en este caso muestra las ips por las que tiene que pasar el dispositivo:

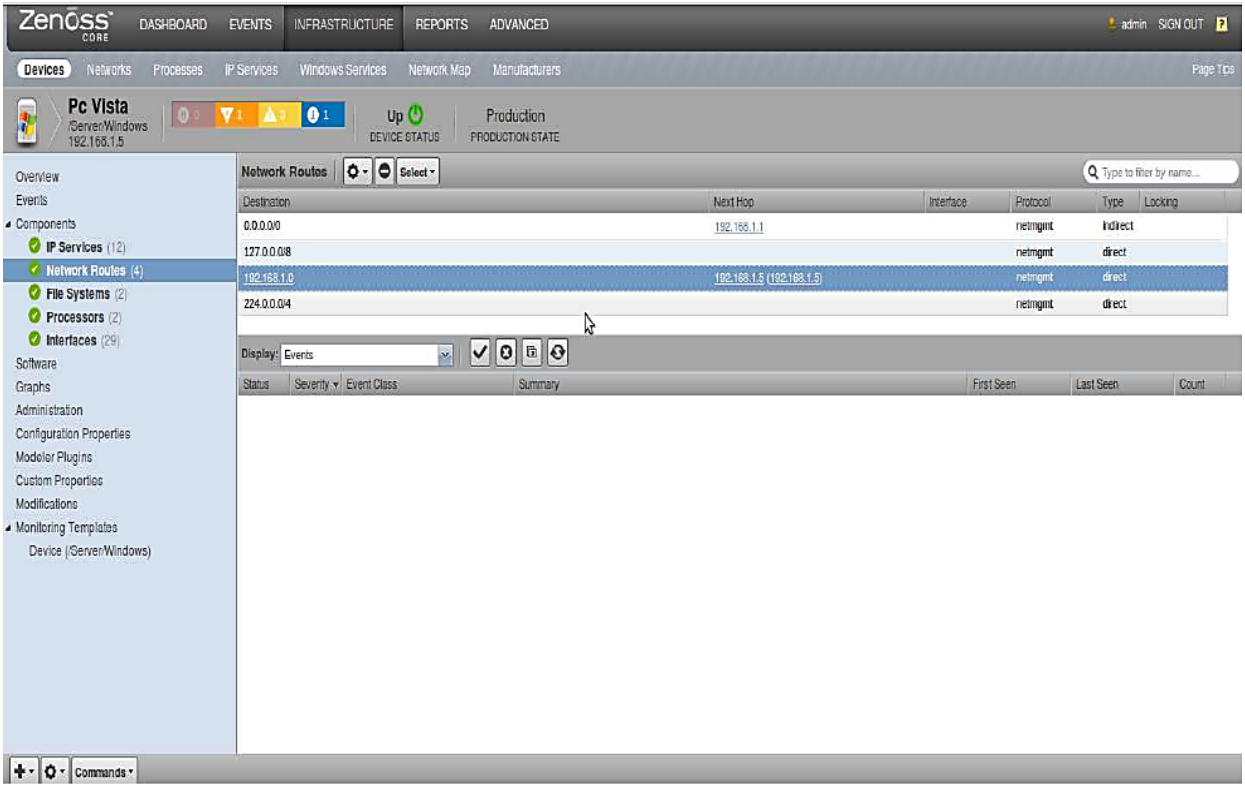


Figura 6.15: Network Routers Zenoss

Elaborado por: Investigador

En la figura 6.16 se muestra la opción file systems donde se puede observar el número de discos o las particiones que se tiene en el dispositivo, además muestra una gráfica de la utilización de los mismos.

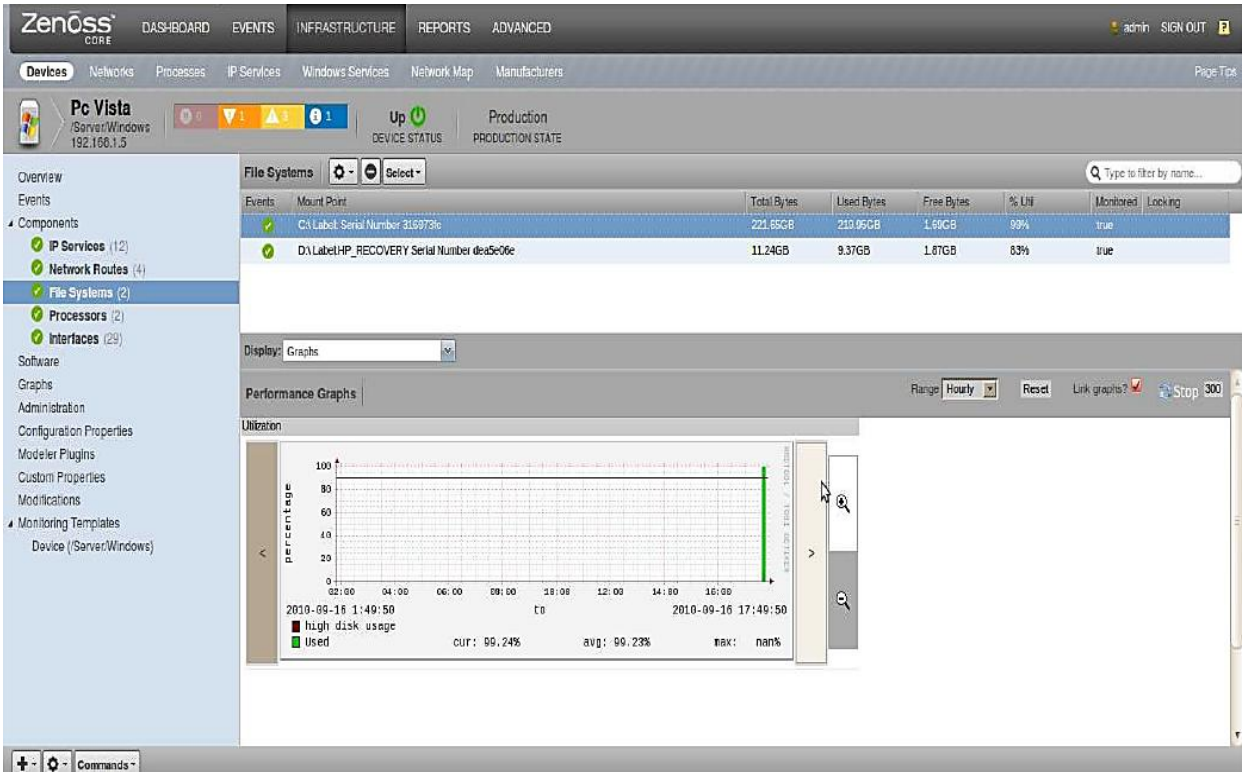


Figura 6.16: File System Zenoss

Elaborado por: Investigador

En la figura 6.17 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 gráficas de throughput, paquetes y errores que se producen, de todas y cada una de las interfaces.

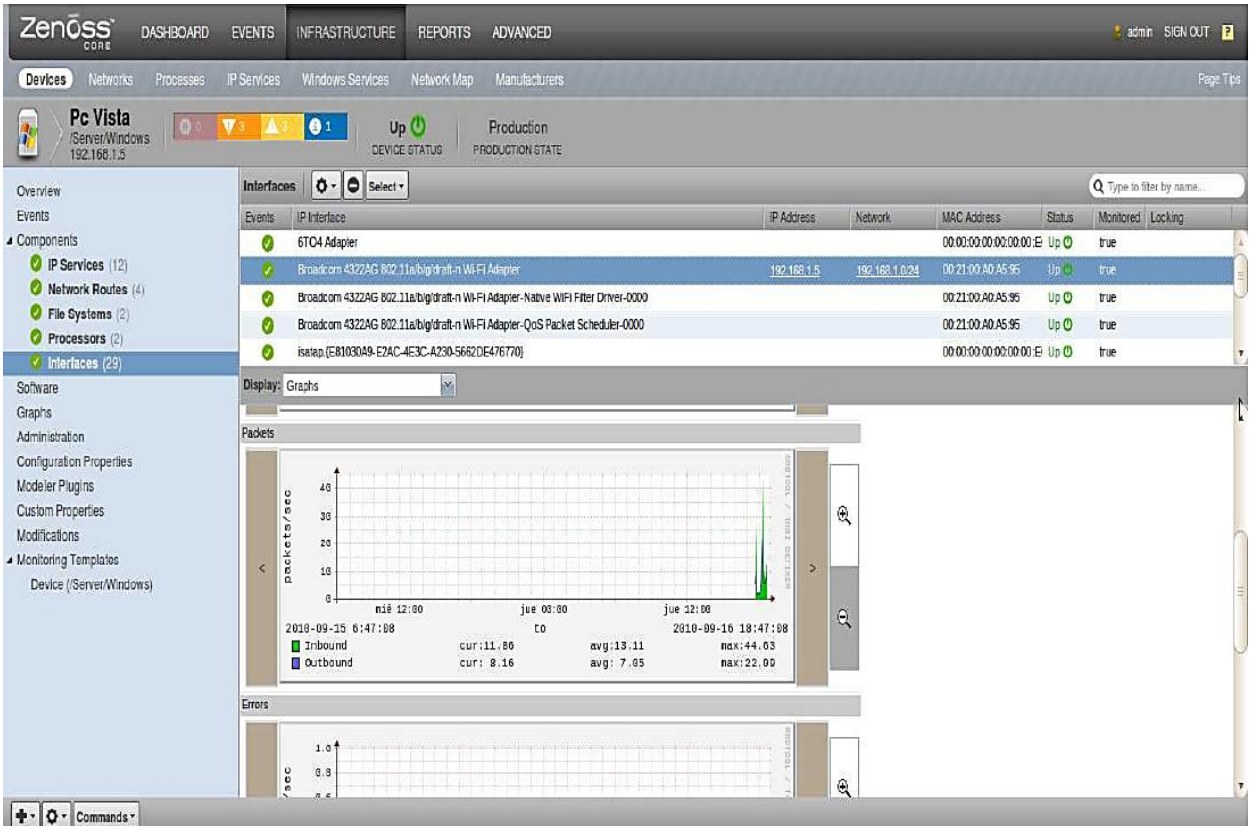


Figura 6.17: Interfaces Zenoss

Elaborado por: Investigador

En la opción software se muestra todos los software que tiene instalados el dispositivo, incluyendo las actualizaciones de Sistema operativo, este componente solamente se activa en PC con Windows como se puede observar en la figura 6.18.

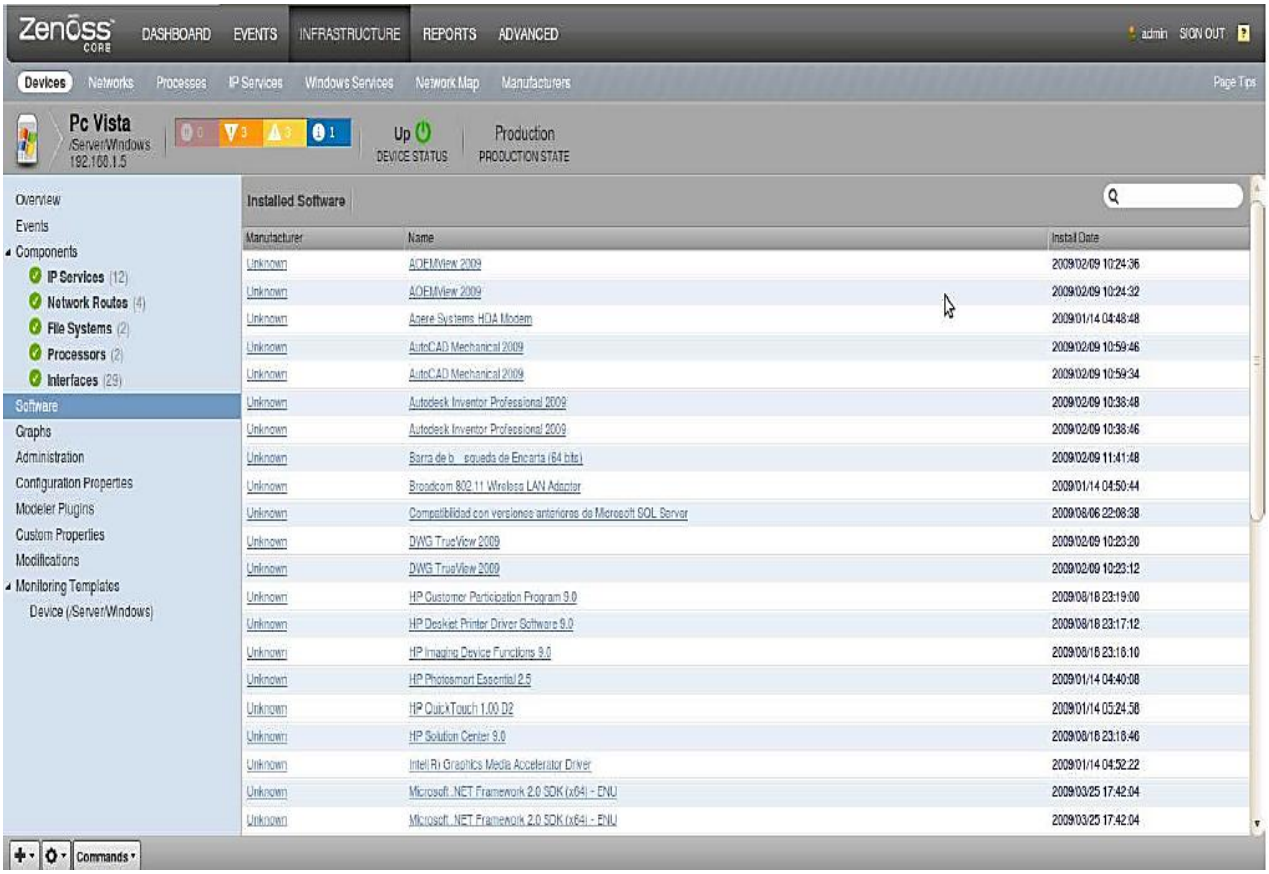


Figura 6.18: Software Zenoss

Elaborado por: 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) como se muestra en la figura 6.19.

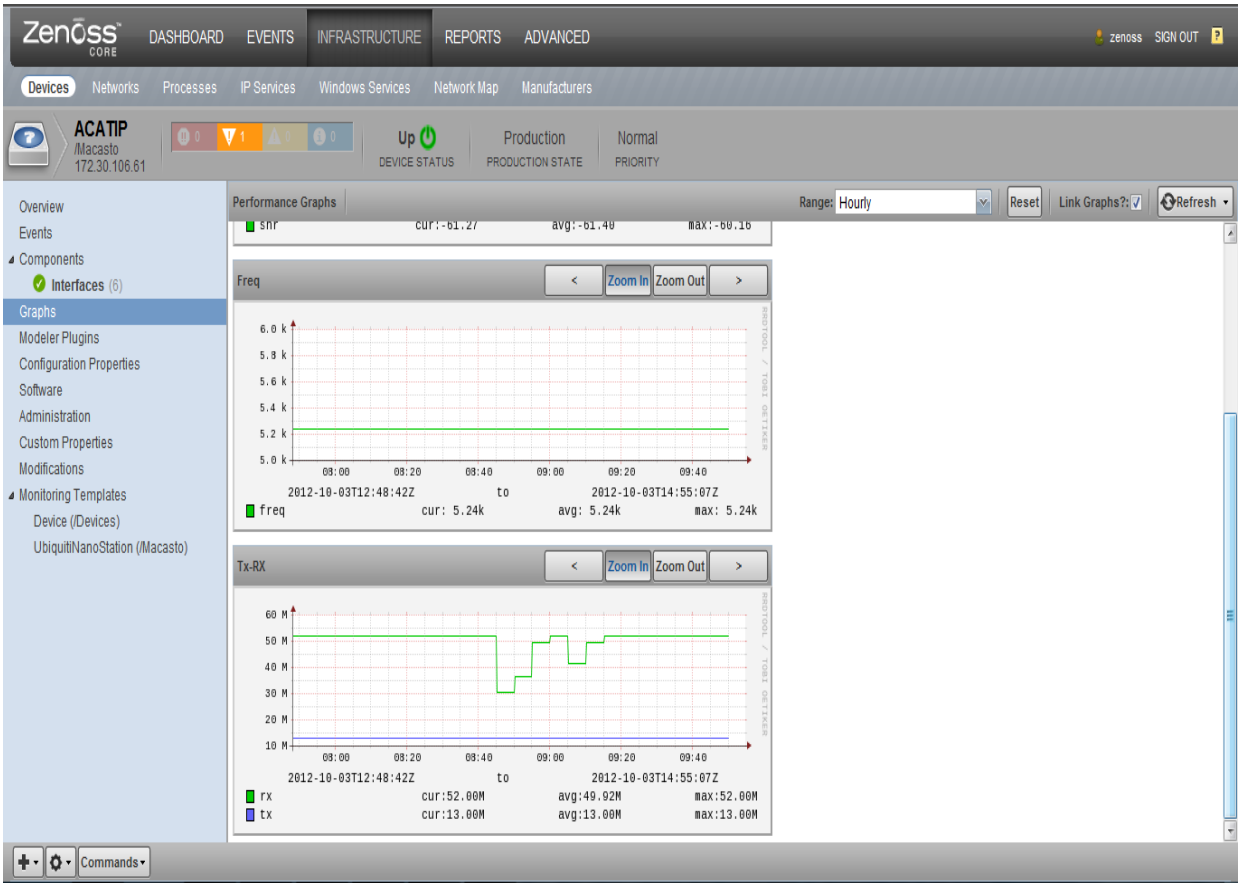


Figura 6.19: Graphs Zenoss

Elaborado por: Investigador

Además se puede correr algunos comandos desde el dispositivo, como ping, snmpwalk, etc, dependiendo de cuales se requiera como se muestra en la figura 6.20.

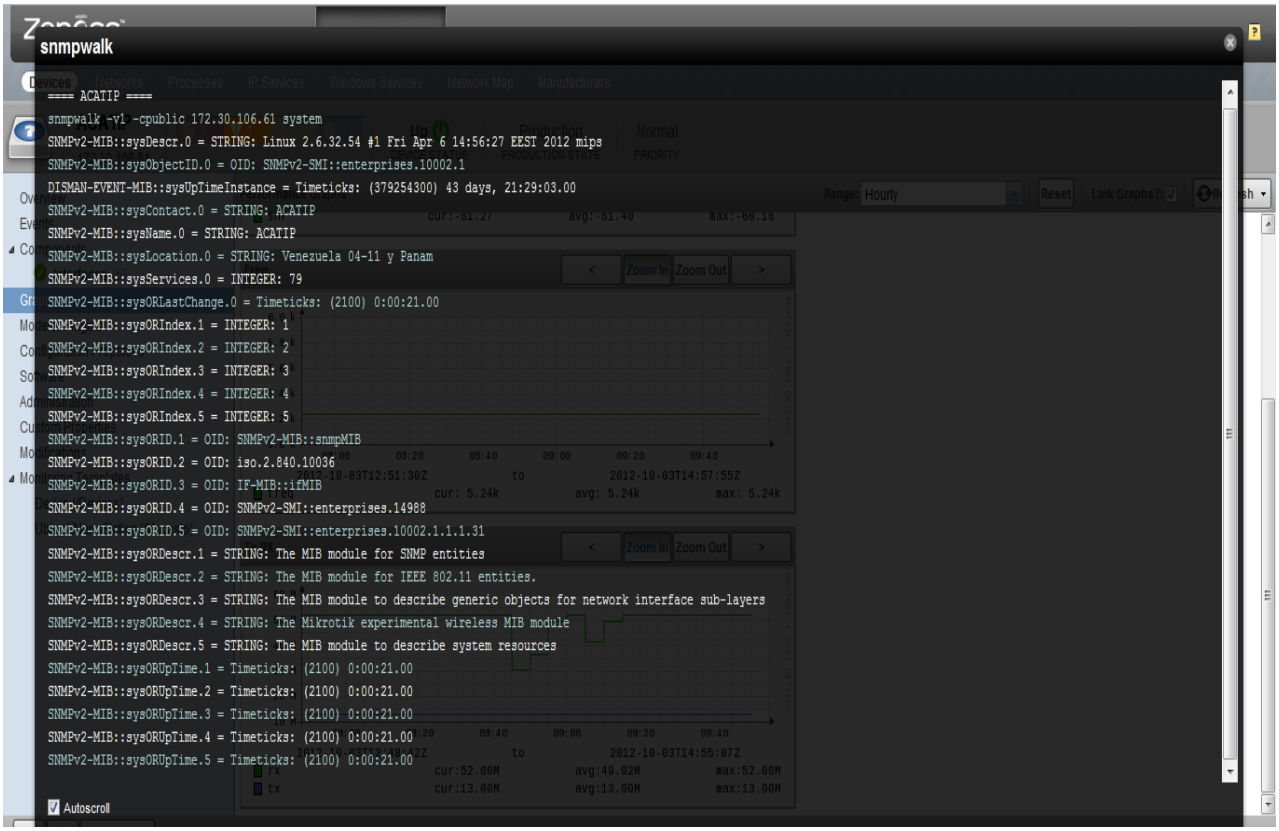


Figura 6.20: Ejecución Comandos Zenoss

Elaborado por: Investigador

Si bien es cierto, una de las características más llamativas e intuitiva con la que cuenta la herrameinta zenoss es el Network Map, que muestra la infraestructura de los dispositivos añadidos a la herramienta, clasificándolos de acuerdo a su clase como se muestra en la figura 6.21.

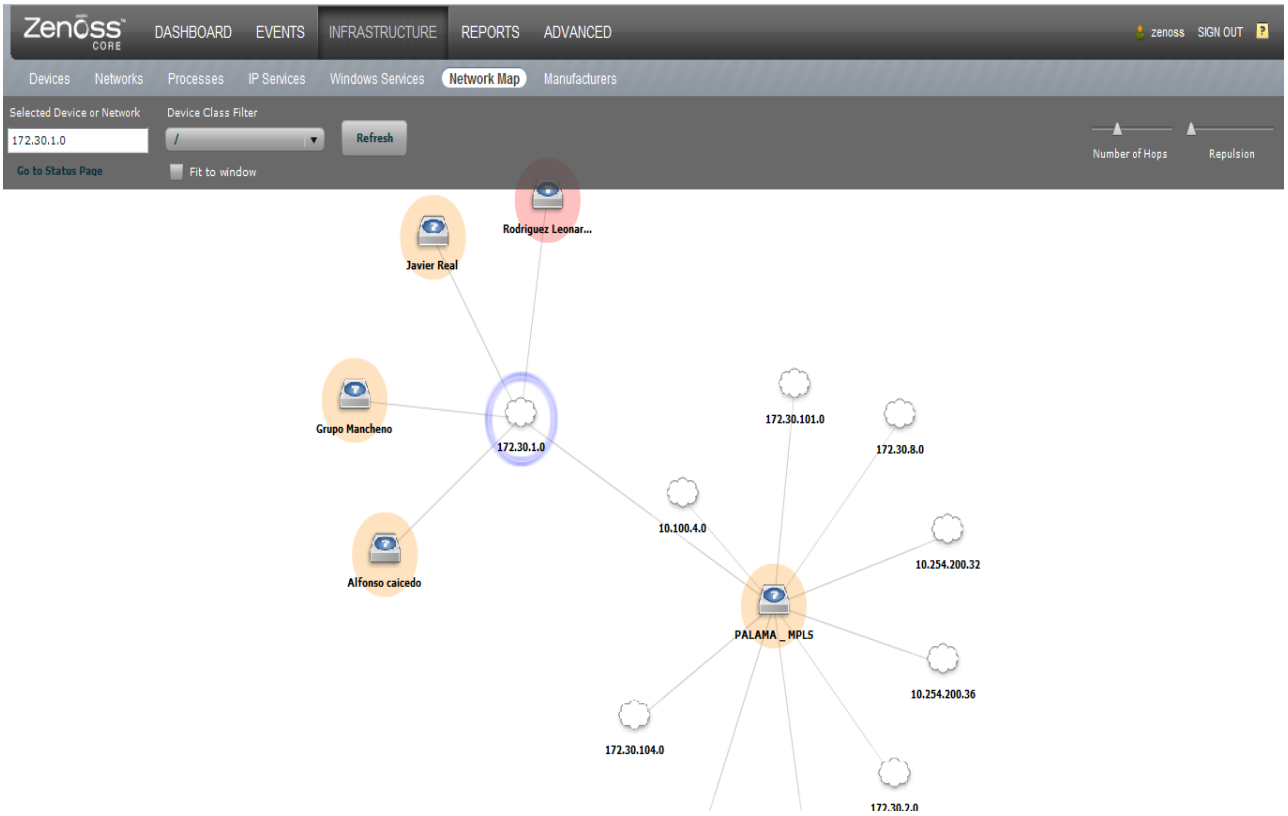


Figura 6.21: Network Maps Zenoss

Elaborado por: Investigador

En la pestaña events se muestra los eventos actuales que están ocurriendo en los distintos dispositivos, siendo estos, si el estado es crítico, warning, error, etc, además también brinda un historial de todos los eventos como se muestra en la figura 6.22.

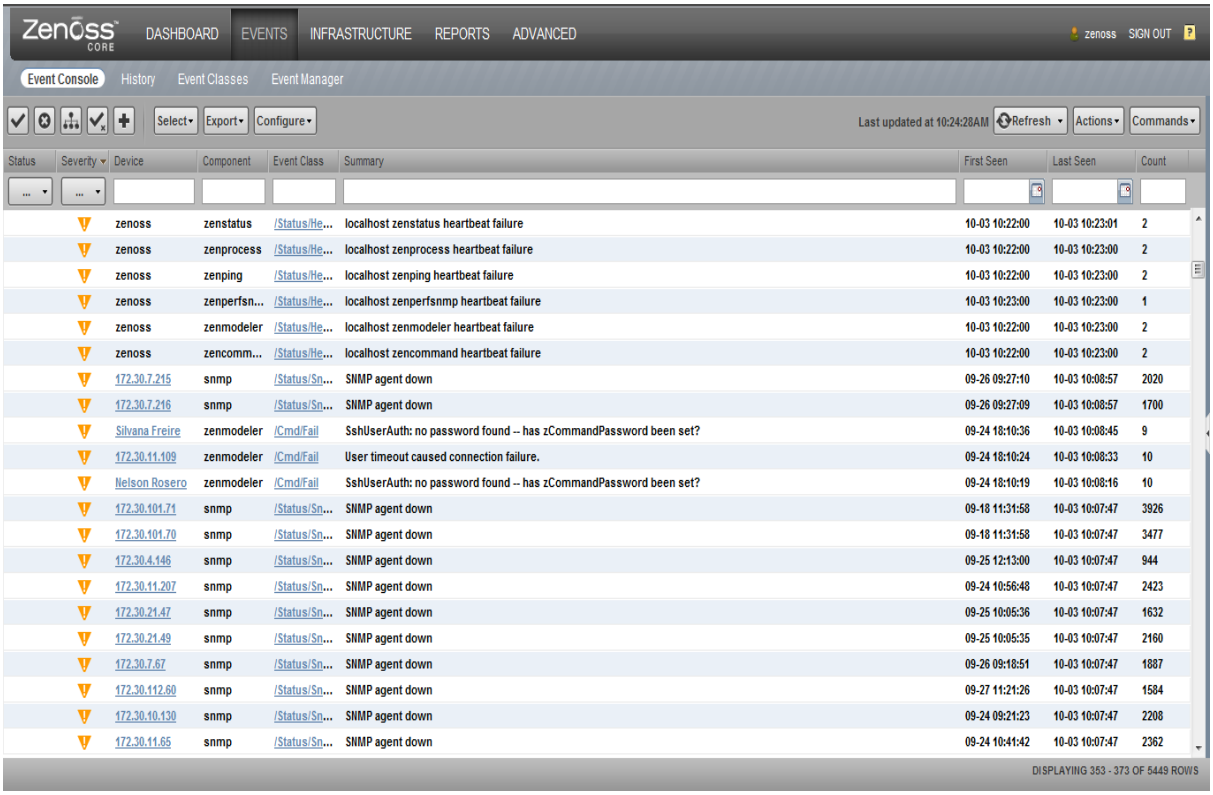


Figura 6.22: Historial de eventos Zenoss

Elaborado por: Investigador

En la figura 6.23 se muestra la opción de Avanzados la cual permite la configuración de la herramienta, administración usuarios, configuración de alarmas, etc.

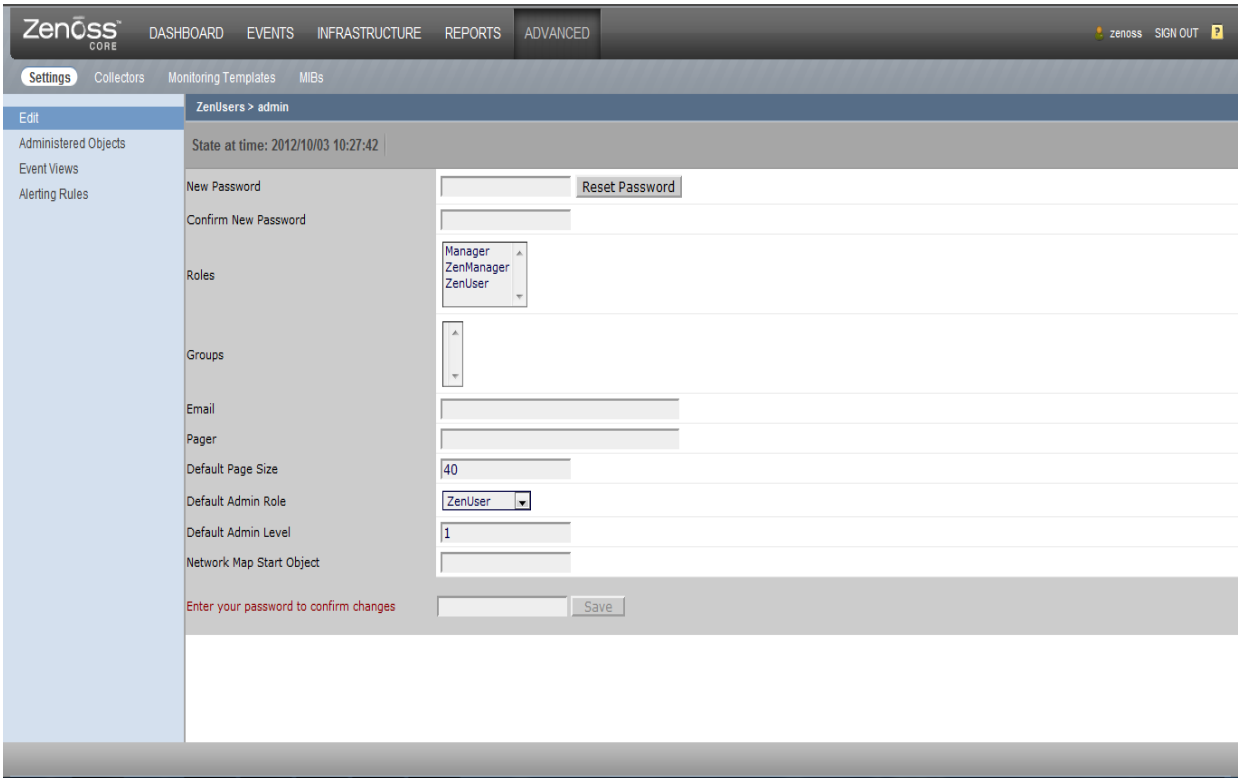


Figura 6.23: Advanced Zenoss

Elaborado por: 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 función, siendo factibles la presentación de informes de forma gráfica o en forma de estadísticas, como se muestra en la figura 6.24**:**

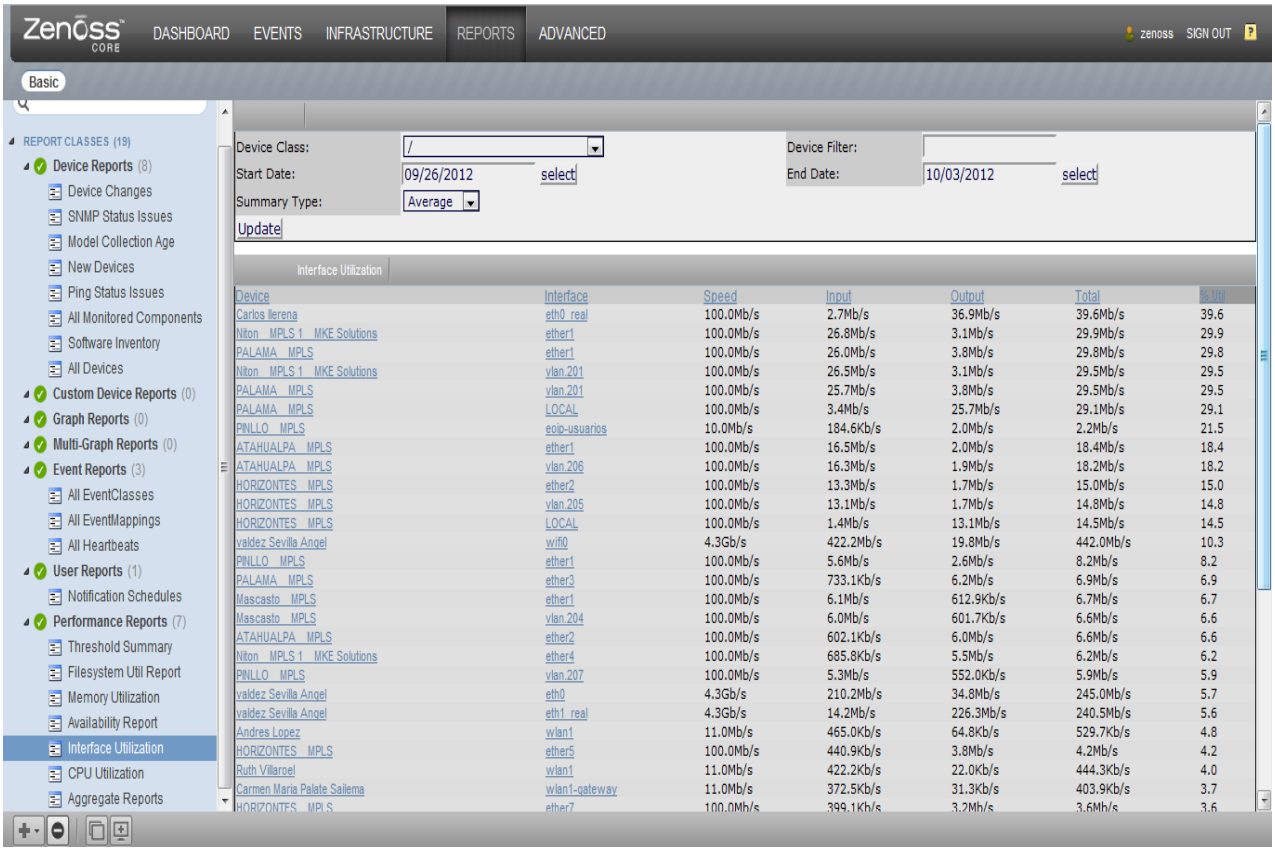


Figura 6.24: Reportes Estadísticos Zenoss

Elaborado por: Investigador

6.6.2.3. Pruebas con la herramienta de Administración y Monitoreo ZABBIX

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.

Después de haber instalado Zabbix, se abre un navegador web: http://localhost/zabbix. Tendremos una interfaz como se muestra en la figura 6.25:

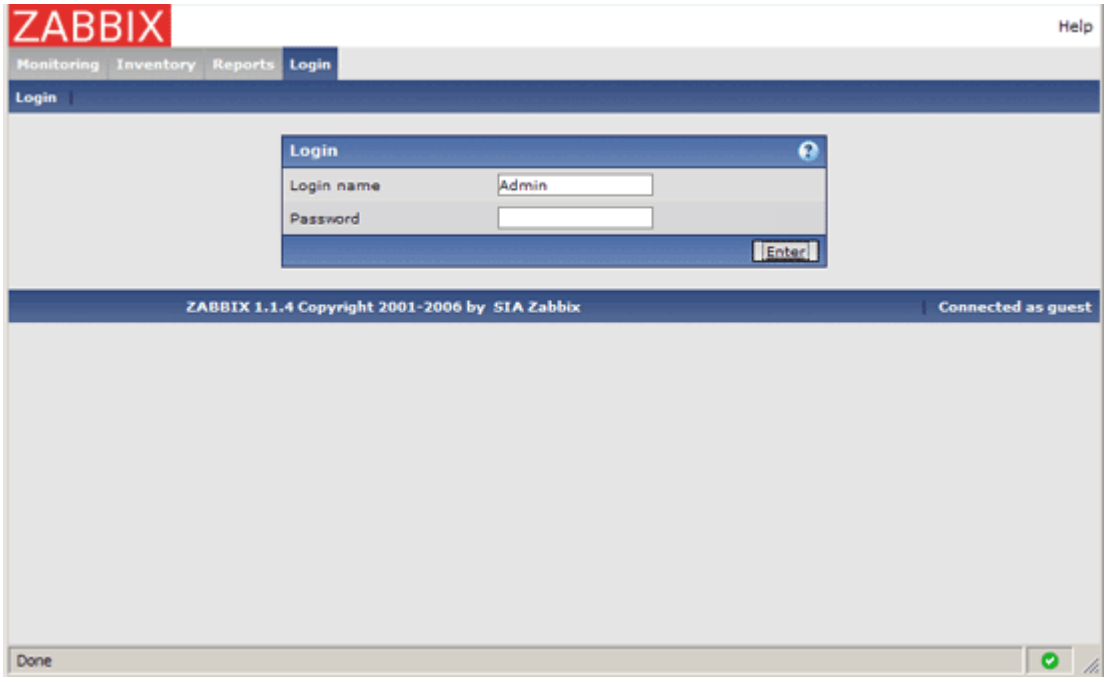


Figura 6.25: Login de Usuario Zabbix

Elaborado por: Investigador

Para poder ingresar y empezar a utilizar zabbix, se debe ingresar el nombre de usuario que por defecto es admin y no tiene ninguna contraseña, la cual se puede editar para mayor seguridad.

En la figura 6.26 se muestra la interfaz inicial con la que arranca Zabbix donde se puede observar todos los parámetros y servicios que tiene a su disposición:

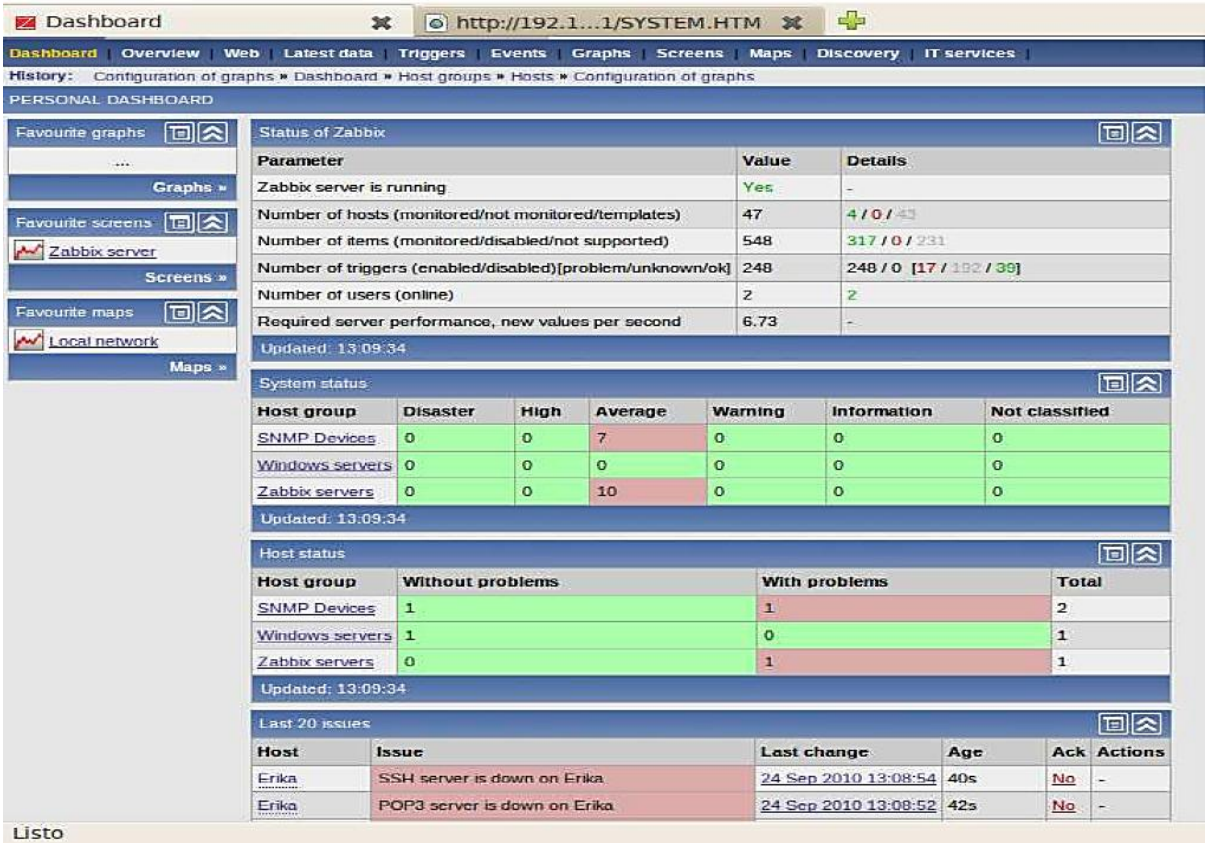


Figura 6.26: Dashboard Zabbix

Elaborado por: Investigador

En la figura 6.27 se muestra la información necesaria que se debe ingresar para añadir un dispositivo a zabbix y empezar a trabajar con este, los cuales son: nombre del dispositivo, el grupo al que se quiere añadir, su ip, status, etc.

Figura 6.27: Añadiendo host Zabbix

Elaborado por: Investigador

Una vez añadido el dispositivo correctamente se puede ir a la pestaña de "Monitoring", para poder visualizar los dispositivos añadidos y sus ítems como se muestra en la figura 6.28 donde en este caso se tiene un gran número de dispositivos agregados.

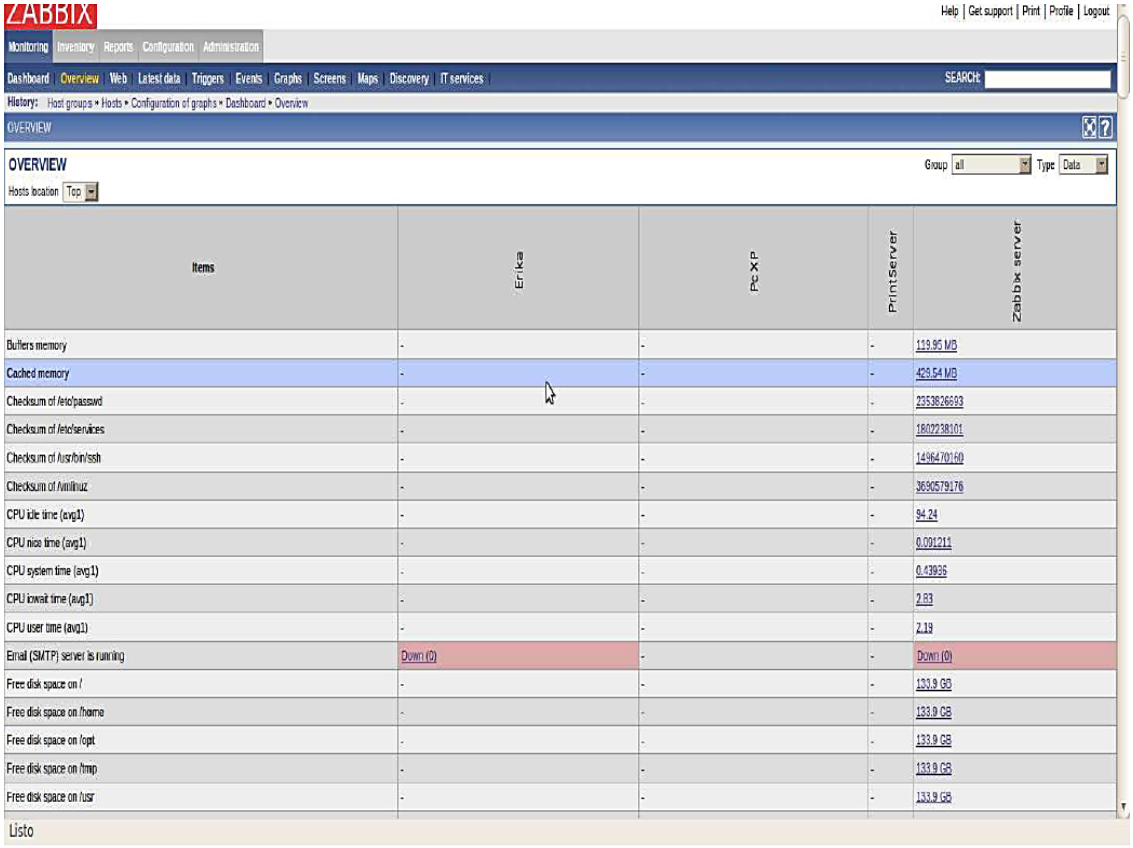


Figura 6.28: Pestaña Monitoring Zabbix

Elaborado por: Investigador

Además en las opciones de "Graph" se muestra una gráfica con los resultados de un estado, en este caso del estado de la red de un dispositivo en el cual la gráfica se muestra el estado de salida y de entrada de datos del dispositivo, como se puede observar en la figura 6.29:

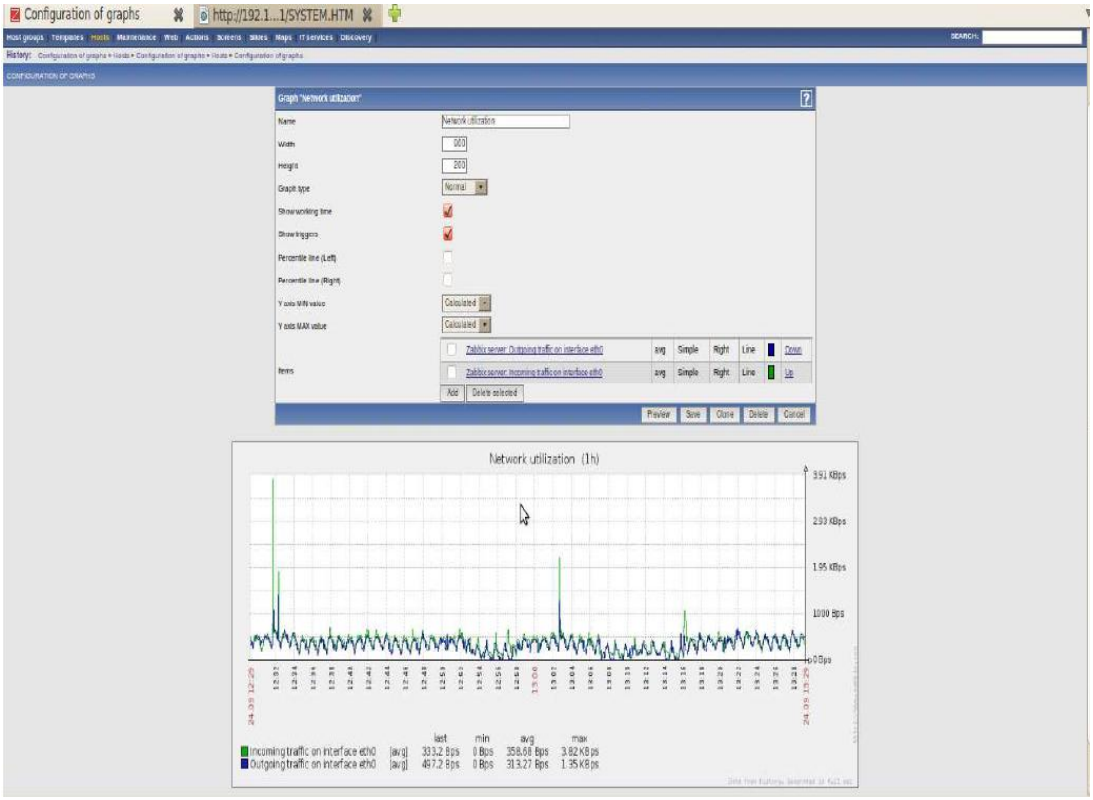


Figura 6.29: Utilización de la red Zabbix

Elaborado por: Investigador

En la figura 6.30 se muestra la gráfica de la utilización de CPU en Zabbix, donde se puede observar el estado del sistema en el cpu, del tiempo del uso del usuario, etc.

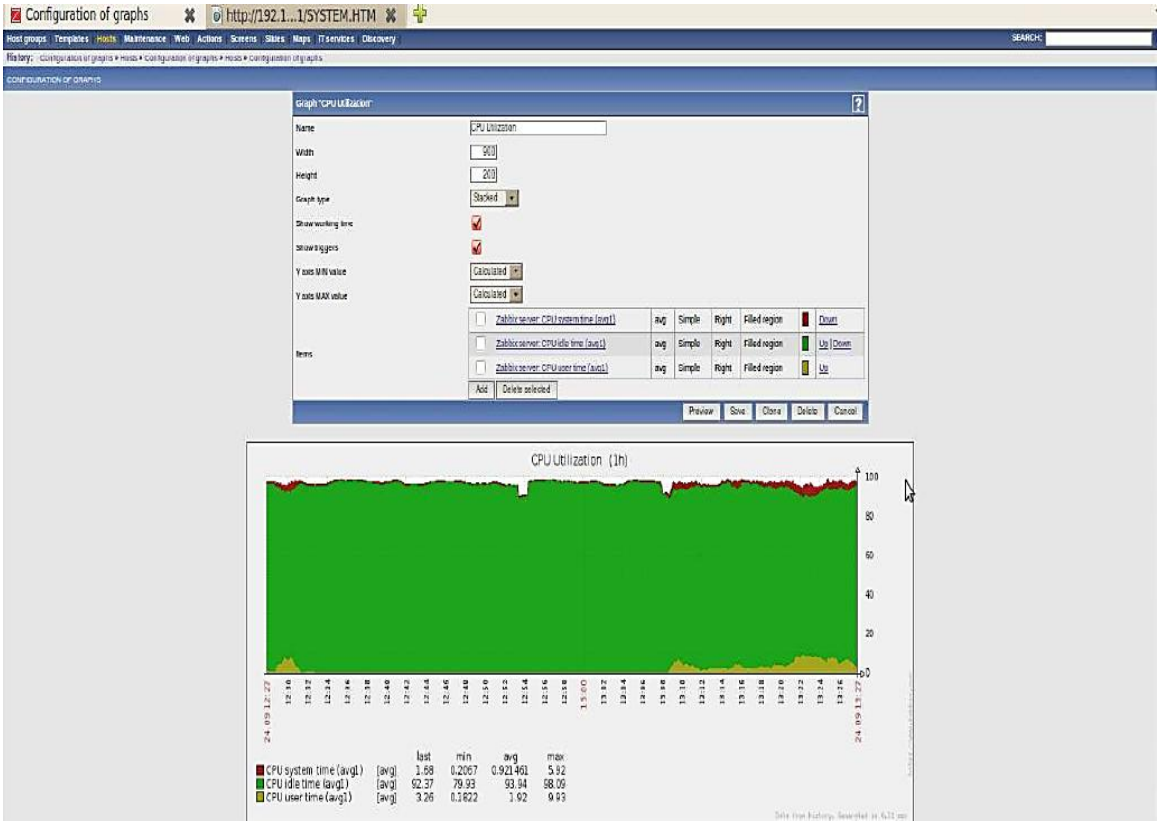


Figura 6.30: Utilización de CPU Zabbix

Elaborado por: Investigador

En la figura 6.31 se muestra la gráfica de la carga de CPU en Zabbix, en donde se puede observar el rendimiento de todos los procesadores con los que cuenta el cpu:

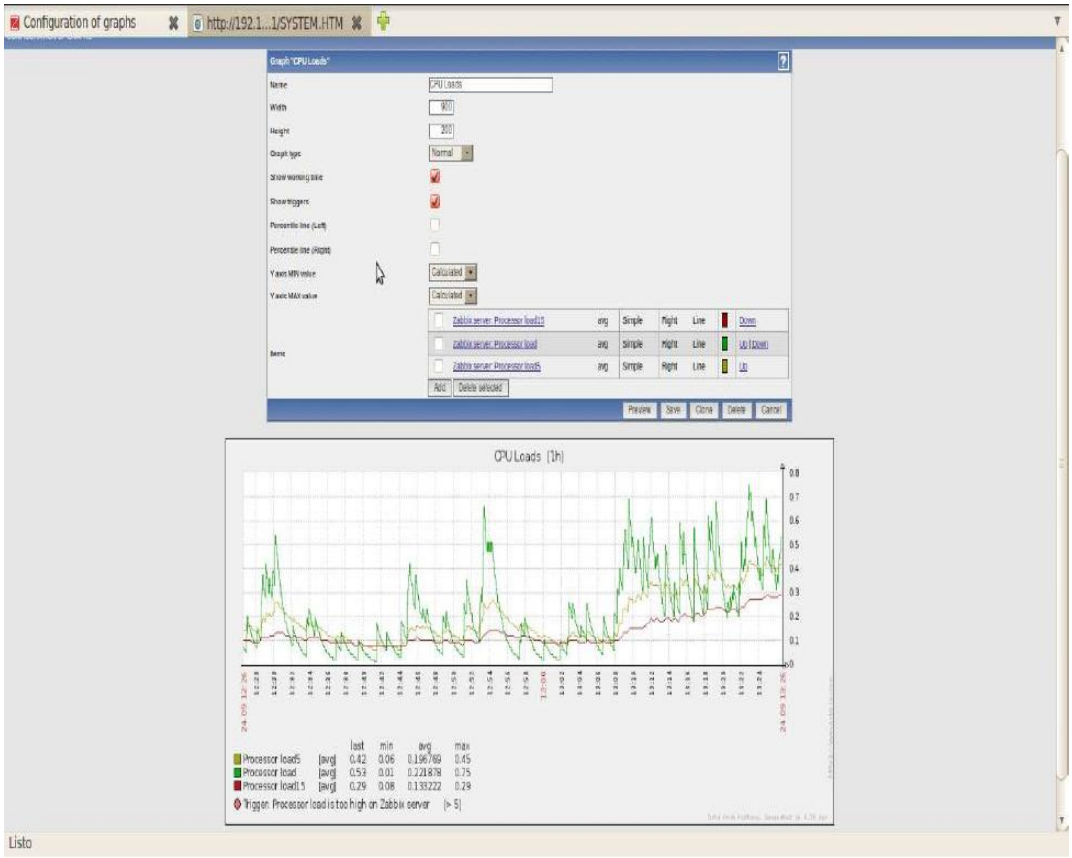


Figura 6.31: Carga CPU Zabbix

Elaborado por: Investigador

En los reportes se muestra el estado de Zabbix server, el número de host monitoreados, número de usuarios, etc, como se muestra en la figura 6.32.

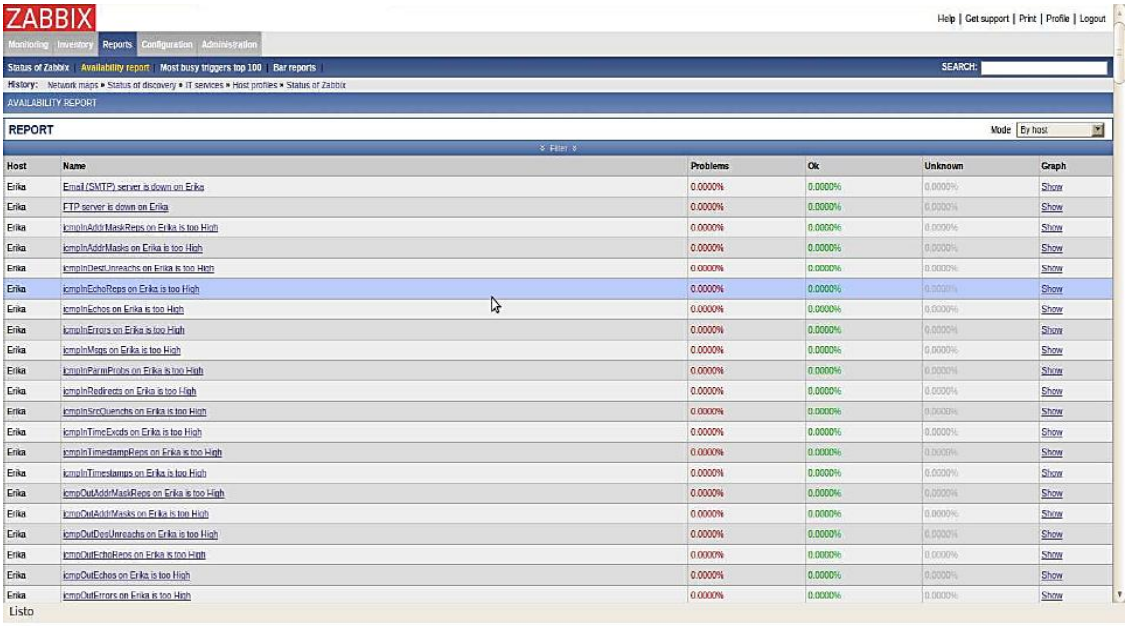


Figura 6.32: Reportes Zabbix

Elaborado por: Investigador

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

- **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, como se muestra en la tabla 6.2.

Tabla 6.2: Escalas de Equivalencia

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

Elaborado por: Investigador

Usabilidad

En la tabla 6.3 se muestra los parámetros de valoración con respecto a la usabilidad que tienen las herramientas de Administración

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

Tabla 6.3: Valoración del Parámetro Usabilidad

Herramienta de Administración	Valoración
CACTI	3
ZENOSS	5
ZABBIX	2

Elaborado por: Investigador

En donde se pudo comprobar que la herramienta Zanoss es el que cumple con todos los parámetros con respecto a la usabilidad.

Gestión de Usuarios

En la tabla 6.4 se muestra los parámetros de valoración con respecto a la Gestión de Usuarios que tienen las herramientas de Administración

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

Tabla 6.4: Valoración del Parámetro Gestión de Usuario

Herramienta de Administración	Valoración
CACTI	3
ZENOSS	5
ZABBIX	4

Elaborado por: Investigador

En donde se pudo comprobar que la herramienta Zanoss es el que cumple con todos los parámetros con respecto a la gestión de usuario.

Recolección de Información

En la tabla 6.5 se muestra los parámetros de valoración con respecto a la Recolección de Información que tienen las herramientas de Administración

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

Tabla 6.5: Valoración del Parámetro Recolección de Información

Herramienta de Administración	Valoración
CACTI	4
ZENOSS	4
ZABBIX	5

Elaborado por: Investigador

En donde se pudo comprobar que la herramienta Zabbix es el que menor tiempo demora en recolectar la información de los dispositivos monitoreados.

Soporte

En la tabla 6.6 se muestra los parámetros de valoración con respecto al Soporte con los que cuentan las herramientas de Administración

Herramienta de Administración	Foros de Discución	IRC	Noticias	Gratuito
CACTI	✓	X	✓	✓
ZENOSS	✓	✓	✓	✓
ZABBIX	✓	✓	✓	X

Tabla 6.6: Valoración del Parámetro Soporte

Herramienta de Administración	Valoración
CACTI	Muy Buena
ZENOSS	Excelente
ZABBIX	Buena

Elaborado por: Investigador

En donde se pudo comprobar que la herramienta Zanoss es el que cumple con todos los parámetros con respecto al soporte ya que es la herramienta que cuenta con el mayor número de sitios que brindan soporte.

Reportes

En la tabla 6.7 se muestra los parámetros de valoración con respecto a los Reportes que brindan las herramientas de Administración

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

Tabla 6.7: Valoración del Parámetro Reportes

Herramienta de Administración	Valoración
CACTI	2
ZENOSS	5
ZABBIX	4

Elaborado por: Investigador

En donde se pudo comprobar que la herramienta Zanoss es el que cumple con todos los parámetros con respecto a los reportes y así tener un mejor monitoreo de la red.

Alertas

En la tabla 6.8 se muestra los parámetros de valoración con respecto a las Alertas que brindan las herramientas de Administración

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

Tabla 6.8: Valoración del Parámetro Alertas

Herramienta de Administración	Valoración
CACTI	1
ZENOSS	5
ZABBIX	5

Elaborado por: Investigador

En donde se pudo comprobar que la herramienta Zanoss y zabbix son los que cumple con todos los parámetros con respecto a las alertas.

Alarmas

En la tabla 6.9 se muestra los parámetros de valoración con respecto a las Alarmas que brindan las herramientas de Administración

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

Tabla 6.9: Valoración del Parámetro Alarmas

Herramienta de Administración	Valoración
CACTI	2
ZENOSS	5
ZABBIX	4

Elaborado por: Investigador

En donde se pudo comprobar que la herramienta Zanoss es el que cumple con todos los parámetros con respecto a las Alarmas lo que nos ayudara a una rápida detección de fallos en la red y a su inmediata reparación.

Auto descubrimientos de Dispositivos

En la tabla 6.10 se muestra los parámetros de valoración con respecto al Auto descubrimiento de Dispositivos que poseen las herramientas de Administración

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

Tabla 6.10: Valoración del Parámetro Auto Descubrimiento de Dispositivos

Herramienta de Administración	**Valoración**
CACTI	1
ZENOSS	5
ZABBIX	4

Elaborado por: Investigador

En donde se pudo comprobar que la herramienta Zanoss es el que cumple con todos los parámetros con respecto al auto descubrimiento de la red facilitando así al usuario el ingreso de dispositivos en la herramienta.

Mapas

En la tabla 6.11 se muestra los parámetros de valoración con respecto a los Mapas que poseen las herramientas de Administración

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

Tabla 6.11: Valoración del Parámetro Mapas

Herramienta de Administración	Valoración
CACTI	1
ZENOSS	5
ZABBIX	3

Elaborado por: Investigador

En donde se pudo comprobar que la herramienta Zanoss es el que cumple con todos los parámetros con respecto a los mapas, haciendo así un control óptimo de los dispositivos y mejor apreciación de los mismos.

6.6.4. 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 tabla 6.12, de esta manera se podrá realizar la elección de una manera más clara y sencilla.

Tabla 6.12: Resumen Comparativo

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**

Elaborado por: Investigador

En donde se pode observar que promediando el valor de los resultados obtenidos en el análisis de las tres herramientas, la herramienta que más se acerca a las necesidades de la empresa es la herramienta Zenoos con un puntaje de 4.88/5 superando a Cacti el cual tiene un puntaje de 2.33/5 y a Zabbix que posee un puntaje de 3.77/5, siendo así Zenoss la herramienta a implementarse

6.6.5. Análisis de Resultados

Cálculo en porcentaje de las calificaciones obtenidas.

Para lo cual utilizaremos la ecuación 6.1 en donde el promedio de 5 sea el 100% en el análisis, y con una regla de 3 simple obtener el resultado porcentual de los valores de cada herramientas obtenidos en el análisis.

Entonces:

$$\begin{array}{rcl} 5 & \rightarrow & 100\% \\ puntaje & \rightarrow & x \end{array} \qquad Ecuación\ (6.1)$$

En donde

Cacti obtuvo una puntuación de 2.33/5 en el análisis, con este valor obtenido se procede a realizar las operaciones mencionadas anteriormente y obtener su resultado porcentual.

$$\begin{array}{cc} 5 & 100 \\ 2.33 & x \end{array}$$

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

Con el resultado obtenido se puede decir que Cacti tiene el valor del 46.6% como resultado del análisis, siendo así la tercera herramienta a utilizar en el análisis.

Zenoss obtuvo una puntuación de 4.88/5 en el análisis, con este valor obtenido se procede a realizar las operaciones mencionadas anteriormente y obtener su resultado porcentual.

$$\begin{matrix} 5 & 100 \\ 4.88 & x \end{matrix}$$

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

Con el resultado obtenido se puede decir que Zenoss tiene el valor del 97.6% como resultado del análisis, haciéndola la herramienta que más se acerca a lo requerido y la numero uno del análisis.

Zabbix obtuvo una puntuación de 3.77/5 en el análisis, con este valor obtenido se procede a realizar las operaciones mencionadas anteriormente y obtener su resultado porcentual

$$\begin{matrix} 5 & 100 \\ 3.77 & x \end{matrix}$$

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

Con el resultado obtenido se puede decir que Zabbix tiene el valor del 75.4% como resultado del análisis, siendo así la segunda herramienta a utilizar en el análisis como se puede observar en el gráfico 6.33.

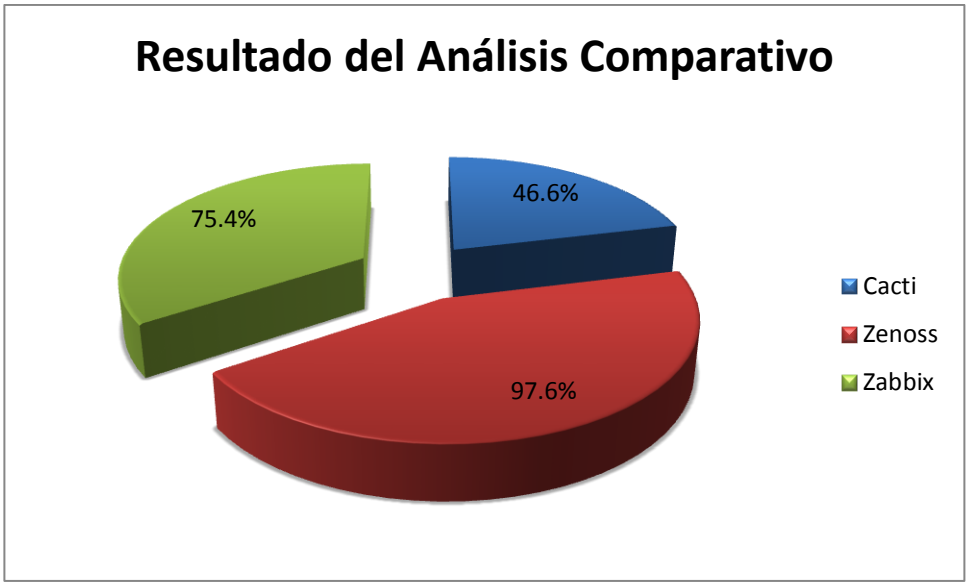


Gráfico 6.33: Resultado Análisis Comparativo

Elaborado por: Investigador

Como se puede observar en el gráfico 6.33, 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 empresa Speedy.

A continuación se presentan conclusiones a las que se ha podido 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 se pudo 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.

6.6.6. Implementación y Utilización de la Herramienta Zenoss

La implementación de la Herramienta Zenoss se la realizo en la plataforma Linux, distribución Centos 6.3

6.6.6.1. Instalación del software Zenoss

Una vez obtenido el instalador del software Zenoss se realiza la instalación del mismo.

Para lo cual se instala la versión Zenoss Core que es la versión libre y gratis que se puede descargar y utilizar.

Para descargar el software se lo puede hacer desde la página de Zenoss la cual es: http://sourceforge.net/projects/zenoss/files/

Para instalar la herramienta Zenoss Core se ejecuta el instalador como se muestra en la figura 6.34.

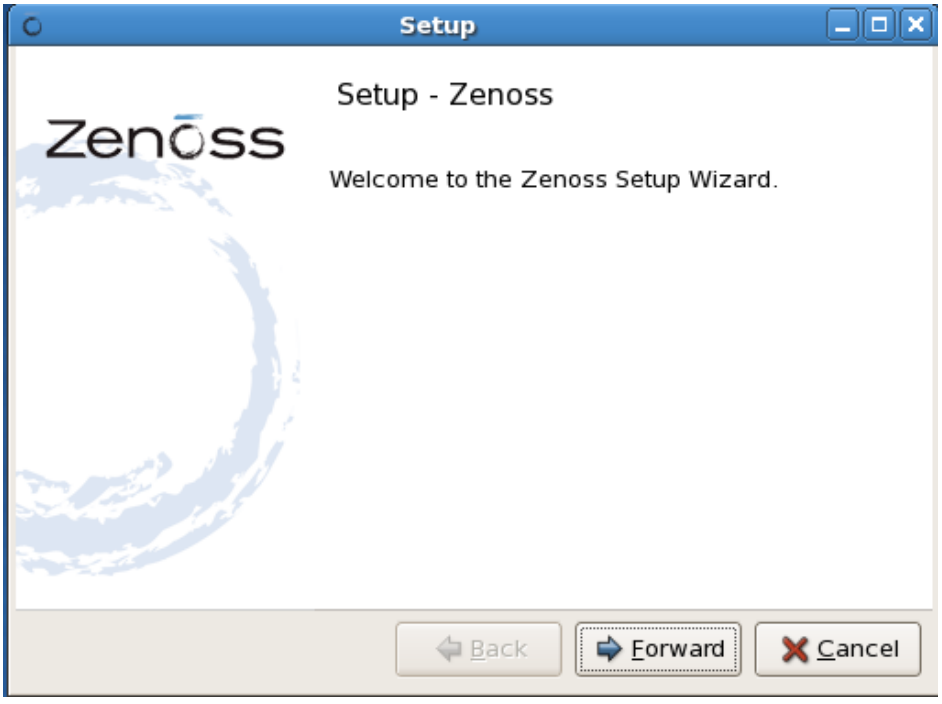


Figura 6.34: Instalando el software Zenoss

Elaborado por: Investigador

Debido a que el software Zenoss que utilizaremos es el Zenoss Core que es la versión libre y gratis solo se debe seguir la guía de instalación sin ningún tipo de restricciones ni códigos de licencia.

Una vez instalado el software, este pedirá configurar 2 pasos importantes para empezar con su óptima utilización como se muestra en la figura 6.35.

Figura 6.35: Pasos a configurar del software Zenoss

Elaborado por: Investigador

Se procede a dar click en el icono Get Started! con lo que se empezara a configurar el primer paso necesario el cual es los detalles del usuario, como lo son: el password para el administrador y crear las cuentas de usuario como se indica en la figura 6.36

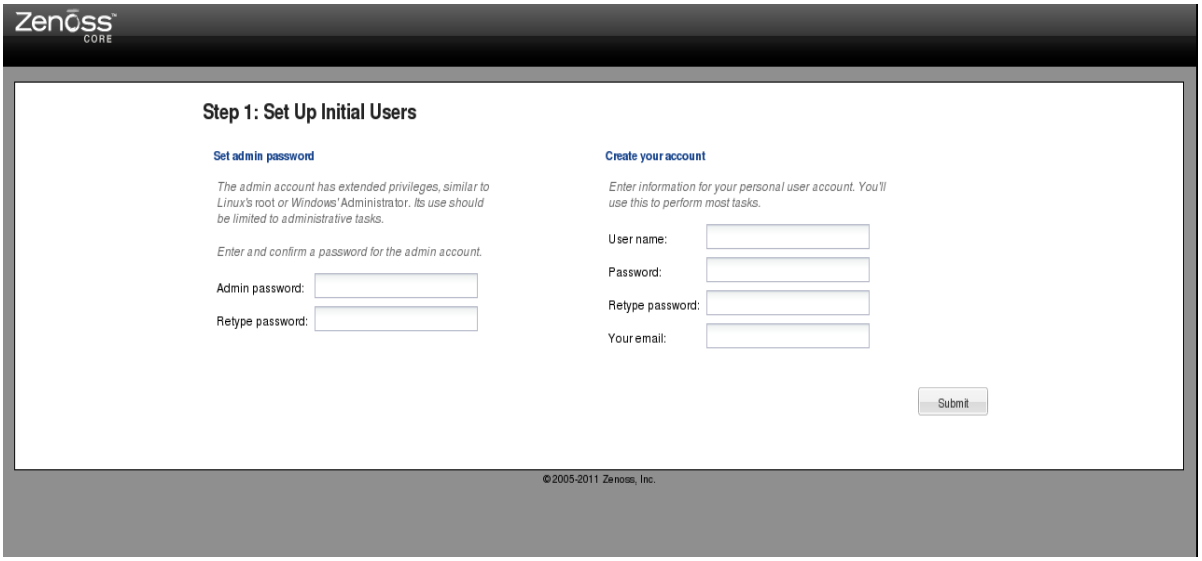


Figura 6.36: Configuración de usuarios del software Zenoss

Elaborado por: Investigador

Una vez configurado el paso uno se procede a configurar el paso 2 el cual se trata del reconocimiento de dispositivos en la red a ser monitoreados, zenoss nos brinda algunas posibilidades para el reconocimiento de los dispositivos.

La primera forma es la forma manual donde zenoss, el cual pedirá que se agregue el nombre del host o la ip del dispositivo a ser monitoreado como se muestra en la figura 6.37.

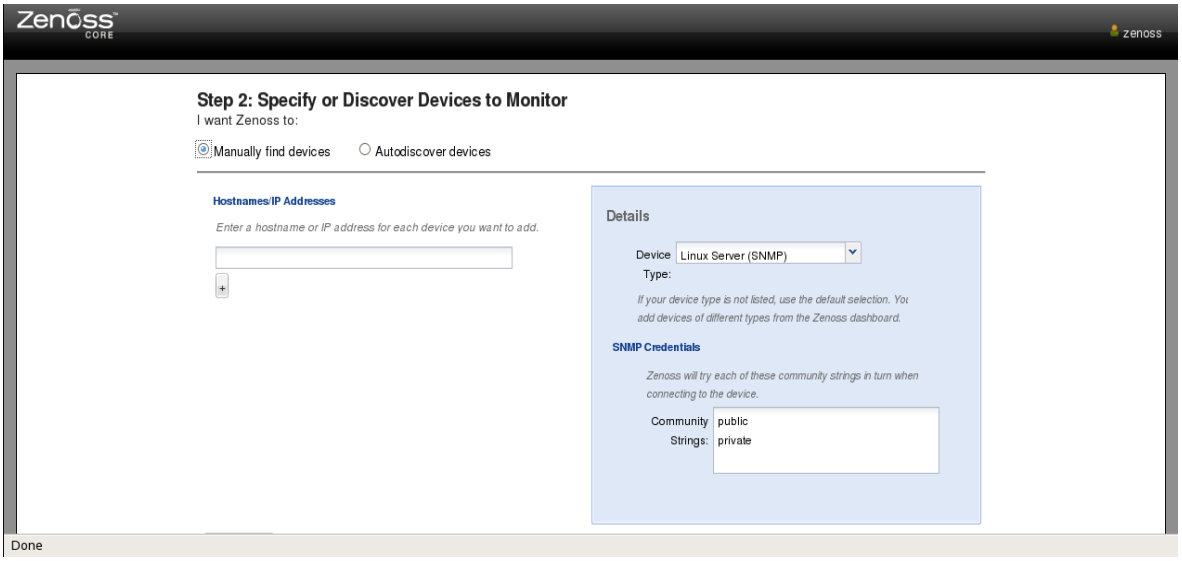


Figura 6.37: Descubrimiento manual de dispositivos del software Zenoss

Elaborado por: Investigador

La segunda forma que brinda zenoss es la del autodescubrimiento de dispositivos, zenoss en este caso pedirá que se agregue la dirección de red o los rangos ip de los dispositivos a ser descubiertos facilitándonos así el descubrimiento de dispositivos en una red grande como se muestra en la figura 6.38

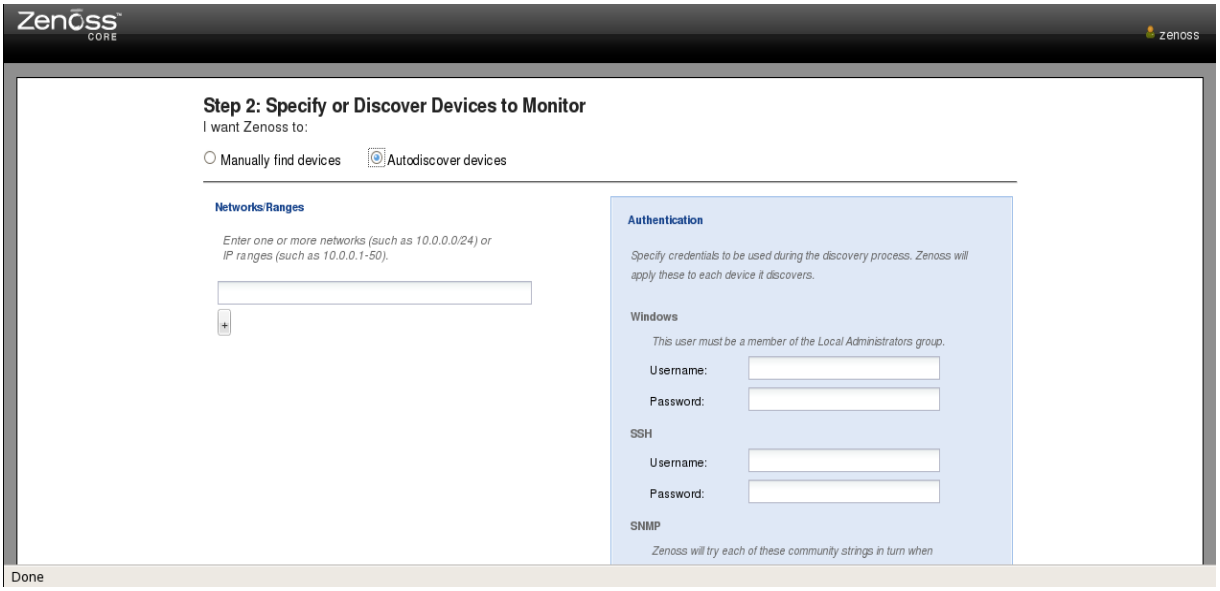


Figura 6.38: Autodescubrimiento de dispositivos del software Zenoss

Elaborado por: Investigador

Como una tercera opción zenoss brinda la posibilidad de saltarnos el paso 2 para poder después de una manera más cómoda ingresar los dispositivos a ser monitoreados desde la interfaz de zenoss.

Una vez configurado todo lo necesario para acceder a zenoss se tendra una interfaz similar a la que se muestra en la figura 6.39, donde se muestra el entorno en donde se manejara el servidor Zenoss.

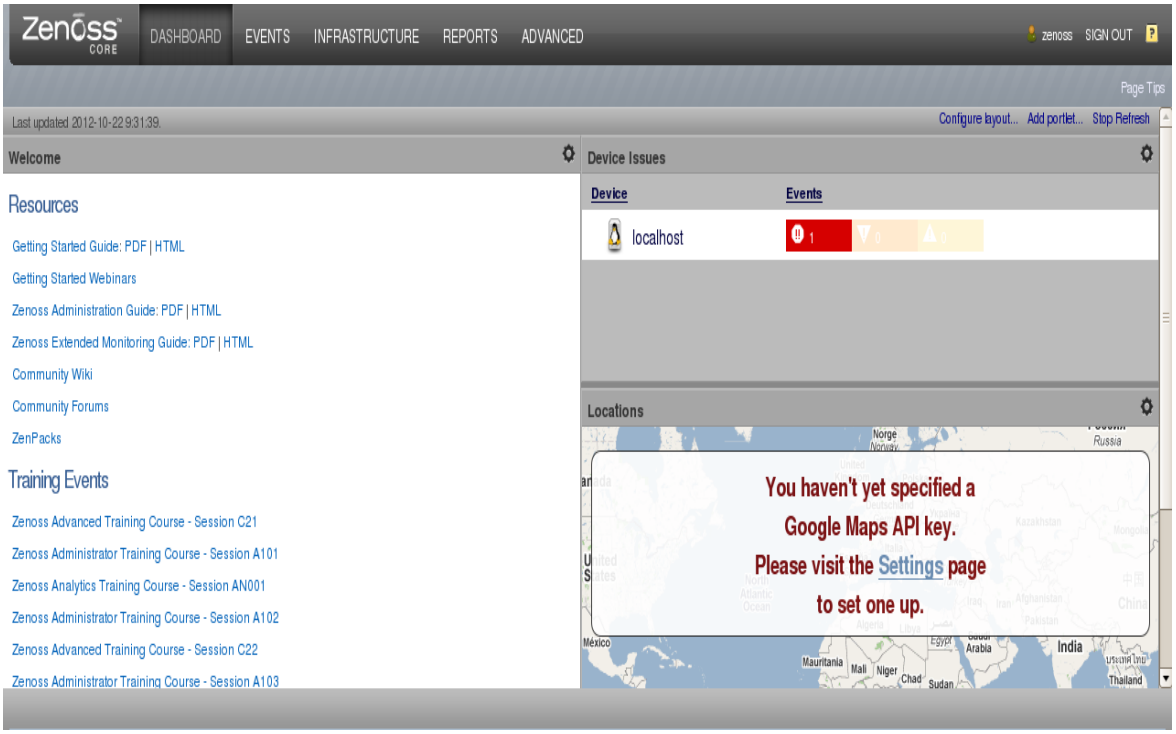


Figura 6.39: Interfaz del software Zenoss

Elaborado por: Investigador

Una vez instalado el servidor Zenoss se ingresa una dirección IP en la tarjeta de red, puesto que el servidor trabaja en la intranet se debe buscar una dirección disponible para evitar conflictos en la red, además para la utilización del software Zenoss se recomienda colocar una IP estática y no mediante DHCP para un mejor rendimiento del software Zenoss para que no haya problemas al momento de monitorear los dispositivos, como se muestra en la figura 6.40.

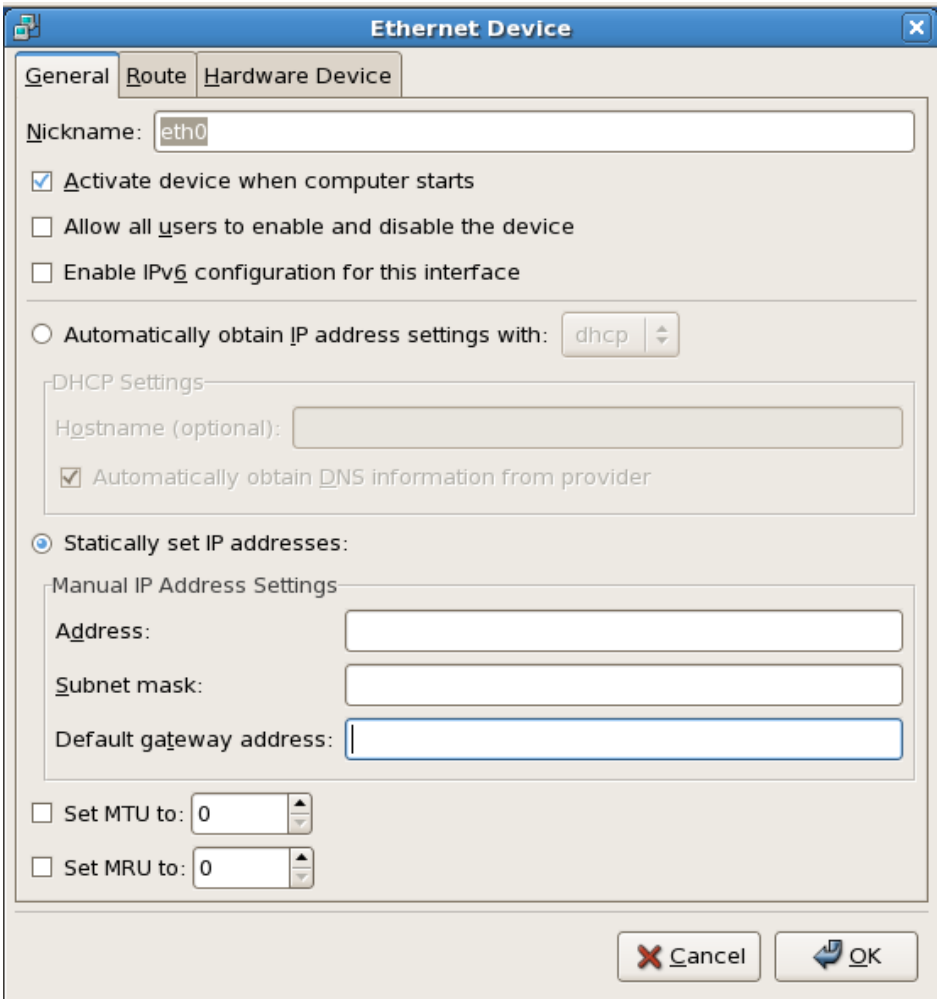


Figura 6.40: Ingreso de direcciones IP en la tarjeta de red

Elaborado por: Investigador

Configurada la tarjeta de red se procede a configurar el software zenoss de acuerdo a las necesidades de la empresa Speedy.

Como se puede observar en la figura 6.41 zenoss nos da la posibilidad de trabajar en conjunto con google maps para poder ubicar los dispositivos que nosotros queramos en puntos estratégicos en el mapa.

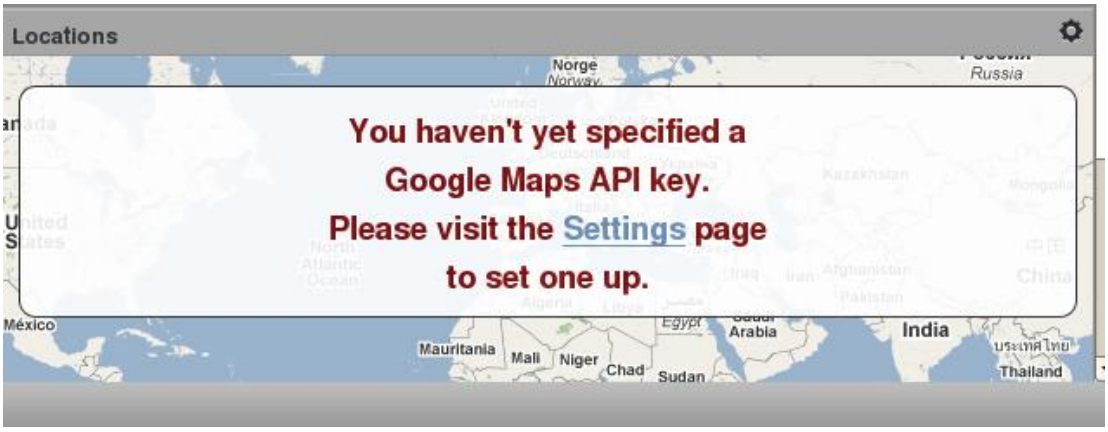


Figura 6.41: Google Maps en Zenoss

Elaborado por: Investigador

Para poder hacer uso de la herramienta google maps en zenoss, este pedirá un API key, el cual se puede obtener de manera gratuita a través de google maps con la url https://developers.google.com/maps/documentation/javascript/tutorial#api_key como se muestra en la figura 6.42 y lo único que queda es seguir los pasos descritos para obtener nuestro api key.

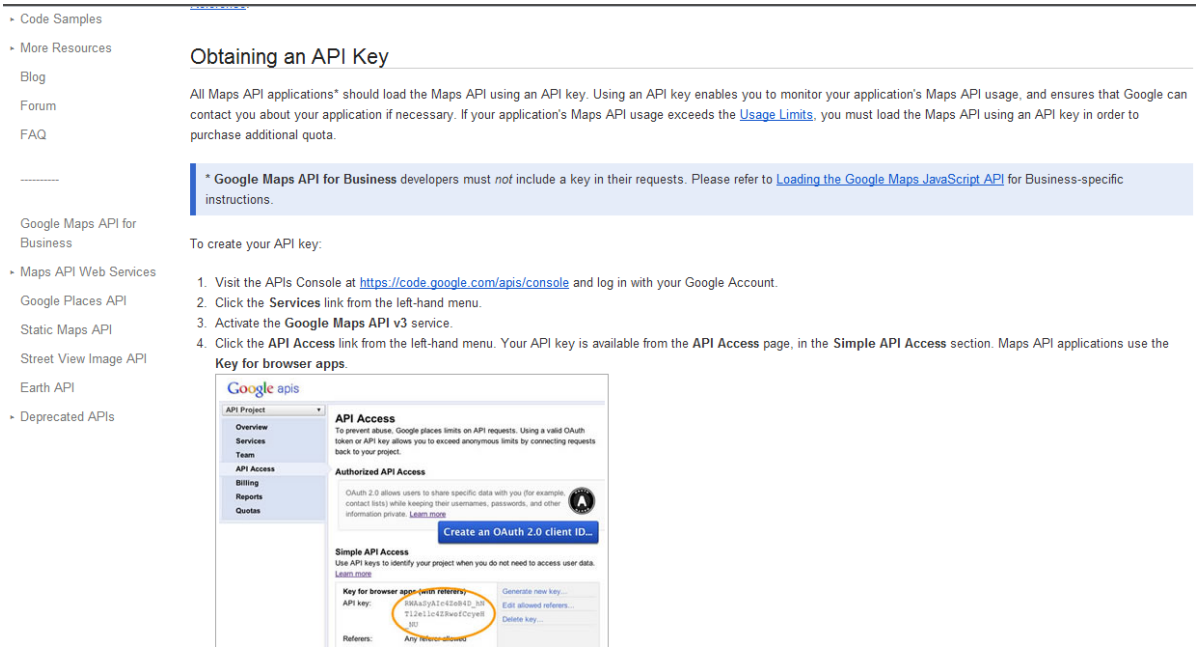


Figura 6.42: Como obtener una API key de google maps

Elaborado por: Investigador

Una vez obtenido el API key de google maps en zenoss, en la interface se acede a la opción Settings que nos ofrece zenoss para poder activar google maps en zenoss y se desplegara una ventana como se muestra en la figura 6.43

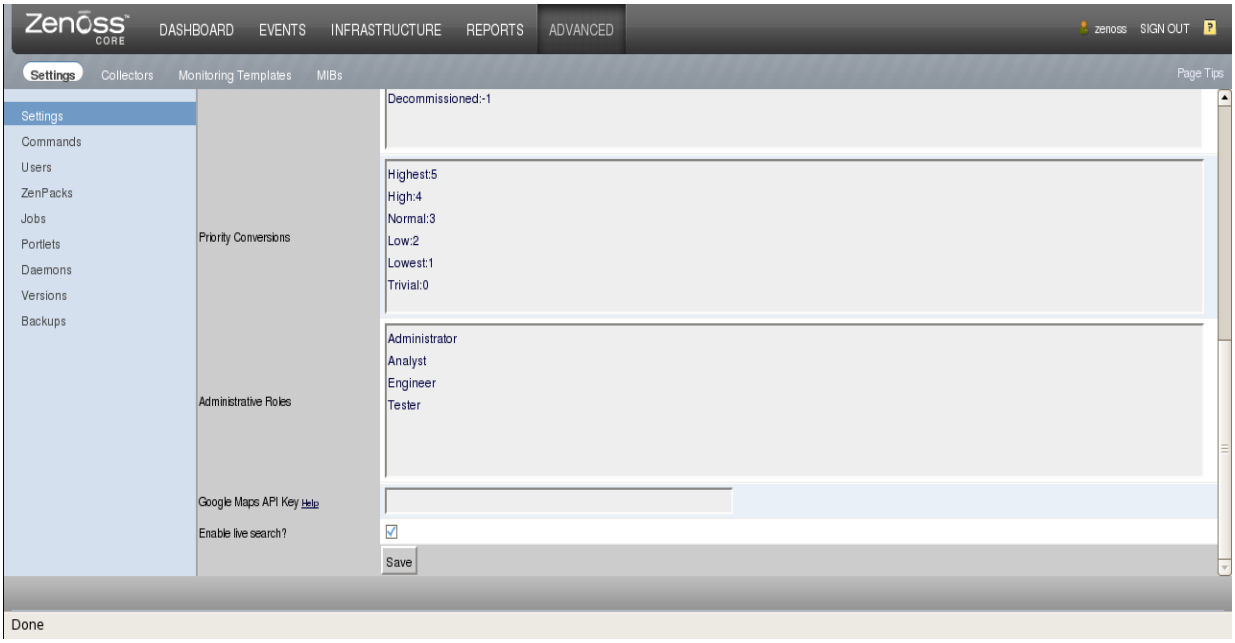


Figura 6.43: Setting (Zenoss)

Elaborado por: Investigador

En la opción Google Maps API Key se introduce el API key anteriormente obtenido y se procede a dar click en save para activar esta opción como se muestra en la figura 6.44

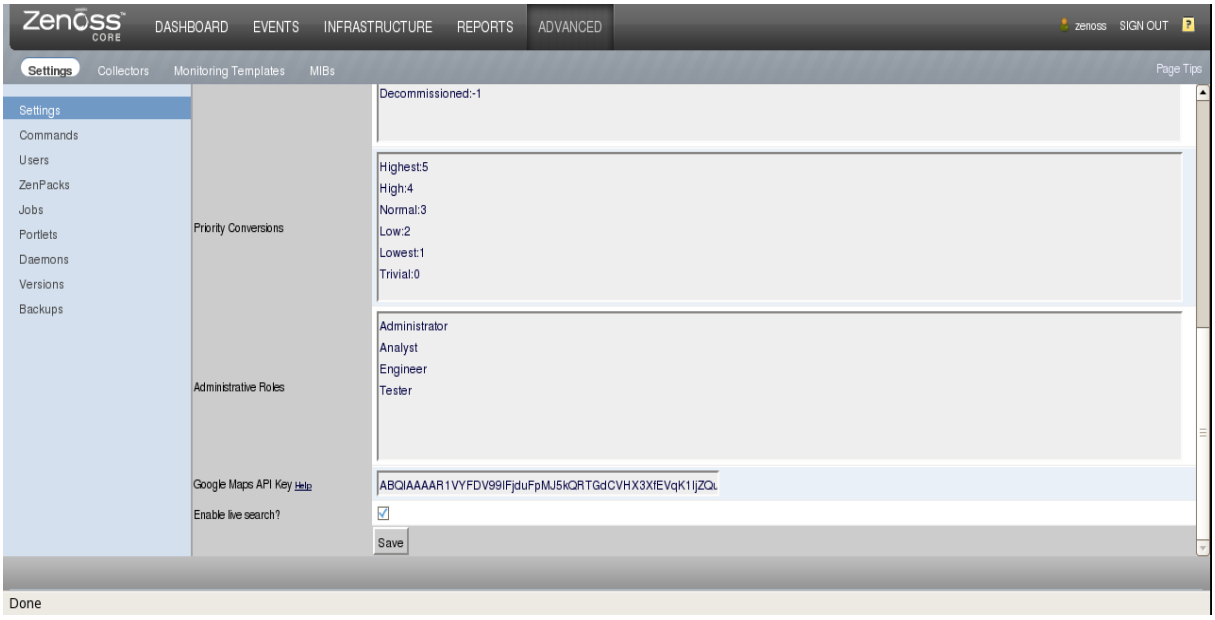


Figura 6.44: Google Maps API Key (Zenoss)

Elaborado por: Investigador

Activado el API Key se puede gozar de las utilidades de Goole Maps en Zenoss y se tendrá una herramienta similar a la que se muestra en la figura 6.45

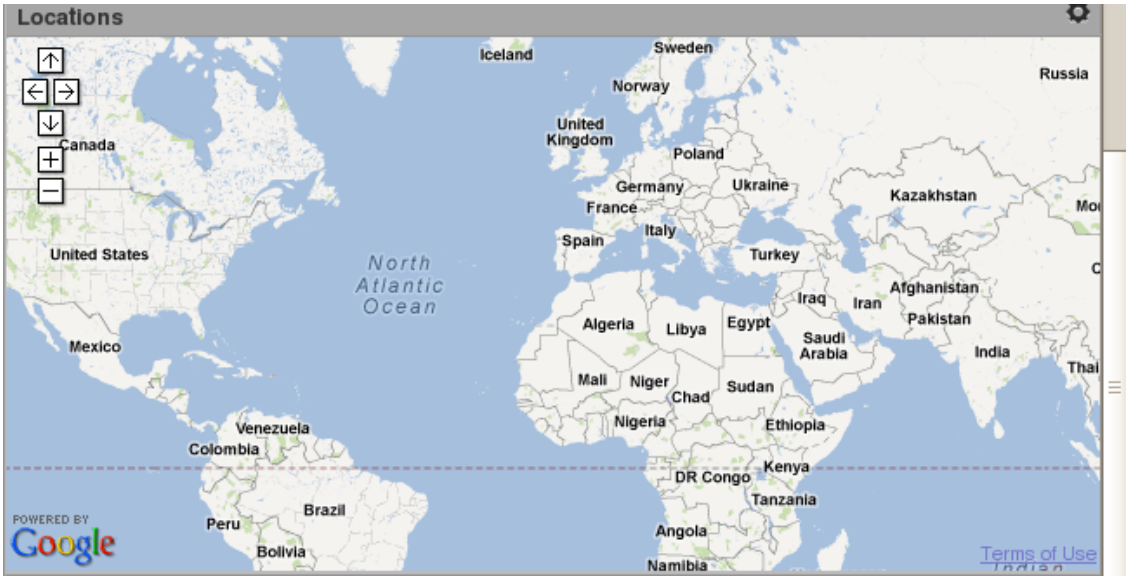


Figura 6.45: Google Maps en Zenoss

Elaborado por: Investigador

6.6.6.2. 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.

Agregar dispositivos de forma manual

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 óptima ya que precisamente esos datos en ciertas ocasiones no se tienen por lo que se recurre a la opción de autodescubrimiento.

Para poder agregar dispositivos en forma manual se lo debe hacer a través de la opción Infraestructura que se encuentra en la barra de menú principal de zenoss como se puede observar en la figura 6.46

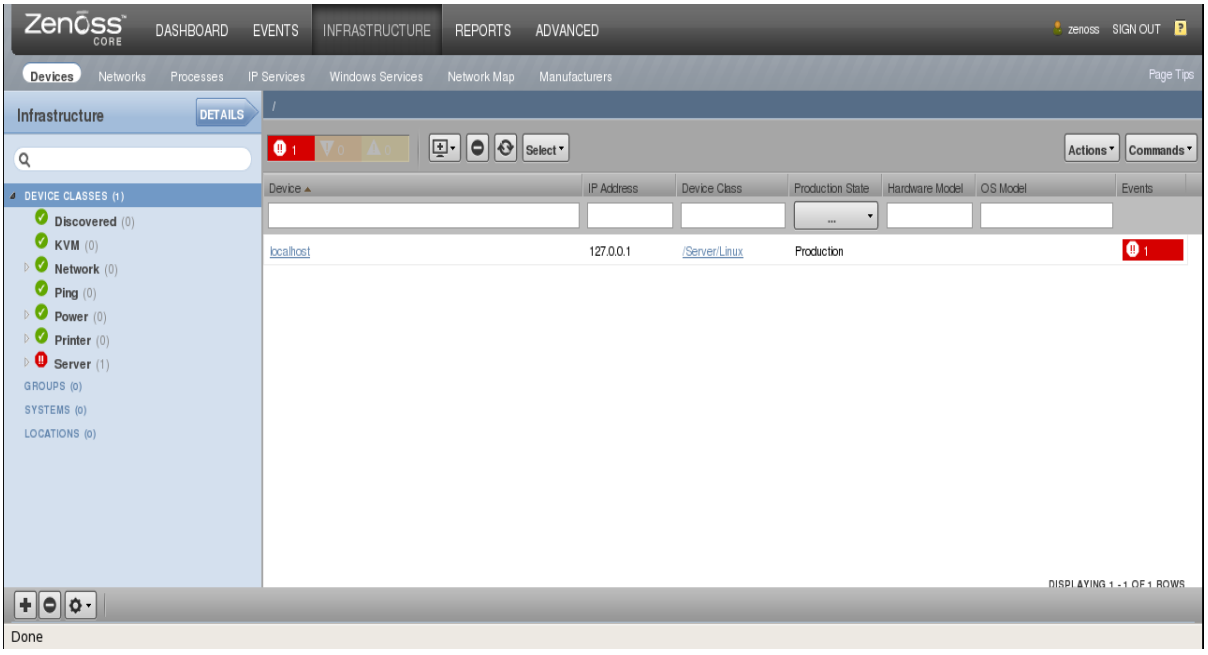


Figura 6.46: Infraestructura Zenoss

Elaborado por: Investigador

Una vez ubicado en infraestructura se dirige a la opción Agregar un dispositivo único  que permitirá agregar un dispositivo, como se muestra en la figura 6.47.

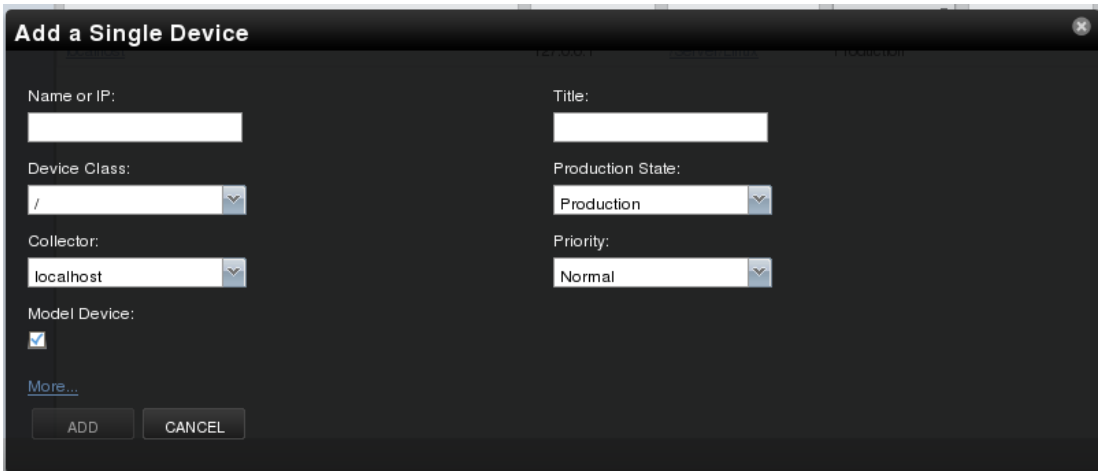


Figura 6.47: Agregar dispositivos en Zenoss

Elaborado por: Investigador

A continuación en esta opción se introduce la información reuqerida, o también permite hacer selecciones para añadir el dispositivo como:

- Nombre o IP - Se escribe la red (DNS) de nombre o la dirección IP del dispositivo.
- Clase de dispositivo - SE selecciona una clase de dispositivo al que pertenece este dispositivo.
- Colector - Por defecto, este es el localhost.
- Modelo - Por defecto, esta opción está activada.

También brinda la opción More para mostrar campos adicionales como:

- Modificar la configuración de SNMP

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

  Snmp Port: Se deja el puerto por omisión 161.

- Establecer información de hardware y sistema operativo si se conoce.
- Añadir comentarios al dispositivo.

Por lo que se tendrá una ventana como la que se muestra en la figura 6.48.

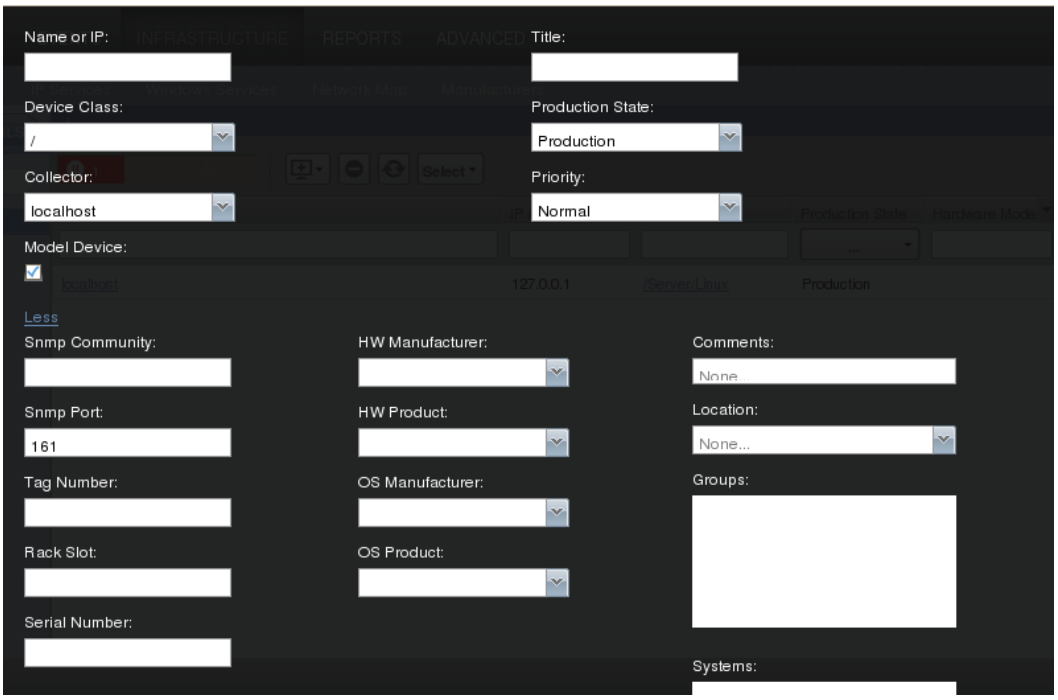


Figura 6.48: Opción more Zenoss

Elaborado por: Investigador

Por último se hace click en la opción agregar.

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.

Añadir múltiples dispositivos

Para seleccionar múltiples dispositivos en la barra de navegación, se selecciona Infraestructura.

Agregar varios dispositivos de la pestaña agregar dispositivos.

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

En el área de detalles, se selecciona un tipo de dispositivo de la lista. Si el tipo de dispositivo no aparece, a continuación, se utiliza la opción predeterminada de selección.

Se ingresa las credenciales adecuadas para la autenticación en el dispositivo.

Si se desea agregar más de un dispositivo, se hace clic en +.

Para agregar los dispositivos, hacer clic en Enviar como se muestra en la figura 6.49.

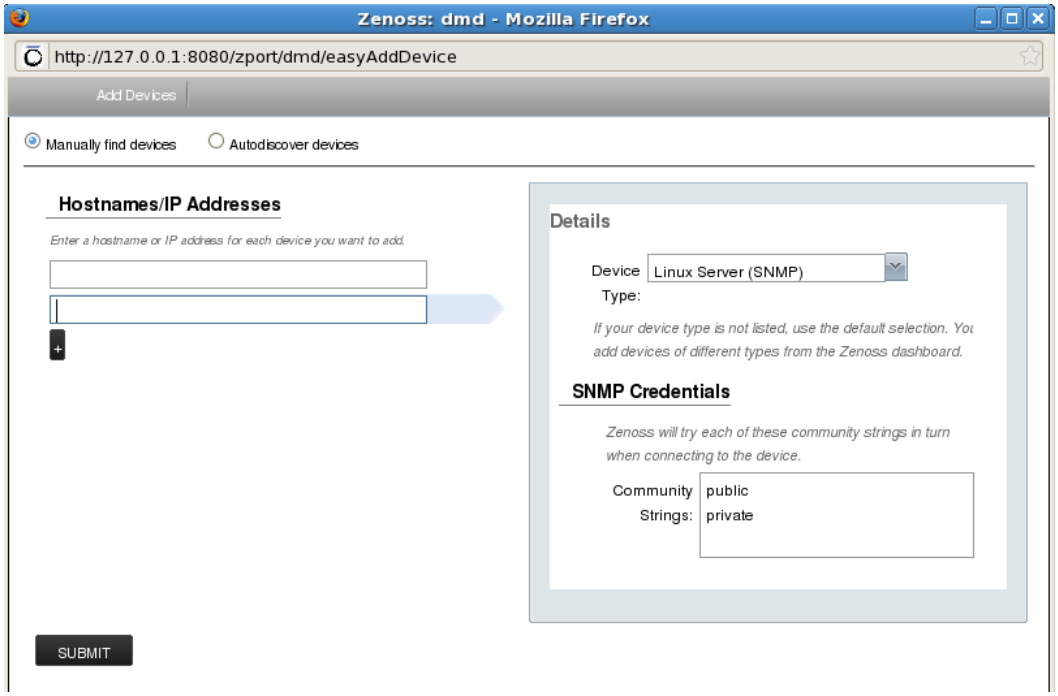


Figura 6.49: Añadir múltiples dispositivos Zenoss

Elaborado por: Investigador

Descubrimiento de dispositivos

Para el descubrimiento de dispositivos lo que se debe hacer es ingresar la red o la dirección IP para que el sistema pueda descubrir los dispositivos.

En la barra de navegación, se selecciona Infraestructura/agregar varios dispositivos.

Se elige la opción de detección automática los dispositivos como se muestra en la figura 6.50.

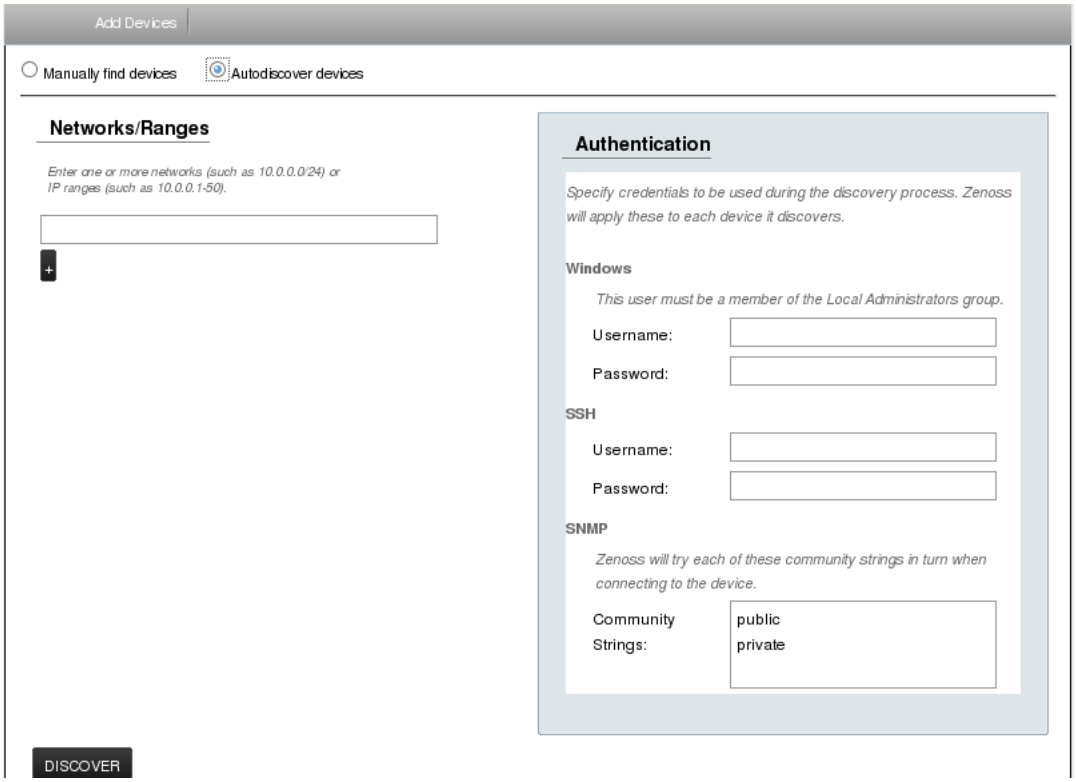


Figura 6.50: Descubrimiento de dispositivos Zenoss

Elaborado por: Investigador

Por ejemplo, se 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

Una vez que se ha seleccionado descubrir los dispositivos, zenoss empezara a reconocer los datos agregados y si se ha seleccionado la opción view job nos presentara información de todo lo que está ocurriendo mientras zenoss reconoce los dispositivos, si todo a finalizado satisfactoriamente Zenoss mostrará el dispositivo desde donde podremos ir al panel de manejo del dispositivo como se muestra en la figura 6.51.

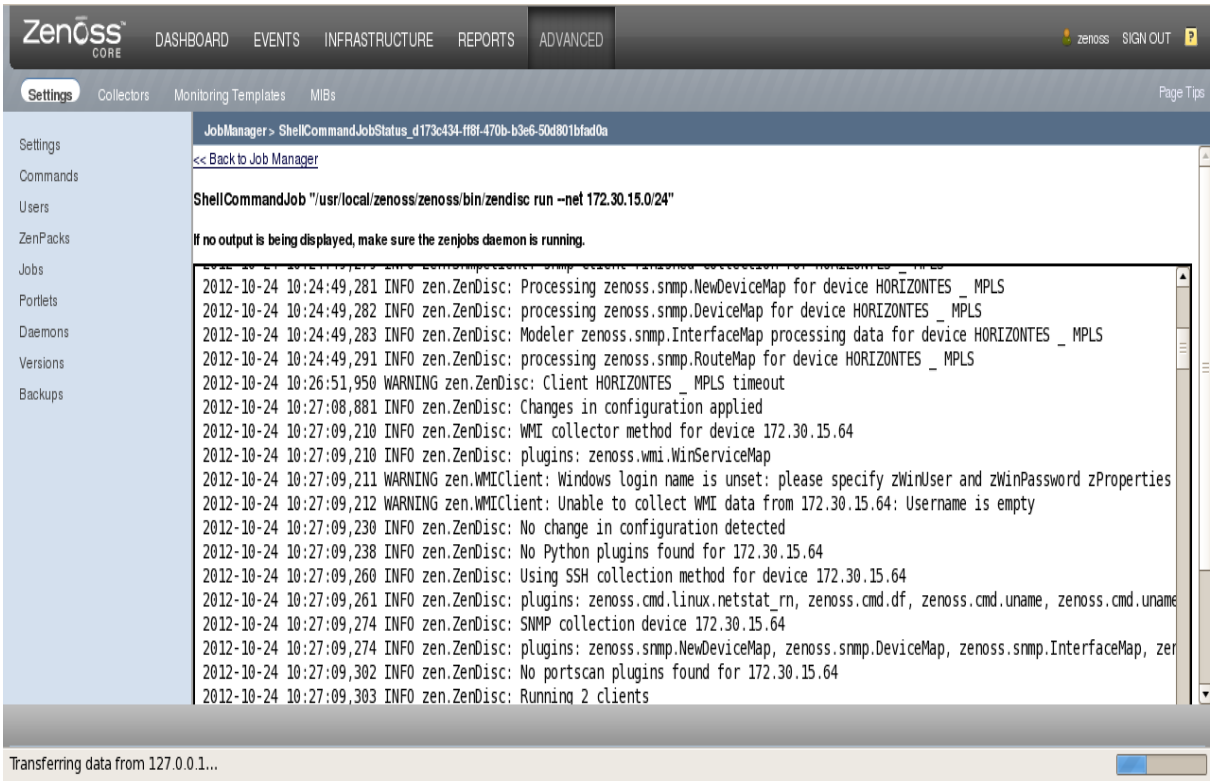


Figura 6.51: Proceso del descubrimiento de dispositivos Zenoss

Elaborado por: Investigador

Para el caso de la empresa Speedy se ha utilizado el autodescubrimiento de dispositivos y se ha dividido la red a sus nodos y usuarios correspondientes a estos los cuales son: Palama, Nitón, Horizonte, Tropezón, Macasto, Atahualpa, etc para una mejor administración y entendimiento.

6.6.6.3. Trabajar con dispositivos

La lista de dispositivos muestra todos los dispositivos del sistema. Desde este punto de vista, se puede buscar los dispositivos y realizar una visualización amplia de las tareas de gestión en todos los dispositivos como se muestra en la figura 6.52.

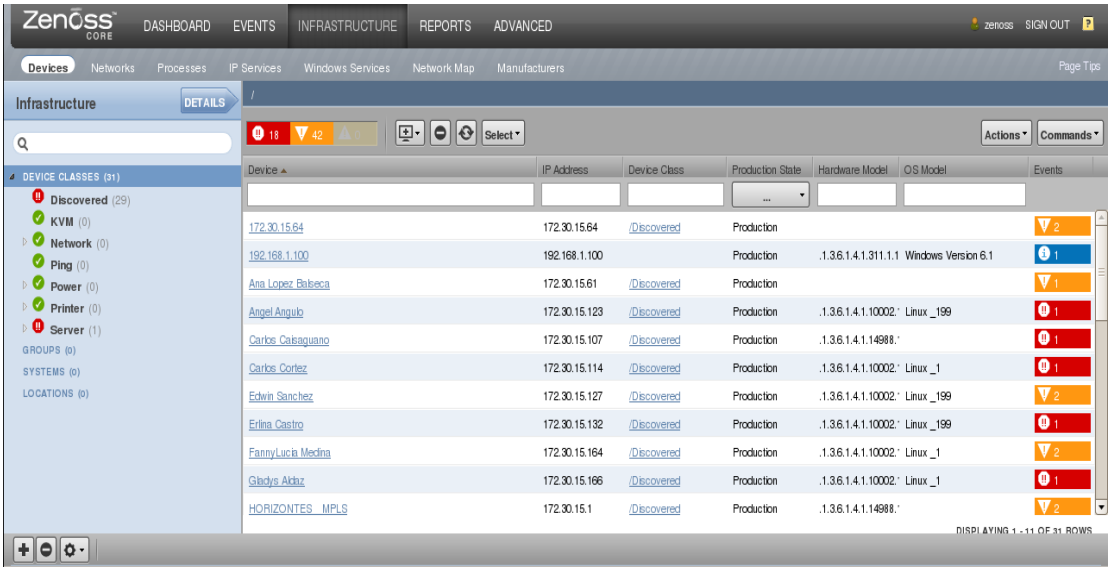


Figura 6.52: Dispositivos monitoreados Zenoss

Elaborado por: 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, se hace clic en el nombre en la lista de dispositivos y se desplegara la página de descripción de dispositivo como se muestra en la figura 6.53.

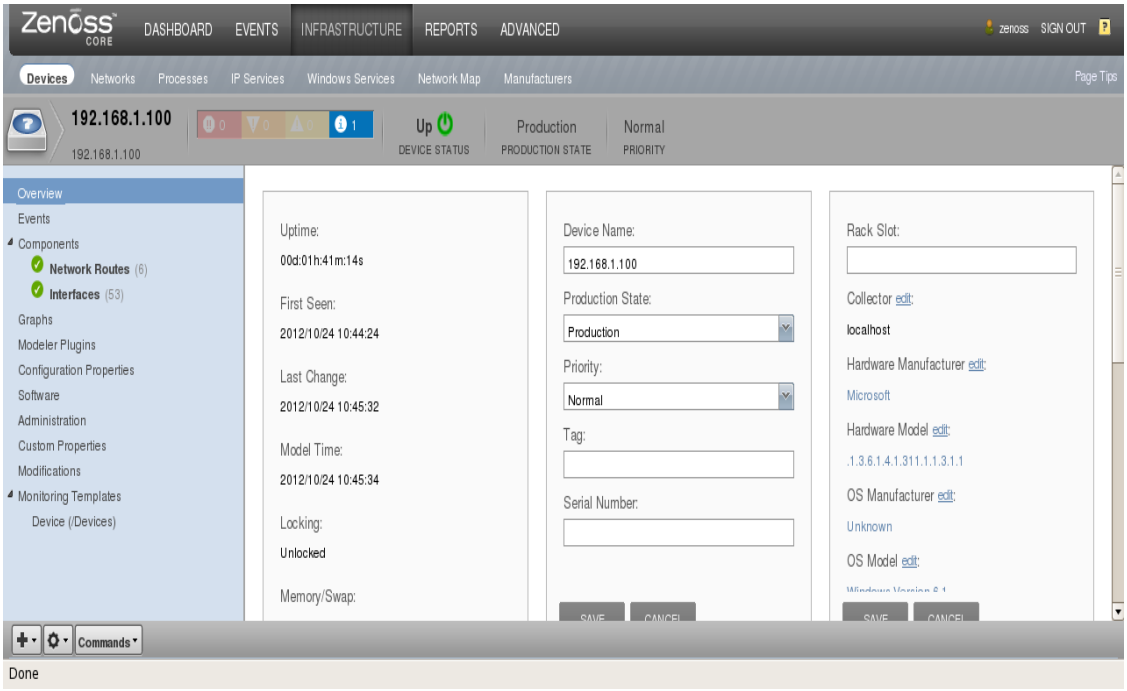


Figura 6.53: Detalles de un único dispositivo Zenoss

Elaborado por: Investigador

El 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 permite acceder a otros puntos de vista de gestión de dispositivos, tales como:

Componentes

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

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

Como se muestra en la figura 6.54

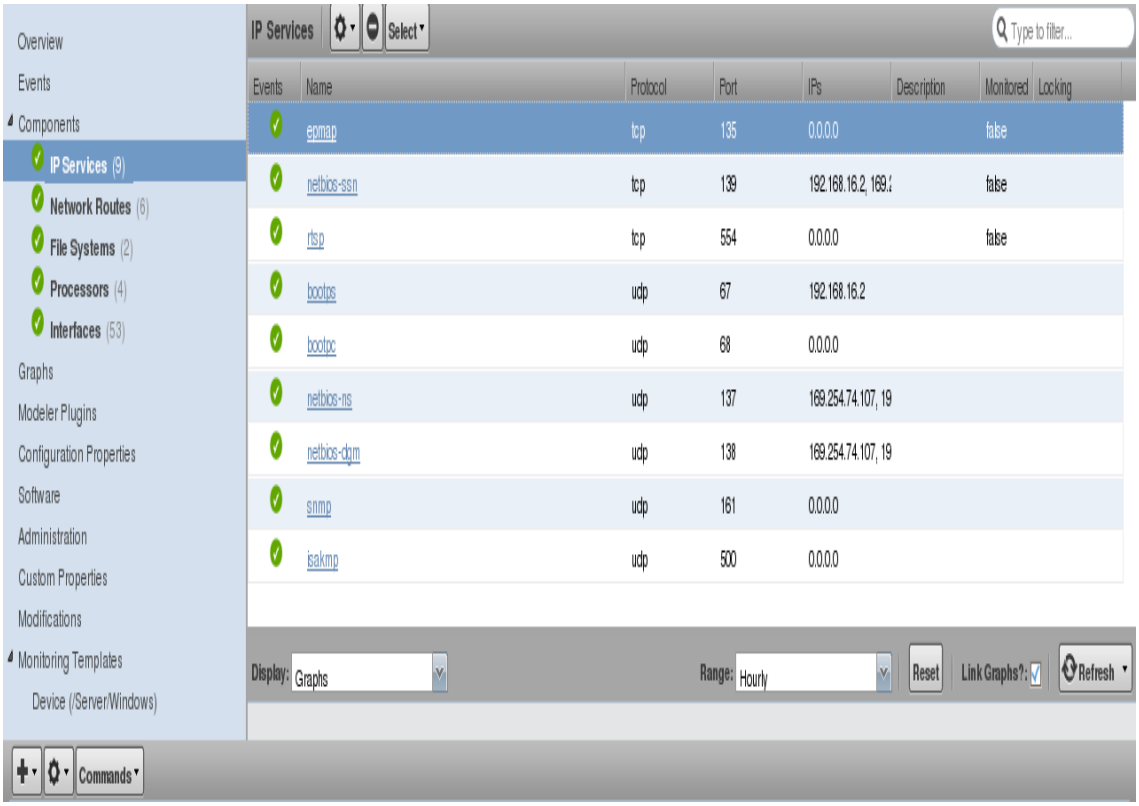


Figura 6.54: Pestaña componentes de un único dispositivo Zenoss

Elaborado por: Investigador

Software

Listas el 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 como se muestra en la figura 6.55.

Figura 6.55: Software de un único dispositivo Zenoss

Elaborado por: Investigador

Gráficos

Muestra los gráficos de rendimiento que se define para el dispositivo como se muestra en la figura 6.56.

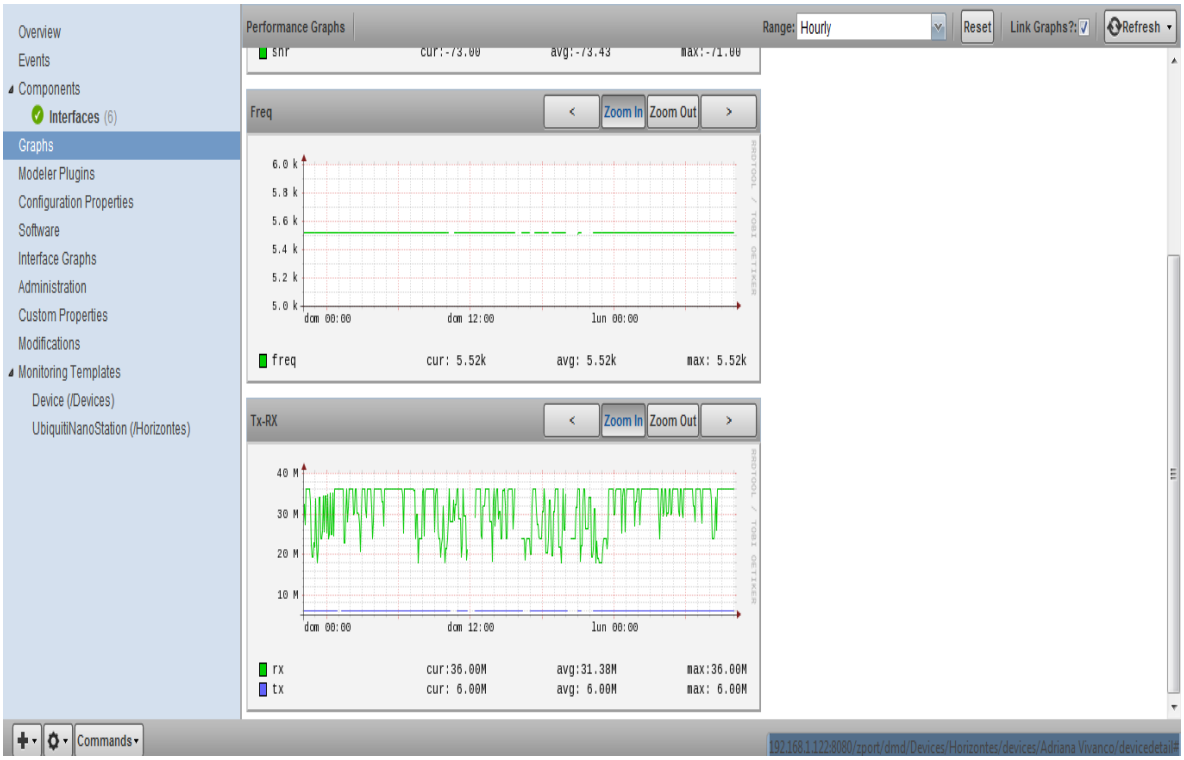


Figura 6.56: Pestaña Gráficos

Elaborado por: Investigador

La opción gráficos presta las opciones donde se 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.

Se puede controlar estas opciones de gráfico de rendimiento:

Rango – se puede seleccionar el período de tiempo que aparece en el gráfico. Se puede seleccionar entre:

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

Administración

En esta opción se puede crear comandos personalizados del usuario y ejecutar comandos.

También se puede configurar la gestión de ventanas de mantenimiento.

Determina que tiene capacidades de administración para el dispositivo, y sus funciones como se muestra en la figura 6.57.

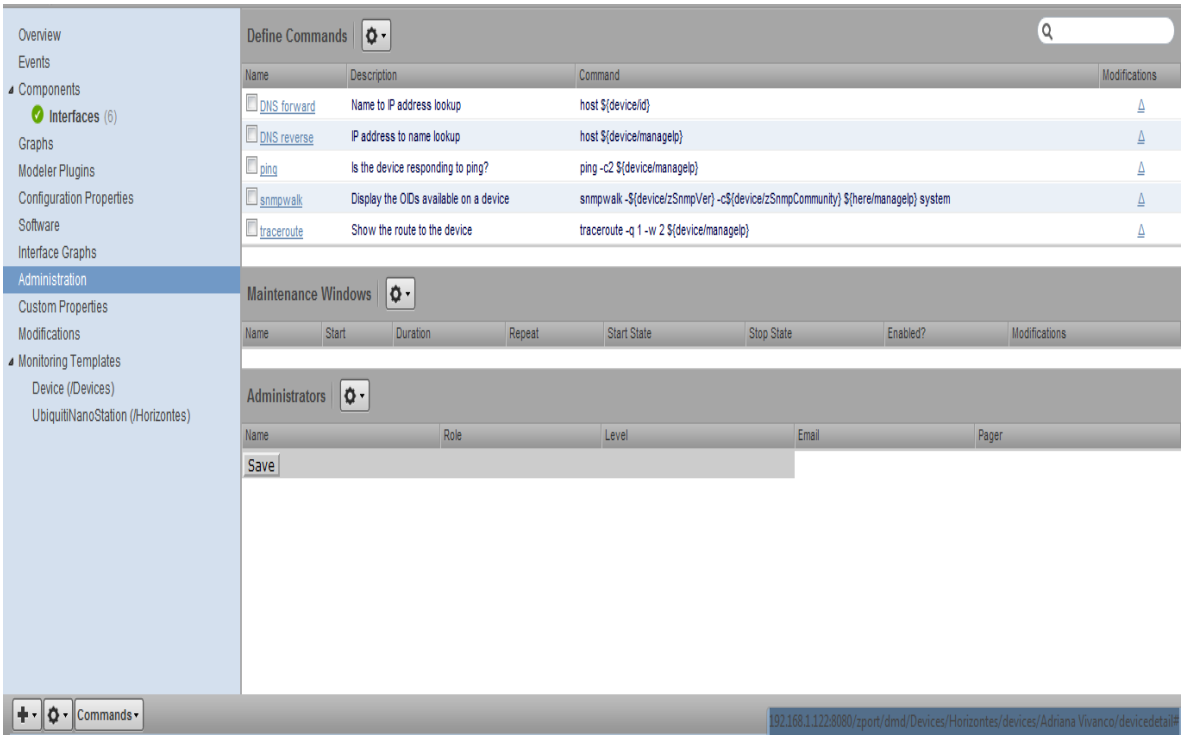


Figura 6.57: Pestaña Administración

Elaborado por: Investigador

Propiedades de configuración

Puede configurar las propiedades de configuración de un dispositivo. Por otra parte, puede eliminar las propiedades locales desde un dispositivo como se muestra en la figura 6.58.

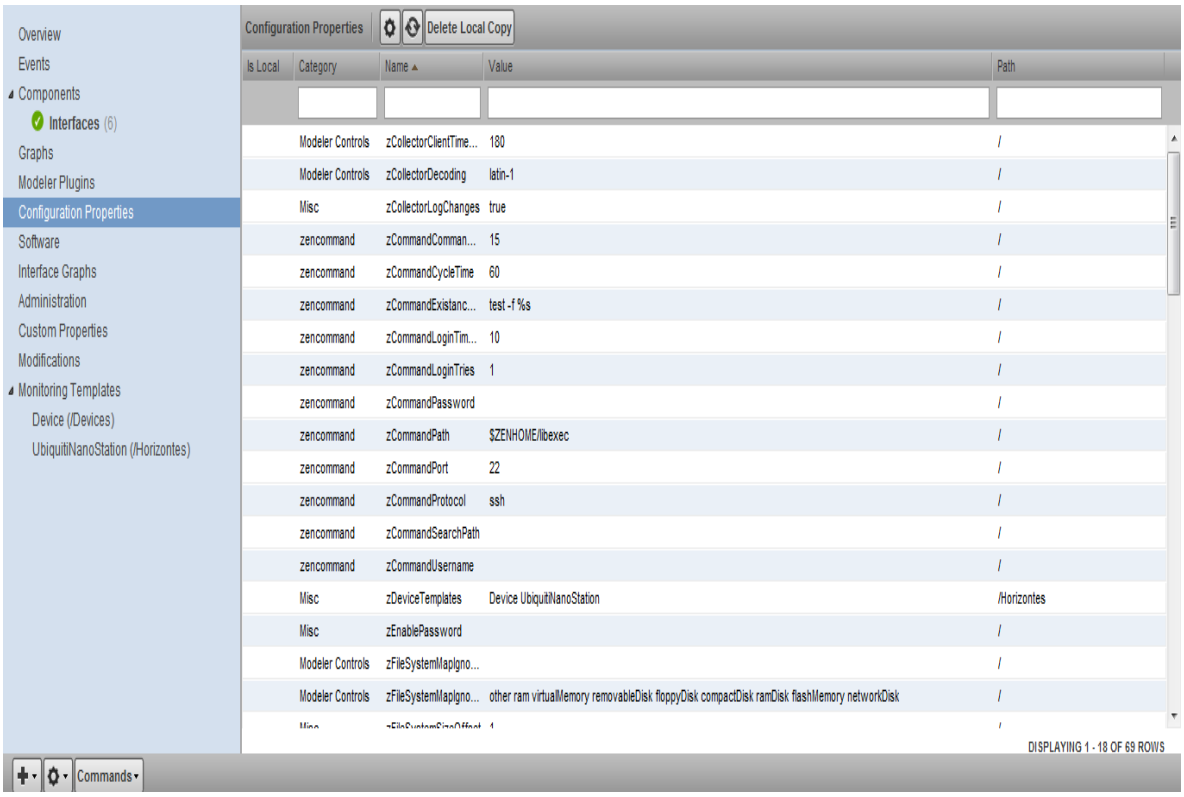


Figura 6.58: Pestaña Propiedades de Configuración

Elaborado por: Investigador

6.6.6.4. Administración de dispositivos y atributos de dispositivos

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.

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 como se puede observar en la figura 6.59.

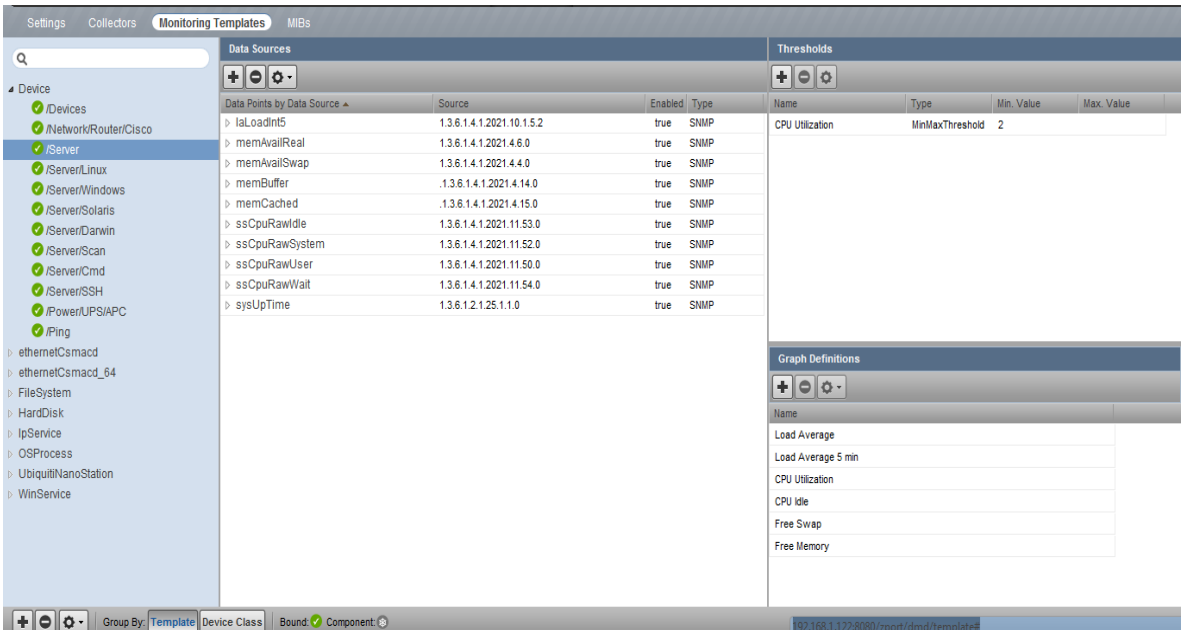


Figura 6.59: Información sobre la supervisión de templates

Elaborado por: Investigador

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:

- En la barra de navegación, se selecciona Infraestructura.
- Se escoge un dispositivo en la lista de dispositivos. Se selecciona Bind Templates.
- Se escoge un template desde la lista habilitada y se mueve al dispositivo

A continuación se tendrá una ventana como la que se muestra en la figura 6.60.

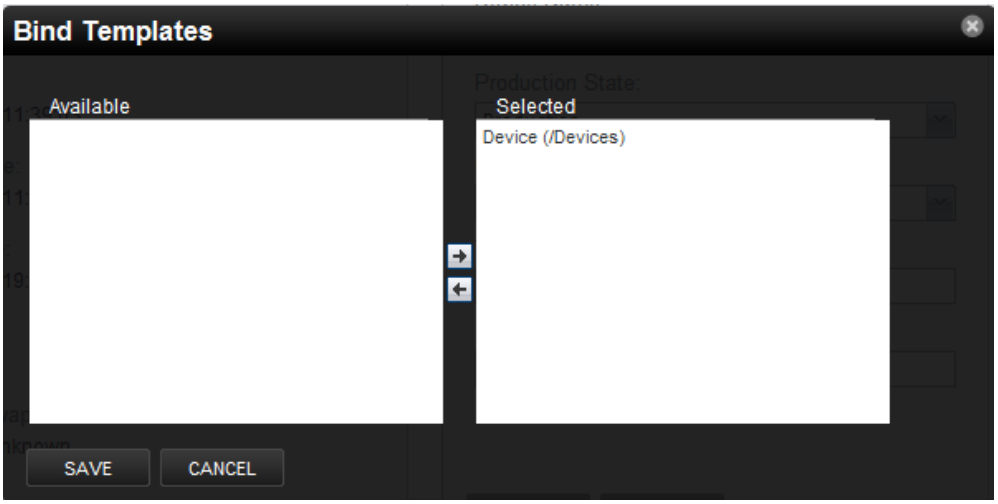


Figura 6.60: Binding templates
Elaborado por: Investigador

Data Sources

En el 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

Para añadir un Data Source se debe hacer lo siguiente:

1. Se selecciona Avanzado en la barra de navegación, a continuación, se escoge Monitoring Templates.
2. En la vista de árbol, se selecciona el Monitoring Template a la que se desea agregar un Data Source.
3. En el área de Data Source, se selecciona (Agregar origen de datos) en el menú Acción.
4. Se sscribe un nombre para el origen de datos y seleccionar el tipo y, a continuación, hacer clic en Enviar.
5. Hacer doble clic en el origen de datos en la lista.
6. Introducir o seleccione los valores para definir el origen de datos.

Se debería tener una ventana similar a la de la figura 6.61.

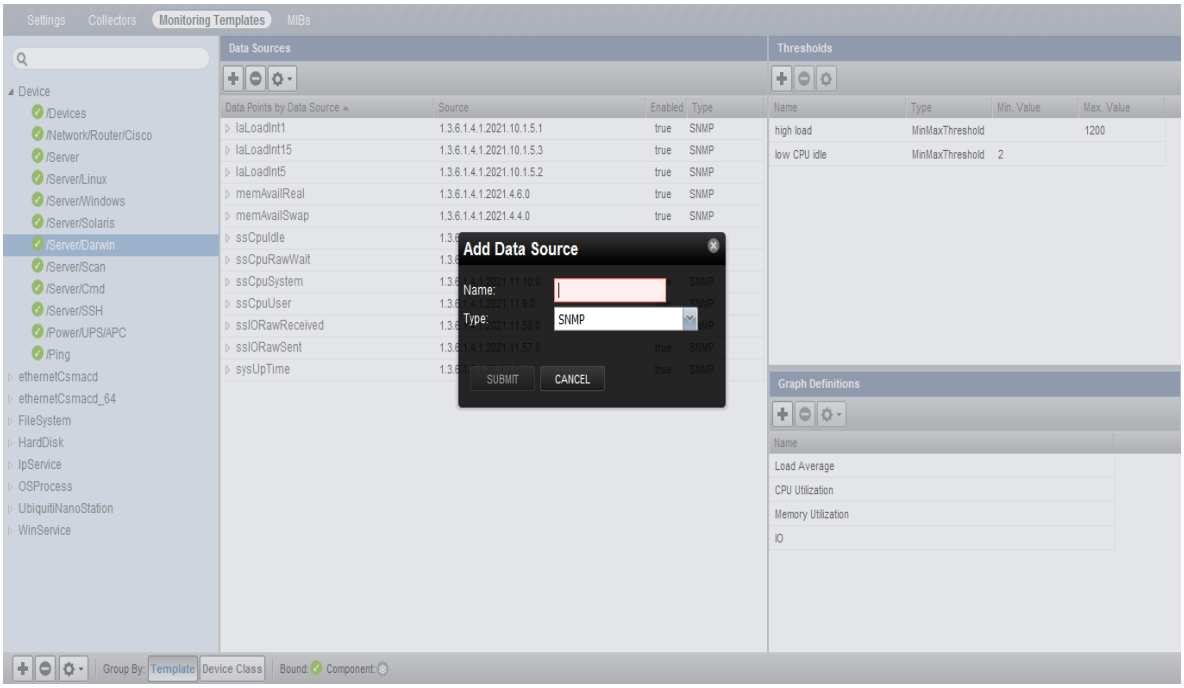


Figura 6.61: Añadir Data Source

Elaborado por: Investigador

Data Points

En el 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)

Para añadir un Data Point se debe hacer lo siguiente:

1. Se selecciona Avanzado en la barra de navegación, a continuación, se escoge Monitoring Template.
2. En el área de Data Sources, se selecciona la fila que contiene un Data
3. Sources.
4. Seleccionar Agregar punto de datos en el menú Acción.
5. Escribir un nombre para el Data Point y, a continuación, hacer clic en Enviar.

6. Hacer doble clic en los datos que acaba de agregar. Introducir la información o hacer selecciones para definir el punto de datos.

Se debería tener una ventana similar a la de la figura 6.62.

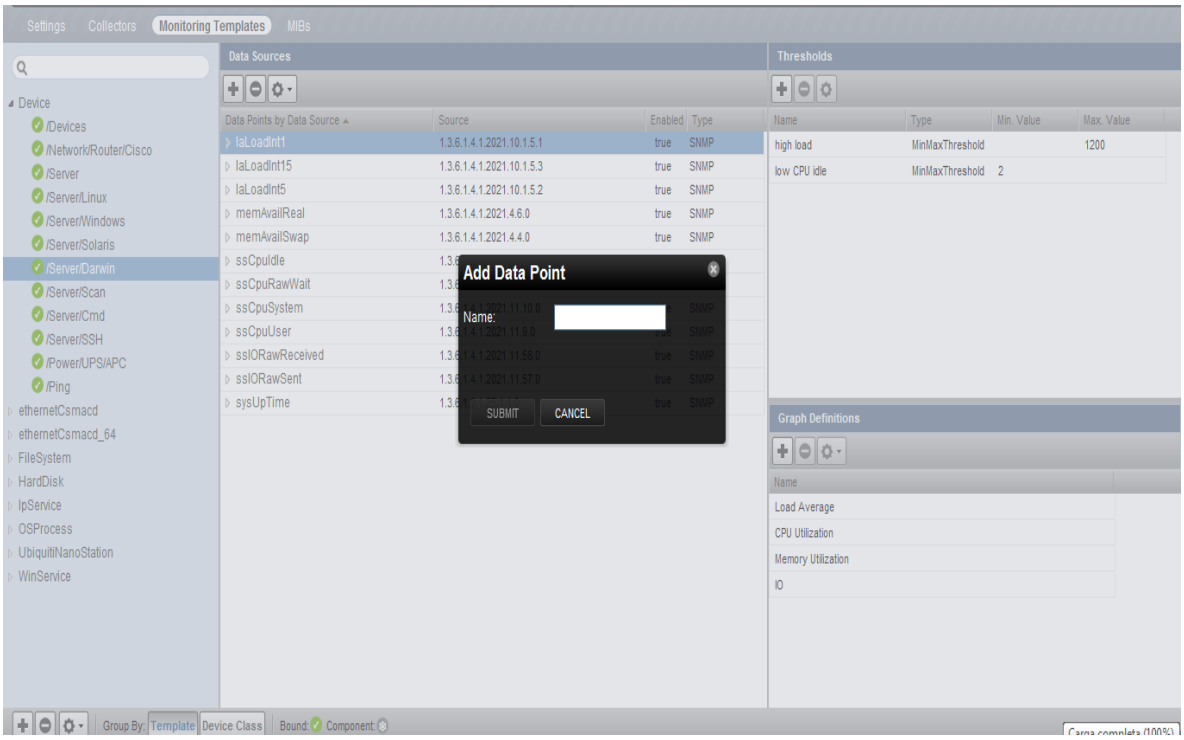


Figura 6.62: Añadir Data Point

Elaborado por: Investigador

Thresholds

En el Threshold 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

Para añadir un Threshold se debe hacer lo siguiente:

1. Seleccionar Avanzado en la barra de navegación, a continuación, se selecciona Plantillas de seguimiento.
2. En la zona de Thresholds, hacer clic en (Añadir).
3. Seleccionar el tipo de Thresholds y escribir un nombre y, a continuación, hacer clic en Agregar.
4. Hacer doble clic en el Thresholds que acaba de agregar en la lista para editar.

Se debería tener una ventana similar a la de la figura 6.63.

Figura 6.63: Edición de Threshold

Elaborado por: Investigador

5. Se ingresa o selecciona 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.-** Seleccionar uno o más puntos de datos a los que este Thresholds se aplicará.
- **Gravedad.-** Seleccionar el nivel de gravedad del primer evento desencadena cuando este Thresholds se rompe.
- **Activado.-** Seleccionar 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 seleccionado 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.-** Seleccionar la clase de evento del evento que se activa cuando este Thresholds se rompe.
- **Escala.-** Introduccir 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.

Para añadir un Gráfico de rendimiento se debe hacer lo siguiente:

1. Seleccionar avanzado en la barra de navegación, a continuación, se selecciona Monitoring Templates.
2. En el área de Grahp Definition, hacer clic en (Ver gráfico).

3. Escribir un nombre para el gráfico y, a continuación, hacer clic en Enviar.
4. Hacer doble clic en el gráfico de la lista para editar. Introducir la información o los valores de selección para definir el gráfico:
    - **Nombre.-** Si se 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.-** Ingresar la altura de la gráfica, en píxeles.
    - **Ancho.-** Ingresar el ancho de la gráfica, en píxeles.
    - **Unidades.-** Ingresar una etiqueta para el eje vertical del gráfico.
    - **Escala logarítmica.-** Seleccionar Verdadero para indicar que la escala del eje vertical es logarítmica. Seleccionar 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.-** Seleccionar si los datos que se gráfica se mide en múltiplos de 1024. De forma predeterminada, este el valor es False.
    - **Min Y.-** Ingresar el valor inferior para el eje vertical del gráfico.
    - **Max Y.-** Ingresar el valor superior para el eje vertical del gráfico.
    - **Resumen.-** Seleccionar True para mostrar un resumen de los datos actuales, la media, y valores máximos en la parte inferior de la gráfica.

Se debería tener una ventana similar a la de la figura 6.64.

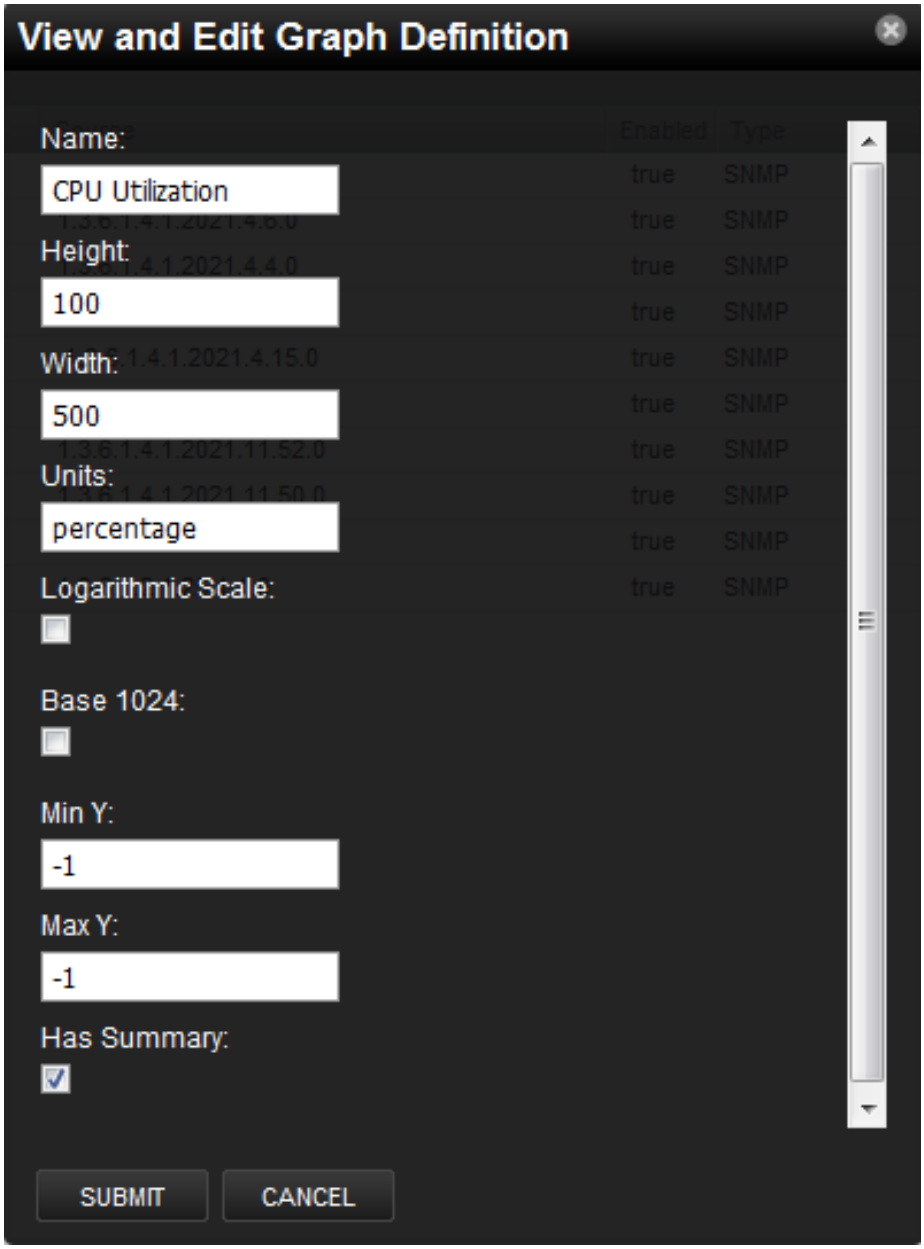


Figura 6.64: Edición de Gráficos de Rendimiento

Elaborado por: Investigador

6.6.6.5. 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.

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

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, seleccionar un comando de la lista de opciones de comandos como se muestra en la figura 6.65.

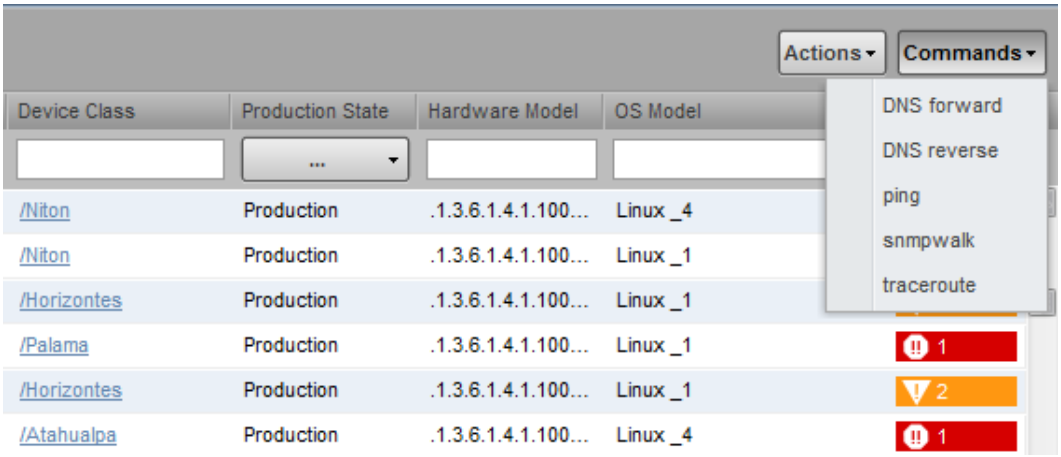


Figura 6.65: Comandos globales de usuario

Elaborado por: Investigador

6.6.6.6. 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.

Creación de cuentas de usuario

Para crear una cuenta de usuario se debe hacer lo siguiente:

1. En la barra de navegación, seleccionar Opciones avanzadas.
2. En el panel izquierdo, seleccionar Usuarios.
3. Desde  (Menú Añadir), seleccionar Agregar nuevo usuario.
4. En el campo Nombre de usuario, introducir un nombre único para la cuenta.

5. En el campo Correo electrónico, escribir la dirección de correo electrónico para la cuenta de usuario. Cualquier alerta que ha configurado para este usuario será enviado a esta dirección.
6. Hacer clic en Aceptar.

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

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, seleccionar los objetos administrados en el panel de la izquierda como se muestra en la figura 6.66.

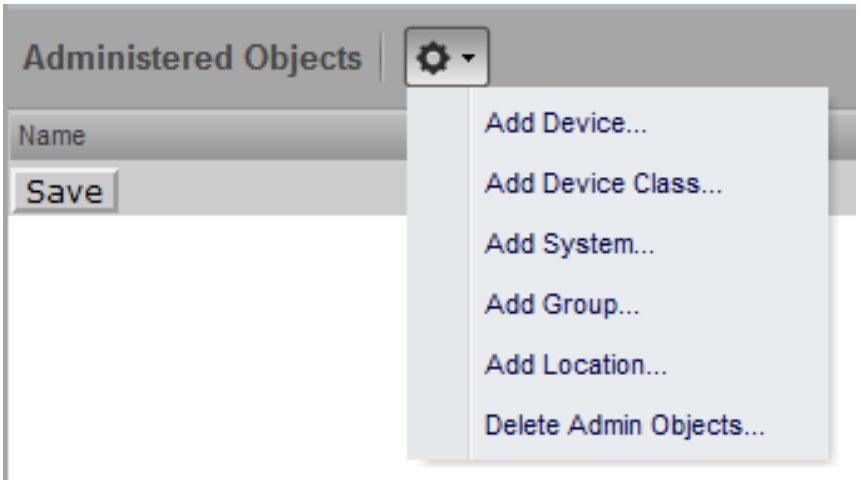


Figura 6.66: Asociación de un objeto a un usuario

Elaborado por: Investigador

2. Seleccionar 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. Hacer clic en Guardar para guardar los cambios.

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

Para crear grupos de usuarios se debe hacer lo siguiente:

1. Seleccionar Avanzado.
2. En el panel izquierdo, seleccionar Usuarios
3. Desde el área de menú Grupos de Acción, seleccionar Agregar nuevo grupo.
4. En el campo de grupo, escribir un nombre para este grupo de usuarios, a continuación, hacer clic en Aceptar.
5. Hacer clic en el nombre del grupo que ha creado.
6. En el menú Acción, seleccionar Agregar usuario.

Se tendrá una ventana como la que se muestra en la figura 6.67

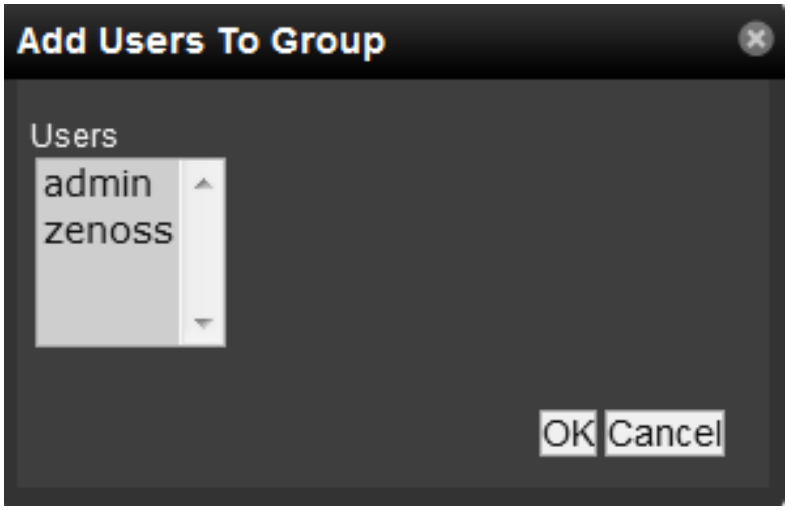


Figura 6.67: Creación de grupos de usuario

Elaborado por: Investigador

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

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

6.6.6.7.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 se debe tener configurado un servidor de correo en la red para poder usarlo como almacenador de correos enviados por Zenoss o en su defecto reenvíen la petición a servidores externos, suponiendo que si se posee el servidor de correos interno, se comienza llenando los campos que hacen referencia a este en la pestaña Settings del panel izquierdo, donde pide la dirección IP del servidor de correo y un nombre para que Zenoss envíe correos a un usuario valido del servidor, una vez configurado guardar los cambios como se muestra en la figura 6.68.

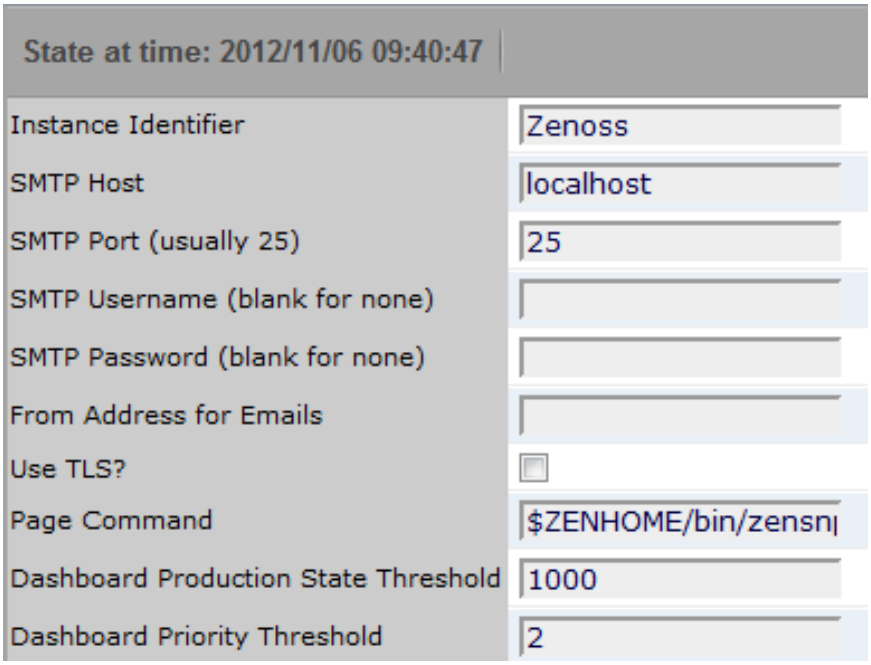


Figura 6.68: Ingreso de datos del servidor de correos

Elaborado por: Investigador

2. En la sección User en esta misma interfaz se ingresa al usuario agregado por omisión admin, Este usuario puede cambiar según la configuración de usuarios administradores.

3. Al ingresar a la consola de este usuario se procede a llenar el formulario según las necesidades, aquí se especifica una dirección e-mail valida en el servidor de correo, a la cual llegara los avisos enviados por Zenoss.

4. Por último hacer el test del correo para verificar que se ha realizado una adecuada configuración, dando clic en test y si todo ha salido bien saldrá un mensaje de test send de lo contrario saldrá test failed con lo cual se deberá revisar los anteriores pasos.

Una vez la prueba resulte exitosa, dar clic sobre el usuario Admin para configurar las alarmas. Después se observa algunas pestañas para configurar la información del administrador, ver eventos y Administrar objetos. A continuación dar click en Alerting Rules y posteriormente en Add Alerting Rule como se muestra en la figura 6.69.

Figura 6.69: Adición de reglas de alertas

Elaborado por: Investigador

Una vez la alerta se encuentre listada, dar click sobre ella, luego presentara tres pestañas. En la pestaña Edit se encuentra 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 se debe configurar algunas reglas, esta configuración es personal y va de acuerdo a las necesidades del administrador. Por último guardar los cambios.
Se debería tener una imagen como la figura 6.70.

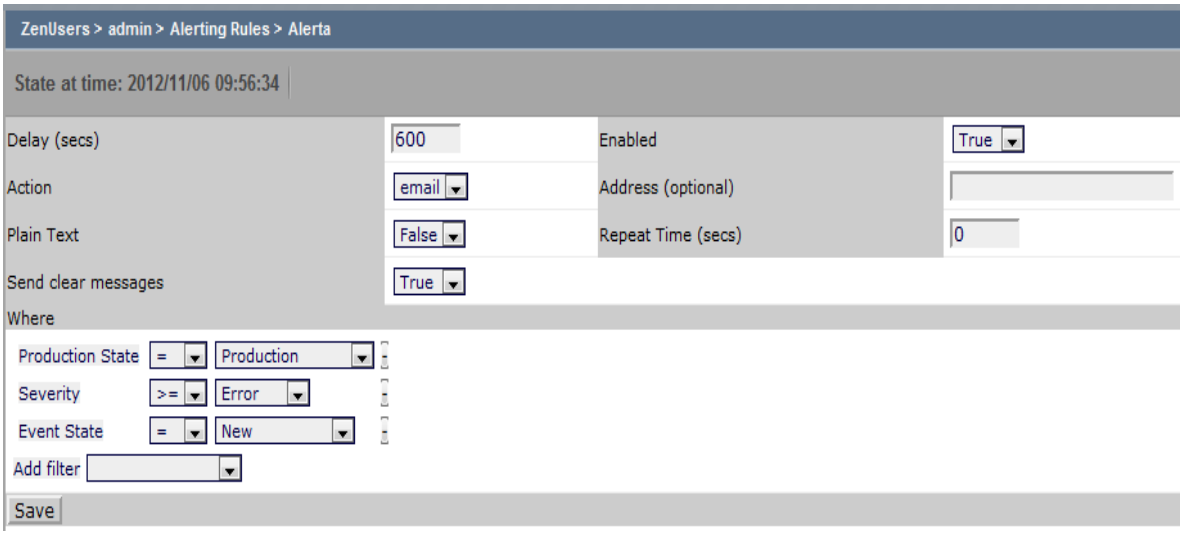


Figura 6.70: Configuración de reglas para alarmas

Elaborado por: Investigador

Mensajes

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

Schedule

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

6.6.6.8.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, seleccionar 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 como se muestra en la figura 6.71.

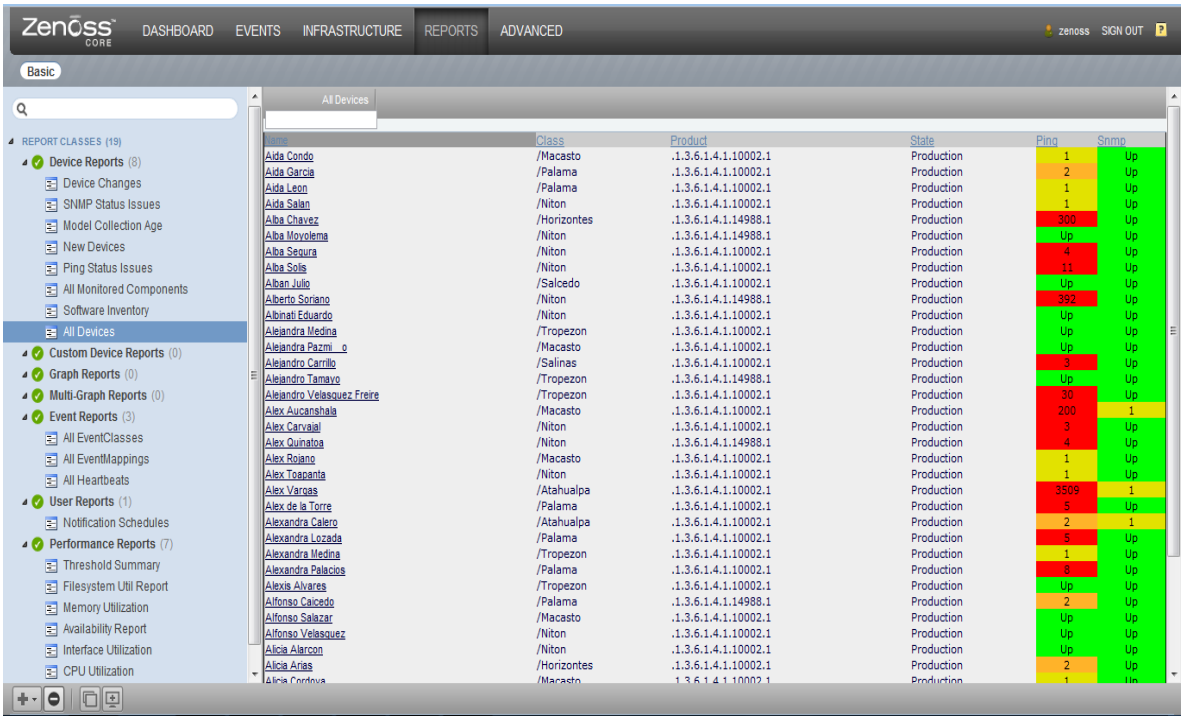


Figura 6.71: Lista de reportes disponibles en Zenoss

Elaborado por: Investigador

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.

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 como se muestra en la figura 6.72.

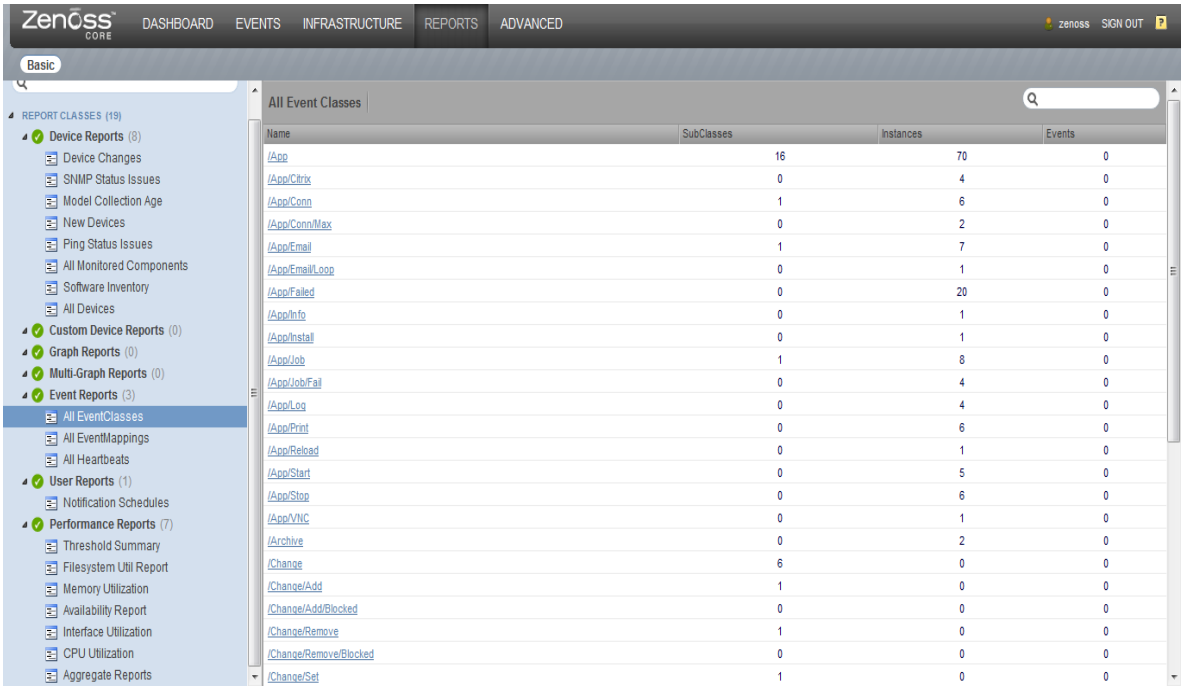


Figura 6.72: Reporte de todas las clases de eventos

Elaborado por: 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 como se muestra en la figura 6.73.

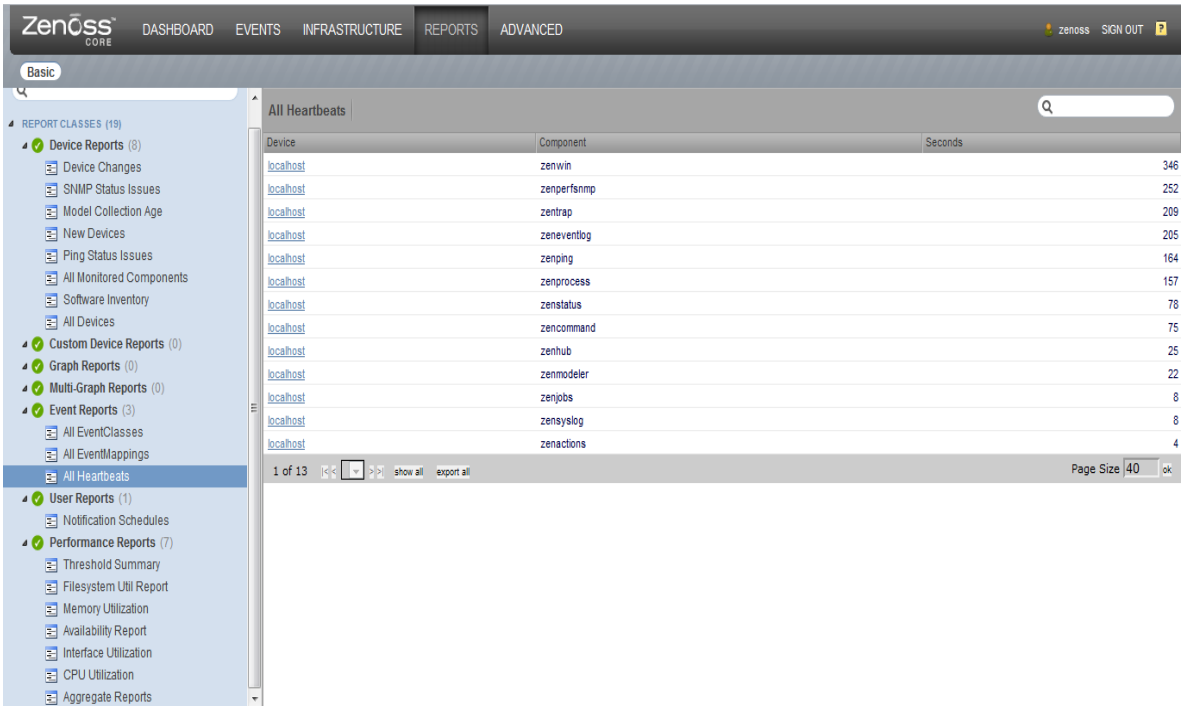


Figura 6.73: Reporte de todas los estados de los demonios

Elaborado por: Investigador

- Todas las asignaciones de eventos.- Muestra todas las asignaciones de eventos definidos actualmente en el sistema de Zenoss como se muestra en la figura 6.74.

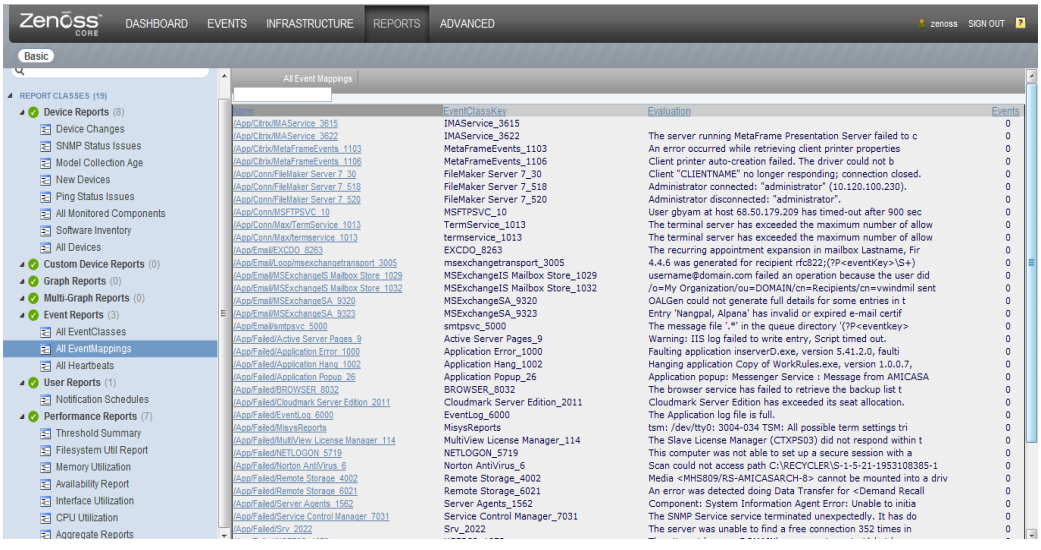


Figura 6.74: Reporte de asignación de eventos

Elaborado por: Investigador

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

Hacer clic en la gráfica para editar los parámetros de gráfico. Se 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

Se tendrá una ventana como la que se muestra en la figura 6.75

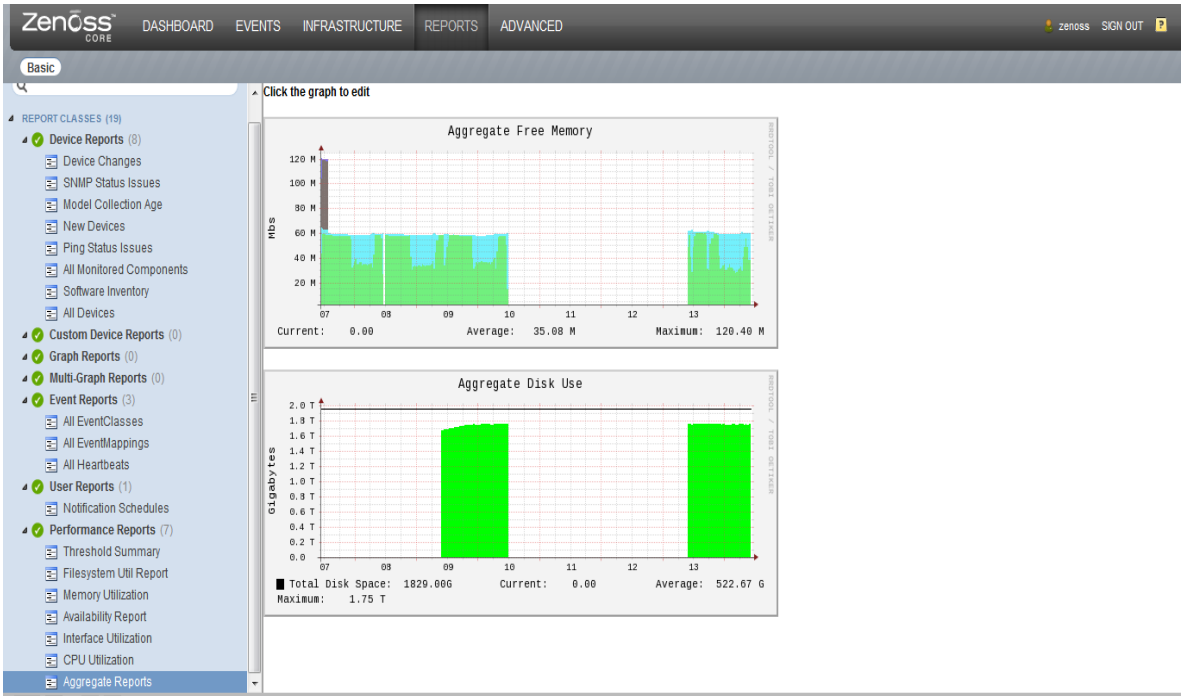


Figura 6.75: Reportes Gráficos

Elaborado por: 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 da el porcentaje de disponibilidad de los últimos siete días para la clase de evento Status/Ping con un nivel de severidad de error.

Se puede cambiar los criterios de presentación de informes sobre la base que se muestra en la tabla 6.13:

Tabla 6.13: Criterios de presentación de Informes

Filtro	Descripción
Dispositivo	Se escribe un nombre de dispositivo para limitar el informe a un solo dispositivo.
Componente	Se escribe 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	Se especifica el primer día del informe.
Fecha de Finalización	Se especifica el último día del informe.
Clase de Evento	Se selecciona el tipo de evento para informar. Por ejemplo: / Status / SNMP.
Severidad	Se selecciona la gravedad de los eventos de utilizar en el cálculo de disponibilidad

Elaborado por: Investigador

Una vez introducidos los criterios del reporte, se puede hacer clic en el botón Actualizar para ver el nuevo informe como se muestra en la figura 6.76.

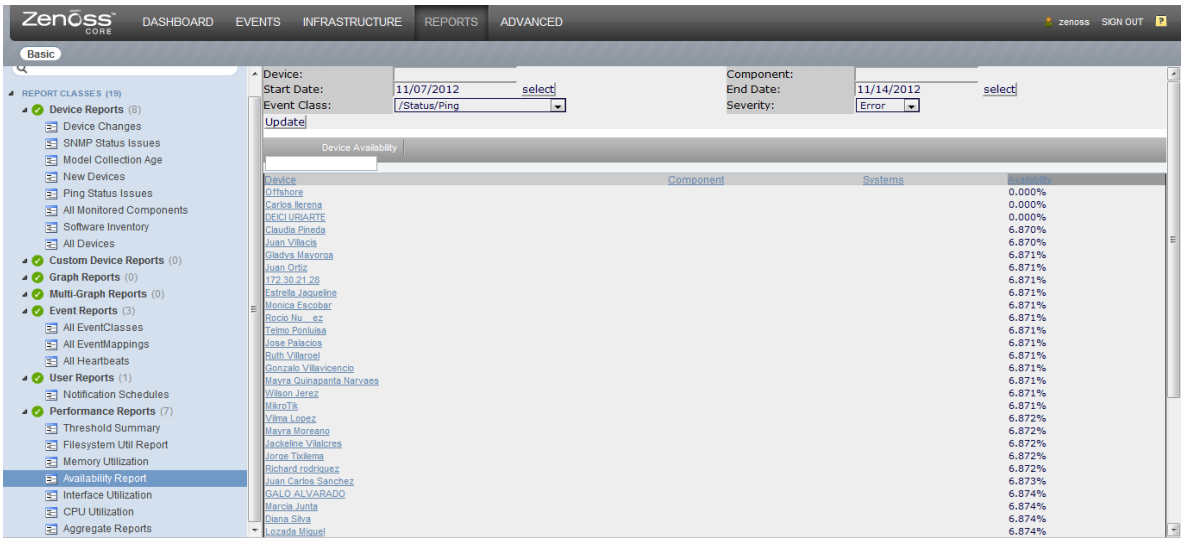


Figura 6.76: Reporte de disponibilidad

Elaborado por: Investigador

Reporte 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". Se puede personalizar fechas de inicio y fin, y el tipo de resumen media o máxima.

Se tendrá una ventana como la que se muestra en la figura 6.77

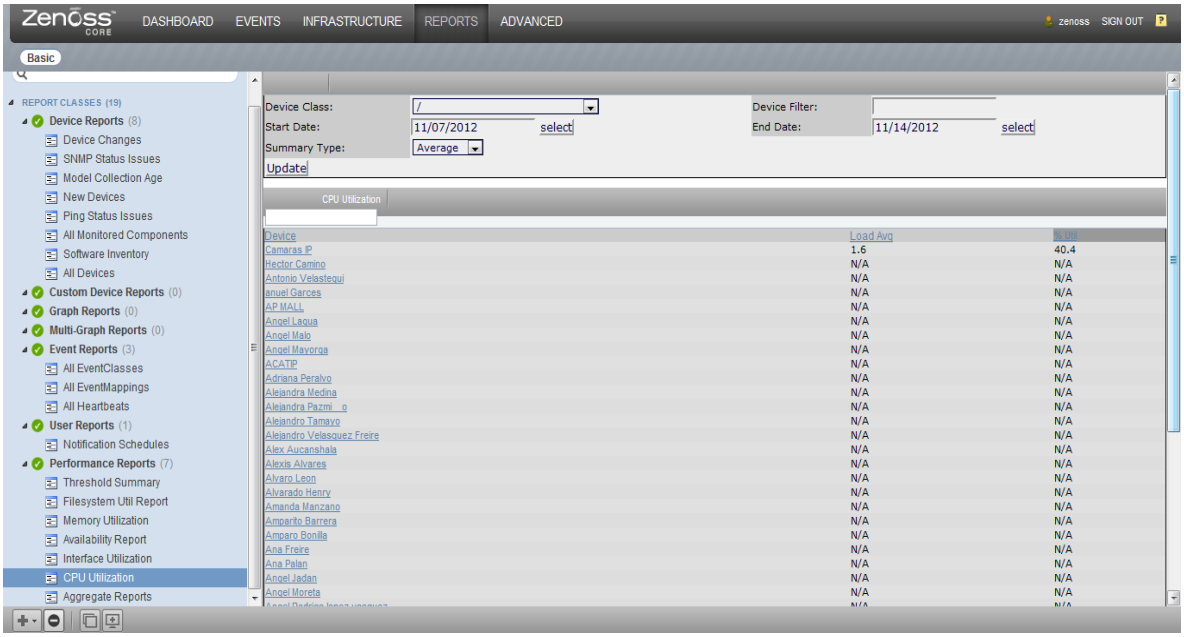


Figura 6.77: Reporte de Utilización de CPU

Elaborado por: 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. Se 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".

Se tendrá una ventana como la que se muestra en la figura 6.78

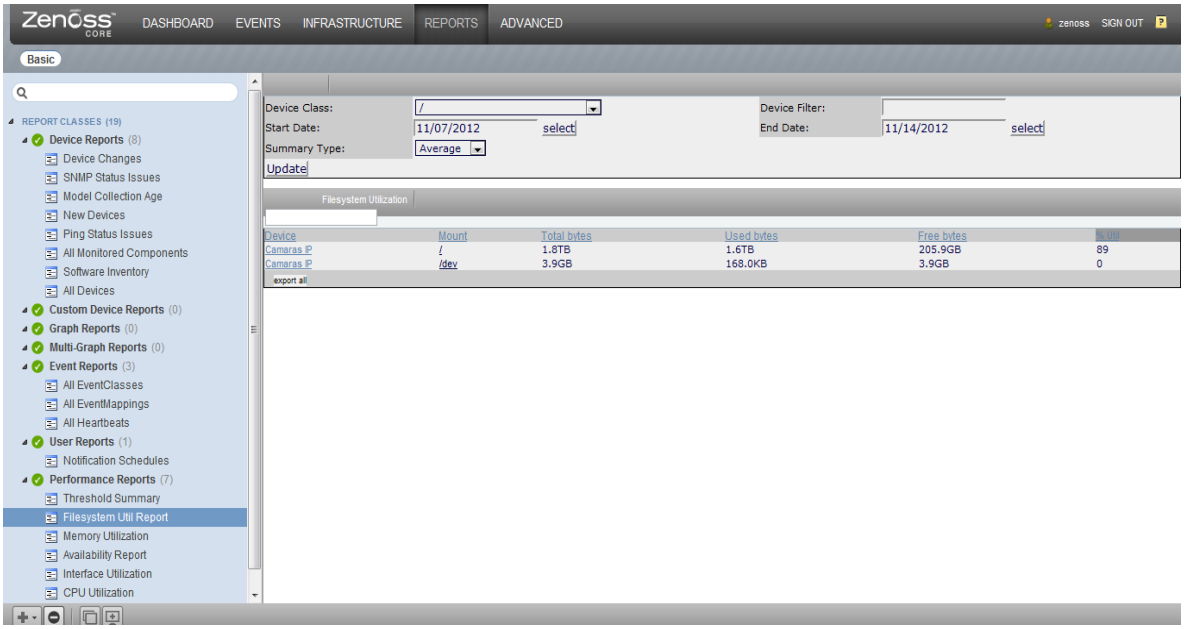


Figura 6.78: Reporte de Utilización de los archivos del sistema

Elaborado por: 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.

Se tendrá una ventana como la que se muestra en la figura 6.79

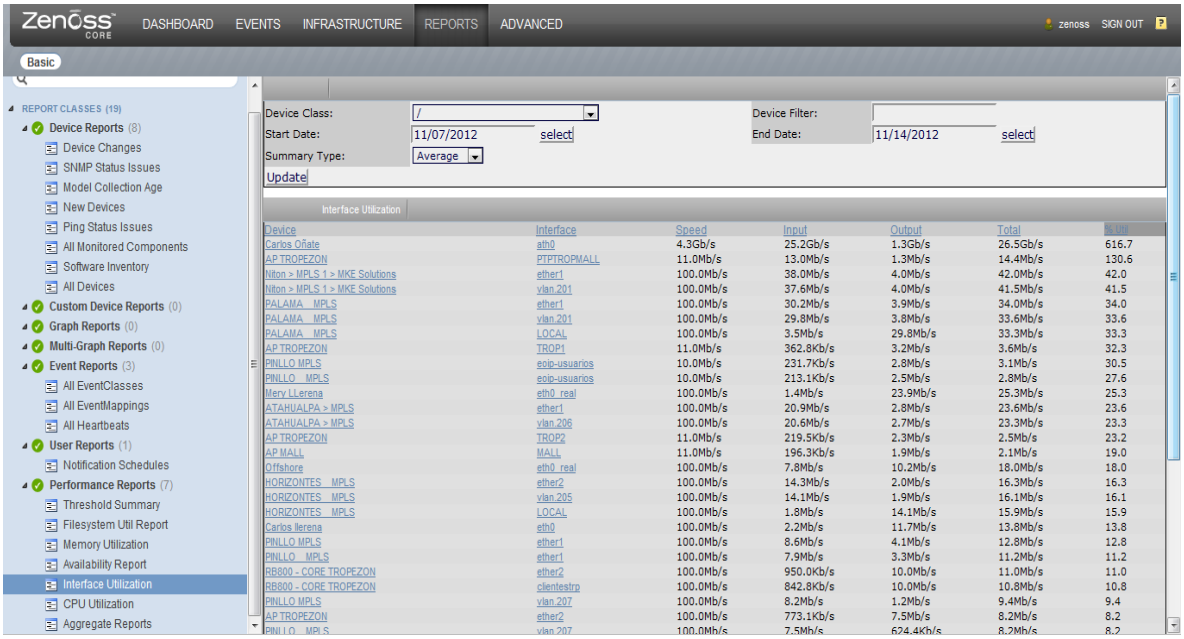


Figura 6.79: Reporte de Utilización de la interfaz

Elaborado por: 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.

Se tendrá una ventana como la que se muestra en la figura 6.80

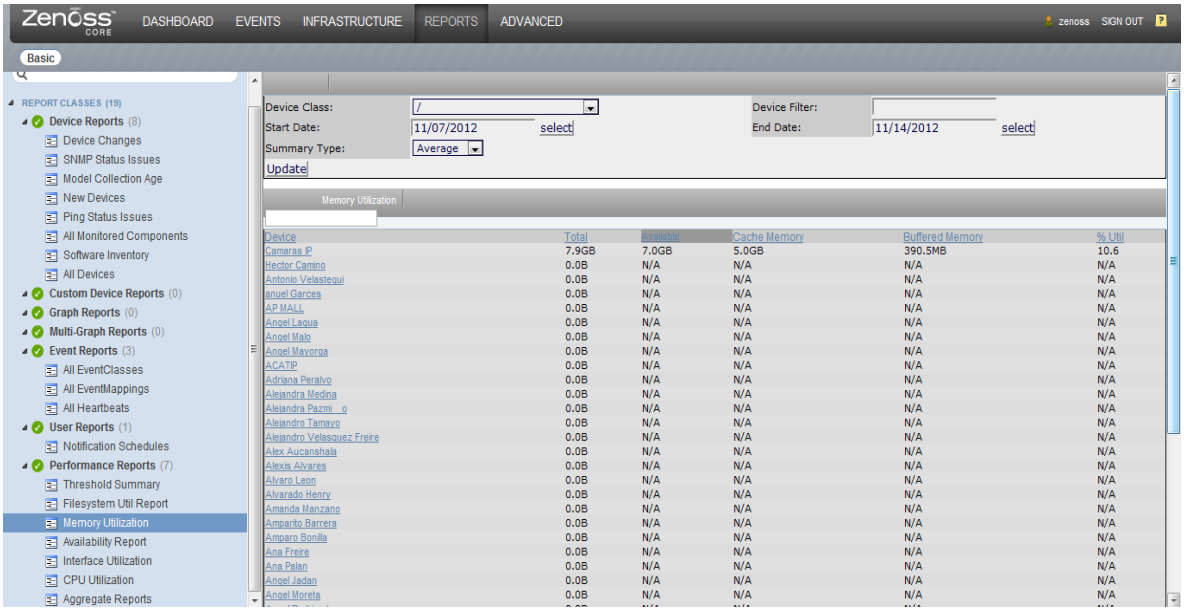


Figura 6.80: Reporte de Uso de Memoria

Elaborado por: Investigador

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

Se tendrá una ventana como la que se muestra en la figura 6.81

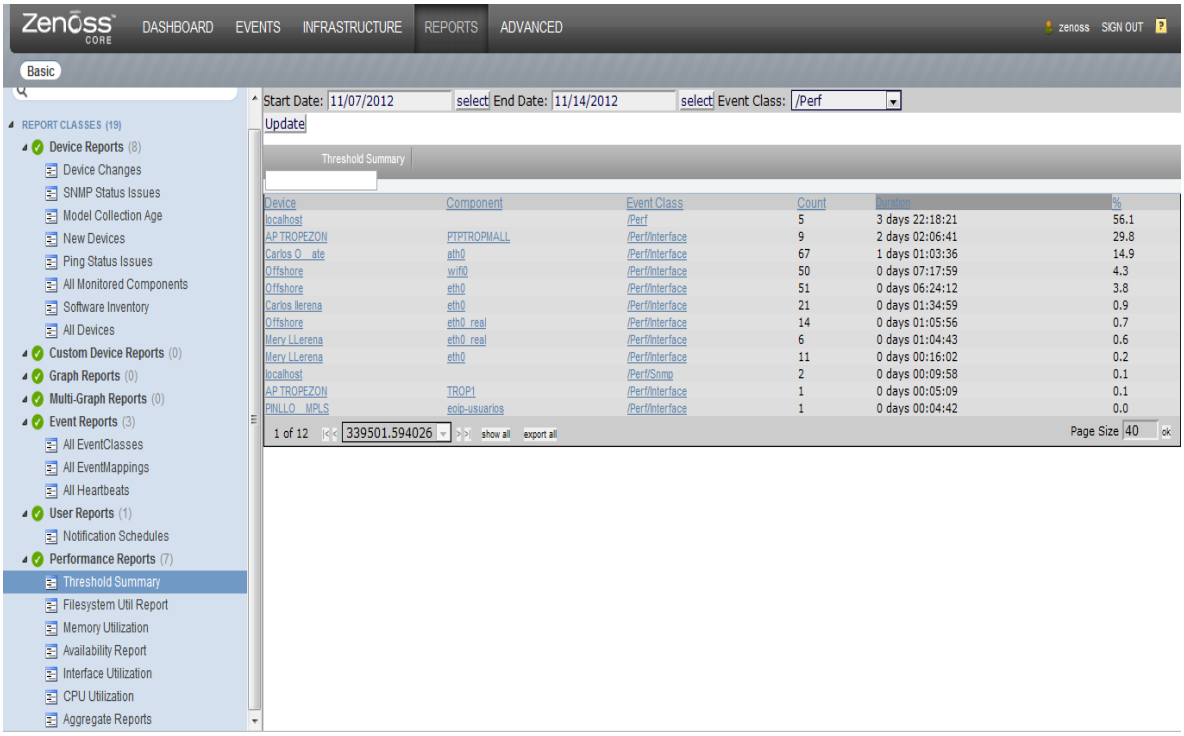


Figura 6.81: Reporte de resumen de threshold

Elaborado por: 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.

Se tendrá una ventana como la que se muestra en la figura 6.82

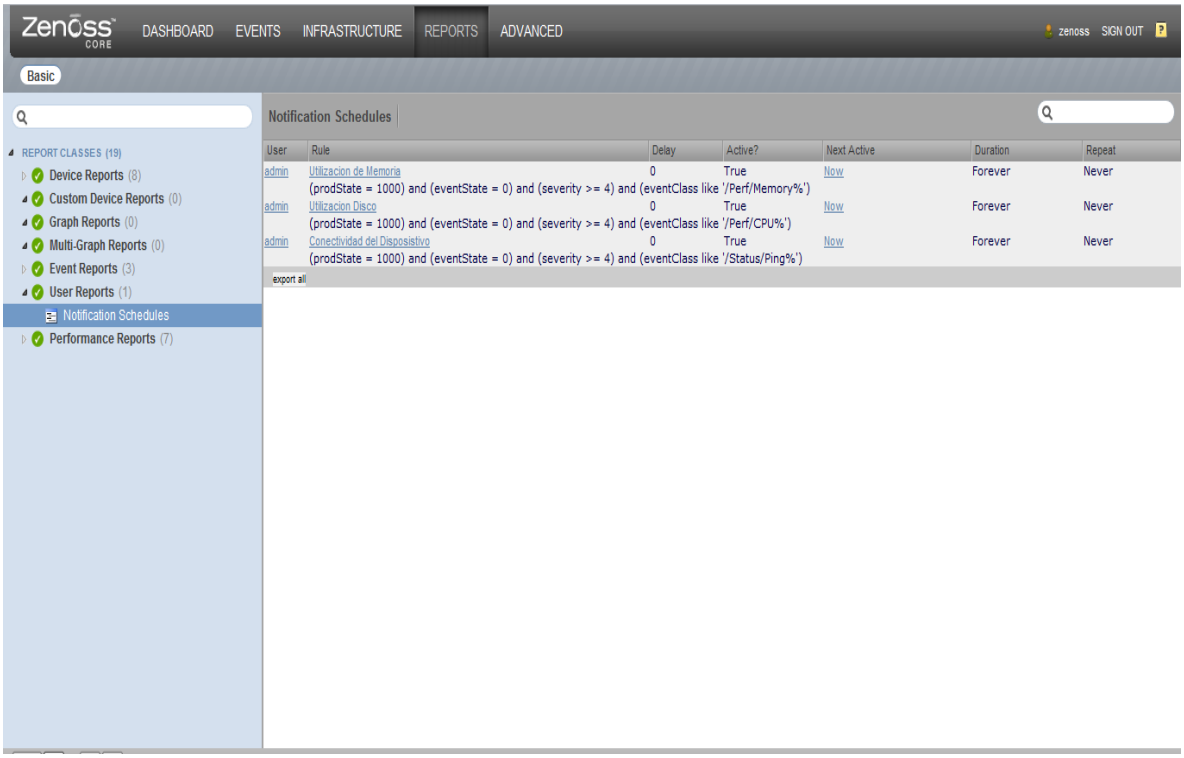


Figura 6.82: Reporte de notificación de horarios a usuarios

Elaborado por: Investigador

6.6.6.9. 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

Para poder crear reportes gráficos se debe seguir los siguientes pasos que se muestran a continuación:

1. En la vista del árbol, se selecciona Añadir Reporte Gráfico de (Menú  Añadir).
2. En el cuadro de diálogo de Crear reporte Gráfico, ingresar un nombre para el reporte y click en Submit.

3. La página de edición del reporte gráfico aparece:

   Ingresar 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.

Como se Muestra en la figura 6.83

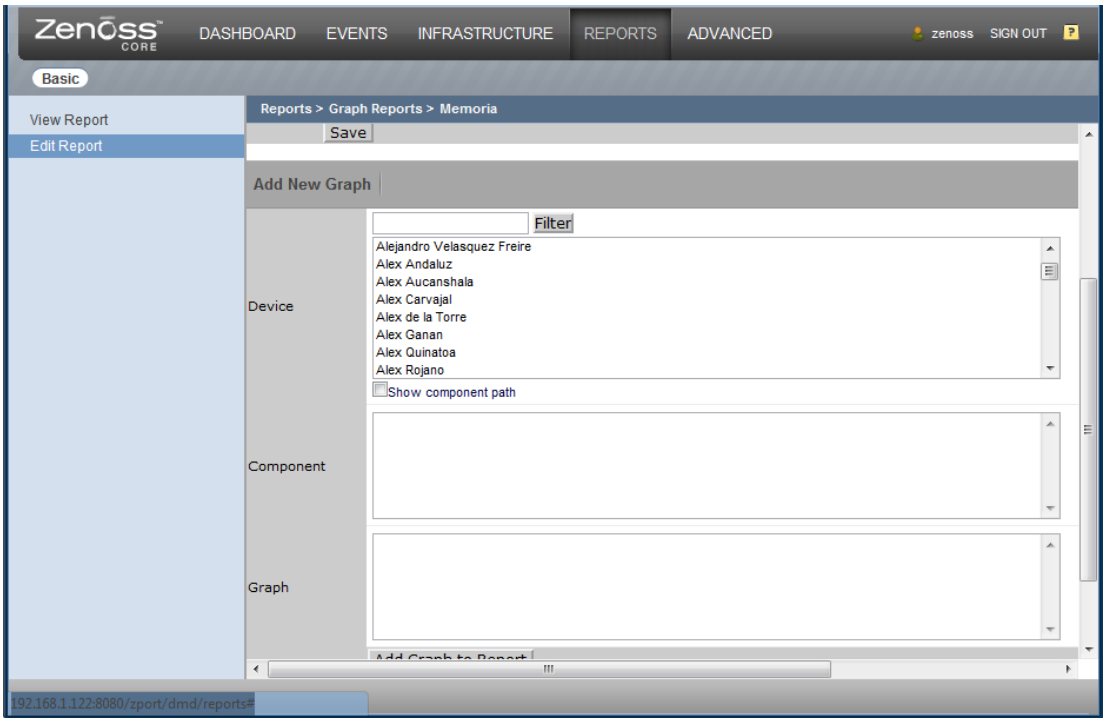


Figura 6.83: Página de edición de Reporte Gráfico

Elaborado por: Investigador

Añadiendo Gráficos

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

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

Como se muestra en la figura 6.84

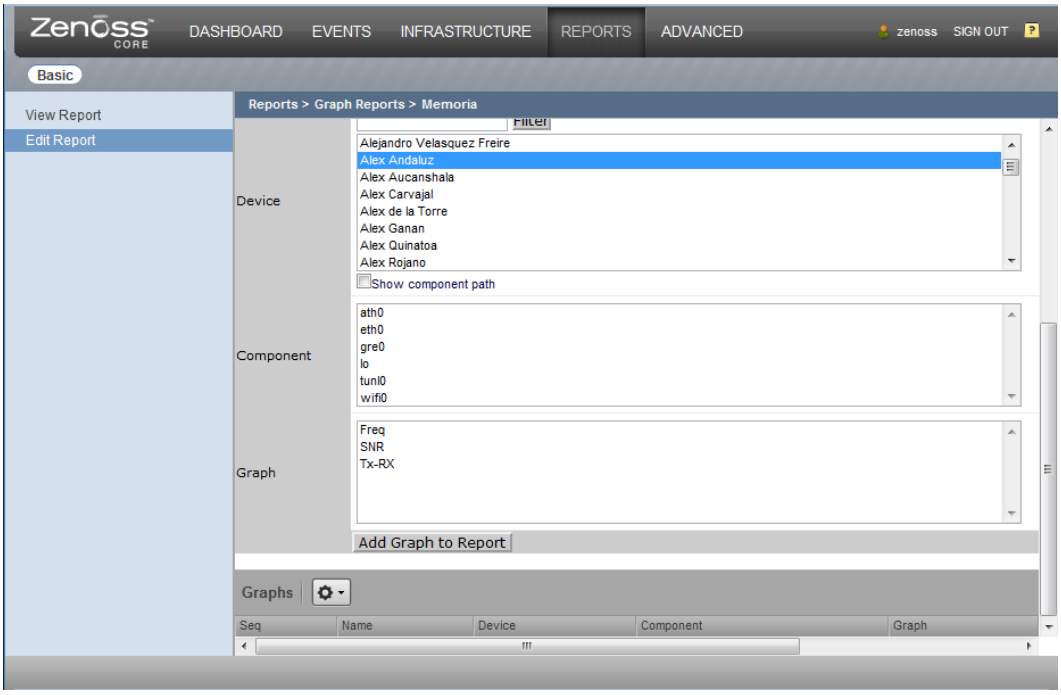


Figura 6.84: Añadir nuevo gráfico a un reporte

Elaborado por: Investigador

A la final tendremos una ventana como se muestra en la figura 6.85 donde se muestra el tráfico de la interfaz del dispositivo como es porcentaje, bytes/seg, etc.

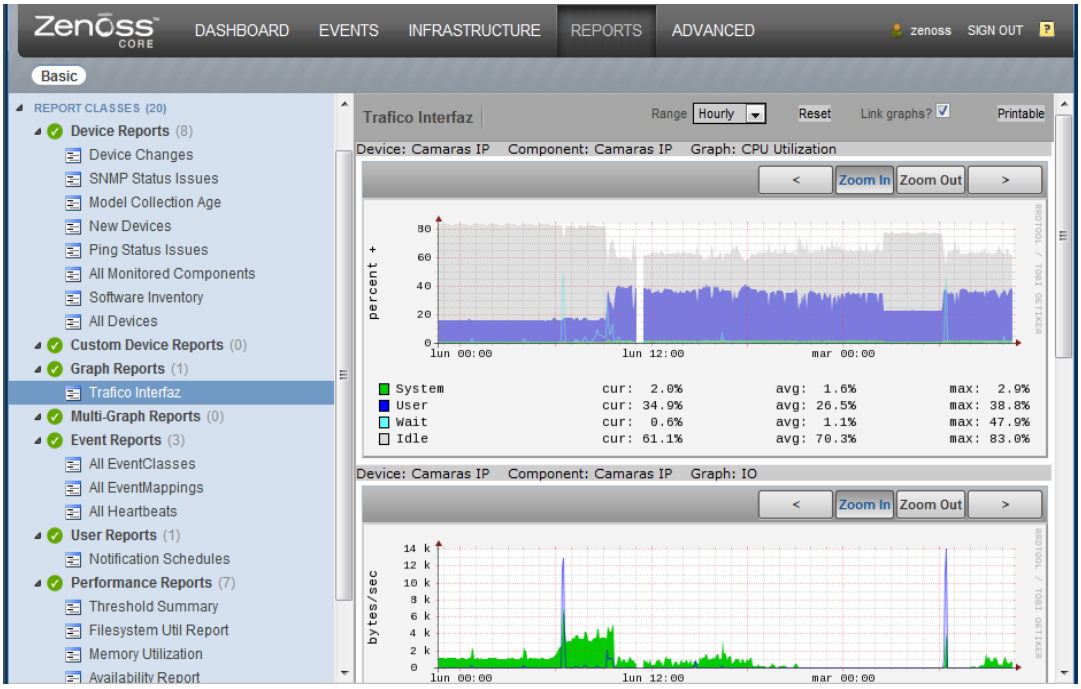


Figura 6.85: Reporte Gráfico

Elaborado por: Investigador

6.6.6.10. 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.

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, seleccionar Opciones avanzadas.
2. En el panel izquierdo, seleccionar 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. Hacer clic en Crear copia de seguridad.

Como se muestra en la figura 6.86

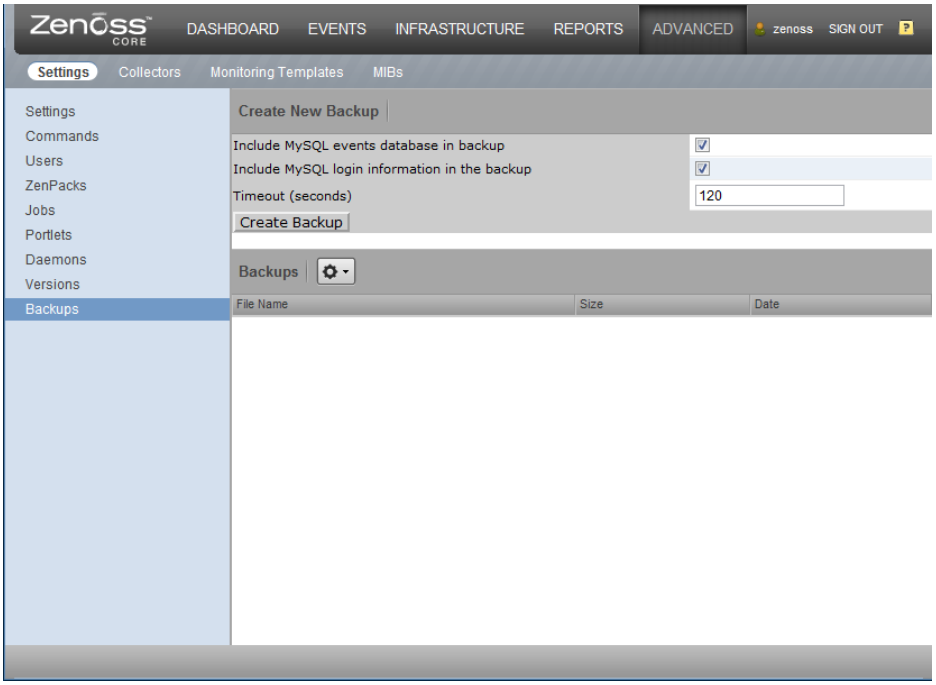


Figura 6.86: Creación de copias de seguridad

Elaborado por: Investigador

Crear copia de seguridad (Comandos)

Para crear la copia de seguridad, se ejecuta 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

Eliminar una copia de seguridad

Para eliminar una copia de seguridad de la interfaz:

1. En la barra de navegación, seleccionar Opciones avanzadas.
2. En el panel izquierdo, seleccionar copias de seguridad.
3. Seleccionar uno o más archivos en la lista y, a continuación, seleccionar Eliminar copia de seguridad en el menú Acción.
4. Hacer clic en Eliminar en el cuadro de diálogo Eliminar copia de seguridad para confirmar la acción.

Restaurar copia de seguridad (zenrestore)

Para restaurar una copia de seguridad hacer lo siguiente:

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

6.6.6.11. 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.

Ítems monitorizados

Los ítems monitorizados con Zenoss en la empresa Speedy son las siguientes:

- SysUptime
- CPU
- Memoria libre
- Memoria Utilizada
- Paquetes enviados y recibidos
- Errores
- Utilización
- Espacio en el Disco
- Bytes de entrada y Salida
- Estado del Ping
- Estado de SNMP

Estos ítems monitorizados se los tendrá en cuanta para todos los dispositivos de la red de la empresa Speedy en especial de sus usuarios para un mejor monitoreo y administración de los mismos.

En la figura 6.87 se observa los ítems monitorizados listados anteriormente del dispositivo de un usuario de la empresa Speedy tomando en cuenta que será similar a la de sus demás usuarios llegando así a lo requerido por la empresa.

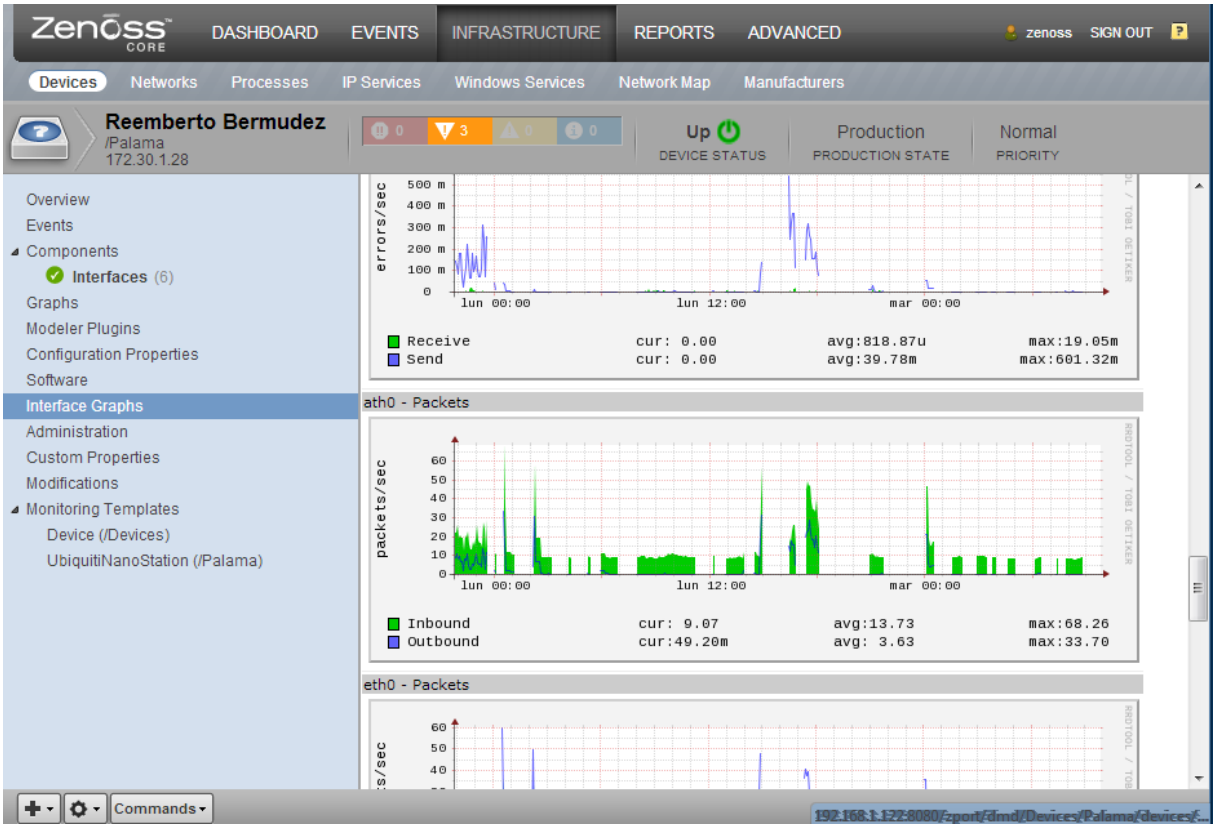


Figura 6.87: Monitoreo de usuario Speedy

Elaborado por: Investigador

6.6.6.12. Resultados obtenidos

Una vez introducidos y categorizados los equipos que conforman la infraestructura de red de la empresa proveedora de internet Speedy en la herramienta de administración y monitoreo ZENOSS, se procede a realizar la monitorización. En esta parte se debe 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.

6.7. Análisis Económico del Proyecto

El análisis económico de Herramienta opensource de administración y Monitoreo basado en snmp para el mejoramiento del funcionamiento de la red en SPEEDY COM CIA LTDA, se realizó en función al monitoreo descrito anteriormente.

6.7.1. Presupuesto de gastos

El presupuesto económico permite determinar cuál es el costo de implementación para la Herramienta opensource de administración y Monitoreo basado en snmp para el mejoramiento del funcionamiento de la red en SPEEDY COM CIA LTDA, y el costo de cada uno de los materiales necesarios.

El servidor utilizado es el Servidor Dell power Edge 1950 debido a sus características, ya que está activo las 24 horas, monitoreando constantemente todos los días y porque la red de Speedy está en un constante crecimiento en sus usuarios. Sus características se las puede observar en el ANEXO C.

El presupuesto necesario para la implementación de la herramienta de administración y monitoreo se puede observar en la Tabla 6.14, costo que fue asumido en su totalidad por la empresa, al ser la principal beneficiaria con el proyecto.

Tabla 6.14: Presupuesto de Gastos de la Implementación

Ítem	Detalle	Unidad	Cantidad	Precio Unitario	Subtotal
1	Servidor Dell power Edge 1950	c/u	1	$ 1.500,00	$ 1.500,00
2	Memoria RAM 8Gb	c/u	2	$ 381,00	$ 762,00
3	Patch cord de 7 pulgadas	c/u	2	$ 15,00	$ 30,00
				TOTAL	$ 2.292,00

Elaborado por: Investigador

En la Tabla 6.15 se puede observar en detalle el costo de mano de obra para realizar la implementación de la Herramienta opensource de administración y Monitoreo basado en snmp para el mejoramiento del funcionamiento de la red en SPEEDY COM CIA LTDA.

Tabla 6.15: Costo de Mano de Obra

Ítem	Descripción	Horas/Hombre
1	Montado del servidor	2
2	Instalación de Zenoss	3
3	Configuración de Zenoss	3
4	Configuración de equipos	3
5	Migración de usuarios a Zenoss	72
6	Pruebas de Monitoreo	5
	TOTAL	88

Elaborado por: Investigador

6.7.2. Análisis de Recuperación de Inversión

Para poder realizar el análisis costo beneficio del presente proyecto de investigación se tomaran datos de la Empres Speedy COM, en la misma se indica que la empresa cuenta con 2500 usuarios en la provincia de Tungurahua. Adicionalmente se cuenta con los siguientes datos de relevancia los mismos se indican a continuación.

Un técnico realiza un promedio de 120 visitas por mes con un costo operativo de $9.11 por cada visita técnica, este valor cubre gastos de movilización y materiales necesarios para realizar las reparaciones respectivas.

Para realizar el análisis se tomó una muestra de 50 clientes de la empresa Speedy COM.

En la Tabla 6.16 se puede observar los gastos operativos de visitas técnicas, estos valores se obtuvo a partir de la muestra antes mencionada.

Tabla 6.16: Costo de visitas técnicas Mensuales de la Empresa

Ítem	Detalle	Unidad	Cantidad	Precio Unitario	Subtotal
1	Visitas Técnicas	c/u	50	$ 9,11	$ 455,50
				TOTAL	$ 455,50

Elaborado por: Investigador

En la Tabla 6.17 se puede observar el resumen del gasto de implementación para los 50 usuarios de muestra.

Tabla 6.17: Gastos de Implementación

Ítem	Detalle	Unidad	Cantidad	Precio Unitario	Costo Total
1	Gastos de la Implementación	c/u	1	$ 2.292,00	$ 2.292,00
2	Costo de Mano de Obra	h/H	88	$ 5,00	$ 440,00
				Subtotal	$ 2.732,00
				Imprevistos (5%)	$ 136,60
				TOTAL	$ 2.868,60

Elaborado por: Investigador

Como se puede observar en la Tabla 6.17 el gasto total necesario para la implementación es de $2868,60. Para poder recuperar la inversión del proyecto en caso de llegarse a implementar depende del gasto operativo el mismo como se puede observar en Tabla 6.16 es de $455,50 siendo este valor correspondiente a cada mes.

$$costo\ anual = costo\ mensual * 12 \qquad Ecuación\ (6.2)$$

$$consto\ anual\ = 455{,}50 * 12 = \$5466{,}00\ anuales$$

En la Ecuación 6.2 se observa el valor anual que gasta la empresa Speedy COM para realizar las operaciones de visitas técnicas.

Para poder determinar si el proyecto es económicamente viable se utilizó el Valor Actual Neto (VAN), este valor expresa en términos absolutos el valor actual de los recursos obtenidos al final del período de duración del proyecto de inversión para lo cual se debe tomar en cuanto los siguientes aspectos.

- Si el VAN es positivo y mayor a 1 significa que es conveniente financieramente.
- Si el VAN es negativo y menor a 1 no es conveniente financieramente.

Para poder calcular el VAN se utiliza la Ecuación 6.3

$$VAN = \sum_{t=1}^{n} \frac{V_t}{(1+k)^t} - I_0 \qquad Ecuación\ (6.3)$$

Dónde:

V_t = Flujos de caja en cada período t

I_o = Valor del desembolso inicial de la inversión

n = Es el numeró de períodos

k = Es la Tasa de descuento

También se utiliza la tasa de interés de retorno (TIR) puede definirse como el % de ganancia que obtienen los inversores por el dinero invertido. El TIR es el tipo de descuento que se hace al igualar a cero VAN.

Para poder calcular estos valores se, considerando un período de amortización de 8 meses con una tasa de descuento de 10%. Para realizar el cálculo del VAN y TIR se utilizó Microsoft Excel.

Tabla 6.18: Análisis de VAN y TIR

	Costo de Inversión	Ingresos Netos							
MES	0	1	2	3	4	5	6	7	8
	-2.292,00	455,50	455,50	455,50	455,50	455,50	455,50	455,50	455,50
								VAN	$ 125,51
								TIR	12%

Elaborado por: Investigador

En la Tabla 6.18 se puede observar los resultados del VAN, el cual es mayor que uno lo que indica que el proyecto es económicamente viable. También se indica el valor del TIR el mismo permite saber que el proyecto proporcionara un 12% de ganancia con respecto a la inversión inicial.

El tiempo de recuperación de la inversión (PRI) es un método que en corto plazo permite determinar el plazo de tiempo que se requiere para que los flujos netos de efectivo de una inversión recuperen su costo o inversión inicial. Este proceso se lo calcula sumando los flujos netos anuales con la inversión inicial cuando este valor se hace positivo o igual a cero sea recuperado la inversión.

El tiempo en el que se recupera la inversión de la propuesta se puede observar en la Tabla 6.19 en la cual se puede observar que la inversión se recupera en el quinto mes.

Tabla 6.19: Período de Recuperación de la Inversión

Mes	Flujo Neto	Saldo
	-2.292,00	-2.292,00
1	455,50	-1.836,50
2	455,50	-1.381,00
3	455,50	-925,50
4	455,50	-470,00
5	455,50	-14,50
6	455,50	441,00
7	455,50	896,50
8	455,50	1.352,00

Elaborado por: Investigador

Para poder determinar el tiempo en el cual se recuperara la inversión se aplica la Ecuación 6.4, en la misma se determina que la inversión será recuperada en 0.52 años.

$$Tiempo\ de\ Recuperación = \frac{Costo\ de\ Implementación}{Costo\ Anual} \qquad Ecuación\ (6.4)$$

$$Tiempo\ de\ Recuperación = \frac{2868{,}60}{5466{,}00} = 0.52\ años$$

El período de recuperación de 0.52 años se lo puede expresar en años y meses como se puede observar en la Ecuación 6.5.

$$Meses = 0.52 * 12 = 6.24 \qquad Ecuación\ (6.5)$$

Por lo tanto la inversión inicial se recupera en un período de 6.54 meses.

6.8. Conclusiones

Al final del trabajo Herramienta opensource de administración y Monitoreo basado en snmp para el mejoramiento del funcionamiento de la red en SPEEDY COM CIA LTDA. se obtuvo las siguientes conclusiones.

- 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.
- 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.
- La Implementación de la herramienta Zenoss para la administración y monitoreo de la red de Speedy, 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.

6.9. Recomendaciones

- Se recomienda al personal del departamento de soporte de Speedy realizar capacitaciones constantes en el correcto uso de la herramienta, para que no exista problemas causados por el desconocimiento en su adecuado uso.
- Se recomienda no olvidar de configurar de una manera adecuada el protocolo SNMP en las antenas de servicio cada vez que estas sean instaladas por los técnicos, para que no se presente ningún problema al momento de monitorear las mismas.
- 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.

Bibliografía:

Libros:

- ✓ MICHAEL BADGER. (2011). Zenoss Core 3.x Network and System Monitoring. PACKT PUBLISHING, Birmingham – Mumbai

Linkografía:

- ✓ Análisis y Monitoreo de Redes. Consultado el 6 de agosto del 2012, http://www.integracion-de-sistemas.com/analisis-y-monitoreo-de-redes/index.html.
- ✓ Arquitectura de la Administración de Redes. Consultado el 6 de agosto del 2012, http://html.rincondelvago.com/arquitectura-de-la-administracion-de-redes.html.
- ✓ Diseño e Implementación de un Ambiente de Administración Distribuida Compatible con el Protocolo SNMP. Consultado el 13 de agosto del 2012, http://www.criptored.upm.es/guiateoria/gt_m123c.htm.
- ✓ Manual de Seguridad en Redes. Consultado el 14 de agosto del 2012, http://www.scribd.com/doc/2926302/Manual-de-Seguirdad-en-Redes.
- ✓ Administración de redes utilizando Protocolo Snmp (Simple Network Management Protocol), Consultado el 15 de agosto del 2012, http://www.digital.unal.edu.co/dspace/bitstream/10245/1106/1/9910555_2009.pdf.
- ✓ SNMP: PROTOCOLO SIMPLE DE ADMINISTRACION. Consultado el 20 de agosto del 2012, http://www.apuntux.com/2009/08/06/snmp-protocolo-simple-deadministracion-de-red-todo-lo-que-quizo-saber-y-no-se-atrevia-a-preguntar/.
- ✓ Características clave de la administración y monitoreo de redes. Consultado el 21 de agosto del 2012, http://support.gfi.com/manuals/es/nsm7/nsm7manual_es-1-03.html.

- ✓ Introducción a la Administración de Redes. Consultado el 27 de agosto del 2012, http://www.slideshare.net/radiocomunicaciones_utpl/introduccin-a-laadministracin-de-redes.
- ✓ Gestión y Monitoreo de Redes. Consultado el 28 de agosto del 2012, http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/solano_v_h/capitulo1.pdf.
- ✓ Monitoreo. Consultado el 28 de agosto del 2012, http://www.seguridad.unam.mx/eventos/admin-unam/Monitoreo.pdf.
- ✓ Como administrar redes, Consultado el 29 de agosto del 2012, http://www.aprendaredes.com/downloads/Como_Administrar_Redes.pdf.
- ✓ Instalar Cacti. Consultado el 3 de septiembre del 2012, http://www.solusan.com/wp-content/2007/07/instalar_cacti.pdf.
- ✓ Monitorización de recursos de red con SNMP y Cacti. Consultado el 3 de septiembre del 2012, http://www.victornuno.com/2008/11/18/monitorizacion-de-recursosde-red-con-snmp-y-cacti/.
- ✓ Cacti. Consultado el 4 de septiembre del 2012, http://www.codigolibre.org/index.php?option=com_content&view=article&id=5387:cacti&catid=36:gnu-cat&Itemid=31.
- ✓ Página Oficial Cacti. Consultado el 5 de septiembre del 2012, www.cacti.com.
- ✓ Instalar agente Zabbix. Consultado el 10 de septiembre del 2012, http://www.rubenortiz.es/2009/05/26/instalar-agente-zabbix-enwindows/.
- ✓ Zabbix en debian 503 lenny. Consultado el 11 de septiembre del 2012, http://www.cdbarra.com/monitorizacion/zabbix-18-en-debian-503-lenny-instalacion.html.
- ✓ Blog Zabbix. Consultado el 12 de septiembre del 2012, http://zabbix-es.blogspot.com/2009_02_01_archive.html.
- ✓ Página Oficial Zabbix. Consultado el 12 de septiembre del 2012, www.zabbix.com.

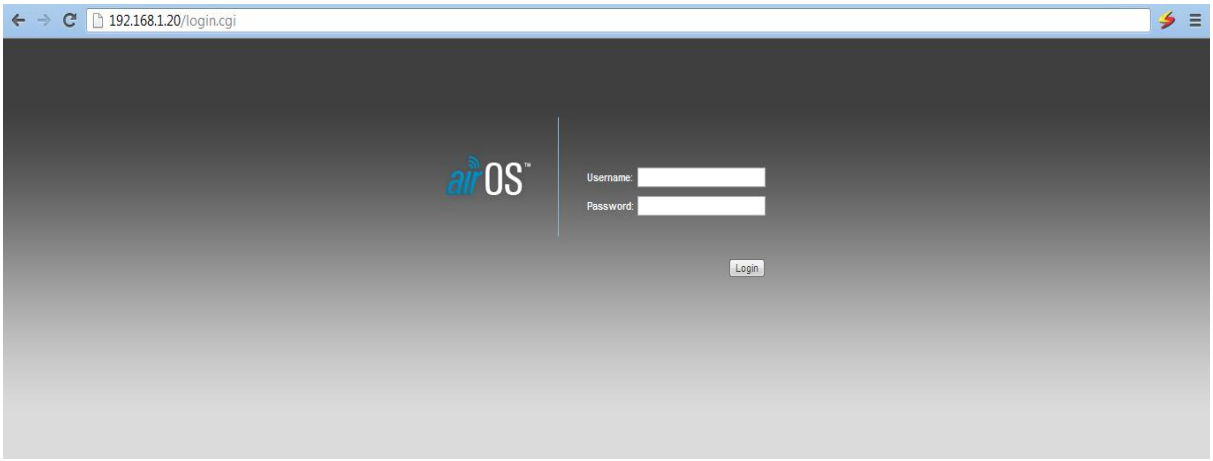
- ✓ Zabbix vs Zenoss. Consultado el 17 de septiembre del 2012, http://www.lastcombat.com/videos.php?one=Zenoss&two=Zabbix&f=Zabbix_vs_Zenoss.
- ✓ Manual Sistema de Monitoreo Zenoss en Ubuntu 8. Consultado el 24 de septiembre del 2012, http://www.scribd.com/doc/8751797/Manualsistema-de-Monitoreo-Zenoss-en-Ubuntu-8.
- ✓ Guía de Administración de Zenoss. Consultado el 25 de septiembre del 2012, http://docs.huihoo.com/zenoss/admin-guide/2.1.1/ch07s05.html.
- ✓ Zenoss. Consultado el 26 de septiembre del 2012, http://www.scribd.com/doc/8113441/zenoss.
- ✓ Monitoreando la red con Zenoss. Consultado el 1 de octubre del 2012, http://www.zenoss.com/product/network-monitoring.
- ✓ Página Oficial Zenoss. Consultado el 2 de octubre del 2012, www.zenoss.com.

ANEXOS

ANEXO A

Configuración del agente SNMP en las antenas Ubiquiti

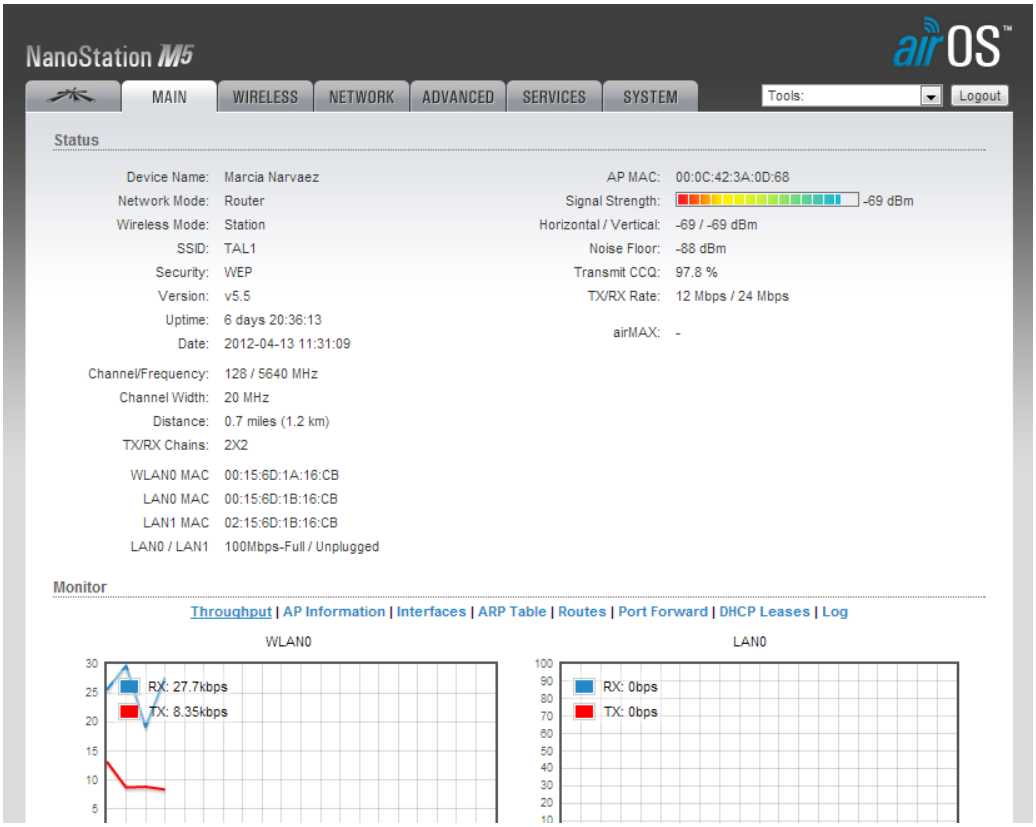
Para poder ingresar y empezar a configurar el agente SNMP en las antenas Ubiquiti, se debe ingresar en cualquier navegador la dirección ip por defecto para poder acceder a la antena el cual en este caso es 192.18.1.20, como se muestra en la siguiente figura.



Elaborado por: El investigador

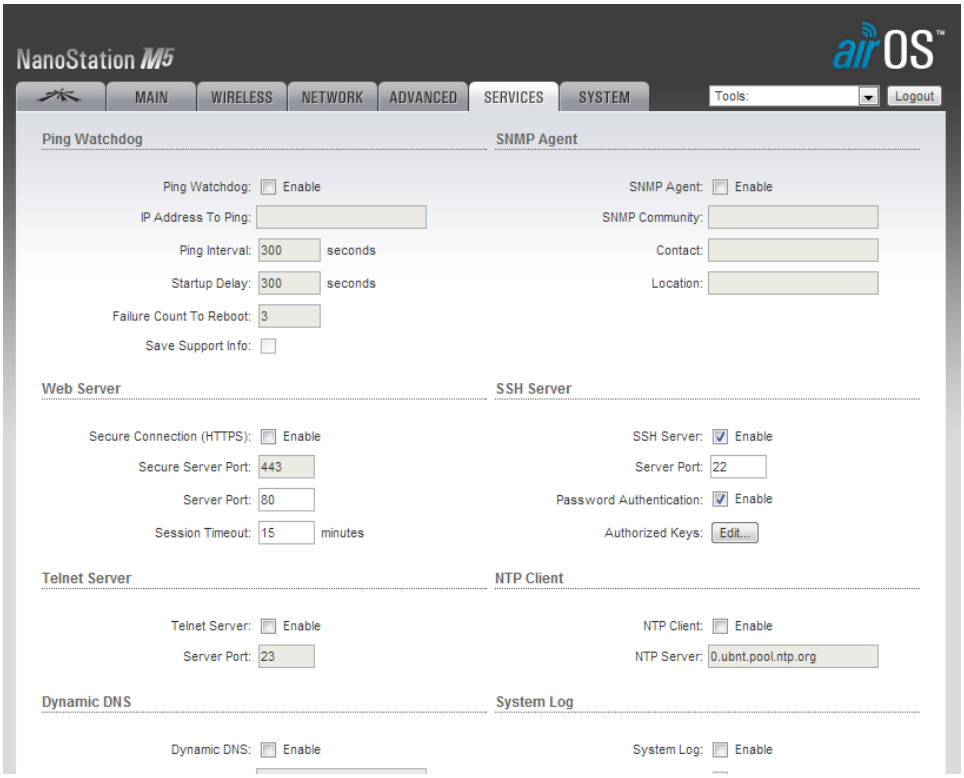
Una vez ingresado al servidor web de la antena se debe ingresar el nombre de usuario que por defecto es ubnt y su contraseña por defecto igual es ubnt, la cual se puede editar para mayor seguridad.

Se tendrá una ventana como se muestra en la siguiente imagen:



Elaborado por: El investigador

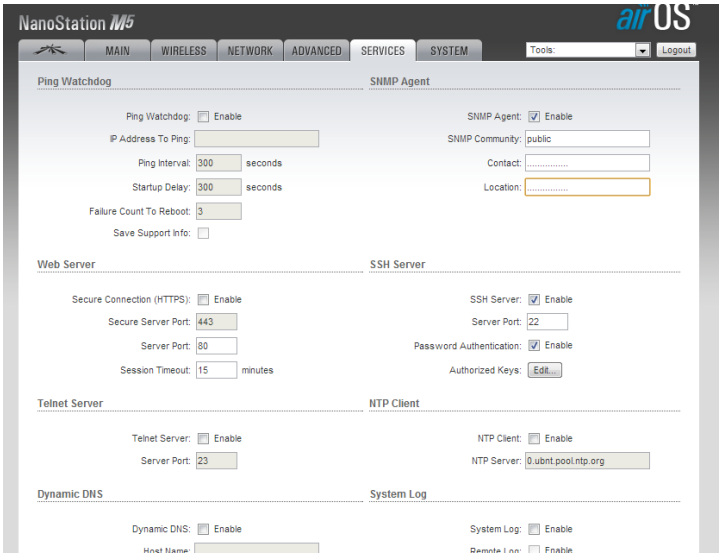
Una vez en el menú principal de configuración de la antena, para poder configurar el agente SNMP, se debe dirigir a la pestaña services el cual mostrara todos los servicios con los que cuenta la antena como se muestra en el siguiente gráfico.



Elaborado por: El investigador

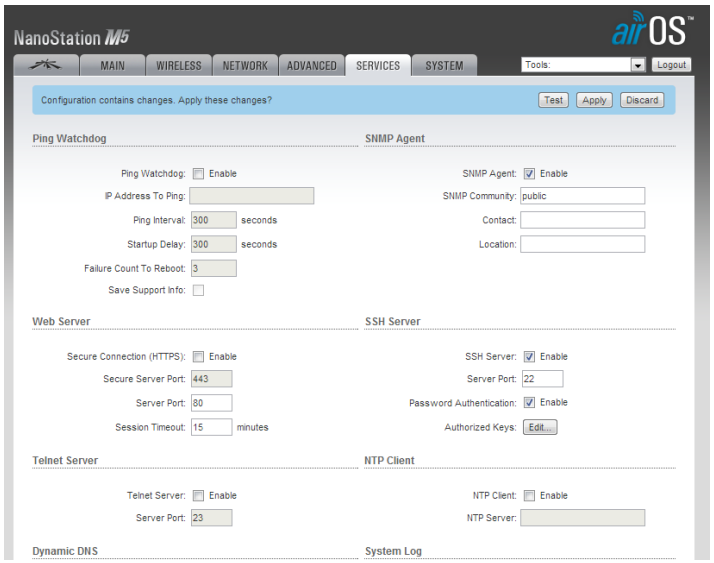
En el gráfico se puede observar que el agente SNMP que es esencial para realizar el monitoreo viene desactivado por defecto, para poder configurarlo lo único que se debe hacer es, primeramente habilitar el agente SNMP y llenar los datos que este pide como lo son SNMP Communiti que por defecto viene como public para que de esta manera el agente sea visto de manera pública, Contact en el cual se debe ingresar el nombre de usuario del agente y por ultimo Location en el cual se debe ingresar la ubicación en la cual se encuentra la antena para una mejor información de la misma.

Se tendrá una ventana como la que se muestra en el siguiente grafico



Elaborado por: El investigador

Como último paso se debe guardar los cambios dando click en la pestaña Change y luego dar click en la pestaña Apply para qué así tener configurado y activo el agente SNMP en la antena, como se muestra en el siguiente gráfico.

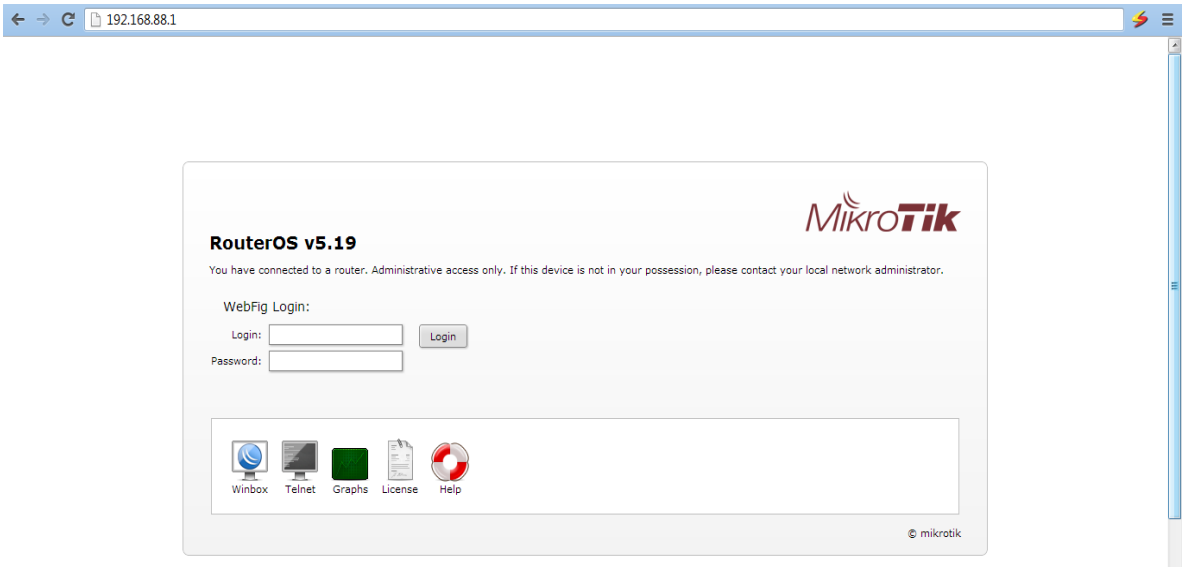


Elaborado por: El investigador

ANEXO B

Configuración del agente SNMP en las antenas Mikrotik

Para poder ingresar y empezar a configurar el agente SNMP en las antenas Mikrotik, se debe ingresar en cualquier navegador la dirección ip por defecto para poder acceder a la antena el cual en este caso es 192.198.88.1, como se muestra en la siguiente figura.



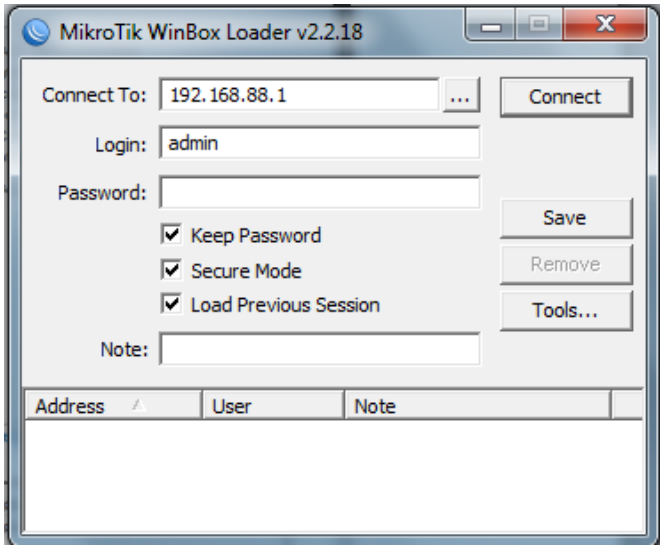
Elaborado por: El investigador

Una vez ingresado al servidor web de la antena se debe ingresar el nombre de usuario que por defecto es admin y no tiene ninguna contraseña, la cual se puede editar para mayor seguridad.

Para una mejor configuración de las antenas Mikrotik se recomienda descargarse el programa Winbox la cual se la puede descargar desde la ventana que muestra la antena.

Una vez descargado el programa Winbox lo ejecutamos e igual como acceder al servidor web de la antena se debe ingresar el nombre de usuario que por defecto es admin y no tiene ninguna contraseña.

Se tendrá una ventana como se muestra en la siguiente imagen:

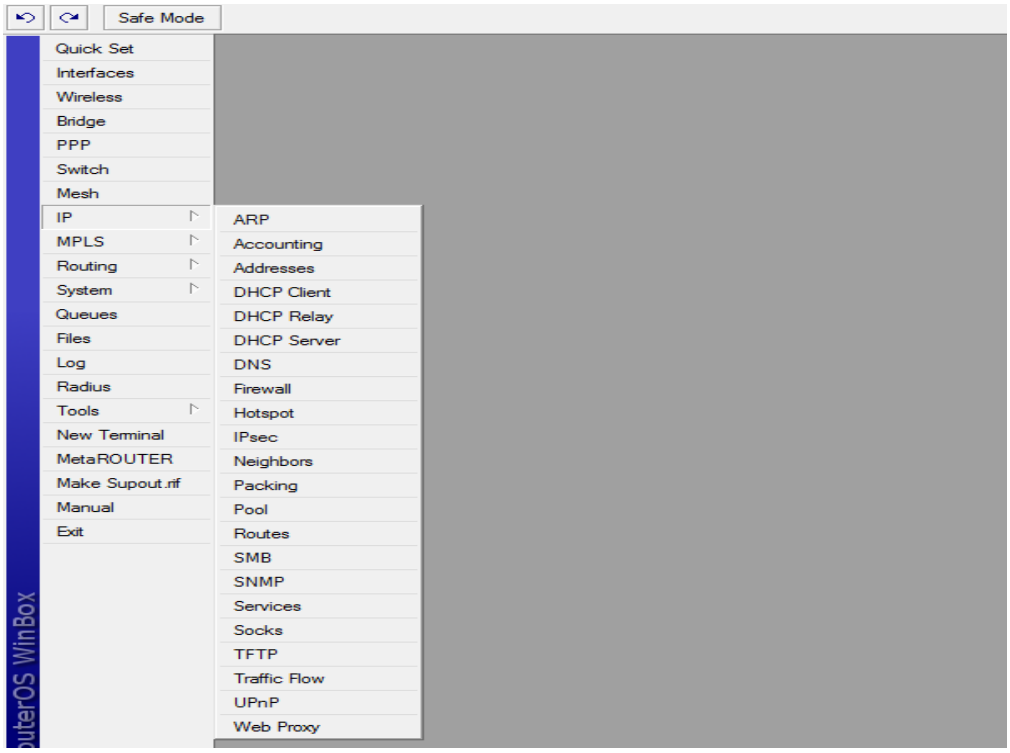


Elaborado por: El investigador

Se ejecuta el programa Winbox y se nos desplegara el menú principal de configuración de la antena, como se muestra en la siguiente figura.

Elaborado por: El investigador

Una vez en el menú principal de configuración de la antena, para poder configurar el agente SNMP, se debe dirigir a la pestaña IP el cual mostrara todos los servicios con los que cuenta la antena, se selecciona la opción SNMP para empezar a configurarlo, como se muestra en el siguiente gráfico.



Elaborado por: El investigador

En el gráfico se puede observar que el agente SNMP que es esencial para realizar el monitoreo viene desactivado por defecto, para poder configurarlo lo único que se debe hacer es, primeramente habilitar el agente SNMP y llenar los datos que este pide como lo son Contact Info en el cual se debe ingresar el nombre de usuario del agente, Location en el cual se debe ingresar la ubicación en la cual se encuentra la antena para una mejor información de la misma, Trap Comunity en el que se recomienda dejarlo como public y por ultimo Trap Version en el cual se puede seleccionar la versión de SNMP con el cual se cuenta, los cuales pueden ser V1, V2 o V3.

Se tendrá una ventana como la que se muestra en el siguiente grafico

Elaborado por: El investigador

Como último paso se debe guardar los cambios dando click en la pestaña Apply, luego dar click en la pestaña OK, para que así se guarden los cambios y tener configurado activo el agente SNMP en la antena.

ANEXO C

Características servidor dell poweredge 1950

SERVIDOR DELL POWEREDGE 1950

SERVICIOS DE INFRAESTRUCTURA DE TI DE DELL

Dell aporta ejecución pura a los Servicios de TI. La planificación, implementación y mantenimiento de su infraestructura de TI no merece menos. La variabilidad en la ejecución puede afectar a la productividad del usuario, los recursos de TI y, en definitiva, a su reputación. Al aprovechar nuestra herencia en la calidad de dirección del proceso, en Dell Services podemos ofrecer un método más inteligente.

No pretendemos hacerlo todo. Nos encontramos en los servicios de infraestructura de TI. Y tomamos un enfoque dirigido hacia el cliente, basándonos en la filosofía de que usted conoce su negocio mejor que nadie. Por eso Dell no intenta tomar decisiones clave sin su conocimiento o le ofrece más de lo que necesita. Todo lo contrario, aplicamos nuestra administración de procesos a nivel mundial y nuestra cultura "sin excusas" para ofrecer lo que nuestros clientes necesitan más actualmente: flexibilidad y calidad constante. Esto es pura ejecución. Esto es Dell en estado puro.

Servicios de evaluación, diseño e implementación

Los departamentos de TI continuamente se enfrentan al reto de evaluar e implementar nuevas tecnologías. Los servicios de evaluación, diseño e implementación de Dell pueden reestructurar su entorno de TI para mejorar el rendimiento, escalabilidad y eficacia al tiempo que contribuyen a maximizar su inversión y minimizar la interrupción de su negocio.

Servicios de implementación

La implementación del sistema es un mal necesario que invade casi todas las organizaciones. Debe implementar nuevos sistemas para ayudar a mejorar el rendimiento y satisfacer los requisitos del usuario. Con los servicios de implementación de Dell, ayudamos a simplificar y acelerar la implementación y el uso de nuevos sistemas para maximizar

Recuperación y reciclado de activos

La eliminación, reventa y donación correctas del equipo informático constituyen una larga tarea que suele encontrarse al final de muchas listas de tareas informáticas. Dell simplifica los procesos de caducidad del equipo informático de modo que maximiza el valor para los clientes.

Servicios de formación

Aporte a sus empleados los conocimientos y habilidades que necesiten para ser tan productivos como sea posible. Dell ofrece extensos servicios de formación que incluyen formación en hardware y software, así como clases de desarrollo profesional. Con la formación de Dell, puede contribuir a mejorar la fiabilidad del sistema, maximizar la productividad y reducir las peticiones del usuario final y el tiempo de inactividad.

Servicios de asistencia técnica a empresas

Con Dell, puede obtener el máximo rendimiento y disponibilidad de su servidor y sistemas de almacenamiento Dell. Los Servicios de asistencia de nuestra empresa ofrecen un mantenimiento proactivo para ayudar a evitar problemas y para responder y solucionar rápidamente los problemas cuando se produzcan. Hemos construido una infraestructura global que ofrece distintos niveles de asistencia para los sistemas de su infraestructura.

Para ayudarle a obtener lo máximo de sus sistemas Dell, visite www.dell.com/services.

Los servicios varían según la zona.

CARACTERÍSTICAS SERVIDOR DELL™ POWEREDGE™ 1950

Formato	Altura en rack de 1U
Procesadores	Hasta dos procesadores de secuencia de doble núcleo Intel® Xeon® 5000 con 3.0 GHz de frecuencia de reloj; o hasta dos procesadores de secuencia de doble núcleo Intel Xeon 5100 con 3.0 GHz de frecuencia de reloj; o hasta dos procesadores de secuencia de cuatro núcleos Intel Xeon 5300 con 2.66 GHz de frecuencia de reloj
Bus frontal	Secuencia 5000: 667 MHz o 1066 MHz Secuencia 5100: 1066 MHz o 1333 MHz Secuencia 5300: 1066 MHz o 1333 MHz
Caché	Secuencia 5000: Caché de nivel 2 de 2 x 2 MB por procesador Secuencia 5100: Caché de nivel 2 de 4 MB por procesador Secuencia 5300: Caché de nivel 2 de 2 x 4MB por procesador
Conjunto de chips	Intel® 5000X
Memoria	Módulos DIMM de 256 MB/512 MB/1 GB/2 GB/4 GB con memoria intermedia completa (FBD) en pares coincidentes; 533 MHz o 667 MHz; 8 zócalos para admitir hasta 32 GB
Ranuras de E/S	Dos ranuras en buses PCI independientes con aumento PCI Express con dos ranuras de 1 x 8 pistaso con aumento PCI-X con 2 ranuras de 64 bits/133 MHz; (opcional) NIC Gigabit integradas; puerto de administración para DRAC5 (opcional)
Drivers integrados	PERC 5/i (opcional): Driver RAID SAS 3 Gb/s con procesador Intel IOP333 y caché de 256 MB; SAS 5/i (base): driver de 4 puertos con procesador ARM966 (no admite RAID)
Driver RAID complementario	PERC 4e/DC opcional (driver RAID PCI Express de canal dual); Adaptador PERC 5/E opcional para almacenamiento RAID externo
Compartimentos de disco duro	Dos opciones: Dos chasis de unidad de disco duro con 2 unidades SAS de 3,5" (a 10.000/15.000 rpm) o SATA (7.200) o cuatro chasis de unidad de disco duro con 4 unidades SAS de 2,5" (a 10.000 rpm); compartimentos para periféricos: 1 compartimento para unidad óptica delgada con opción para unidad de CD-ROM opcional, DVD-ROM opcional o unidad combinada de CD-RW/DVD-ROM
Almacenamiento interno máximo	Hasta 600 GB[2] (con 2 disco duros SAS de 3,5")
Discos duros[2]	SAS de 2,5" (a 10.000 rpm): unidades de disco duro de 36 GB o 73 GB conectables en marcha; SAS de 3,5" (a 10.000 rpm): unidades de disco duro de 73 GB, 146 GB, 300 GB conectables en marcha; SAS de 3,5" (a 15.000 rpm): unidades de disco duro de 36 GB, 73 GB, 146 GB conectables en marcha; SATA de 3,5" (a 7.200 rpm): unidades de disco duro de 80 GB, 160 GB, 250 GB conectables en marcha[1]
Almacenamiento interno	CD-ROM iniciable opcional; 2 unidades SAS de 3,5" conectables en marcha (a 10.000 y 15.000 rpm) o unidades SATA (7.200); 4 unidades SAS de 2,5" conectables en marcha a 10.000 rpm
Almacenamiento externo	Dell PowerVault™ 22xS, PowerVault MD1000, productos Dell/EMC
Opciones de copia de seguridad en cinta	Internas: ninguno
Tarjeta de interfaz de red	NIC Gigabit Ethernet Broadcom® NetXtreme II™ 5708 dual integrada[3] NIC Ethernet con compensación de carga y capacidad de recuperación. TOE (motor de carga TCP/IP) compatible con Microsoft Windows Server 2003, SP1 o superior con Scalable Networking Pack. Tarjetas NIC complementarias opcionales: NIC Intel® PRO/1000 PT de puerto dual, Gigabit, Copper, PCI-E x4; NIC Intel® PRO/1000 PT de un solo puerto, Gigabit, Copper, PCI-E x1; NIC Intel® PRO/1000 PF de un solo puerto, Gigabit, óptica, PCI-E x4; NIC Gigabit Broadcom® NetXtreme™ 5721 de un solo puerto, Copper, PCI-E x1; NIC Gigabit Broadcom® NetXtreme II™ 5708 de un solo puerto con TOE, Copper, PCI-E x4
Fuente de alimentación	670 vatios, fuente de alimentación redundante opcional conectable en marcha (1+1)
Disponibilidad	Unidades de disco duro conectables en marcha; fuente de alimentación redundante opcional conectable en marcha; refrigeración redundante; memoria ECC; banco de reserva; Single Device Data Correction (SDDC); tarjeta secundaria PERC 5/i integrada con caché DDR2 con reserva de memoria por batería de 256 MB; soporte de conmutación por error de alta disponibilidad; DRAC5
Vídeo	ATI ES1000 integrada con memoria de 16 MB
Administración remota	Driver de administración de la placa base estándar compatible con IMPI 2.0; DRAC5 opcional para funciones avanzadas
Administración de sistemas	Dell OpenManage™
Compatibilidad con rack	4 postes (rack Dell), 2 postes y guías Versa de terceros, guías móviles y brazo para la manipulación de cables
Sistemas operativos	Microsoft® Windows® Server™ 2003 R2, Standard, ediciones Enterprise y Web, x64 R2; ediciones Standard y Enterprise; Red Hat® Linux® Enterprise v4, ES EM64T, ES; SUSE® Linux® Enterprise Server 9 EM64T, SP3

[1] Soporte de disco duro de 250 GB en Q3CY06.

[2] Para las unidades de disco duro, GB significa 1.000.000.000 de bytes; la capacidad total accesible varía en función del material preconfigurado y el entorno operativo y será inferior.

[3] Este término no conlleva una velocidad de funcionamiento real de 1 GB/seg. Para la transmisión de alta velocidad se necesita una conexión a un servidor Gigabit Ethernet e infraestructura de red.

PURE DELL
www.dell.com