UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

TESIS PARA OBTENER TÍTULO DE
INGENIERO EN COMPUTACIÓN

GESTIÓN Y MONITOREO DE UN LABORATORIO CON HERRAMIENTAS OPEN SOURCE

PRESENTA:
RAMOS GALICIA JUAN CHRISTIAN

DIRECTOR DE TESIS:
M. en I. OSCAR RENÉ VALDEZ CASILLAS

Ciudad Universitaria, México, 2012

Agradecimientos

La presente tesis es un trabajo en el cual participaron varias personas directa o indirectamente, leyendo, opinando, teniéndome paciencia, dándome ánimos y apoyo en general. Por ello es para mí un placer utilizar este espacio para expresar mis agradecimientos hacia estas personas.

Agradesco primeramente de manera especial y sincera al MI.Oscar Rene Valdez por aceptarme para realizar ésta tesis bajo su dirección, su confianza y aporte invaluable de conocimientos ayudaron a guiar mis ideas para ser plasmadas en este trabajo.

Agradesco también a la Ing. Laura Sandoval y MI. Elba Karen Saenz por su apoyo al facilitarme el uso del laboratorio de Intel para llevar acabo todas las actividades de implementación durante el desarrollo de esta tesis.

A mi madre Isabel que con su cariño y conprensión siempre me apoyo día a día para seguir adelante en este proyecto. A mi padre Wenceslao que siempre estuvo atento en lo que hacia para ofrecerme sus consejos que me ayudaron bastante de forma personal. A mis hermanas Reyna y Wendy que con su alegría y ánimo me contagiaban y me motivaban.

A mis abuelitos Juan y Guadalupe que fueron mis primeros maestros en la vida al inculcarme valores y darme su cariño y comprensión.

A toda mi familia en general, gracias por confiar en mí y muy en especial gracias a dios que me dio la fortaleza para terminar ésta etapa de mi vida.

ÍNDICE

IMÁGENES

INTRODUCCIÓN

Las redes de datos tienen como principal objetivo compartir información y permitir la comunicación entre los usuarios, pero para que este objetivo tenga un funcionamiento permanente y eficiente los administradores de la red necesitan conocer y manejar herramientas de software que permitan una mejor gestión y administración de la red.

Existen varias herramientas que tienen la capacidad de gestionar ciertos servicios y equipos de red, con sus ventajas y desventajas cada una, siendo Open Source (libres) o propietarias (con licencia), por lo cual, en esta investigación se realiza algunas comparaciones de tres diferentes herramientas, enfocándose principalmente en una que resulto ser la más completa y útil para el ambiente de un Laboratorio con computadoras en red, esta herramienta se llama Zenoss Core, aunque también existe la versión llamada Zenoss Enterprise la cual tiene un costo por el soporte y algunos ZenPacks agregados.

Este trabajo de investigación se realizó con el objetivo de conocer paso a paso la implementación de dicha herramienta, obteniendo información útil para el análisis de los enlaces y computadoras de la red con lo que se conocerían las ventajas que se obtienen al gestionar y monitorear una red de computadoras en un laboratorio, logrando una mejor administración de los recursos, tanto en un ambiente virtual como en un laboratorio con equipos reales.

En la presente tesis se comienza con un marco teórico detallado con los principales temas de Redes de Datos, mencionando el modelo OSI y TCP/IP, que ofrecen un conocimiento general de la actividad interna que se realiza en una red, dando posteriormente una idea de cómo y dónde actúa el software de gestión y monitoreo, además de ayudar a comprender las principales características o acciones de estas herramientas.

Para la realización de las pruebas y porque en la actualidad es un tema de suma importancia en las redes se menciona también el tema de virtualización, sus ventajas y desventajas, algunas herramientas de software existente para virtualizar equipos físicos y además la elección más adecuada de una herramienta para la simulación virtual de un laboratorio de cómputo monitoreado, todo esto debido aque la solución tenía que ser directa para no estar interrumpiendo con pruebas el uso del laboratorio en la implementación.

Al final, la investigación mostró utilidad y fue comprobable, pues se realiza y se menciona la implementación, adaptación, gestión y monitoreo de el Laboratorio de computo con equipos reales, analizando la información que se obtiene de este y mostrándo la utilidad de la herramienta en dicho Laboratorio, con lo cual se adquirió ademas una guía muy completa para su uso y un conocimiento más profundo en el monitoreo y gestión de redes.

CAPÍTULO 1 *Marco Teórico*

1.1ANTECEDENTES DE LAS REDES DE COMPUTADORAS

Es muy importante la función que han tenido las redes en los últimos años; pues han permitido compartir o intercambiar información eficientemente entre usuarios, por medio de aplicaciones como el correo electrónico, bibliotecas virtuales, sistemas para transacciones e incluso redes sociales entre otras.

Una definición general para una red de dispositivos electrónicos es: "Es una interconexión de dos o más equipos con el objetivo de compartir recursos, información y servicios", siendo esto lo que le da a las redes su potencia y atractivo en la sociedad.

En un lugar de trabajo con computadoras y equipos de comunicación, una red siempre debe alcanzar buenos objetivos como son: la eficiencia, la disponibilidad de la información y servicios, además de la reducción de costos, esto se puede lograr por ejemplo, teniendo en cuenta el buen funcionamiento de puntos importantes en una red como podrían ser:

- *Compartir información (o datos):* La eficiencia aumenta cuando los datos están disponibles para cualquier usuario y en el momento que los necesite, compartiendo información incluso con grandes grupos, siempre y cuando también la información sea entregada sin pérdidas ni daños.

- *Compartir Hardware y software:* En el pasado el compartir la impresora significaba hacer turnos para sentarse en el equipo conectado a ésta, lo que provocaba perder tiempo y para una empresa, perder dinero. En la actualidad las redes permiten compartir simultáneamente cualquier periférico o aplicación e identificarse entre sí.

- *Centralizar la administración y el soporte:* Con una red centralizada se facilitan las diferentes tareas y servicios, ya que es más eficiente dar soporte y configurar varios equipos del mismo modo, que hacer configuraciones de manera individual.

Después de que se ha platicado un poco de la utilidad y buen funcionamiento que debería tener una red, se mencionará la forma en que se pueden clasificar éstas, como puede ser de acuerdo a su tamaño, ámbito geográfico que abarcan y a la tecnología que se utiliza para la transmisión de la información.

Red de Área Local (LAN, Local Área Network): La principal función en esta red es el intercambio de información entre grupos de trabajo y compartir recursos tales como impresoras, discos duros, etc. Se caracterizan por tres factores: extensión (de unos cuantos metros hasta algunos kilómetros), su tecnología de transmisión (cable de par trenzado UTP, coaxial o fibra óptica, portadoras con infrarrojo o láser, radio y microondas en frecuencias no comerciales) y su topología (anillo, bus único o doble, estrella, árbol y completas).

Los estándares más comunes son el de Ethernet con la especificación IEEE 802.3 y en estos tiempos el más utilizado IEEE 802.11 Wireless o red inalámbrica.

Redes Metropolitanas (MAN): Aun que ya no es considerada por varios autores con éste nombre, el tipo de redes MAN es como se le llamaba a una versión más grande de una LAN, que pueden abarcar un conjunto de oficinas corporativas o empresas en una ciudad. De manera más general cualquier red de datos, voz o videos con una o varias decenas de kilómetros era considerada una MAN, ahora la mayoría de los autores la clasifican como LAN.

Redes de Área Extensa (WAN): Estas redes abarcan una gran zona geográfica como puede ser un estado, país o continente. Como las redes LAN que unen nodos de los usuarios con diversos aparatos de red (llamados *routers o* ruteadores). Las redes WAN unen las diversas redes con líneas de comunicación que abarcan mayor área.

La transmisión en las tres clasificaciones de red (LAN, MAN y WAN), puede ser por medio de microondas, cable de cobre, fibra óptica o alguna combinación de estos medios. Sin darle importancia al medio de transmisión, los datos en algún punto se convierten e interpretan como una secuencia de unos y ceros para formar *frames* de información, después los *frames* son ensamblados y así forman paquetes, los cuales a su vez construyen archivos o registros específicos de alguna aplicación del usuario final.

Por lo general, las organizaciones individuales alquilan las conexiones a través de una red de proveedores de servicios de telecomunicaciones (TSP), para interconectar las LAN en las distintas ubicaciones geográficas.

1.1.1 MODELO OSI (Open Systems Interconnection-Interconexión de sistemas abiertos)

En 1977 la Organización Internacional de Estándares conocida también por sus siglas en ingles como ISO creó un subcomité con el objetivo de desarrollar estándares de comunicación de datos que dieran accesibilidad universal e inter-operatividad entre dispositivos de diferentes fabricantes, dando por resultado el modelo de Interconexión de Sistemas Abiertos también conocido como OSI. (Fecha obtenida de [3, PAG 6])

El Modelo OSI es un lineamiento funcional para tareas de comunicaciones, por lo que varios estándares y protocolos cumplen con este modelo, facilitando la resolución de los problemas en una red, ya que un problema general se divide en problemas más pequeños y específicos, de ahí la utilidad de las capas del Modelo OSI.

Al margen de la función específica de cada capa, todas a excepción de la capa física integrada por dispositivos de hardware, adjuntan un encabezado (los encabezados vienen representados por cuadritos en la Fig1.1) a los datos.

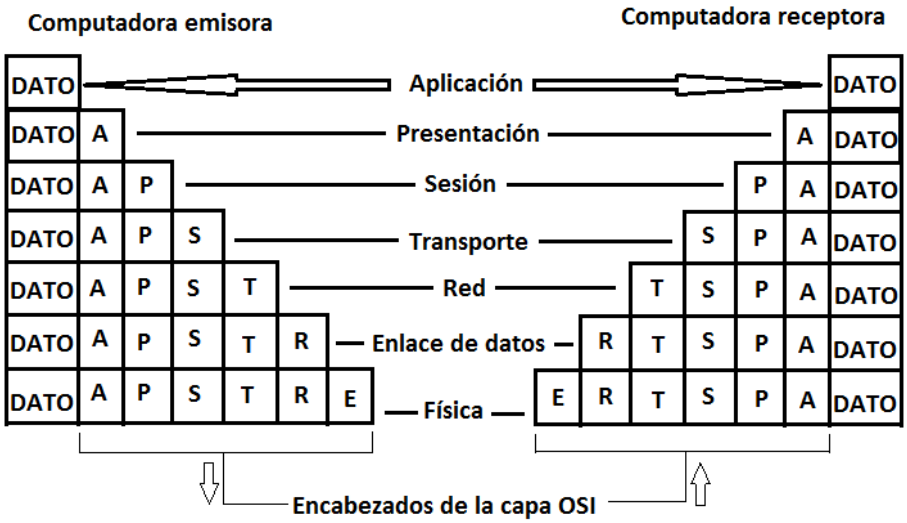


Fig1.1 Recepción y envio de información en OSI [13, pag 35, Figura 2.2]

Los datos enviados según la fig 1.1, bajan por la computadora emisora y se reciben en la capa física de la computadora destino, subiendo por toda la pila OSI. Conforme van subiendo los datos el encabezado de cada una de las capas se va eliminando hasta llegar a la capa de aplicación y así el destinatario podrá recibir los datos.

Las capas del modelo OSI están diseñadas basadas en los siguientes principios:

1. Una capa se creará en situaciones en las que se requiera un nivel diferente de abstracción.
2. Cada capa deberá realizar una función bien definida.
3. La función que realiza cada capa deberá seleccionarse tomando en cuenta la minimización del flujo de información a través de las interfaces.
4. El número de capas será suficientemente grande como para que funciones diferentes no estén en la misma capa, y suficientemente pequeño para que la arquitectura no sea difícil de manejar. [14, PAG 12]

1.1.1.1 CAPAS DEL MODELO OSI DE ISO

A continuación se explicará cada una de las capas que componen el modelo OSI, comenzando en la parte superior de la pila (Nivel 7, Nivel de aplicación), para ir descendiendo hasta la capa 1, Nivel Físico.

Capa de Aplicación: Es la capa que proporciona la interfaz entre las aplicaciones que utiliza el usuario final para comunicarse y la red subyacente en la cual se transmiten los mensajes. Los protocolos de la capa de aplicación se utilizan para intercambiar datos, entre los programas que se ejecutan en diferentes hosts de origen y destino, entregando la información y recibiendo los comandos que dirigen dicha comunicación, algunos protocolos utilizados por programas o aplicaciones en esta capa son el HTTP (*Hypertext Transfer Protocol*), SMTP (*Simple Mail Transfer Protocol*), SNMP (*Simple Network*

Management Protocol),TELNET, FTP (***F****ile* ***T****ransfer* ***P****rotocol*) e IMAP(*Internet Message Access Protocol*).

La capa también implementa la operación con referencias del sistema interactuando con la capa de presentación.

Capa de Presentación: Como definición general, se puede decir que ésta capa es un protocolo de paso de información de sus capas adyacentes, ya que permite la comunicación entre aplicaciones en distintos sistemas informáticos, resultando la comunicación clara entre éstos, pues se ocupa del formato y su traducción, además de la representación de los datos y de una característica adicional que es la de ordenar y organizar estos datos antes de su transferencia. Así, esta capa se encarga de la presentación, de tal manera que los dispositivos puedan comprenderlos.

Algunas de las principales funciones de esta capa son:

- Se ocupa de la sintaxis y la semántica de la información que transmite en la red.
- Determina la forma de presentación de los datos.
- Se puede hacer cargo de la compresión y encriptación de los datos que se intercambian.
- Proporciona servicios para el nivel de aplicaciones, al interpretar el significado de los datos intercambiados.
- Opera el intercambio.
- Opera la visualización.

Capa de Sesión: La Capa de Sesión se encarga de establecer el enlace de comunicación o sesión entre los equipos pues se ocupa de la sincronización entre estos. Este nivel gestiona la sesión que se establece entre los nodos y controla el flujo de datos. Posteriormente de establecida la sesión entre los nodos que se comunican, la capa de sesión pasa a encargarse de ubicar puntos de control en la secuencia de datos, para dar tolerancia a fallos en la comunicación, restableciendo la sesión a partir de estos puntos, sin pérdida de datos. Los protocolos que operan en la capa de sesión pueden proporcionar dos tipos de comunicación: la comunicación orientada a la conexión y la comunicación sin conexión.

Los protocolos orientados a la conexión funcionan muy parecido a una llamada telefónica, ya que establecen una sesión al llamar a otra persona, manteniendo una conexión directa al estar hablando y termina la sesión cuando ambos cuelgan.

En cuanto a los protocolos sin conexión funcionan como un correo normal, se da la dirección para el envío de los paquetes y como si se metieran a un buzón, suponiendo que con la dirección llegarán los paquetes a su destino, sin necesidad de algún permiso de la computadora receptora.

Entre algunos de los protocolos importantes que utiliza esta capa están: SSL (*Secure Sockets Layer*), RPC (*Remote Procedure Call*) y SCP (*Secure CoPy*).

Capa de Transporte: La capa de transporte actúa como un puente entre los tres niveles inferiores orientados a las comunicaciones y los tres niveles superiores orientados al procesamiento, garantizando la entrega de información confiablemente pues permite la segmentación de datos y brinda el control necesario para re-ensamblar las partes dentro de los distintos streams de comunicación.

El control de flujo, es otra de las labores importantes de esta capa porque identifica y diferencia las conexiones existentes, además de que determina el momento en que inician y terminan las conversaciones. Esta capa identifica las aplicaciones asignando un identificador a cada aplicación, los protocolos TCP/IP denominan a este identificador como número de puerto.

Capa de Red: El principal objetivo de la capa de red es que la información o datos lleguen desde el origen al destino aún si ambos no se encuentran conectados directamente y están ubicados en redes geográficamente distintas, pues el direccionamiento en esta capa dirige los datos a los dispositivos finales con una dirección, llamada dirección IP.

Posteriormente del direccionamiento se realiza el proceso de encapsulación permitiendo que su contenido pase con carga mínima a una red destino. Cuando se hace referencia a la capa de Red, denominamos paquete a una PDU (*Protocol Data Units*).

El enrutamiento o conmutación de capa 3 es el nivel donde se decide la mejor ruta, para dirigir los paquetes hacia el segmento y el puerto de salida adecuados. A cada ruta que toma un paquete para llegar al próximo dispositivo se la llama salto.

Al llegar al host destino se procesa el paquete en la capa 3, examinando la dirección de destino para verificar que el paquete fue direccionado a ese dispositivo. Si la dirección es correcta, el paquete es revisado por la capa de Red para pasarlo a la siguiente capa.

La decisión de cómo encaminar los paquetes de información, se realiza basándose en tablas estáticas o dinámicamente en función del tráfico de red, ya que en ésta capa se detecta y corrigen problemas de congestión de tráfico.

Los protocolos más utilizados de la capa de Red son:

- Versión 4 del Protocolo de Internet (IPv4),
- Versión 6 del Protocolo de Internet (IPv6),
- Intercambio Novell de paquetes de internetwork (IPX), AppleTalk, y
- Servicio de red sin conexión (CLNS/DECNet).

Capa de Enlace de Datos: Ésta capa es la encargada de enviar tramas de la capa de red a la física y en el equipo receptor de empaquetar los bits puros del nivel físico, controlando los impulsos que entran y salen del cable de red con lo cual ayuda a resolver problemas creados por algún deterioro, pérdida o duplicidad de tramas a través del nivel físico.

La capa de Enlace de Datos, también ofrece varios servicios a la capa de red como la de sincronización y control de errores que son servicios propios de esta capa. También proporciona el servicio de control de congestión o control de flujo, que evita que un emisor muy rápido sature a un receptor muy lento. Además, se pueden ver procesos de multiplexado y de compactación.

Capa Física: Ésta capa es la que se encarga de las propiedades físicas relacionadas con características eléctricas o electrónicas y la interpretación de señales de una trama, también se puede mencionar lo relacionado con la velocidad en que se transmiten los datos y si ésta transmisión es unidireccional o bidireccional (símplex, dúplex o full-dúplex).

Algunos conceptos en esta capa que son importantes mencionar para su conocimiento, son:

- La definición del medio físico para la comunicación entre los que podemos mencionar: el cable de par trenzado, coaxial, guías de onda, aire y fibra óptica entre otros.
- La definición de materiales como componentes y conectores de interfaz, cuyas características eléctricas y de señalización son utilizadas en la transmisión por los medios físicos.
- El observar y aclarar las funcionalidades de la interfaz para establecer, mantener y liberar el enlace físico con el que se cuenta o se contará.
- Contar con una buena transmisión de información (bits) por el medio físico.
- Conocimiento de las señales eléctricas/electromagnéticas para su manejo.
- Garantizar la conexión y si es posible la fiabilidad del medio.

1.1.2 MODELO TCP/IP

Lo interesante de la Arquitectura del TCP/IP, también llamada Arquitectura de Internet, es su adopción casi universal. Debido a que el TCP/IP e Internet están entrelazados, en este capítulo se hablará de la historia y uso de ambos.

Internet fue un método para probar redes de intercambio de paquetes, propuesta por DARPA (Defense Advanced Research Projects Agency) o también llamada Advanced Research Projects Agency (ARPA).

Según Tim Parker menciona "En este proyecto ARPA previó una red de líneas arrendadas conectadas por nodos interruptores, a esta red la llamó ARPANET y a los nodos interruptores los llamó Internet Message Processors (Procesadores de Mensajes Entre Redes) o IMP".[1, pag 38]

Los principales objetivos que se buscaban en una red, eran la capacidad de transferir archivos desde un equipo a otro y el soporte de manera remota; debido a que en ese entonces el protocolo usado no manejaba estas funcionalidades, fueron desarrollados, perfeccionados y probados nuevos protocolos, hasta que finalmente fue puesto en práctica el protocolo llamado Network Control Program (NCP; Programa de Control de la Red) que

cumplía con los requerimientos anteriores. Este protocolo fue útil hasta 1973 ya que posteriormente, fue incapaz de manejar el volumen de tráfico y nuevas funcionalidades que se requerían.

Tim Parker señala que "el protocolo TCP/IP fue conocido por primera vez en un artículo publicado por Cerf y Kahn, describiendo un sistema que proporcionaba un protocolo de aplicación estandarizada y que además utilizaba reconocimiento de extremo a extremo, aunque estos conceptos no eran nuevos en ese tiempo, lo que llamo más la atención es que sugirieron que el nuevo protocolo fuera independiente de la red y el hardware de computadoras, además de que tuvieran una conectividad universal a través de la red, con esto se permitiría participar en la red a cualquier clase de plataforma".[1, pag 39]

Douglas E Comer señala que "La internet global se inició alrededor de 1980 cuando ARPA comenzó a convertir las maquinas conectadas y redes de investigación, en máquinas con el nuevo protocolo TCP/IP" esto termino cuando en 1982 se sustituyó al NCP como el protocolo dominante de red.[3, Pag. 7]

Posteriormente se dividió en dos redes diferentes, MILNET para tráfico militar no clasificado y ARPANET para la investigación y otros propósitos. Pronto se dieron cuenta de que la comunicación por red sería en el futuro una parte crucial en la investigación científica, por lo que TCP/IP comenzó a crecer para poder comunicar primeramente a científicos e investigadores y después al mundo, convertiendose en lo que es hoy internet.

Douglas E Comer menciona al "IAB pues es quien establece la dirección Técnica y decide cuando los protocolos se convierten en estándares. Es el grupo conocido como Internet Architecture Board (Junta de Arquitectura de Internet o IAB), el cual también proporciona el enfoque y coordinación para el desarrollo de TCP/IP, guiando la evolución de Internet y decidiendo que protocolos son parte obligatoria del grupo TCP/IP estableciendo políticas oficiales".[3, pag 8]

1.1.2.1 CAPAS TCP/IP

El TCP/IP está diseñado en una estructura en capas, sin originarse de un comité de estándares, proveniente más bien de investigaciones, respecto al conjunto de protocolos que lo conforman. Cada una de las capas, es responsable de llevar a cabo una tarea específica de comunicación. Concretamente, el TCP/IP se organiza en cuatro capas conceptuales que se construyen sobre una quinta capa física o capa de hardware:

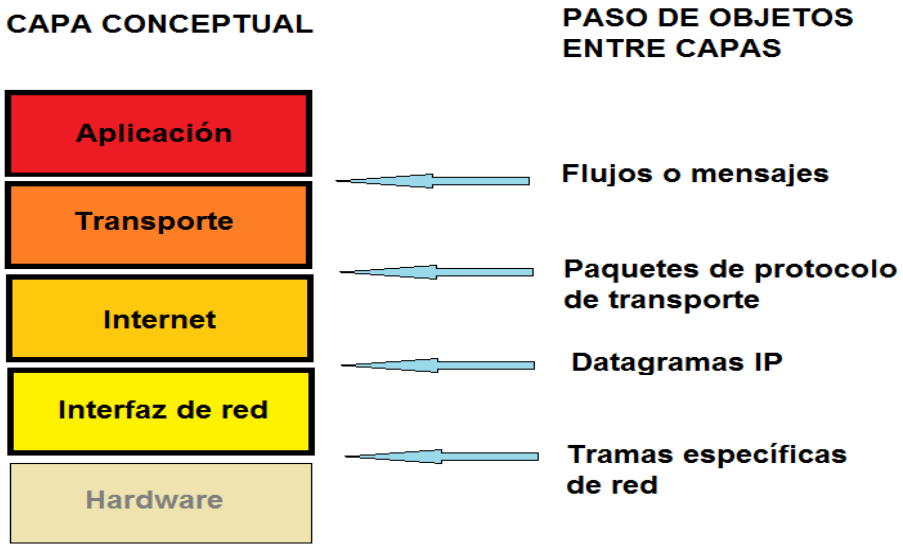


Fig 1.2 Capas del modelo TCP/IP [3, Pag. 168, Figura 11.5]

Capa de Interfaz de red: Esta capa se relaciona a los medios físicos de comunicación y a las capas de enlace y física en el modelo OSI (capas 1 y 2). Este nivel consiste de controladores o algún subsistema que utiliza un protocolo de enlace de datos, ya que controlan las tarjetas de red y toda la gestión de la conexión del hardware de red.

Capa de Internet: Es la encargada de la comunicación entre las maquinas. Esta capa inicia su trabajo, aceptando una solicitud para poder enviar paquetes desde la capa de transporte con la identificación de la maquina destino. La capa envía y recibe paquetes a través de la red, manejando y verificando la entrada de datagramas, además de que con un algoritmo de ruteo se decide si el datagrama se procesa localmente o se transmite para llegar a su destino. Esta capa se relaciona con la capa de red del Modelo OSI.

Capa de transporte: Se encarga de manejar y regular los flujos de datos entre equipos, aunque su principal función es proporcionar comunicación entre programas de aplicación ofreciendo un transporte confiable, pues hace llegar los datos sin errores y en secuencia. Para enviar información la capa de transporte divide el flujo de datos en pequeños fragmentos conocidos como paquetes, los cuales contienen la dirección destino. Existen dos protocolos principalmente a este nivel: TCP, un protocolo fiable y orientado a conexión, y UDP, un protocolo más simple pero que no garantiza la recepción de los datos, es decir, no orientado a conexión. Es relacinada con la capa que lleva el mismo nombre en el modelo OSI, la capa de transporte

Capa de aplicación: Esta capa es equivalente a las capas 5,6 y 7 del modelo OSI, además, es la que da a los usuarios acceso a servicios disponibles en la red de redes TCP/IP, pues provee una interfaz entre el software que es ejecutado en una computadora y la red en sí. Los programas de aplicación seleccionan el tipo de transporte necesario, el cual puede ser una secuencia de mensajes individuales o un flujo contínuo de octetos. En este nivel existen protocolos tales como: TELNET, FTP, HTTP, SMTP, SNMP, NFS, NNTP.

1.1.2.2 PROTOCOLO INTERNET (IP)

IP es un protocolo perteneciente a la capa 3 o capa de red, que cuenta con información de direccionamiento y control para el ruteo de paquetes, este protocolo se puede encontrar en el RFC 791. IP realiza la entrega de datagramas con el mejor esfuerzo y sin conexión, también fragmenta y re-ensambla datagramas para así soportar enlaces de datos con tamaños diferentes de las MTU (Unidades de Transmisión Máxima).

Douglas E. Comer indica el dato del tamaño de un datagrama IP diciendo :"El tamaño máximo posible de un datagrama IP es de 2^{16} o 65535 octetos".[3,Pag 95]

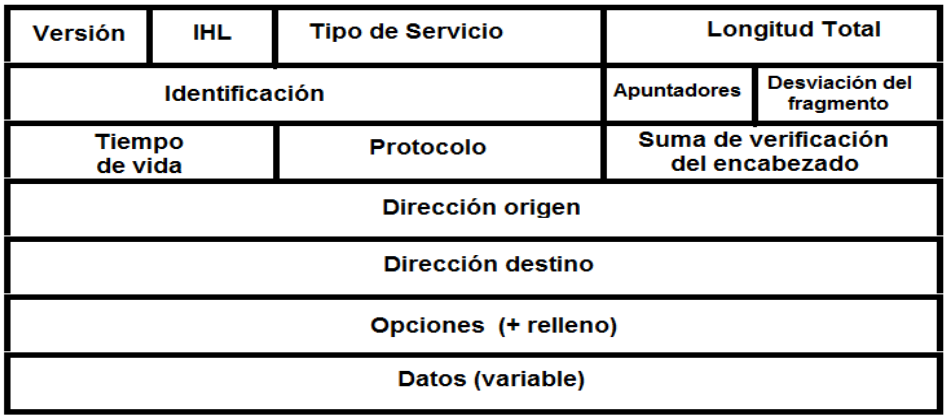


Fig. 1.3 Los 14 campos en un paquete IP
[5, Pag. 368, Figura 28-2]

A continuación se ofrece la explicación de los primeros 2 campos que da Douglas E. Comer, seguidos de la explicación de los demás campos por Ford, Lew, Spanier, y Stevenson, encontradas en su libro Tecnologías de interconectividad de redes [5, Pag 368 y 369].

VERSION: Contiene la versión del protocolo IP, que se utilizó para crear el datagrama, siendo este un campo de 4 bits. Se utiliza para verificar que el emisor y el receptor de acuerdo con el formato del datagrama.

IHL(Longitud del Campo IP): También de 4 bits, proporciona el encabezado del datagrama con una longitud medida en palabras de 32 bits. [3,Pag 94]

TIPO DE SERVICIO: Especifica como desearía un protocolo de las capas superiores que se manejara un datagrama y les asigna diferentes niveles de acuerdo con su importancia.

LONGITUD TOTAL: Muestra la longitud total, en bytes, del paquete IP, incluyendo los datos y el encabezado.

IDENTIFICACIÓN: Consta de un numero entero que identifica el datagrama actual. Este campo se utiliza para ayudar a reconstruir los fragmentos del datagrama.

APUNTADORES: Este es un campo de 3 bits, de los cuales 2 bits de menor orden (los menos significativos) controlan la función de fragmentación. El bit de menor orden especifica si se puede fragmentar el paquete. El bit de en medio especifica si el paquete es el último fragmento en una serie de paquetes fragmentados. El tercer bit, o bit de orden mayor no se usa.

DESPLAZAMIENTO DEL FRAGMENTO: Indica la posición de los datos del fragmento, en relación con el comienzo de los datos en el datagrama original, lo cual permite que el proceso IP del destino reconstruya adecuadamente el datagrama original.

TIEMPO DE VIDA: Conserva un contador que disminuye gradualmente hasta llegar a cero, donde se elimina. Esto evita que los paquetes circulen en ciclo de manera indefinida.

PROTOCOLO: Indica qué protocolo de las capas superiores recibe los paquetes entrantes una vez terminado el procesamiento IP.

SUMA DE VERIFICACIÓN DEL ENCABEZADO: Ayuda a asegurar la integridad del encabezado.

DIRECCION ORIGEN: Especifica el nodo emisor.

DIRECCIÓN DESTINO: Especifica el nodo receptor.

OPCIONES Permite que el protocolo IP soporte diferentes opciones como la seguridad.

DATOS: Contiene información de las capas superiores.

1.1.2.3 PROTOCOLO DE CONTROL DE TRANSMISIÓN (TCP)

TCP permite la transmisión confiable de información, especificando el formato de los datos y los acuses de recibo que intercambian las computadoras para que su transferencia sea confiable en un ambiente IP, además de los procedimientos que la computadora utiliza para asegurarse de que los datos lleguen a su destino.

Entre los servicios que da TCP se encuentran:

- *Transferencia de Datos en ráfagas:* En este servicio se entrega una ráfaga no estructurada de bytes, identificada por una secuencia de números, así los datos no se fragmentan en bloques para ser entregados a TCP facilitándole el trabajo a las aplicaciones.

- *Confiabilidad:* Esta función permite una entrega de paquetes de extremo a extremo de forma segura, orientado a la conexión, además, permite que los dispositivos puedan reparar errores como; paquetes mal leídos, duplicados, retrasados o perdidos.

- *Control de flujo eficiente:* significa que cuando se dan confirmaciones de regreso al origen, el proceso de recepción de TCP muestra un número de secuencia mayor que puede recibir sin saturar sus dispositivos de almacenamiento internos.

- *Operación Dúplex*: Es cuando los procesos de TCP se envían y reciben al mismo tiempo.

- *Multiplexaje:* Indica que es posible multiplexar varias conversaciones de las capas superiores de manera simultánea, a través de una sola conexión.

TCP utiliza las conexiones que se identifican por medio de un par de puntos extremos, definiendo como punto extremo a un par de números enteros (anfitrión, puerto) en donde anfitrión es la dirección IP y el puerto, un número que identifica el servicio. Ejemplo, el punto extremo (128.10.2.3, 25), que se refiere al puerto TCP 25 en la máquina con dirección IP 128.10.2.3. [3,Pag 201]

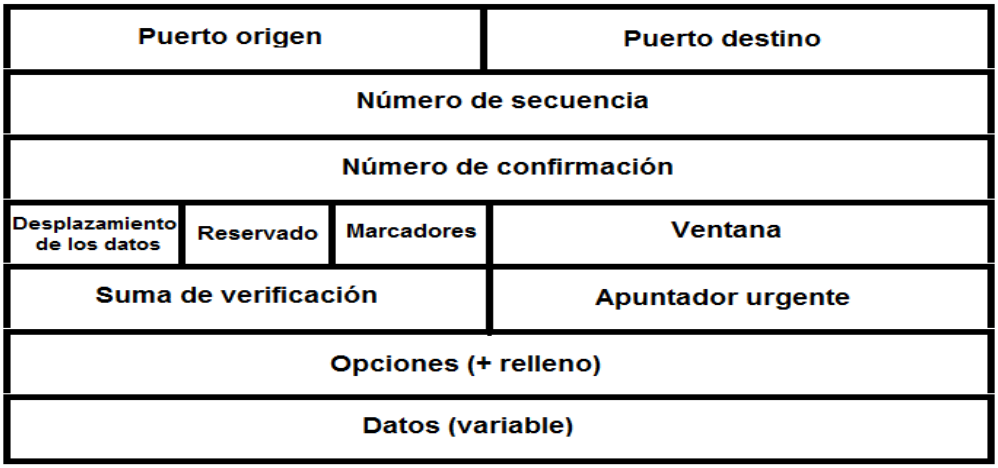


Fig 1.4 Los 12 campos de un paquete TCP
[5, Pag. 384, Figura 28-10]

En esta parte, se mencionan los campos del paquete TCP descritos por Ford, Lew, Spanier, y Stevenson en su libro Tecnologías de interconectividad de redes:

PUERTO ORIGEN Y PUERTO DESTINO: Identifican los puntos en que los procesos origen y destino de las capas superiores reciben los servicios TCP.

NÚMERO DE SECUENCIA: En general, especifica el número que se asigna al primer byte de datos en el mensaje actual. En la fase de establecimiento de la conexión, este campo también puede utilizarse para identificar un número de secuencia inicial que será utilizado en una transmisión futura.

NUMERO DE CONFIRMACIÓN: Contiene el número de secuencia del siguiente byte de datos que el emisor del paquete espera recibir.

DESPLAZAMIENTO DE DATOS: Indica el número de palabras de 32 bits en el encabezado TCP.

RESERVADO: Permanece reservado para su uso en un futuro.

APUNTADORES: Transportan una gran variedad de información de control, incluyendo los bits de SYN (Synchronize, Activa/desactiva la sincronización de los números de secuencia) y ACK (Acknowledgement, acuse de recibo) utilizados para el establecimiento de la conexión y el bit FIN que se utiliza para la terminación de la conexión.

VENTANA: Especifica el tamaño de la ventana del receptor del emisor (esto es el espacio de almacenamiento disponible para los datos entrantes).

SUMA DE VERIFICACIÓN: Indica si el encabezado se dañó durante su viaje.

APUNTADOR DE URGENTE: Apunta hacia el primer byte de datos urgente en el paquete.

OPCIONES: Especifica las diferentes opciones de TCP.

DATOS: Contiene información de las capas superiores.
[5, Pag 384 y 385]

1.1.2.4 PROTOCOLOS EN TCP/IP

Aunque el nombre TCP/IP hace pensar que es solo la combinación de los dos Protocolos; Protocolo de Control de Transmisión (Transmission Control Protocol) y Protocolo de Internet (Internet Protocol), el término TCP/IP se refiere a un conjunto más grande de protocolos que proporcionan los servicios de red, como registros remotos, transferencias de archivos remotas y correo electrónico.

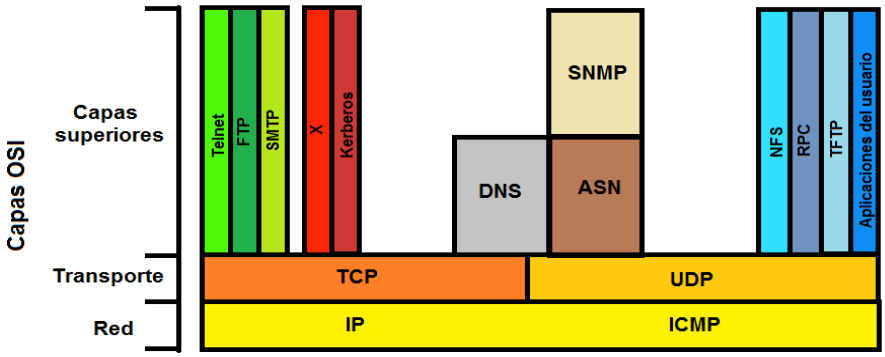


Fig 1.5 Protocolos TCP/IP
[1, Pag. 34, Figura 2.1]

En la fig 1.5, se puede observar de forma gráfica, la relación de dichos protocolos en las comunicaciones, y su relación lógica con respecto a los modelos de capas, ayudando a entender o comprender mejor su interacción entre sí, ya que por ejemplo; la figura señala en bloques algunos de los protocolos de la capa superior que dependen del TCP (como telnet y FTP), mientras que algunos dependen de UDP (como TFTP y RPC). La mayor

parte de los protocolos TCP/IP de las capas superiores usan sólo uno de los dos protocolos de transporte (TCP o UDP), y unos cuantos, incluyendo DNS (Domain Name Service), pueden usar ambos.

A continuación se enlistan los nombres completos de los protocolos que aparecen en la fig 1.5.

- Telnet – (TELecommunication NETwork)
- *FTP – (*File Transfer Protocol *)*Protocolo de Transferencia de Archivos
- SMTP – (Simple Network Management Protocol) Protocolo Simple de Transferencia de Correo
- X- Sistema X Windows
- Kerberos- Protocolo de Autenticación (Seguridad)
- DNS- (Domain Name System) Sistema de Nombre de Dominio
- ASN- (Abstract Syntax Notation)Notación de Sintaxis Abstracta
- SNMP- (Simple Network Management Protocol) Protocolo Simple de Administración de Redes
- NFS- (Network File System) Servidor de Archivos de Red
- RPC- (Remote Procedure Call) Llamadas de procedimiento Remoto
- TFTP- (Trivial File Transfer Protocol)Protocolo Trivial de Transferencia de Archivos
- TCP- (Transmission Control Protocol) Protocolo de Control de Transmisiones
- UDP- (User Datagram Protocol) Protocolo de Datagramas de usuario
- IP- (Internet Protocol)Protocolo Internet
- ICMP- (Internet Control Message Protocol) Protocolo Internet de Mensajes de Control

1.2MAQUINAS VIRTUALES

1.2.1 VIRTUALIZACIÓN

Realizando una definición simple de virtualización, se puede decir que es cuando un programa o aplicación que se instala en un sistema operativo (llamado anfitrión) permite instalar y ejecutar otro SO o aplicación dentro del primero, como si fuera un equipo completamente diferente, tomando el nombre este ultimo de maquina virtual.

La definición en el manual de "Irochka (2008)" sobre virtualización dice: "Esta capa de aplicación, que puede ser una aplicación o directamente un sistema operativo (hypervisor), permite aislar los sistemas operativos virtualizados del sistema físico, proporcionándoles un hardware virtual uniforme. De este modo, la memoria RAM, las CPUs, los discos duros y los dispositivos de red, pasan a ser recursos que se ofrecen a las Máquinas Virtuales". [23, pag 6]

La virtualización, ofrece una nueva idea en el uso de recursos, que es la de eliminar el antiguo modelo utilizado de "un servidor una aplicación" y colocar varias máquinas virtuales en cada máquina física de un laboratorio o empresa, mejorando la eficacia y

disponibilidad de los recursos y aplicaciones de TI. En la parte económica o de gastos también es importante, ya que, aproximadamente el 70% de un presupuesto de TI no virtualizado se dedica a mantener la infraestructura existente y gastar en más hardware, provocando que la innovación se detenga, en este caso para esta investigación servirá para representar un ambiente real de laboratorio y realizar pruebas. [54]

Como se sabe es mejor realizar pruebas de configuraciones en una máquina que no es crítica para el laboratorio o negocio, esto es lo que ofrecen las máquinas virtuales, ya que éstas se pueden recuperar en muy poco tiempo, sin que ni siquiera afecte el ambiente de trabajo del equipo real.

Se espera que en los próximos años la virtualización mueva su éxito con relación a el almacenamiento, los servidores, el desarrollo en redes y centros de datos permitiendo construir versiones de software que representen switches, routers, balanceadores de carga, aceleradores y cache, exactamente como se necesitan en hardware.

Si los proveedores de virtualización prometen estos avances los cambios que alguna vez estuvieron fuera de cuestionamiento o que al menos requerían de un considerable riesgo, gasto, tiempo, personal capacitado y operación, serán hechos en minutos, rutinariamente y a bajo costo, esto hace imaginarse que en un futuro la virtualización podría convertirse en una completa simulación de sistemas reales, que podrían no solo ser hardware de computación, si no motores, conectores, válvulas, puertas, maquinaria, vehículos y sensores, corriendo en paralelo con equipos físicos y en tiempo real.

1.2.2 CONCEPTO DE MÁQUINA VIRTUAL

En 1972 nace el concepto de máquina virtual junto al sistema VM/370 de IBM. Pues se tuvo la idea en mente de querer ejecutar varios sistemas operativos simultáneamente, sobre el mismo hardware. Para lograr esto, fue necesario separar dos funciones básicas de un sistema de tiempo compartido: multiprogramación y abstracción del hardware.

La definición de máquina virtual se dio en el tema anterior (1.2.1VIRTUALIZACION), de la cual, se puede explicar que es como un contenedor de software especializado, perfectamente aislado y se encarga de emular un PC físico o real y puede ejecutar sus propios sistemas operativos y aplicaciones, como si fuera un equipo completamente diferente, además existen diferentes tipos y para diversas aplicaciones.

El comportamiento de estos equipos virtuales es como lo hace una computadora física y contiene sus propios CPU, RAM, disco duro y tarjetas de interfaz de red (NIC) virtuales (basados en software), lo que hace pensar, que el sistema operativo no puede establecer una diferencia entre una máquina virtual y una máquina física, ni tampoco lo pueden hacer las aplicaciones u otras computadoras de una red. Incluso se puede imaginar que la propia máquina virtual se considera una computadora “real”..

El único inconveniente de las máquinas virtuales y una característica importante, es que los procesos que ejecutan están limitados por los recursos y abstracciones proporcionados por el equipo real, así una computadora con gran capacidad en hardware y software adecuado para la virtualización puede alojar varias máquinas virtuales, todas ellas compartiendo los componentes físicos de la máquina física.

Existen en sí dos tipos de maquinas virtuales, con diferente definición y funcionalidad:

- *Máquinas virtuales de sistema:* Permiten a la máquina física subyacente multiplexarse entre varias máquinas virtuales, cada una ejecutando su propio sistema operativo. A la capa de software que permite la virtualización se la llama monitor de máquina virtual o "hypervisor". Un monitor de máquina virtual puede ejecutarse directamente sobre el hardware o bien sobre un sistema operativo.

    - Virtualizacion a nivel Sistema Operativo: En éste tipo de virtualización la base o anfitrión es un sistema operativo donde se instala un programa de virtualizacion que permite instalar a su vez otros sistemas operativos (invitados) trabajando estos sobre el SO principal, gracias a la capa de virtualización colocada por un software como Vmware Workstation o virtual Pc.

    - Virtualizacion a nivel de Hardware: En ésta virtualización de servidores, el hipervisor o software de virtualización se instala antes de cualquier SO, presentando el hardware de la computadora a todos los sistemas operativos instalados y emulando los recursos que esta tiene. El hipervisor es el encargado de coordinar el acceso a los recursos del servidor, este tipo de virtualizacion se divide en:

        - Virtualización Nativa: Virtualiza sólo los recursos necesarios para aislar el Sistema Operativo.

        - Paravirtualización: Comparte los recursos por intervalos de tiempo cortos o da mayor prioridad al SO que los necesite, ofreciendo mayor cantidad de recursos como procesador, memoria o tarjeta de red al SO que lo pide e intercalando el uso de estos recursos con todos los sistemas operativos que tenga instalados. [49]

- *Máquinas virtuales de proceso (Máquina virtual de aplicación):* Esta se ejecuta como un proceso normal dentro de un sistema operativo y soporta un solo proceso. La máquina se inicia automáticamente cuando se lanza el proceso que se desea ejecutar y se detiene cuando éste finaliza. Su objetivo es el de proporcionar un entorno de ejecución independiente de la plataforma de hardware y del sistema operativo, que oculte los detalles de la plataforma subyacente y permita que un programa se ejecute siempre de la misma forma sobre cualquier plataforma.El ejemplo más conocido actualmente de este tipo de máquina virtual es la máquina virtual de Java. Otra máquina virtual muy conocida es la del entorno .Net de Microsoft que se llama "*Common Language Runtime*".

En esta tesis solo se tratarán máquinas virtuales de sistema y en esta división las que son de Virtualizacion a nivel sistema operativo, esto para tener una mejor percepción de la virtualización de los equipos para el lector y entre otras cosas por que si se instala Virtualizacion a nivel Hardware no todos los accesorios o dispositivos con los que cuenta el equipo de pruebas son soportados por el hipervisor, pues este es la capa de software que tiene que manejar los dispositivos y pasar los requerimientos de los sistemas operativos invitados.

1.2.3 VENTAJAS Y DESVENTAJAS DE LAS MÁQUINAS VIRTUALES

A continuación se resumen y se examinará algunas ventajas de las maquinas virtuales como son:

Compatibilidad: Las máquinas virtuales deben ser plenamente compatibles con la totalidad de sistemas operativos, aplicaciones y controladores de dispositivos estándar, de modo que se utilice una máquina virtual para ejecutar el mismo software que se puede ejecutar en un computadora física.

Aislamiento: Aunque las máquinas virtuales y la real comparten los recursos de hardware, permanecen completamente aisladas unas de otras, como si estuvieran independientes. Por ejemplo, si existen cuatro máquinas virtuales en un solo servidor físico y fallara una de ellas, las demás siguen funcionando.

Encapsulamiento y portabilidad: Una máquina virtual es básicamente un contenedor de software que agrupa o "encapsula" un conjunto completo de recursos de hardware virtuales, así como un sistema operativo y todas sus aplicaciones dentro de un paquete de software. El encapsulamiento hace que las máquinas virtuales sean portátiles y fáciles de gestionar ya que se pueden copiar de un lugar a otro como cualquier otro archivo.

Configuración Independiente de hardware: La configuración de los componentes virtuales (tarjeta de red, dispositivos de almacenamiento, etc.) se puede realizar de manera independiente a la del equipo físico sin afectar a este. Las máquinas virtuales del mismo servidor físico por ejemplo, pueden tener una IP diferente cada una, aun utilizando la misma interfaz física de red.

Agilidad en la creación y clonación: La rapidez para crear una máquina virtual es de gran importancia, pues si se necesita un nuevo servidor se tiene casi al instante, sin pasar por el proceso de compra, e incluso solo clonando alguna ya existente.

Recuperación rápida en caso de fallo: Al tener un respaldo de los archivos de configuración de la máquina virtual, en caso de desastre o falla, la recuperación es más

rápida, pues la solución solo es arrancar la máquina virtual con el respaldo de configuración guardado. No se necesita reinstalar, recuperar backups y otros procedimientos largos que se aplican en las máquinas físicas.

Reducción del "TCO": El costo total de la inversión en hardware y software (Total Cost of Ownership) se puede ver reducido debido a la virtualización, pues se reduce el consumo de electricidad, la generación de calor, el espacio utilizado y los costos de mantenimiento. Asimismo se pueden aprovechar características de los equipos modernos, tales como los 64 bits de los microprocesadores, los procesadores múltiples y el "hyper threading". Se ha reportado que la reducción de equipos puede ser tan dramática que ciento veinte servidores pueden ser contenidos en tan sólo cuatro equipos.

Así como existen ventajas en el uso de maquinas virtuales, también es necesario conocer las desventajas y limitaciones de estas como son:

Rendimiento inferior: El rendimiento de un sistema operativo virtualizado es menor que si estuviera instalado en el equipo físico. Esto se debe al hipervisor definido en la pag anterior, ya que este introduce una capa intermedia en la gestión del hardware para administrar peticiones de acceso y la concurrencia al mismo, por lo cual el rendimiento de la máquina virtual se ve afectado. Dependiendo de las operaciones que se realicen, las soluciones de virtualización difieren en su rendimiento.

Hardware virtual obsoleto o que no soporta el software de virtualizacion: El programa de virtualización o hipervisor impone una serie de dispositivos virtuales como tarjetas de vídeo y red que no se podrán cambiar.

El hardware viejo como el USB 1.0, Firewire 400, Ethernet 100 son algunos de los dispositivos obsoletos.

Proliferación de máquinas virtuales: Ya que no se compra equipo físico, el número de máquinas y servidores virtuales se dispara en todos los ámbitos. Los efectos se perciben posteriormente al aumentar el trabajo de administración y riesgos de seguridad.

Avería del servidor anfitrión: La avería del servidor anfitrión de virtualización afecta a todas las máquinas virtuales alojadas en él. Se debe pensar más que nunca, en adoptar soluciones de alta disponibilidad como clustering y replicación para evitar caídas de servicio de múltiples servidores con una única avería pues los entornos virtualizados dependen de la estabilidad de su anfitrión, por lo cual se pensará antes de aplicar actualizaciones y parches, ya que estos provocan reiniciar y suspender servicios.

Costo: Los programas de virtualización con mejor rendimiento, tienen un costo, que se deberá pagar para disfrutar de sus beneficios.

Referencias [23, 24, 26, 54, 55]

1.2.4EJEMPLOS DE SOFTWARE DE VIRTUALIZACIÓN

Hay variedad de software para virtualizar, algunos de ellos son comerciales, otros GNU o Open Source, etc. Estos son algunos de los más conocidos:

- VMWare Workstation 7
- Virtual Box
- Parallels
- Microsoft Virtual PC
- Citrix XenServer 5.5
- Microsoft Hyper-V server 2008
- VMware Sphere
- Fusion(para MAC)
- Cameyo(Virtualiza aplicaciones)
- NComputing
- Xen de Virtual Iron (VI)(IBM y HP)
- QEMU CPU Emulator
- KVM

1.2.5 USO DE MAQUINAS VIRTUALES POR PROFESIONALES EN COMPUTACIÓN

La virtualización tiene muchas aplicaciones o usos, principalmente en el área de la computación, por lo cual vamos a mencionar los principales usos de la virtualización para los profesionales de esta área:

Desarrolladores: Cuando se desarrollan, varios servicios en un centro de cómputo, principalmente los servicios web, suelen necesitarse varios servidores. Las maquinas virtuales son de gran utilidad para simular todos los PCs, servidores o redes en un solo computadora, sin la necesidad de cualquier tipo de servicio externo. Después de que todo se prueba y funciona correctamente, se traslada al servidor real. Estos son ejemplos que se podrían virtualizar: Servidores web, gestores de bases de datos, sistemas de control de versiones, etcétera.

Administradores de sistemas: Un administrador necesita realizar bastantes pruebas cuando salen actualizaciones o parches de diferentes versiones de software o Sistema Operativo que se tenga instalado. Si se realizan actualizaciones de parches en máquinas que están en producción es muy arriesgado, pues el servicio podría dejar de funcionar. Por lo cual se recomienda probar en una máquina que sea una réplica de la que se quiere actualizar, lo cual se realiza más rápido con una maquina virtual y así se prueba un funcionamiento correcto, para posteriormente realizar el procedimiento en el equipo real.

*Administradores de redes***:** En una red media-grande surgen varios problemas de mantenimiento. En estas redes es muy común hacer pruebas de un nuevo servicio a instalar, probar el funcionamiento de firewalls u otro equipo de seguridad, simular clientes reales de la red, etc. O también se tiene un gran número de PCs y se puede crear máquinas virtuales que simulen un ambiente real, lo que se realiza en esta investigación principalmente.

Administradores/Auditores de seguridad: Para empresas y gente encargada de seguridad el concepto y uso de máquinas virtuales está a la orden del día, dado que tienen que probar infinidad de sistemas y simular todo tipo de situaciones.

Curiosos: Para las personas que no se encuentran dentro de ninguno de los anteriores grupos, pero les gusta probar todo tipo de cosas, también son muy útiles. Ya que hay gente que ha rescatado sus viejos juegos de MS-DOS en máquinas virtuales, otros que tienen un juego de Linux en Windows (o viceversa) para no afectar su equipo de trabajo. Las maquinas virtuales son muy útiles para estudiantes que necesiten hacer prácticas con otros sistemas operativos y no deseen instalarlo en su computadora y así como estos se podrían nombrar infinidad de casos, en los cuales se mencionaría la gran utilidad de la Virtualización.[27]

1.2.6 ELECCIÓN DE UNA HERRAMIENTA DE VIRTUALIZACIÓN

La elección de la herramienta de Virtualizacion fue basada en su rendimiento y en los beneficios que ofrecia al ser instalada con los dos principales sistemas operativos a utilizar los cuales fueron Windows y Linux. La elección de la herramienta de Virtualizacion en cuanto al rendimiento que ofrecían fue basada en la Tesis del Ing. Albert López Medina llamada "Analisis de la virtualización de sistemas operativos" en la cual se ofrece un estudio detallado con pruebas realizadas evaluando varias de las características de las maquinas virtuales.

Entre estas características se puede mencionar algunas que son de gran relevancia para la investigación que se realiza.

Nombre	Ubuntu	Debian	Suse	OpenSuse	Mandriva	Fedora	Red Hat	CentOS	TurboLinux	Sun Solaris	BSD	Otro Linux 2.6 Kernel
VirtualBox 3.08												
Parallels for Linux 4												
VMware Workstation 7												
Windows VirtualPC												
Citrix XenServer 5.5												
VMWare EXXi 4												
Microsoft Hyper-V Server 2008												

Fig 1.6 Compatibilidad de los SO Linux Invitados.
[21, Pag 32, Fig. 2.17]

En esta imagen se aprecia que VMWare tiene compatibilidad con la mayoría de Sistemas Linux lo cual es una característica importante, ya que la herramienta a utilizar será necesariamente instalada en Linux.

	PC físico Windows 7	VirtualBox (Win y Linux)	Virtual PC (Win)	VMware (Win y Linux)	Parallels (Win y Linux)
Nombre CPU	Intel Core i5 750	Intel Core i7	Intel Core i7	Intel Core i7	Intel Core i7
Voltaje CPU	1.144 v	-	-	-	-
Núm. de núcleos	4	4	1	4	2
Núm. de Threads	4	4	1	4	2
Core Speed	2891.9 Mhz	3000.2 Mhz	3189.3 Mhz	2892.1 Mhz	2992.7 Mhz
FSB	167.7 Mhz	1000.1 Mhz	-	-	310.98
Instrucciones SSE4	Si	No	No	Si	Si
Cache L3	8 Mb	-	8 Mb	8 Mb	8 Mb
Placa Base	Asus P7P55D	Virtualbox	Microsoft Corporation	Intel 440BX Desktop	Parallels Virtual Plataform
Chipset	Intel DMI Host Bridge	Intel i440FX	-	-	Intel P965 / G965
Southbridge	Intel P55	Intel 82371SB (PIIX3)	-	-	Intel 82801HB/HR (ICH8/R)
GPU	Nvidia GeForce 6600GT	Virtualbox graphics adapter	-	-	Parallels vídeo adapter

Fig. 1.7 Identificación de componentes de Hardware con CPU-Z.
[21, Pag 68, Fig 4.1.1]

Como en la simulación que se creará es necesario que el hardaware sea identificado lo mejor posible por la herramienta, esta tabla muestra el estudio realizado con el programa de nombre CPU-Z para identificar el hardware en los sistemas de Virtualización, en el cual se observa que aunque VMWare no logró identificar todo el hardware del equipo fisico, identificó el número de núcleos total, lo cual es una ventaja pues se vuelve mas confiable.

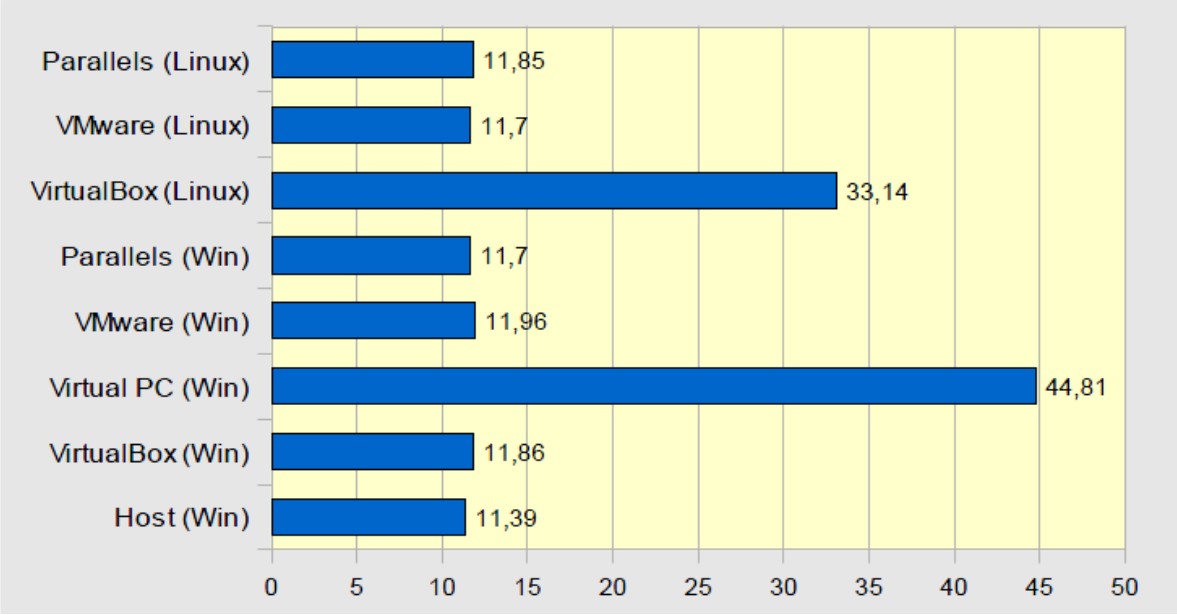


Fig. 1.8 Cálculo de 32 Millones de raíces cuadradas.
[21, Pag 72, Fig 4.1.7]

Esta prueba consistió en calcular las primeras 32 millones de raíces cuadradas en multiproceso para determinar la velocidad de cálculo del procesador, lo cual dejo a VMWare en una buena posición tanto en sistemas Windows como en sistemas Linux

mostrando un menor tiempo de respuesta, lo que quiere decir que realiza mejor dichas operaciones que los demás programas.

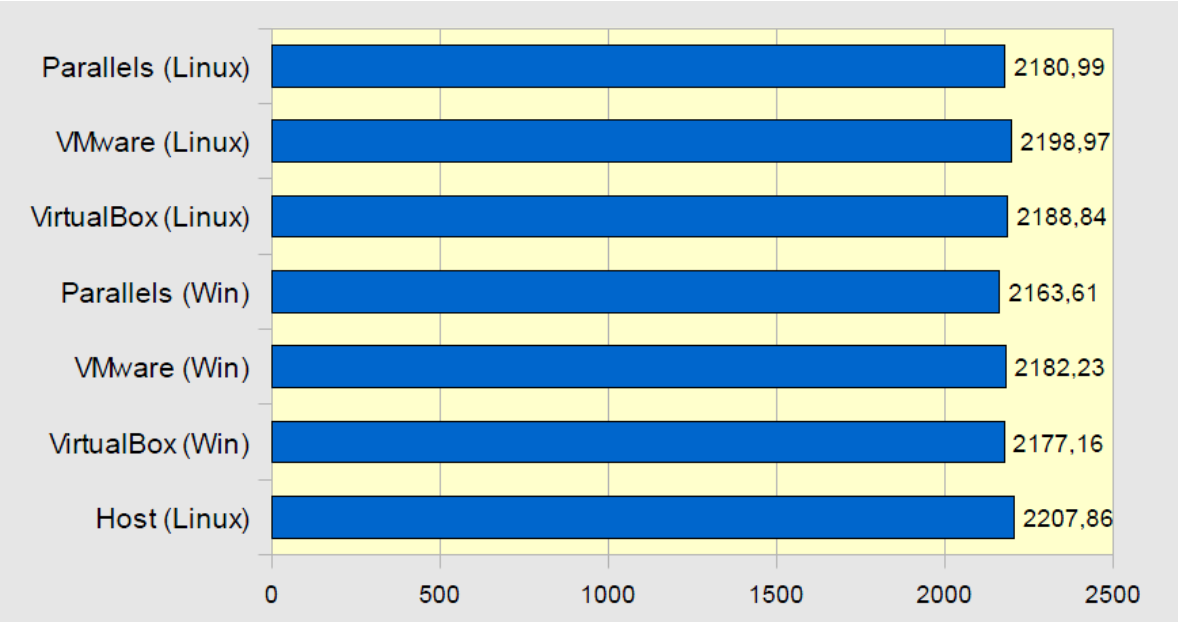


Fig. 1.9 Prueba de memoria cache con CacheBench.
[21, Pag 32, Fig 4.2.6]

Esta imagen muestra la prueba de la memoria y el rendimiento del ancho de banda de la memoria cache, siendo importante para el rendimiento en la virtualizacion y en la cual VMWare con Linux sale victorioso sobre los demás, pues tuvo una mejor velocidad de lectura en Kb/s

Se demuestra así en las pruebas de rendimiento que VMware es el elegido para la simulación, además que para la administración y recuperación con la herramienta Zenoss, existen maquinas virtuales gratuitas en VMWare donde dicha herramienta ya esta preinstalada y se evita realizar todo el proceso de instalación si se trabaja con servidores virtualizados, lo que facilita también el realizar pruebas más rápidamente con versiones actuales. Otra de las causas de la elección de VMWare, es porque ésta empresa siempre esta inovando en cuanto a virtualización se refiere, lo que da confianza al usuario, pues las actualizaciones siempre están disponibles.

1.3 SISTEMAS OPERATIVOS

1.3.1DEFINICIÓN DE SISTEMA OPERATIVO Y SUS FUNCIONES

El **sistema operativo** es el software más importante de una computadora, el cual contiene un conjunto de programas para administrar los recursos del hardware y así el usuario pueda trabajar directamente con el sistema operativo o con programas llamados Software de Aplicación, que funcionan encima del sistema operativo, permitiendo su cómodo manejo y utilización, siendo esta característica un factor importante para la elección del SO.

Tres de las funciones que siempre debe realizar un SO son:

1. Administración de recursos en la computadora.
2. Aplicación de servicios para programas.
3. Ejecución de órdenes de los usuarios.

De cualquier forma un SO es como una interfaz entre los usuarios/aplicaciones y el hardware de un sistema informático.

Las tres principales funciones del SO se realizan en 3 capas principalmente, como se muestra en la figura 1.10.

Núcleo (Kernel): Es la capa más cercana al Hardware la cual gestiona los recursos hardware del sistema y suministra la funcionalidad básica del sistema operativo como: el procesador, la memoria, los dispositivos de E/S.

Capa de servicios o llamadas al sistema: Ésta capa ofrece a los programas, servicios en forma de una interfaz de programación o API (application programming interface); facilitando la creación de programas aplicando las funciones que le suministra el SO.

Intérprete de comandos o Shell: Suministra la interfaz para que el usuario pueda comunicarse de manera interactiva con la computadora. El Shell recibe las órdenes del usuario; los interpreta y si puede los ejecuta. Algunos autores no consideran el Shell como parte del sistema, ya que se ejecuta a nivel de usuario.

En sistemas grandes, el sistema operativo puede tener mayor responsabilidad y poder, ya que se asegura que los programas y usuarios que funcionan al mismo tiempo, no se interfieren entre ellos, además de ser responsable de la seguridad, para que usuarios no autorizados no tengan acceso al sistema. [6]

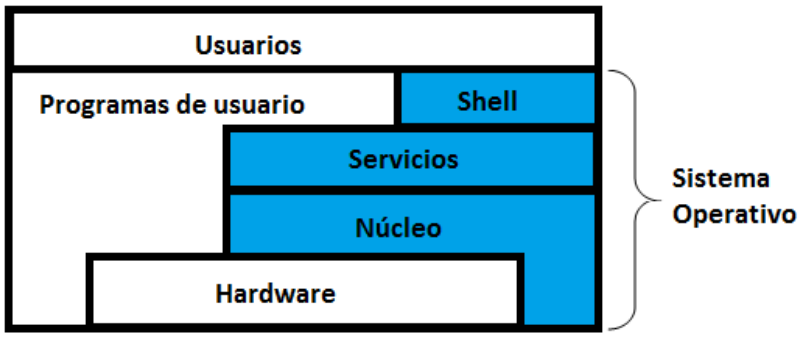


Fig.1.10 Los Niveles del Sistema Operativo
[6,Pag 3, Imagen 2.15]

En este tema se conocerán las capacidades de desempeño y rendimiento de dos sistemas operativos de los más conocidos, que son Windows y Linux; tomando en cuenta consideraciones importantes como su rendimiento y eficiencia conforme a las herramientas de monitoreo.

1.3.2WINDOWS

Microsoft fue creado en 1975 por William H. GatesIII y Paul Allen que compartían la afición a programar. Desarrollaron juntos la primer versión del lenguaje Basic para la Altair 8800, la primera computadora personal, compraron la licencia de este software a Instrumentation and Telemetry Systems (MITS) la empresa creadora de la Altair, y así desarrollaron otras versiones para otras compañías como Apple Computer, fabricante del equipo Apple, Commodore, fabricante del PET, y Tandy Corporation, fabricante del equipo Radio Shack TRS-80. En 1977 Microsoft sacó Microsoft FORTRAN, un nuevo lenguaje de programación, posteriormente sacó nuevas versiones del lenguaje BASIC para los microprocesadores 8080 y 8086.

IBM contrato Microsoft en 1981 para la creación del sistema operativo IBM PC, Microsoft presionados por el tiempo compró QDOS (Quick and Dirty Operating System) a Tim Paterson por 50.000 dólares y le cambió el nombre a MS-DOS. El contrato firmado con IBM permitía a Microsoft vender el sistema operativo a otras compañías, otorgando licencias a 200 fabricantes de equipos informáticos, siendo así el más utilizado.

Hasta que en 1985 Microsoft lanzó Windows, que ampliaba las prestaciones de MS-DOS e incorporaba por primera vez una interfaz gráfica de usuario, siendo una bendición para usuarios de computadoras no acostumbrados al uso de exhaustivo de MS-DOS. Windows 2.0, salió en 1987, con mejor rendimiento y nuevo aspecto visual. Tres años después apareció Windows 3.0 a la que le siguieron Windows 3.1 y 3.11, cuyas versiones ya venían instaladas en casi todos los equipos llegando a ser el más utilizado del mundo, así en 1990 fue la empresa líder de programas informáticos, mejorando cada vez más sus productos, hasta llegar a la familia Windows NT y versiones más actuales como Windows 7 de 64 bits.[2, 6, 7]

La familia Windows NT cuenta con versiones como:

- Windows NT
- Windows NT 3.1
- Windows NT 3.5/3.51
- Windows NT 4.0
- Windows 95
- Windows 98
- Windows 98 Second Edition
- Windows Millenium Edition
- Windows 2000
- Windows XP
- Windows Server 2003
- Windows Vista
- Windows Server 2008
- Windows 7

1.3.3 LINUX

Linux aparece en los 90´s realizado por Linus Torvalds, quien se inspiró en MINIX un sistema operativo realizado por Andrew S. Tanenbaum. La primera versión 0.01 incluía los principios del núcleo del sistema y funcionaba sobre el sistema MINIX instalado, pero nunca fue anunciada.

La primera versión oficial con numeración 0.02 se anuncio el 5 de octubre de 1991, logrando ejecutar ya el bash (GNU Bourne Shell) y el gcc (GNU C compiler), pero no se pensaba en términos de soporte, documentación o distribución.

Posteriormente de la versión 0.03, Linus cambió la numeración hasta la 0.10, pues programadores en internet trabajaron en el proyecto. En marzo de 1992 se incremento la versión a la 0.95, en diciembre de 1993 el núcleo del sistema estaba en la versión 0.99, llegando la versión 1.0 en marzo de 1994, así día a día se fue mejorando el sistema.

Las distribuciones de Linux, son empresas que recopilan programas y archivos organizados y preparados para instalación, lo cual proporciona un gran beneficio y comodidad para los usuarios.

Estas distribuciones se pueden obtener en internet vía FTP sin pago alguno o comprando los CD´s de las mismas. Así existen Distribuciones como:

- Red Hat- Fedora
- Mandrake Linux
- Debian
- Knoppix
- SuSE- Novell Linux Desktop

[58, Historia de Linux, PI]

1.4 PROBLEMÁTICA A RESOLVER EN UN LABORATORIO DE CÓMPUTO

Un laboratorio de cómputo es un núcleo muy importante para satisfacer las necesidades de información y aprendizaje en una institución, de manera veraz y oportuna, en tiempo y forma, centralizando, custodiando y procesando la mayoría de la información con la que se opera.

Sin embargo, en la actualidad las redes de computo se vuelven más complejas y la exigencia de una buena operación en ellas es cada vez mas demandante e importante ya que soportan aplicaciones y servicios estratégicos e importantes de las organizaciones, las cuales si fallan, sin saber el punto de ruptura pueden causar pérdidas de información, dinero, tiempo e incluso dar una mala imagen para la entidad.

Por lo cual, mejorar la disponibilidad, estabilidad y visibilidad del uso de recursos informáticos, es de gran relevancia, ya que en materia de seguridad y de efectividad en transmisión de datos siempre hay obstáculos que impiden el buen desempeño de la red. Para esto, se debe establecer medidas de seguridad adecuadas que anticipen posibles fallas del sistema y de forma efectiva protejan los activos de la red.

Los problemas que pueden existir en un laboratorio de computo son bastantes, y se incrementan cuando no existe una buena administración, lo que se ve reflejado en el rendimiento y funcionamiento de la red, además de la falta de seguridad informática, entre otros. Existiendo fallas en la capa física (cableado, conexiones, distribución física, etc.), de los equipos activos que intervienen (switchs, hubs, routers, wireless, tarjetas de red, pcs, etc.), así como fallas de la organización lógica de los protocolos de comunicación utilizados y de la organización de administración de la red (VLAN, direccionamiento, enrutamiento, protocolos nuevos a utilizar y la implementación de QoS calidad de Servicio).

La falta de seguridad informática es también una de las razones por las que existen varios de los principales problemas en una red o en el laboratorio en general. El objetivo de la seguridad informática, se puede sintetizar en 5 aspectos principales: Confidencialidad, Integridad, Disponibilidad, control de acceso y no repudio, siendo que la ausencia de estos puede causar problemas más graves para el centro de cómputo.

Por lo cual es recomendable tener un análisis detallado, que surge a partir del estudio de la red del laboratorio, lo que ofrece un conocimiento de su funcionamiento y en caso de existir algún error, dar acción inmediata a su restablecimiento, siendo ésta la definición de "Monitoreo del laboratorio de cómputo".

Ayudando a evitar problemas como:

- Perdida de información confidencial
- Malware

- Caída de enlaces
- Denegación de servicio
- Distribución no acorde al uso efectivo de los servicios
- Demanda que supera la capacidad de transmisión de los enlaces.
- Paquetes perdidos
- Retransmisiones de paquetes
- Retardos elevados
- Tormentas de broadcast
- Etc…

Una Tormenta de broadcast se produce cuando existen tantas tramas de broadcast atrapadas en capa 2 que se consume todo el ancho de banda disponible, dejando la red inservible siendo un ejemplo de las consecuencias de estos problemas.

El monitoreo ofrece también información estadística para pasar de una cultura reactiva y correctiva, a una cultura proactiva y preventiva, por parte de quienes toman las decisiones, y así tener en cuenta por ejemplo la escalabilidad, ya que una red escalable puede expandirse rápidamente para admitir nuevos usuarios y aplicaciones, sin afectar el rendimiento del servicio enviado a los usuarios actuales o encontrar áreas utilizadas en exceso y las áreas utilizadas insuficientemente, además de identificar dónde ocurren la mayoría de los errores, que suelen ser pieza clave para la creación de nuevas políticas de red, entre otras acciones preventivas, que si no se toman en cuenta pueden llegar a convertirse en un problema más grave.

1.4.1DISPOSITIVOS PARA MONITORIZAR

Una definición formal de monitoreo en el área de redes es: "Análisis detallado del estudio de la red supervisada, ofreciendo un conocimiento de su funcionamiento y en caso de tener algún error dar acción inmediata a su restablecimiento".[37]

La importancia de vigilar el tráfico en una red, es su seguridad y mantener de manera correcta su funcionamiento, este es el objetivo principal para los administradores, ya que no se puede considerar secundaria, debido a que es vital que los sistemas funcionen todo el tiempo para dar servicio al usuario final.

Se necesitan herramientas eficientes para la detección de posibles errores o saber con anticipación sobre posibles caídas del sistema, fluctuación en la velocidad de transmisión de datos y varios elementos más que resultan oro molido para el administrador de la red, permitiéndole incrementar la productividad del sistema administrado. De aquí, la importancia de realizar un análisis y monitoreo de redes convirtiéndose en una labor cada vez mas importante y de carácter pro-activo evitando problemas futuros.

Siendo la diferencia entre el simple análisis de datos y monitorear una red, el que se pueda realizar acciones específicas en caso de que una infraestructura de redes pueda tener algún tipo de problema y que al momento de detectar el error en el servidor encargado para

monitorear la red, el administrador pueda reaccionar restaurando la infraestructura de la red para su correcto funcionamiento.

Los recursos que son administrados en las redes de computadoras, abarca el monitoreo y control de hardware además de componentes de software de redes diferentes. Estos son algunos de los componentes de hardware:

1. Conexiones físicas: incluye equipo relacionado con las capas físicas y de enlace.
2. Componentes de Computadora: incluye dispositivos de almacenamiento, procesadores, impresoras y otros.
3. Componentes de interconexión y conectividad: se refiere a los componentes de hardware tales como repetidores, bridges, ruteadores, gateways, hubs y módems, .
4. Hardware de telecomunicaciones: estos son módems, multiplexadores y switches.

El software típico que se monitorea incluye:

1. Software del sistema operativo: Windows, Linux, etc.
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 módems.
5. Software de aplicación en modelo cliente servidor: incluye servidores de base de datos, servidor de archivos y servidores de impresión, entre otros servicios que se ofrecen en una red.
6. Software de telecomunicaciones y comunicación de datos: software de administración, relacionado a la comunicación de datos y protocolos de telecomunicación.

1.5 FUNDAMENTOS EN EL MONITOREO DE RED

Son varias las razones que llevan a monitorizar una red, pero la más común es el deseo de saber cuándo está fallando algo. Además de que se localizan fallos, monitorizar sirve también, para predecir situaciones determinadas o evitar otras desagradables. Sabiendo, por ejemplo, que el disco de algún servidor se encuentra al 95% de su capacidad total, se puede anticipar y añadir más espacio antes de que se tengan problemas.

Otra ventaja de la monitorización de la red es que facilita los planes de ampliación. Por ejemplo, el proporcionar datos de históricos informará, sobre qué emails se ven incrementados en un 10% mensual, ayudando a decidir si en x meses será necesario un nuevo servidor de correo o no.

1.5.1CARACTERÍSTICAS Y PROFUNDIDAD DEL MONITOREO

El monitoreo de una red se puede realizar obteniendo datos al recolectar y analizar el tráfico de ésta, empleando dispositivos como sniffers, ruteadores, computadoras con software de análisis de trafico y en general dispositivos con soporte para SNMP, RMON entre otros, o también realizando un análisis más profundo basado en:

- *Basado en ICMP*.
  - Diagnosticar problemas en la red
  - Detectar retardo, pérdida de paquetes.
  - 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)

[37,Pag 2]

Comunmente para caracterizar y contabilizar el tráfico en la red se utilizán técnicas que describe Vicente Altamirano en su trabajo llamado "Monitoreo de recursos de red" [37] las cuales se describen acontinuación:

- *Solicitudes remotas*

Mediante SNMP: Esta técnica es utilizada para obtener estadísticas sobre la utilización de ancho de banda en los dispositivos de red, para ello se requiere tener acceso a dichos dispositivos. Al mismo tiempo, este protocolo genera paquetes llamados *traps* que indican que un evento inusual se ha producido.

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

- *Captura de tráfico*

Se puede llevar a cabo de dos formas:

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

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 dispositivos 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 routers o mediante dispositivos que sean capaces de capturar tráfico y transformarlo en flujos. También es usado para tareas de facturación (billing). [37,Pag 3]

Además la mayoría de las aplicaciones de monitorización se han centrado en una de las tres áreas siguientes:

*Monitoreo de Fallas o de Estados (Fault Monitoring):*El principal objetivo del sistema de monitoreo de fallas, es que este puede servir para detectar, reportar, aislar, reparar o darle un seguimiento a la falla o problema lo más pronto posible, siendo la funcionalidad base de la mayoría de los sistemas de gestión de redes. Un agente de monitoreo de fallas podría mantener un registro (log) de eventos importantes y de errores. Comúnmente el agente de monitoreo de fallas tiene la capacidad de reportar los errores a uno o más gestores.

Un buen sistema de monitoreo de fallas será capaz de anticipar fallas. Esto implica la creación de umbrales y emitir un reporte cuando una variable de monitoreo cruce un umbral. Por ejemplo si el nivel de la trasmisión de paquetes que sufren error excede un cierto valor, este podría indicar que un problema es desarrollado a lo largo de un camino en las comunicaciones. Si el umbral es colocado a un nivel bajo, el administrador de red puede ser alertado a tiempo para tomar acciones que eviten una falla en el sistema principal.
El sistema de monitoreo de fallas, debe también ayudar a aislar, diagnosticar la falla y finalmente corregirlas.

Monitoreo de Rendimiento (Performance Monitoring): Un requisito absoluto para la administración de una red de comunicaciones, es la habilidad para medir el rendimiento de la red o mejor dicho realizar un Performance Monitoring (monitoreo de rendimiento).

El Performance Monitoring, consiste en observar y recolectar la información referente al comportamiento de la red, como servicios, reporte de fallas y datos sobre el comportamiento y evaluación de la eficiencia de los recursos en aspectos como:

a) Utilización de enlaces: Se refiere a la cantidad de ancho de banda utilizado por cada uno de los enlaces de área local ya sea por elemento de la red o en conjunto.

b) Caracterización de tráfico: Es la tarea de detectar los diferentes tipos de tráfico que circulan por la red, con el fin de obtener datos sobre los servicios de red más utilizados.

c) Porcentaje de transmisión y recepción de información: Sirve para detectar elementos de la red que más solicitudes hacen y atienden, como servidores, estaciones de trabajo, dispositivos de interconexión, puertos y servicios.

d) Utilización de procesamiento: Es importante conocer la cantidad de procesador que un servidor ésta consumiendo para atender una aplicación.

Monitoreo de Contabilidad de Registros o Logs (Accounting): El monitoreo de contabilidad es principalmente el seguimiento de usuarios usando los recursos de la red, pues virtualmente toda aplicación genera logs para informar sobre qué está sucediendo y qué puede estar yendo mal. La gestión de registros o logs es un conjunto de funciones que habilita la medición del uso de servicios de red. El monitoreo de contabilidad de registros debería facilitar, el establecer parámetros en la utilización de algún servicio.

Por ejemplo, el conteo de logs en sistemas internos, puede ser usado únicamente para evaluar el uso general de los recursos. Pues se puede medir el tiempo y otras características de acceso en la red por los usuarios.

Los ejemplos de recursos que pueden ser sujetos al monitoreo de contabilidad de logs, incluye a los siguientes:

- Equipos de comunicación: en LAN´s WANs, líneas arrendadas, líneas dial-up, y sistemas PBX, Hardware de computadora: Workstations y servidores.
- Sistemas y software: aplicaciones y software de utilidad en servidores, un centro de datos, y sitios de usuarios finales.
- Servicios: Incluye todas las comunicaciones comerciales y servicios de información disponibles para usuarios de red.

Para algunos tipos de recursos dados, los datos son recolectados y posteriormente contados, estos son basados en los requerimientos de la organización.

El conjunto de estas herramientas es lo que se conoce como sistema de monitorización de redes dedicándose a la observación y análisis de estados además del comportamiento de los sistemas finales.

1.5.2 TIPOS DE INFORMACIÓN EN EL MONITOREO DE UNA RED

La información que podría estar disponible en el monitoreo de red puede ser clasificada de la siguiente manera:

Estática: Esta es la información característica y no cambia o lo hace con poca frecuencia, basándose en la actividad de la red, manteniendo una configuración actual y sus elementos, tales como números de identificación de puertos en un router. Sirve además para monitorizar la gestión de configuraciones en equipos, estando la información disponible para un agente monitor si este cuenta con el agente apropiado.

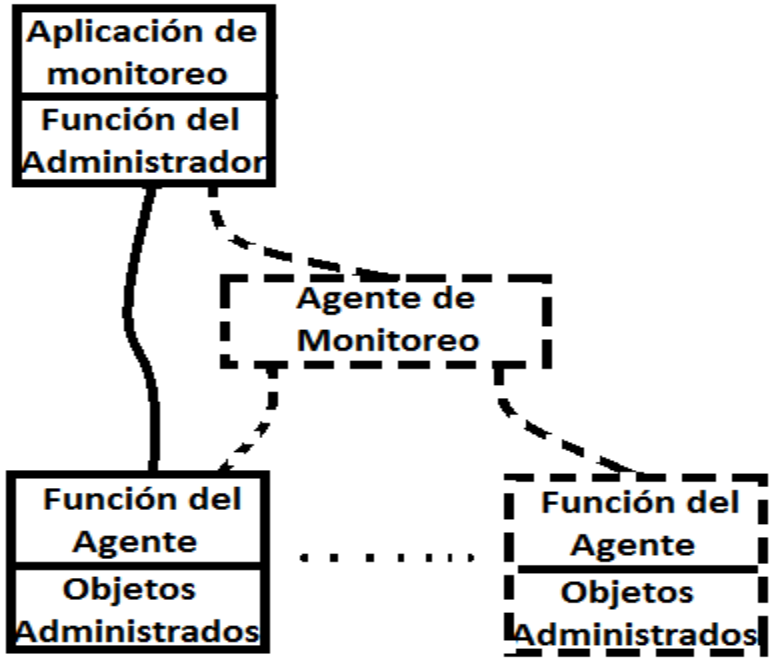
Dinámica: Esta información está relacionada con eventos en la red evolucionando continuamente, como podría ser un cambio de estado de protocolos en un sistema o la transmisión de un paquete en una red, la información suele capturarse por elementos de la red responsables de eventos importantes permitiendo incluso gestionar fallos al observar los cambios en los estados de los dispositivos.

Estadística: Esta información podría ser la derivada de la información dinámica, tales como el número promedio de paquetes transmitidos por unidad de tiempo o por algún sistema final, proporcionando un mayor significado de gestión mediante medidas, varianzas, etc. Es capturada por cualquier sistema que tenga acceso a la información dinámica elemental.

La información estadística suele ser generada por datos llamados "raw" que son trasmitidos al equipo monitor. Donde esta información es analizada y resumida.

1.5.3 ARQUITECTURA DEL MONITOREO DE RED

La figura 1.11 ilustra la arquitectura del monitoreo de red en términos funcionales. La parte (a) de la figura muestra los 4 componentes principales de un sistema de monitoreo de red.



(a) Administrador – Agente modelo (b) modelo resumen

Fig 1.11 Arquitectura para el monitoreo de red
[9, Pag 28, fig 2.3]

Cada uno de los componentes, se describen basados en la obra de William Stalling, titulado: "SNMP, SNMPv2, SNMPv3, and RMON 1 y 2":

Aplicación de Monitoreo: Este componente incluye las funciones de red de monitoreo que son visibles para el usuario, tales como rendimiento de monitoreo, fallas de monitoreo, y monitoreo contable.

Función de Administrador o Gestor: Este es el modulo del monitor o gestor de red que realiza las funciones básicas de monitoreo, como el recoger o recuperar información de los elementos de la red.

Función del Agente: Este modulo recoge y almacena la información administrada por uno o más elementos de red y comunica o envía la información al monitor (gestor).

Objetos Administrados: Esta es la información administrada que representa a los recursos y sus actividades, es útil para resaltar un módulo funcional adicional en cuestión con información estadística

Agente de Monitoreo: Este módulo genera resúmenes y análisis estadísticos de la información administrada. Si este modulo es remoto al gestor, actúa como un agente y comunica la información estadística que genera a dicho gestor. (figura 1.9 part (b)). [9,Pag 26]

La estación que contiene la aplicación de monitoreo, es un elemento de red sujeto al monitoreo de otros equipos en la LAN, de esta manera, el monitor o gestor de red generalmente incluye un software agente y un conjunto de objetos administrables. En realidad, este es vital para monitorear el estatus y comportamiento del propio gestor de red y asegurar que este continúe bien para realizar sus funciones y para evaluar la carga en sí mismo y en la red.

Un consejo es que el protocolo de administración de red sea utilizado para monitorear la cantidad de tráfico de red dentro y fuera del gestor de red.

1.5.4 TÉCNICAS DE MONITOREO.

La información que es útil para el monitoreo de red es recolectada y almacenada por agentes y puesta a disposición de uno o más sistemas gestores o administradores. Dos técnicas usadas para poner la información del agente a disposición del gestor o administrador son: polling y event reporting.

1.5.4.1 POLLING O SONDEO

Polling es un acceso periódico a la información de gestión con interacción entre un gestor y un agente. El administrador puede consultar algún agente (del cual tiene autorización) y solicita los valores de varios elementos de información; el agente responde con información de su MIB local.

Las peticiones pueden ser de dos tipos:

Específica: Pidiendo y enlistando uno o más nombres de variables concretas.

Genérica o de búsqueda: Preguntando al agente sobre los reportes de información que coincidieron con ciertos criterios de búsqueda, o para suministrar al administrador información acerca de la estructura de la MIB en el agente.

Un sistema de administración, puede usar polling para aprender acerca de la configuración que está administrando, obteniendo periódicamente una actualización de condiciones o también, para investigar un área en detalle después de haber sido alertado de un problema. Polling es además, utilizado para generar un reporte en el comportamiento de un usuario y para responder a peticiones de usuarios específicos.

1.5.4.2 EVENT REPORTING O NOTIFICACIONES

Con event reporting (Informe de eventos), el agente toma la iniciativa y el administrador o gestor esta como oyente, esperando por información entrante. Un agente puede generar un reporte periódicamente, para dar al administrador un estatus actualizado de los elementos. El reporte periódico, puede ser pre-configurado o establecido por el

administrador. Un agente puede también generar un reporte cuando un evento relevante ocurre (por ejemplo, un cambio de estado), o un evento inusual (por ejemplo una falla).

Este sistema de comunicación es útil para detectar problemas tan pronto como estos ocurran, siendo más eficiente que polling o sondeo para monitorizar los objetos que cambian de estados o valores, cambiando relativamente con poca frecuencia.

Ambos polling y event reporting son útiles, y un sistema de monitoreo de red podría típicamente emplear ambos métodos. El relativo énfasis puesto en los dos métodos varía gradualmente en diferentes sistemas, los sistemas de administración de telecomunicaciones tienen tradicionalmente puesta una muy alta dependencia en eventos reportados. En contraste, el SNMP tiene poca confianza en event reporting. Sin embargo SNMP y OSI administran sistemas tan bien como muchos esquemas propietarios, permitiendo al usuario una confianza considerable en la determinación o énfasis en los dos enfoques.

La elección del énfasis, depende en un determinado número de factores, incluyendo los siguientes:

- La cantidad de tráfico de red generado por cada método.
- Robustez en situaciones criticas
- El tiempo de retardo en la notificación de administración de red
- La cantidad de procesamiento en dispositivos de administración
- La compensación de la transferencia confiable contra la no confiable
- La aplicación de monitoreo de red con apoyo
- Las contingencias necesarias en caso de una notificación de un dispositivo de fallas antes del envió de un reporte.

[9,Pag 29]

Zenoss utiliza las 2 tecnicas pues utiliza el demonio Zenprocess para preguntar la disponibilidad y rendimiento de los procesos en los dispositivos remotos. Posteriormente Zenprocess hace uso de ZenossHRSWRunMap para recolectar la información, el cual depende de SNMP MIB para su objetivo, pero si el agente detecta algo raro en la información, es enviada al administrador, el cual genera una alerta de algún cambio de estado o falla.

1.6 PRINCIPALES ESTÁNDARES Y PROTOCOLOS DE MONITOREO DE REDES

En los 70´s no había protocolos de administración como tal, la única herramienta que fue efectivamente utilizada para la administración fue el Internet Control Message Protocol (ICMP) y el Trace-route. ICMP ofrecía un medio para la transferencia de mensajes de control de routers y de otros host a otro host, para proveer información acerca de los problemas en el ambiente de red. ICMP está disponible en todos los dispositivos que soportan IP. Para un punto de vista de administración en una red, la característica más útil de ICMP es el mensaje echo/echo-reply. El ejemplo más notable de este es el PING (Packet Internet Groper).

El inicio en la creación de herramientas de administración de red fue el Simple Gateway Monitoring Protocol (SGMP) en 1987 el cual era importante para el monitoreo de gateways. Provocando la necesidad para el desarrollo de más herramientas de propósito general en la administración de redes [10]. Tres fueron los prototipos en salir:

- *High-Level Entity Management System (HEMS):* esta fue una generalización de quizás el primer protocolo de administración de redes usado en el internet, Host Monitoring Protocol (HMP).

- *Simple Network Management Protocol (SNMP):* Este fue una versión más moderna de SGMP.

- *CMIP sobre TCP/IP (CMOT):* Este fue un intento para incorporarse a la máxima extensión posible de protocolos, servicios, y estructuras de bases de datos, siendo estandarizada por ISO para administración de redes.

En 1988, el Internet Arquitecture Board (IAB) revisó estas propuestas y aprovechó el más desarrollado de todos que fue SNMP, como una solución a corto tiempo, desarrollándose posteriormente nuevas versiones de éste, además de otros estándares y protocolos, que se revisaran más adelante.

1.6.1 INTRODUCCIÓN A SNMP (SIMPLE NETWORK MANAGEMENT PROTOCOL)

SNMP, *Simple Network Management Protocol (*Protocolo Simple de Administración de Red) fue diseñado por McCloghrie, Rose, and Waldbussera a mediados de los 80´s, como una solución temporal a problemas de comunicación entre diferentes tipos de redes, Al no realizarse mejores diseños, SNMPv1 se convirtió en la única opción para la gestión de red elegido por los comités técnicos de Internet para ser utilizado como una herramienta de gestión de los distintos dispositivos en cualquier red [10].

El funcionamiento de SNMP es simple, como lo dice su nombre, aunque su implementación requiere algo de tiempo. SNMP es un protocolo de la capa de aplicación y utiliza la capa de transporte de TCP/IP mediante el envío de datagramas UDP, sin embargo, el hecho de usar UDP, hace que el protocolo no sea fiable (en UDP no se garantiza la recepción de los paquetes enviados, como en TCP).

El protocolo SNMP está cubierto por un gran número de RFC (*Request For Comments*), entre ellos:

SNMPv1	La primera versión del protocolo. (RFCs 1157, 1215)
SNMP v2C	Autentificación basada en los llamados "community strings"
SNMP v2U	Orientada a usuarios (RFC´s del 1441-1452 y 1901, 1905, 1906, 1909, 1910)

Aparte de estas existen otras versiones, como son:

SNMPsec	Es una versión poco aceptada y no tan conocida, implementa un nivel de seguridad más fuerte. RFC's 1351,1352, 1353
SNMPv2p	En esta versión se introdujeron muchas mejoras, pero es anterior a las 2C & 2U
SNMPv2*	Esta es la versión más avanzada del SNMPv2, pues combina lo mejor de todas las anteriores.
SNMPv3	Es el estándar nuevo e interesante de SNMP (del 2570 al 2575 v3).

Estas versiones de SNMP están compuestas por:

El administrador o Gestor, que es un modulo de software en un sistema responsable de una parte administrativa o de toda la configuración de aplicaciones para la gestión de la red y usuarios.

Y los Agentes, donde cada agente es un software en un dispositivo controlado de la red, responsable del mantenimiento local de la administración de la información, y de enviar información a un administrador para ser leídas o modificadas. Asimismo, un agente puede enviar "alertas" a otros agentes para avisar de eventos importantes que tengan lugar.

La definición formal de SNMP según su pagina dice: "El Simple Network Management Protocol (SNMP) es el estándar de operaciones y protocolo de mantenimiento para internet. SNMP fue basada en administración no solo en la producción de soluciones de administración de sistemas, aplicaciones, dispositivos complejos y sistemas de ambientes controlados si no también provee la administración de internet para soluciones de soporte de servicios Web. SNMPv3, el mas reciente estándar aprobado por el the Internet Engineering Task Force (IETF), agrega capacidades de seguridad (como encriptacion)". [84]

1.6.1.1BASE DE INFORMACIÓN DE ADMINISTRACIÓN (MIB)

MIB, es en esencia una base de datos lógica con información de gestión de red, residente en cada uno de los agentes, ésta tiene estructura en forma de árbol; además son accedidas usando un protocolo de administración de red como por ejemplo; SNMP o CMIP. Estas MIB incluyen objetos administrables, los cuales son encontrados por identificadores de objetos. Un objeto administrado (algunas veces llamado objeto MIB, objeto, o MIB) es una de las diversas características específicas de un dispositivo administrado, es decir, cada sistema en (Workstation, server, router, bridge, etc) una red o interred mantiene un MIB que refleja el estatus de los recursos administrados del equipo.

Alexis Wol señala en su Catedra de Telematica que "Una base de información de administración (MIB) es una estructura o colección de información que está organizada jerárquicamente."
Existen dos tipos de objetos administrados: escalares y tabulares. Los objetos escalares definen una simple instancia de objeto. Los objetos tabulares definen múltiples instancias de objeto relacionadas que están agrupadas conjuntamente en tablas MIB. [64, Pag 62 PI]

El concepto SMI (Structure of Management Information), identifica los tipos de datos que pueden ser usados en el MIB y especifíca como los recursos en el MIB son representados y nombrados; también se puede considerar como un conjunto de reglas que describe la estructura de una MIB.

La MIB actual es MIB-II y está definida en el RFC 1213, aunque hay múltiples extensiones definidas en otros RFCs es importante debido principalmente a que es una forma de determinar la información que ofrece un dispositivo SNMP y la forma en que se representa.

La MIB está descrita en ASN.1 (Notación de sintaxis abstracta 1), que es notación estándar y flexible para describir estructuras de datos que pueden ser usadas para representar, codificar, transmitir y decodificar datos lo que facilita su transporte transparente por la capa de red.

Cada agente SNMP ofrece información dentro de una MIB, tanto de la general (definida en los distintos RFCs), como de aquellas extensiones que desee proveer cada uno de los fabricantes. Por lo que algunos fabricantes de routers han extendido las ramas privadas del árbol MIB estándar incluyendo información específica de sus equipos.

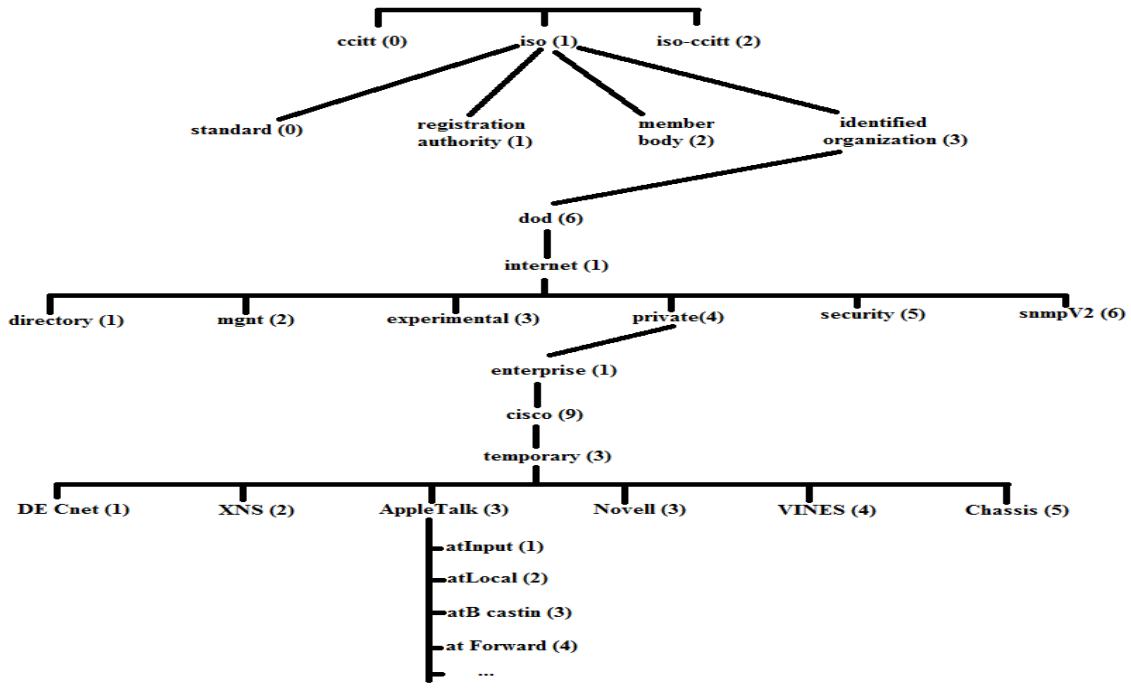


Fig.1.12 El árbol MIB con jerarquías de organizaciones

1.6.1.2 FUNCIONES DE SNMP

SNMP es un mundo muy complejo y amplio, pues con SNMP se puede monitorizar el estado de un enlace punto a punto para detectar cuando está congestionado y tomar así medidas oportunas, se puede hacer que una impresora alerte al administrador cuando se ha quedado sin papel, o que un servidor envíe una alerta cuando la carga de su sistema incrementa significativamente. SNMP también permite la modificación remota de la configuración de dispositivos, de forma que se podría modificar las direcciones IP de una computadora a través de su agente SNMP, u obligar a la ejecución de comandos (si el agente ofrece las funcionalidades necesarias), así pues se pueden monitorizar variables de agentes en un servidor o cualquier otro equipo con alguna herramienta de gestión, programar una interfaz para tomar medidas en base a la consulta (monitorización de variables de un elemento SNMP) o programar una interfaz para recibir alertas SNMP y tratarlas como sea necesario.

Es en principio una típica aplicación cliente-servidor, donde el agente de snmp presenta información acerca de si mismo en un árbol jerárquico, información como el nombre del administrador, de la maquina, las configuraciones de sus tarjetas de red, etc. El servidor de snmp, usa para la comunicación con el cliente (el llamado manager) el protocolo udp, y generalmente escucha en los puertos 161 y 162 (este último para el snmptrapd). Traps son paquetes enviados por el agente para informar de acontecimientos inusuales en su entorno, por ejemplo: un reboot, que haya demasiado tráfico en la red, un router que deja de responder.

Para solicitar información del agente, el manager emplea un mecanismo denominado get-request, a lo que el agente responde con un (lógico) get-response. Toda la información del agente como se mencionó se guarda en una base de datos denominada MIB.

1.6.1.3PRINCIPALES MEJORAS EN SNMP

No obstante este protocolo no era perfecto, además no estaba pensado para poder gestionar la inmensa cantidad de redes que cada día iban apareciendo. Para subsanar sus carencias surgió la versión 2 (SNMP v2). Las mayores innovaciones respecto a la primera versión son:

Introducción de mecanismos de seguridad, totalmente ausentes en la versión 1. Estos mecanismos protegen la privacidad de los datos, confieren autentificación a los usuarios y controlan el acceso.

Se añaden estructuras de la tabla de datos para facilitar el manejo de los datos. El hecho de poder usar tablas hace aumentar el número de objetos capaces de gestionar, con lo que el aumento de redes dejo de ser un problema.

Realmente esta versión 2 no supuso más que un parche, realizando innovaciones como los mecanismos de seguridad que se quedaron en pura teoría, es decir, no se llegaron a

implementar. Por estas razones se ha producido la estandarización de la versión 3. Con dos ventajas principales sobre sus predecesores:

Añade algunas características de seguridad como privacidad, autentificación y autorización a la versión 2 del protocolo.

Uso de Lenguajes Orientados a Objetos (Java, C++) para la construcción de los elementos propios del protocolo (objetos). Estas técnicas confieren consistencia y llevan implícita la seguridad, por lo que ayudan a los mecanismos de seguridad.

1.6.2 REMOTE MONITORING (RMON)

Quizás la más importante iniciativa de desarrollo que aumento la capacidad de SNMP fue RMON. RMON dio a la administración de red la habilidad para monitorear subredes como un todo o mejor dicho como un dispositivo individual en la subred. Así, tanto vendedores y usuarios vieron a RMON como una extensión esencial para SNMP.

RMON ofrece la capacidad de administrar y gestionar una red a un nivel más grande, es decir, muestra información estadística sobre una red total y su comportamiento.

RMON en si proporciona una forma efectiva y eficiente de monitorizar el comportamiento de la red reduciendo la carga en otros agentes y en las estaciones de gestión**.** En este protocolo no se estudia a cada agente (nodo) en la red, si no que busca un comportamiento general de todo un conjunto. Para hacer esto el protocolo RMON agrega a la existente MIB II (Base de información de gestión, versión 2) una nueva estructura de MIB RMON. Por lo tanto cualquier plataforma en la que se vaya a emplear como monitor RMON, debe soportar previamente el protocolo SNMP".
RMON trabaja mediante un Monitor de Red. (También llamado Analizador de red ó Sonda). Estos analizadores envían las estadísticas e información a la Estación Central de Gestión de Red. [36,Pag 2]

El agente RMON necesita ser configurado para que trabaje adecuadamente, además de que se maneja mediante el uso de una MIB en la que se especifican dos tablas: una de configuración y una de datos. Estas dos tablas están íntimamente relacionadas mediante índices, en donde la tabla de configuración especifica el tipo de datos a utilizar y el modo en que serán recogidos por el gestor. Esta tabla es de lectura y escritura, en cambio, la tabla de datos solo es de lectura.

RMON versión 2:
En 1994 se empezó a trabajar en una extensión de la MIB de RMON, posteriormente a este trabajo se le definió como RMON-2 (versión 2), el cual está diseñado para que pueda monitorear tráfico por encima del nivel MAC, es decir puede monitorear paquetes desde la capa 3 hasta la capa 7 del modelo OSI.

Con esto RMON puede monitorear tráfico a nivel de aplicación tales como ftp, mails, etc.

1.6.3 WINDOWS MANAGEMENT INSTRUMENTATION (WMI)

Instrumental de administración de Windows mejor conocido por sus siglas WMI, es la implementación de Microsoft que cumple con WBEM (Web-Based Enterprise Management); estableciendo normas estándar para acceso y compartición de información de administración a través de la red. WBEM ofrece compatibilidad integrada al Modelo de Información Común (CIM, Common Information Model), para describir objetos existentes en un entorno de administración.

WMI tiene compatibilidad con CIM (Common Information Model), que describe los objetos de una base de datos en un entorno de administración, controlando la recopilación y manipulación de estos objetos, además de reunir información de proveedores de WMI.

Estos proveedores de WMI, son como intermediarios entre los componentes del sistema operativo, las aplicaciones y otros sistemas, además proporcionan información de sus componentes, las propiedades a establecer o los sucesos que se alertan debido a modificaciones en dichos componentes.

Las herramientas de administración de equipos, pueden utilizar WMI como ayuda para un mejor control. WMI también se utiliza en otras tecnologías y herramientas de Microsoft, como también es usado por otros fabricantes de sistemas de administración de equipos, al realizar aplicaciones que los unen por medio de la programación o de secuencias de comandos (como Windows Script Host), para así obtener la información de configuración de la mayor parte de los aspectos en los sistemas informáticos, incluidas las aplicaciones de servidor o para realizar cambios en los mismos más eficientemente.

1.7 COMPARACIÓN DE HERRAMIENTAS OPEN SOURCE

En la actualidad, las empresas invierten en nuevos equipos tecnológicos y software más avanzado, muchas veces con el objetivo de administrar sus procesos o procurar mejorar el rendimiento productivo en las tareas y actividades que se realizan. Las instalaciones de redes, servidores, y estaciones de trabajo son grandes inversiones para mejorar el modo en que opera la organización, provocando la necesidad de asumir un rol de control sobre estas tecnologías y su estado de operatividad y obsolescencia. Para esto existen diversos programas que ayudan en la gestión y monitoreo de redes, ya sean de software libre o licenciados. Un problema muy frecuente para administradores, es que no todos los programas complementan las actividades que se realizan de manera íntegra. Por tal motivo el administrador de la red debe manejar varias herramientas y así realizar un eficiente monitoreo de la red, observando incluso el rendimiento o estado de cada equipo que forma parte de la red.

De tal forma podemos decir que una buena gestión y monitoreo de red ayuda a prevenir problemas futuros, detectando los posibles efectos que pueden ocasionar dichos problemas a la hora de prestar ciertos servicios, pues al anticiparse a ellos se logra estar preparado con la búsqueda de soluciones lo que permite reaccionar más rápidamente en caso de que sucedan fallas, disminuyendo los riesgos de perdidas y al mismo tiempo ofreciendo un mejor servicio.

Los aspectos de eficiencia en la seguridad informática también están involucrados, pues por ejemplo la utilización del ancho de banda representa un factor crítico y distinguir el tipo de información que es enviada por medio de ésta, así como el volumen de tráfico que genera cada usuario o dispositivo, es importante para asegurarse que todo está en su normalidad y no hay nada extraño.

En este tema se aclaran dos conceptos muy relacionados e importantes como son el de monitoreo y gestión los cuales se definen de la siguiente manera:
Monitoreo: Es seguir de manera continua el funcionamiento de una red para localizar posibles fallos.
Gestión: Observar si algún servicio, dispositivo está funcionando para poder probar, analizar y controlar su estado.

Teniendo en claro ciertos conceptos es necesario elegir una herramienta de monitoreo y gestión que cumpla con los requerimientos del laboratorio para que este mejore y facilite su administración.

REQUERIMIENTOS DEL LABORATORIO

De acuerdo a los requerimientos del laboratorio, la herramienta de monitoreo debe cumplir con las siguientes características:

- Ser un sistema Open Source.
- Monitoreo de hardware de los equipos de cómputo y equipos de red (discos duros, memoria ram).
- Monitoreo de servicios, procesos aplicaciones, software etc.
- Monitoreo de Windows y Linux.
- Monitoreo del tráfico de la red.
- Monitoreo atraves de un agente instalado en el cliente.
- Debe permitir exportar datos a una base de datos relacional Open Source.
- Ser Implementado en varios sistemas operativos Linux.
- Generar alertas e informar al administrador de la red.
- Debe generar graficado de los recursos que se monitorean.
- Debe ser seguro.
- Compatible con plugings de otros sistemas de monitoreo.
- La herramienta debe contar con una comunidad de ayuda que lo respalde y página web.

- Existencia de soluciones a errores, publicación de nuevas versiones o actualizaciones en fechas recientes.
- Ser reconocida y utilizada como buena herramienta de monitoreo por empresas o usuarios que la puedan referenciar.
- Creación e instalación de complementos o plugins.

Entre las Herramientas más conocidas que cumplen varios de los requerimientos del laboratorio se encuentran 3 que son: Cacti, Nagios y Zenoss, con las que se realizarán comparaciones de acuerdo a las referencias e información existente, seleccionando la más adecuada para la realización de pruebas en la simulación con maquinas virtuales, y así identificar los problemas más comunes que se presenten tanto en la instalación como administración de ésta, lo que posteriormente permitirá realizar la Implementación en el laboratorio con equipos reales de una forma más directa.

Acontinuación se describen de forma resumida cada una de las herramientas mencionadas.

1.7.1 Nagios®

Nagios es una herramienta GPL (General Public License) de monitoreo que permite el control de los servicios, procesos y recursos de equipos de red, está escrito en C y su licencia que lo determina como Software Libre asegurando que siempre se tendrán actualizaciones disponibles y que hay una gran comunidad de desarrolladores soportándolo.

Esta herramienta OpenSource corre bajo SO Linux, funcionando correctamente también en SO UNIX, siendo una alternativa para la gestión de infraestructuras TI empresariales, ya que su funcionamiento consiste en una arquitectura cliente-servidor que realiza una ejecución de Zondeo o Polling periódico checando los recursos (con agente) y servicios (sin agente) sobre sistemas cliente, informando proactivamente a administradores de red o clientes finales de posibles problemas de red y servicios. Cuando es detectado un error Nagios es capaz de alertar a contactos administrativos sobre diferentes modos de comunicación para informar del estado del servicio que ha provocado el error, incluyendo informes de estado, de logs e históricos web.

Además facilita diferentes tareas, pues ofrece herramientas como ejecución de Zondeo o Polling periódico, el histórico de actividad y rendimiento de servicios y un visor de diagramas de red con el estado actual de cada equipo.

Internamente Nagios cuenta con un Núcleo que construye la interfaz de usuario y *plugins* que representan sus ojos y oídos, ya que son los que se encargan de recopilar información. Estos *plugins* pueden estar programados en diversos lenguajes como C, C++, Python, Perl, PHP, Java, Bash etc, pues Nagios es independiente del lenguaje en el cual se desarrolle el plugin, y solo procesa los datos recibidos de este para la elaboración y envío de notificaciones a los encargados de la administración del sistema.

Entre las principales características con las que cuenta están:

-Monitorización de servicios de red (SMTP, POP3, HTTP, NTTP, ICMP, SNMP).
-Monitorización de los recursos de un host (carga del procesador, uso de los discos, logs del sistema) en varios sistemas operativos, incluso Microsoft Windows.
-Monitorización remoto, a través de túneles SSL cifrados o SSH.
- Diseño de plugins, que permiten a los usuarios desarrollar sus propias políticas de verificación servicios dependiendo de sus necesidades, usando sus herramientas preferidas (Bash, C++, Perl, Ruby, Python, PHP, C#, Java, etc.).
- Verificación de servicios paralizados.
- Posibilidad de definir la jerarquía de la red, permitiendo distinguir entre host caídos y host inaccesibles.
- Notificaciones a los contactos cuando ocurren problemas en servicios o hosts, así como cuando son resueltos (Vía email, pagina, SMS o cualquier método definido por el usuario junto con su correspondiente complemento).
- Soporte para implementar hosts de monitores redundantes.
- Reportes y estadísticas del estado cronológico de disponibilidad de servicios y hosts.
-Portal web que permite consultar el estado de los elementos gestionados, las notificaciones realizadas, los problemas acontecidos, el estado de los servicios, la administración básica, etc.

1.7.2 

Es una herramienta completa de graficado en formato PNG y monitorización de redes, creada para aprovechar el almacenamiento y la funcionalidad de graficar con RRDtool (*Round Robin Database tool*). Cacti es desarrollada en PHP y provee plantillas de gráficos avanzadas, múltiples métodos para la recopilación de datos, y manejo de usuarios. Ofreciendo la facultad de administrar y controlar los servicios que presta nuestra red en todo momento y casi en tiempo real.

Su interfaz es sencilla de utilizar resultando conveniente para instalaciones del tamaño de una LAN, así como también para redes complejas con cientos de dispositivos (Routers, Switches, Dispositivos inalámbricos, etc).

Cacti tiene como principal finalidad el tratamiento de datos temporales y datos seriales como temperaturas, transferencias en redes, cargas del procesador, etc. Además tiene la ventaja de ser una herramienta multiplataforma funcionando en S.O como Linux y Windows.

Un componente importante en esta herramienta son las RRDtool (Round Robin Database tool), lo que quiere decir que trabaja con una Base de Datos (BD) manejando Planificación Round-robin, la cual es una técnica que trabaja tratando la BD como si fuera un círculo, es decir, sobrescribiendo los datos almacenados una vez alcanzada la capacidad de la BD. La capacidad de la BD depende de la cantidad de información como historial que se quiera conservar. La RRD almacena datos de cualquier tipo, en series temporales de datos, es decir realizando medidas en algunos puntos de tiempo para proveer esta información a la RRDtool para que la almacene.

Al igual que la mayoría de las herramientas de monitoreo utiliza SNMP (Simple Network Management Protocol) para realizar consultas a dispositivos sobre el valor de los contadores que ellos tienen, siendo este valor el guardado en la RRDtool.

Características

Fuente de datos: En la recopilación de datos se utilizan scripts o comandos que se relacionan con cacti, el cual reúne los datos y los carga en la BD MySQL, al igual que los archivos de planificación Round-robin que deba actualizar. Para la creación de fuentes de datos se utilizan scripts, por ejemplo, al querer graficar los tiempos de ping hacia algún equipo, se utiliza un script que realice el ping y devuelva el valor en milisegundos. Posteriormente de definir las opciones para la RRDtool, como la forma de almacenar los datos, se pueden también definir información adicional como la fuente de entrada de datos, es decir la IP del host al cual se le hace ping. Después de que una fuente de datos es creada es automáticamente mantenida cada 5 minutos.

Gráficos: Con los datos obtenidos de las fuentes de datos RRDtool, crea una gráfica. Por lo cual Cacti puede crear graficas variadas, utilizando todos los estándares de tipos de graficas de RRDtool y funciones de consolidación además de tener varias formas de mostrarlas, siendo estas formato PNG.

Manejo de usuarios: Entre las diversas funciones que ofrece Cacti, se cuenta con el manejo de usuarios, para que al agregar usuarios se le den ciertos permisos en ciertas áreas de cacti. Lo que permite tener usuarios que puedan cambiar parámetros de un gráfico, mientras que otros sólo los pueden ver. Con lo cual cada usuario maneja su propia configuración de vista de gráficos.

Plantillas: Cacti puede agregar un gran número de fuentes de datos y gráficos a través de plantillas, también permitir crear plantillas para definir cualquier gráfico o fuente de datos asociados a ésta, para verificar sus capacidades, así Cacti utiliza esta información para agregar un nuevo host.

1.7.3 Zenoss

Zenoss es una alternativa libre para la administración IT open Source es decir de código abierto licenciado bajo GNU GPLv2 escrita en Python/Zope, que a través de la integración del monitoreo IT administra el estatus y rendimiento de la infraestructura de red por medio de una sencilla interfaz Web, monitoreando la disponibilidad de servicios, inventario de hardware y software, configuración del sistema, rendimiento, eventos entre otras cosas, con el fin de reducir costos empresariales para estas tareas. En Zenoss se creó una base de datos llamada Inventory and Configuration Management Database (CMDB) para ayudar a descubrir y administrar recursos, servidores, redes u otros dispositivos en el ambiente IT. Zenoss se basada en otras herramientas como Cacti y Nagios (ambas open source) y en el servicio de aplicaciones Zope que utiliza el servicio SNMP.

Sus aplicaciones y características están preparadas para funcionar bajo un entorno de software libre, como Linux o Unix pero también trabaja en plataformas Windows siendo totalmente compatible y utilizable en este sistema. Su implementación en Windows es posible gracias a la virtualizaión de la aplicación VMplayer.

Casi todas estas funciones se realizan por medio de SNMP o WMI para los sistemas Windows, además se instalan *ZenPacks que* son grupos empaquetados de funciones y modelos de plantillas para tipos específicos de dispositivos, logrando una mejor supervisión de estos.

Zenoss se ofrece en dos tipos de producto**;** la versión Core **y** la versión Enterprise**.** La última es una versión comercial, que se distingue por ofrecer soporte profesional y algunas herramientas adicionales no indispensables en este momento para monitorear un Laboratorio. La versión Core, es la disponible gratuitamente y elaborada por la comunidad. Su diseño ofrece una eficiente administración centralizada que se realiza desde su interface web para la gestión de todas las herramientas tecnologías del laboratorio.

Cuenta con Thresholds que son umbrales dinámicos, que permiten manejar valores distintos dependiendo de la organización, así pues, si se sobrepasan estos límites se mandaran alertas a los administradores de la red. Un ejemplo podría ser en un negocio que en día 15 sus servidores tienen mayor carga, siendo un comportamiento normal ese día, pero de repente ocurre este comportamiento el día 20, lo que indicaría que existe un problema, y con los Thesholds se realizarían alertas a los administradores de la red.

Otra peculiar característica de Zenoss es que integra una herramienta para la detección de nueva tecnología realizando búsquedas de nuevos recursos o dispositivos en una red. Para entenderlo mejor, se podría imaginar un nuevo sistema instalado en una de las estaciones, sin autorización, o la derivación de información de la empresa sin autorización; gracias a este sistema se podrá detectar automáticamente cualquier variación en la red.

Zenoss es una herramienta que permite un excelente Monitoreo de Red pues está diseñada estrictamente para trabajar en el análisis de las actividades, realizando

evaluaciones basadas en las IP´s de los equipos, u otras características. También ofrece la posibilidad de verificar los recursos con los que cuenta cada una de las estaciones en la red, e incluso verificar cómo se está compartiendo la información, la ubicación de los equipos y su hora de conexión mediante una herramienta llamada Dashboard Configuration**.**

Para ejemplificar lo que puede llegar a lograr esta herramienta**,** se puede pensar en una organización, que provee a sus empleados de computadoras móviles. Con una configuración previa en estos equipos y Zenoss se podrá acceder a la información de su ubicación y su hora de conexión automáticamente, siendo útil para permitir poner en contacto a las unidades de negocio, a cualquier hora y en cualquier lugar, e incluso localizarla gráficamente con la integración de Google Maps.

Posteriormente se mencionaran algunos de sus componentes más utilizados para la administración en red.

Con la evaluación realizada, Zenoss promete ser una opción importante de código libre para infraestructuras IT**,** muy necesaria en las organizaciones modernas.
[41, 42, 43]

1.7.4 Comparación de Cacti, Nagios y Zenoss

Nagios se utiliza para comprobar la disponibilidad de servicios en los servidores (http, pop, smtp…). Además de ser una herramienta en la cual se pueden configurar alertas para ser recividas por los administradores, pudiendo ser enviadas de distintas formas (email, paginas, etc). Pero tiene deficiencias como herramienta de monitoreo pues no responde a preguntas como:

- ¿Por qué se ha caído el servicio?
- ¿Qué estaba ocurriendo en la máquina cuando se cayó?
- ¿Qué otros servicios de esa máquina podrían estar influyendo en el problema?

Se informa de la disponibilidad pero no de las posibles causas.

Siendo un buen complemento de esta herramienta Cacti, pues responde a estas cuestiones de un modo muy eficaz e incluso a muchas más preguntas en caso de error como:

- ¿Qué actividad de Apache había?
- ¿Y de MySQL**?**
- ¿Cómo se encontraba el tráfico de correo?
- ¿Y de DNS?

Más aún…

- ¿Será un fallo hardware por la temperatura o los ventiladores de la máquina?
- ¿Falta de espacio en disco?
- ¿Nos hemos quedado sin memoria?
- ¿Qué servicio está provocando el incremento de CPU?

Esto se logra revisando las gráficas de actividad de los principales servicios y ver cual tiene una actividad por encima de lo normal, respondiendo así a varias preguntas más fácilmente pues el sistema de graficado es mejor.
[66, 69]

Acontinuacion se muestra una tabla donde se comparan las 3 herramientas elegidas y algunas de sus características que más destacan y cumplen con los requerimientos que pide el laboratorio, entre otras.

CARACTERISTICAS

(A)NOMBRE
(B) GRAFICADO
(C)ESTADÍSTICAS
(D)AGENTES
(E)AUTODESCUBRIMIENTO
(F)PLUGINGS
(G)ALERTAS
(H)ALMACENAJE DE BASES DE DATOS
(I)APLICACIÓN WEB
(J) TOPOLOGÍA O MAPAS DE RED
(K)SEGURIDAD
(L)ADMINISTRACIÓN DE EVENTOS
(M)REPORTES O INFORMES
(N)COMANDOS DE ADMINISTRACIÓN AGREGADOS ALA HERRAMIENTA
(O)AGREGADO DE MULTIPLES DISPOSITIVOS ALA HERRAMIENTA
(P)INVENTARIO SOFTWARE Y HARDWARE
(Q)DETECCIÓN AUTOMÁTICA DE NUEVOS EQUIPOS EN LA RED
(R)PÁGINA WEB Y FOROS DE APOYO

(A)NOMBRE	B	C	D	E	F	G
Nagios	Si	Si	snmp	Agregando plugin	Si	individual
Cacti	Si	Si	snmp	Agregando plugin	Si	individual
Zenoss	Si	Si	snmp,wmi	Si	Si y compatible con Plugins de Nagios	individual o en grupo

H	I	J	K	L	M	N	O	P	Q	R
SQL	Solo visualización	Si	Si	Si	si	No	No	MEDIO	No	Si
RRDTools y SQL	control total	No		No	No	No	No	MEDIO	No	Si
RRDTools y SQL	control total	Si	Si	Si	si	si	si	COMPLETO	Si	Si

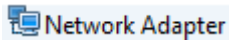
Fig. 1.13 Tabla de comparación entre Cacti, Nagios y Zenoss

Se observa que Zenoss cumple con los requerimientos e incluso se puede decir que es una combinación de Cacti y Nagios en una sola herramienta, permitiendo ofrecer un mejor desempeño y facilidad en el monitoreo y gestión de la red, ya que es adaptable a nuevas tecnologías, escalable y compatible con plugins de Nagios, por tal motivo fue elegida para la implementación a realizar en el laboratorio y con la cual primeramente se realizarán pruebas simulando el laboratorio en VMWare.

CAPÍTULO 2 *Ambiente controlado (Virtual)*

2.1 INSTALACIÓN DE LA HERRAMIENTA OPEN SOURCE EN UN AMBIENTE VIRTUAL

2.1.1Preparación del Sistema Operativo para instalar Zenoss

La máquina virtual en la que se instala Zenoss es una máquina virtual creada en VMWare Workstation y sistema operativo Linux Ubuntu 9.04 con conexión a internet, para lograr esto se recomienda configurar la tarjeta de red de VMWare en modo bridge, esta tarjeta se localiza en la parte inferior derecha cuando está encendida la maquina virtual, o con este icono 

en la pestaña de Devices. Con esta configuración la maquina obtiene una IP de la red real a la que está conectada nuestra máquina física, además se recomienda tener funcionando solo la maquina virtual en la que se instala zenoss para que el rendimiento sea mejor en la instalación y más rápido, claro todo depende de los recursos del servidor donde se está instalando. En cuanto a Ubuntu se eligió sólo para tener variedad de Sistemas Operativos y mostrar diferentes maneras de instalación, tanto en Sistemas basados en Debian como en Red Hat por ejemplo Centos, además se puede utilizar la máquina ya preconfigurada que se encuentra en la página de Zenoss, sin embargo se intentara mostrar un manejo mas general de la herramienta.

Primeramente se recomienda descargar todas las actualizaciones ya sea con la interfaz gráfica o por consola, aun que esto implique incluso modificar la versión del SO.

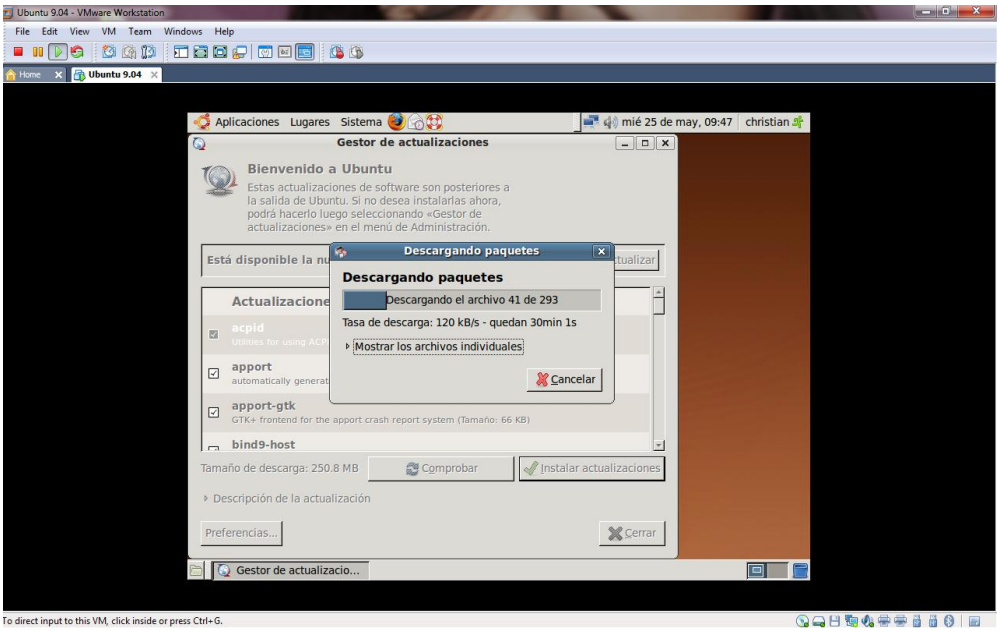


Fig 2.1 Actualizaciones en modo gráfico

Este proceso es tardado, pues un cambio de versión del sistema modifica varios archivos. Es recomendable actualizarlo por versiones más actuales y estables.

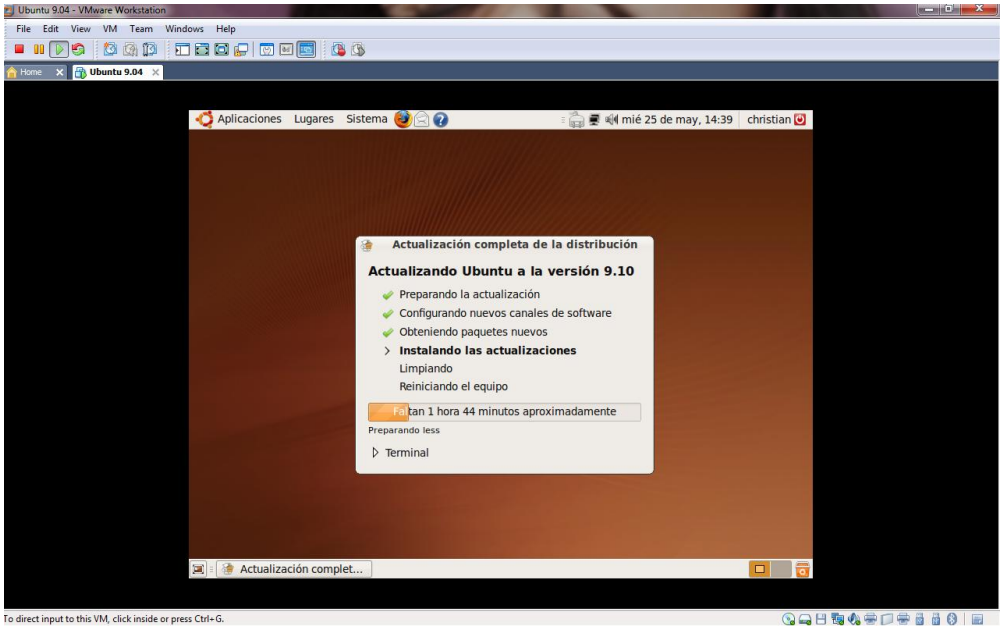


Fig 2.2 Actualización de Ubuntu en modo gráfico

Estos son los comandos utilizados para realizar la actualización en modo consola:

```
#apt-get update
#apt-get upgrade
```

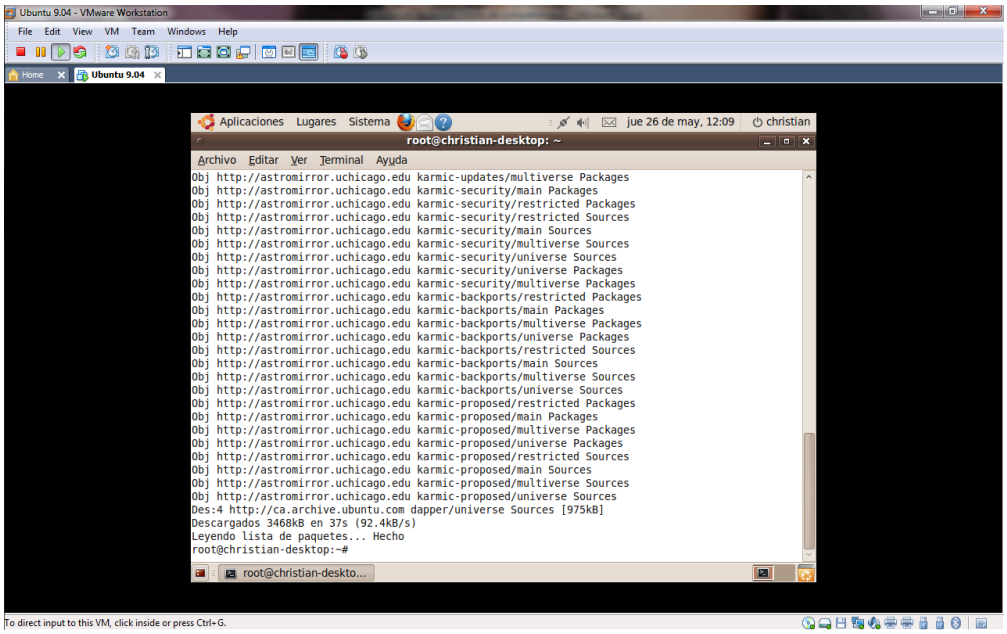


Fig 2.3 Actualización en modo consola

En algunas ocasiones se llega a presentar un error de desbordamiento, sin poderse descargar e instalar actualizaciones y otros programas por lo cual se recomienda el método descrito a continuación.

Cuando este mensaje aparece existe el error:

```
E: Dynamic MMap corrió fuera de la sala. Incremente el tamaño de APT::Cache-
Limit. Valor actual: 25165824. (man 5 apt.conf)
E: Ocurrió un error mientras se procesaba language-pack-kde-he (NewVersion1)
E: Problem with MergeList
/var/lib/apt/lists/ve.archive.ubuntu.com_ubuntu_dists_karmic-updates_main_binary-
i386_Packages
W: Unable to munmap
E: No se pudieron analizar o abrir las listas de paquetes o el archivo de estado.
```

Las medidas que se toman son las de ampliar la memoria para que no exista desbordamiento, esto se realiza con los siguientes comandos.

```
#echo 'APT::Cache-Limit "100000000";' | sudo tee -a /etc/apt/apt.conf.d/70debconf

#sudo apt-get clean
#sudo apt-get update
```

Al realizar de Nuevo el update no volverá a mandar este error y se actualizará sin problemas. [82 PI]

Si la instalación de las actualizaciones se realiza con éxito no hay que realizar ninguna modificación.
Despues de actualizar el SO se deben agregar los siguientes repositorios al equipo con el siguiente comando y como usuario root.

```
#nano /etc/apt/sources.list
Deb http://ca.archive.ubuntu.com/ubuntu/ dapper universe
Deb-src http://ca.archive.ubuntu.com/ubuntu/ dapper universe
```

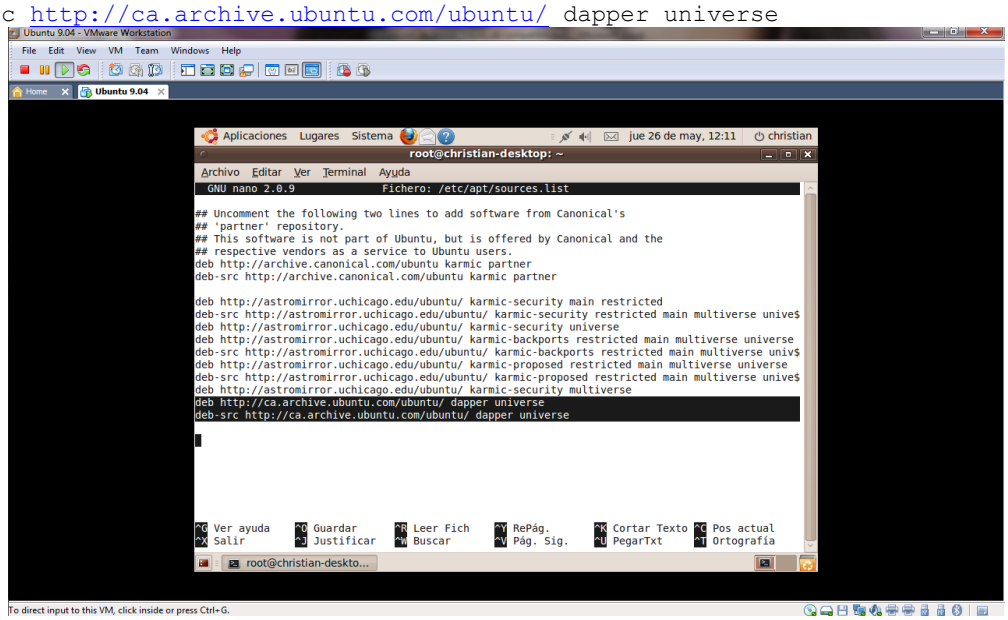


Fig 2.4 Agregado de repositorios nuevos

Antes de instalar Zenoss Core, se necesitan instalar las siguientes dependencias, ya que son librerías necesarias para construir el módulo de Zenoss, según los requerimientos del equipo y el sistema operativo.

- *python-dev:* Lenguaje de programación o entorno de desarrollo para este sistema capaz de entender y ejecutar programas desarrollados en python, es decir que es el editor de código, compilador o depurador.
- *libmysqlclient15-dev:* Dependencias para agentes clientes de la base de datos MYSQL
- *mysql-server:* Agente servidor de la base de datos
- *build-essential:* Lista informativa de paquetes esenciales para poder compilar
- *binutils:* Es una colección de herramientas de programación para la manipulación de código de objeto en varios formatos de archivos objeto.
- *make:* Es una herramienta de generación o automatización de código
- *swig:* Aplicación que genera todo el código necesario para utilizar desde multitud de lenguajes de alto nivel (desde Python hasta OCaml pasando por Java o C#) hasta librerías de C.
- *autoconf:* Es la herramienta de GNU para la configuración multiplataforma.

Éstas se instalan con el comando:

```
#apt-get install python-dev libmysqlclient15-dev mysql-server build-essential
binutils make swig autoconf
```

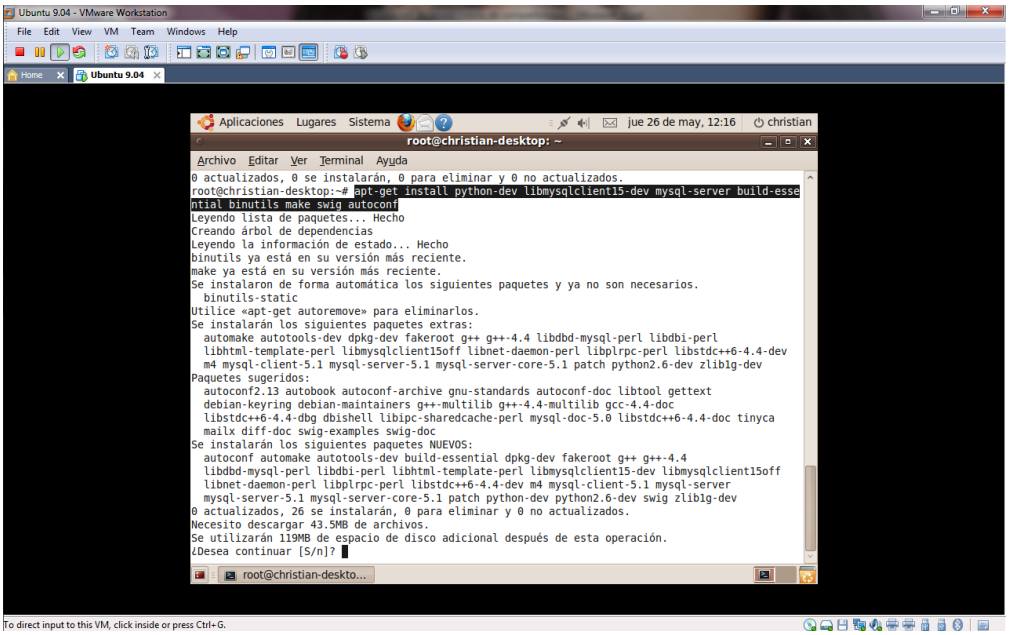


Fig 2.5 Instalación de dependencias para el módulo Zenoss

Posteriormente muestra una pantalla azul para colocar un password como usuario root de MySQL.

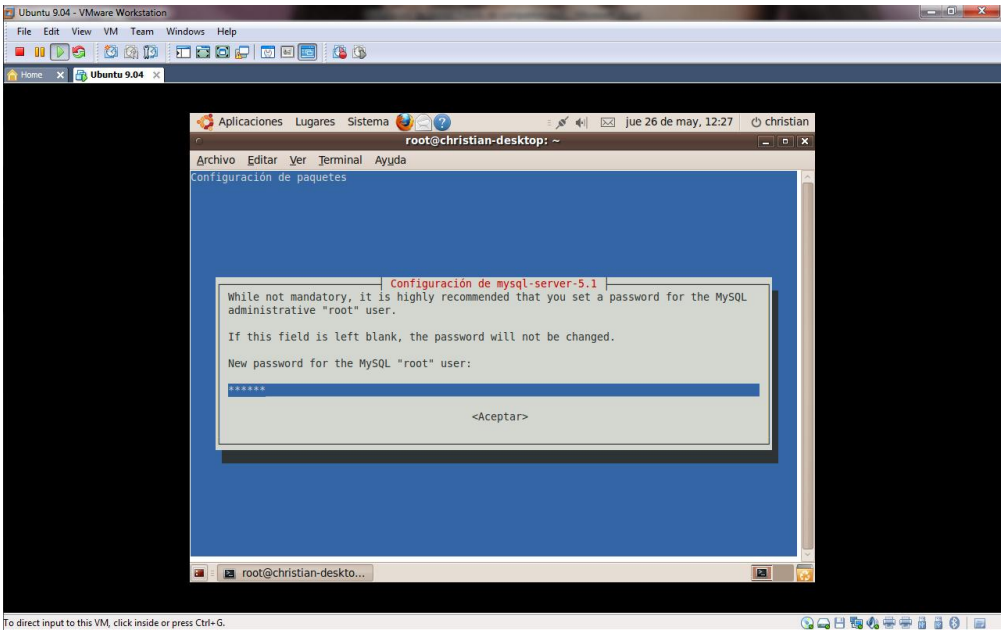


Fig 2.6 Password del administrador de MySQL

Se repite el password para la siguiente pantalla azul.

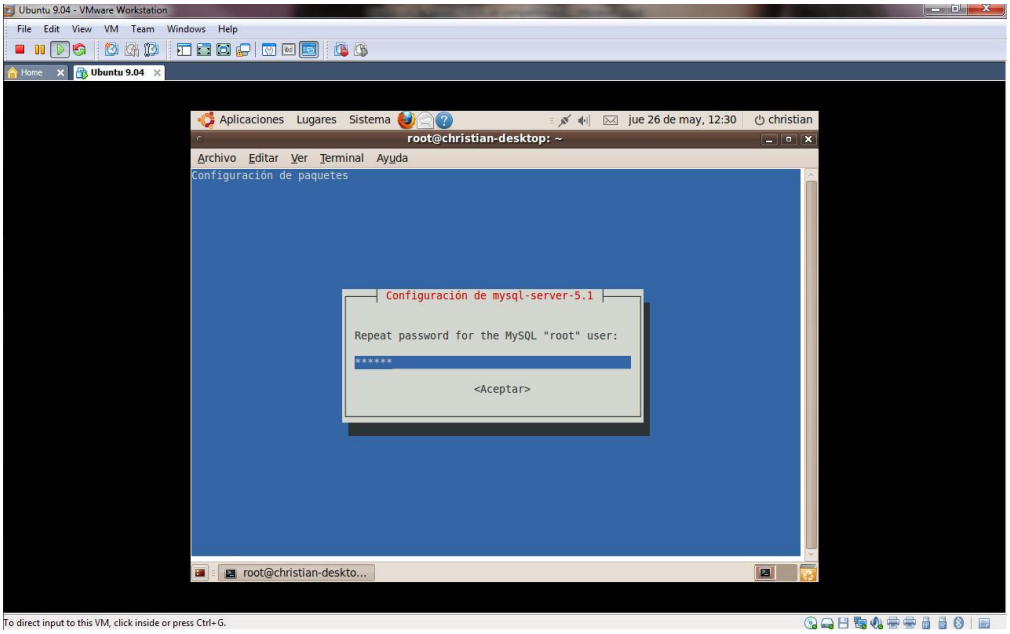


Fig 2.7 Confirmación de contraseña

Y sigue con la preconfiguración de paquetes.

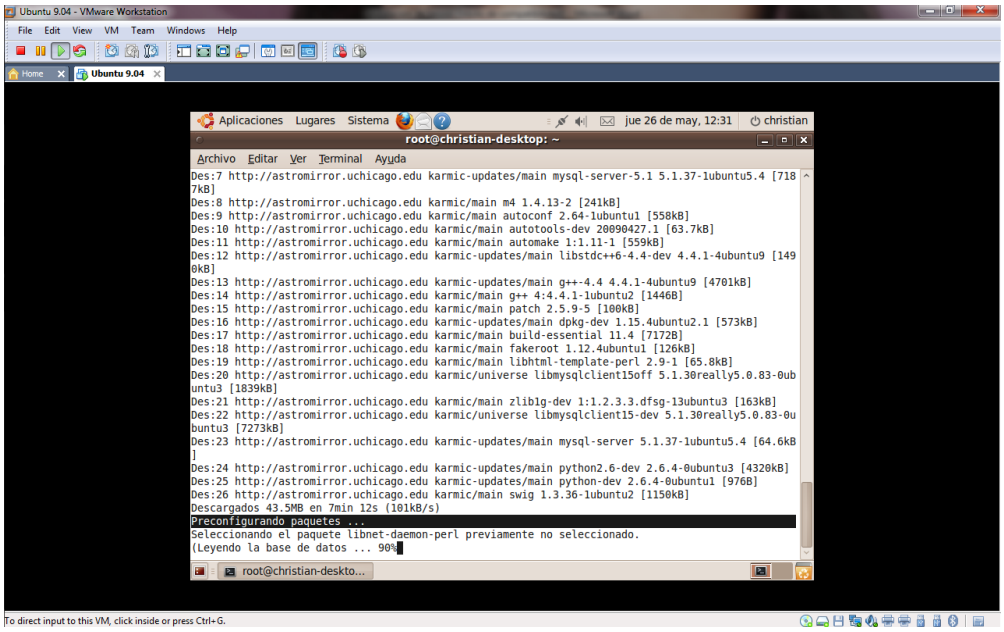


Fig 2.8 Preconfiguración de paquetes

En esta pantalla se puede apreciar el final de la instalación de dichos paquetes.

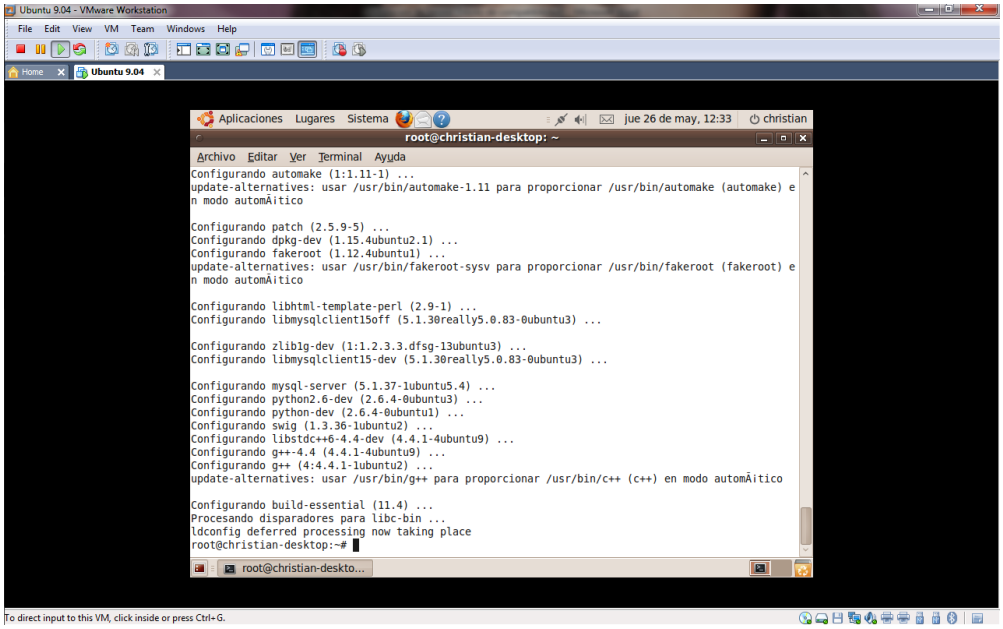


Fig 2.9 Fin de la instalación de dependencias

Ahora se debe crear un usuario llamado zenoss en el sistema con su home.
En la contraseña se le asigna un password y la repite para poder entrar al usuario zenoss,
Los pasos para crearlo son los siguientes:

```
#adduser zenoss
```

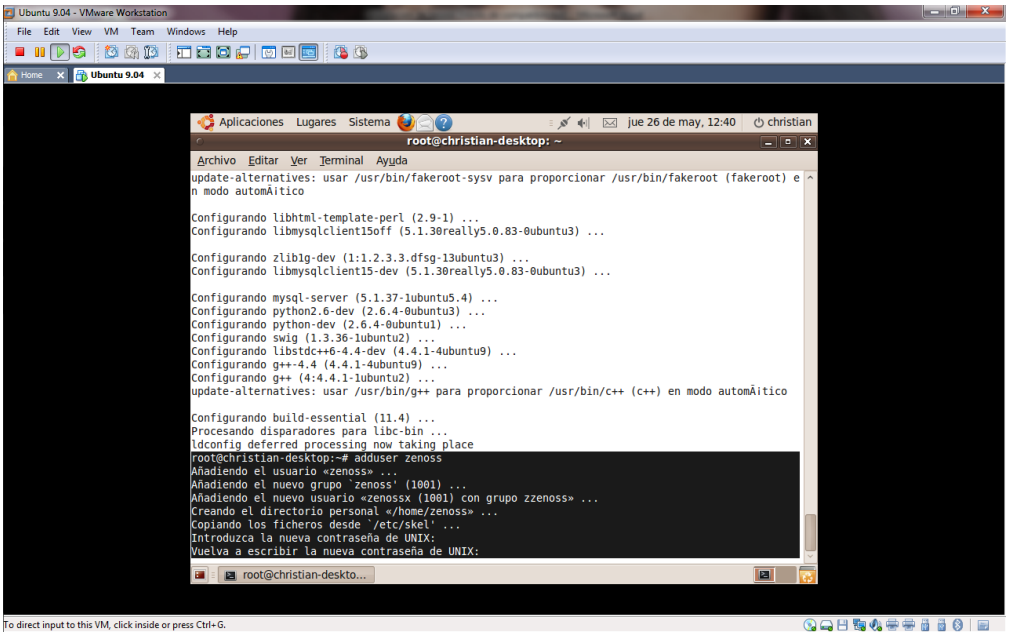


Fig 2.10 Creación de usuario llamado zenoss

Si las contraseñas no coincidieran, preguntará si queremos repetir el proceso, al cual se le dirá que si y se procederá a escribir las contraseñas como se muestra en la imagen.

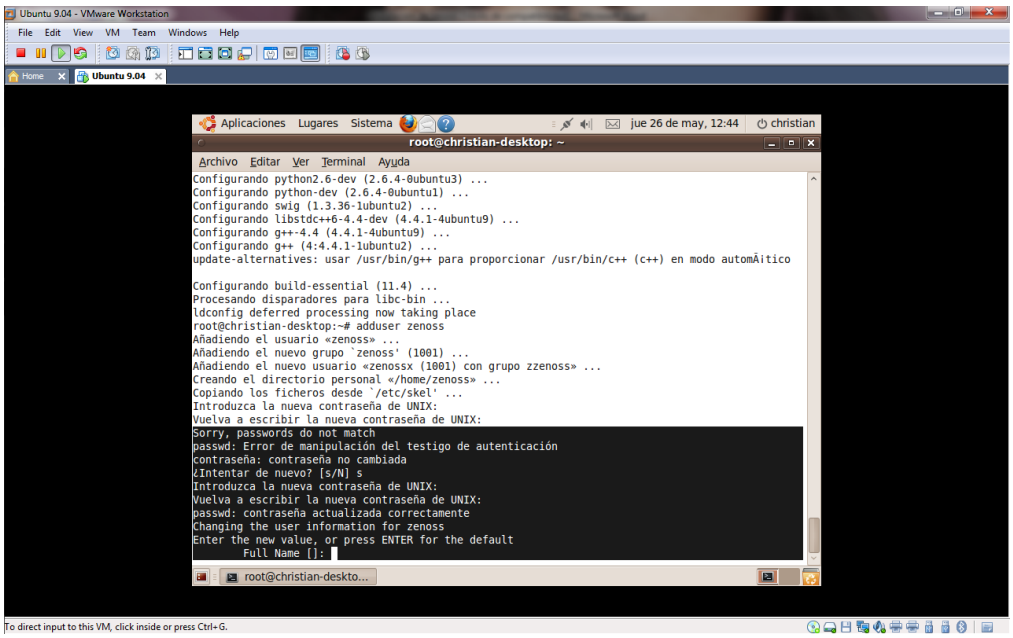


Fig 2.11 Error de contraseñas diferentes

Así termina el proceso, pidiendo información adicional del usuario la cual se puede omitir presionando **Enter**.

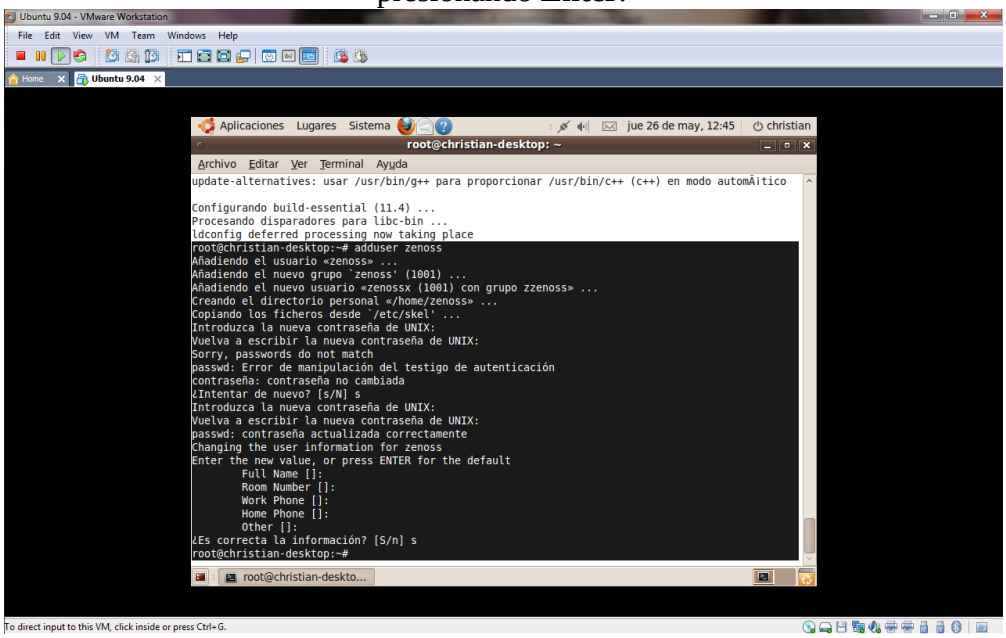


Fig 2.12 Información adicional

Ahora es necesario ingresar como usuario zenoss en la consola y verificar que efectivamente se encuentra logueado como usuario zenoss, utilizando el comando whoami u observando el cambio de usuario en el prompt, el cual cambia de #(Usuario administrador "root") a $ (Usuario sin privilegios).
El comando que se aplica para cambiar de usuario es el siguiente:

```
#su zenoss
```

Como se muestra en la Fig 2.13.

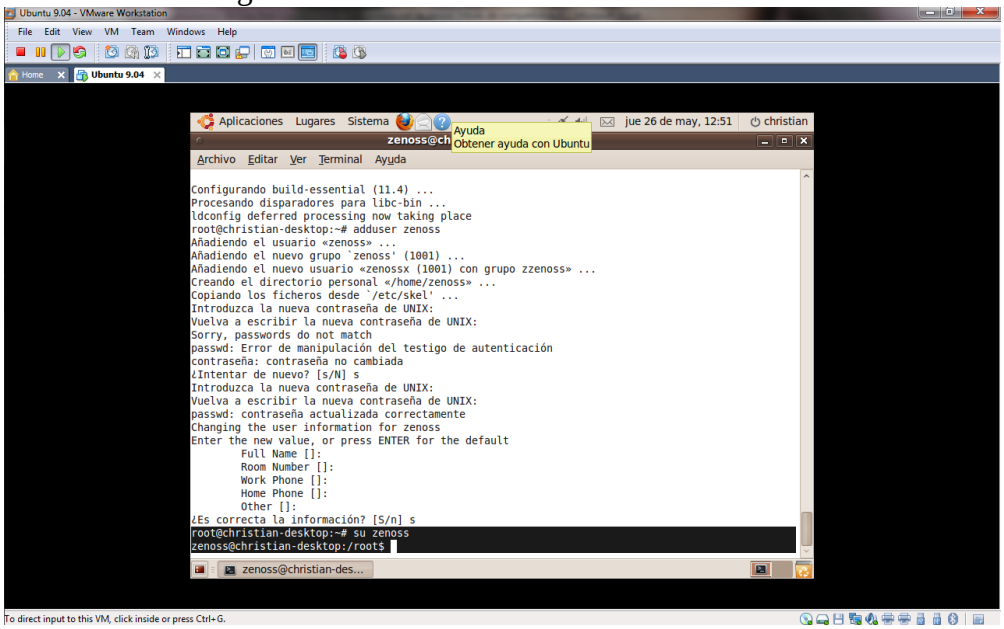


Fig 2.13 Cambio de usuario root al usuario zenoss

Se necesita cambiar de ubicación al home del usuario Zenoss con el comando
`$cd /home/zenoss/`

y se edita el archivo .bashrc:

`$nano .bashrc`

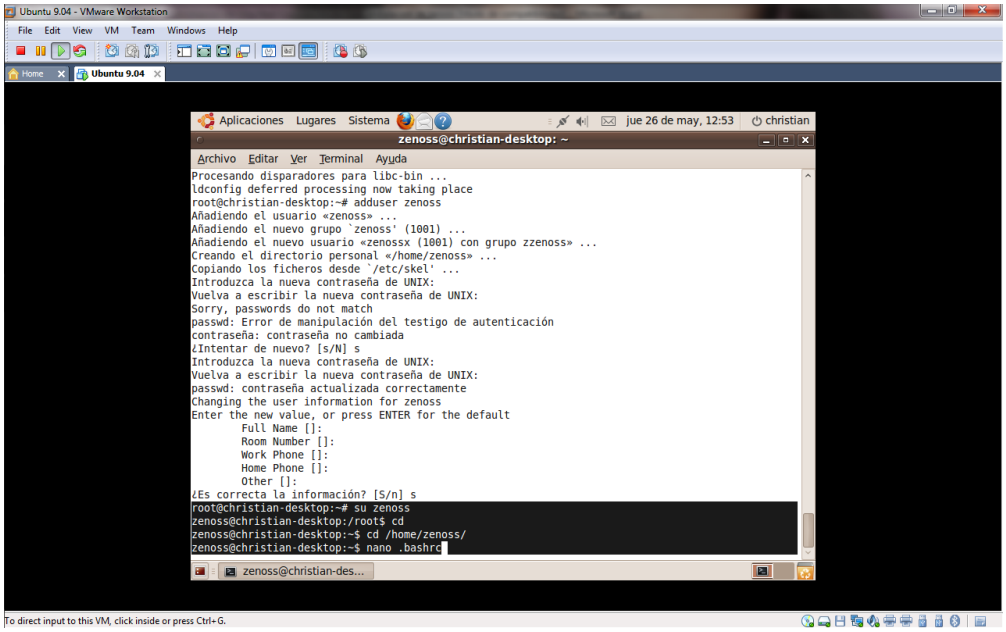


Fig 2.14 Edición del archivo .bashrc

Este es uno de los tres archivos que guarda funciones globales, configuraciones y alias comúnmente utilizadas por el Shell "bash". Se colocan las siguientes tres líneas que se muestran en la imagen al final del archivo.

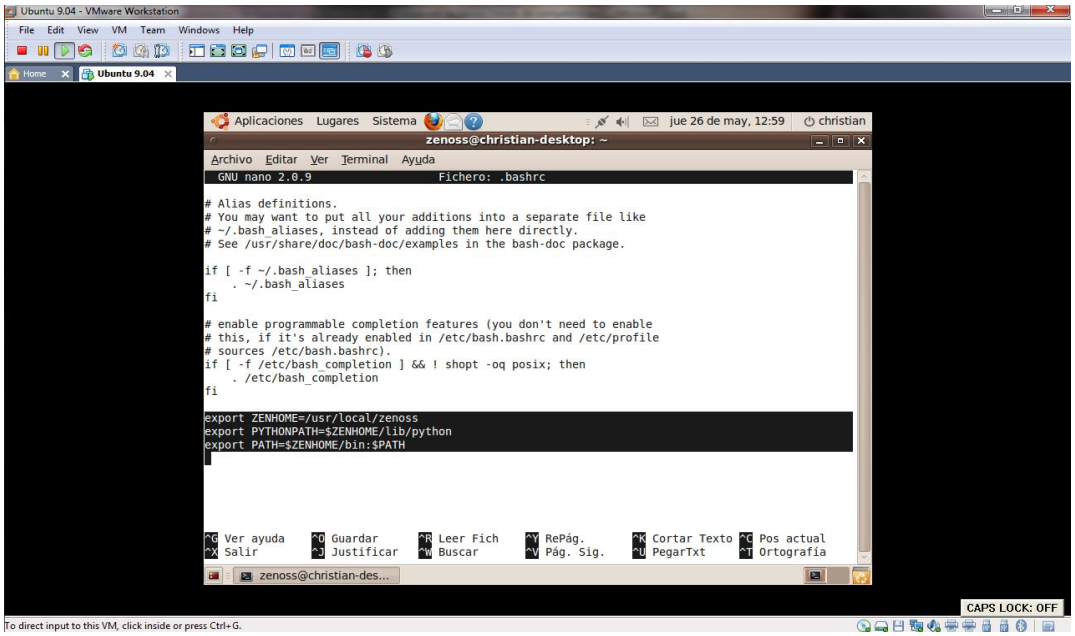


Fig 2.15 Agregado de variables

Estas variables definen:

export ZENHOME=/usr/local/zenoss: La ruta donde se instalará zenoss, será la raíz para el correcto funcionamiento de zenoss. Ahí se encuentran todos los archivos necesarios para su ejecución, tales como Zope, RDD, PySNMP, Twisted,etc.

Es recomendable que zenoss sea instalado en esta ruta o en alguna diferente a la del home del usuario es decir /home/zenoss asi, sí se desea desinstalar o se tiene problemas en la instalación y se requiere instalar de nuevo será más fácil la reinstalación.

export PYTHONPATH=$ZENHOME/lib/python: Es la ruta de la librería de python que permite encontrar las bibliotecas que se utilizarán en zenoss

export PATH=$ZENHOME/bin:$PATH: Ésta es la Ruta de los binarios ejecutados por zenoss.

Como se puede observar en las líneas anteriores ZENHOME apuntan a una ruta inexistente en ese momento por lo cual es necesario crear un directorio llamado zenoss, desde el usuario root. Si existe la pregunta del por qué se crea el home de zenoss, si ya se tiene un home y se enuentra en /home/zenoss, la respuesta es que; si existen problemas en la instalación de zenoss, la desinstalación y reinstalación será mas sencilla pues no se afectará a otros archivos del sistema.

La creación del directorio se realiza de la siguiente manera:

```
#mkdir /usr/local/zenoss
```

Se cambia de propietario, el cual será zenoss, si no se realiza el cambio se tendrá problemas para desempaquetar el tar.gz de zenoss esto se realiza con la siguiente línea (se puede observar en la imagen).

```
#chown zenoss /usr/local/zenoss
```

Antes de comenzar a instalar Zenoss se debe cerciorar de que el server mysql se encuentra corriendo, si no es así, se inicia con el comando:

```
#/etc/init.d/mysql status
```

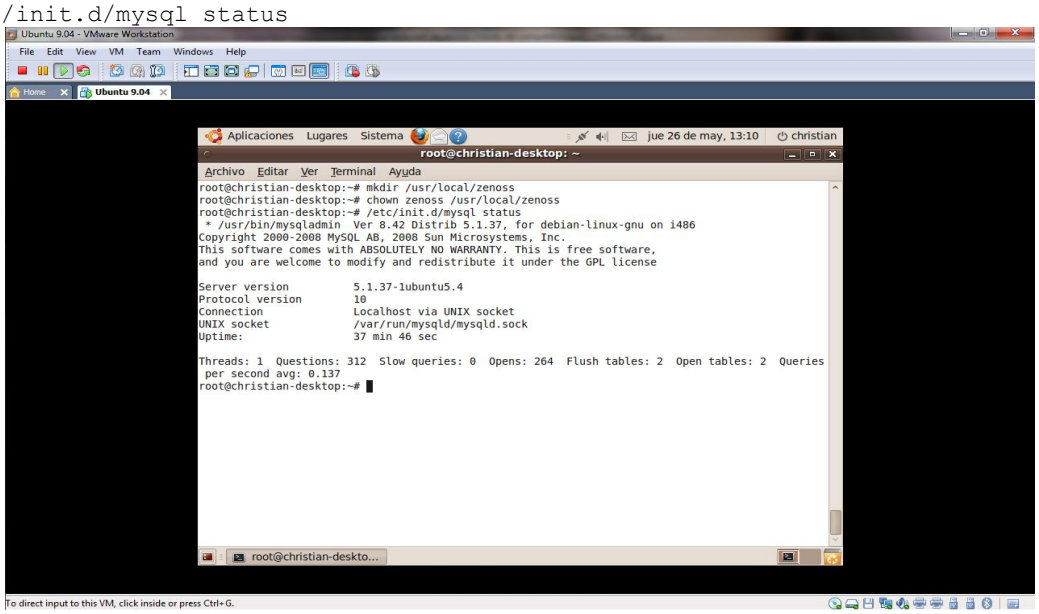


Fig 2.16 comando de verificación del servidor MySQL

2.1.2 Instalación de Zenoss

Como principio se debe descargar Zenoss Core de las siguientes páginas:
1.-http://community.zenoss.org/community/download?view=overview

Si se registra, se recibirá información por parte de zenoss a su correo, ya que es la página oficial de zenoss.

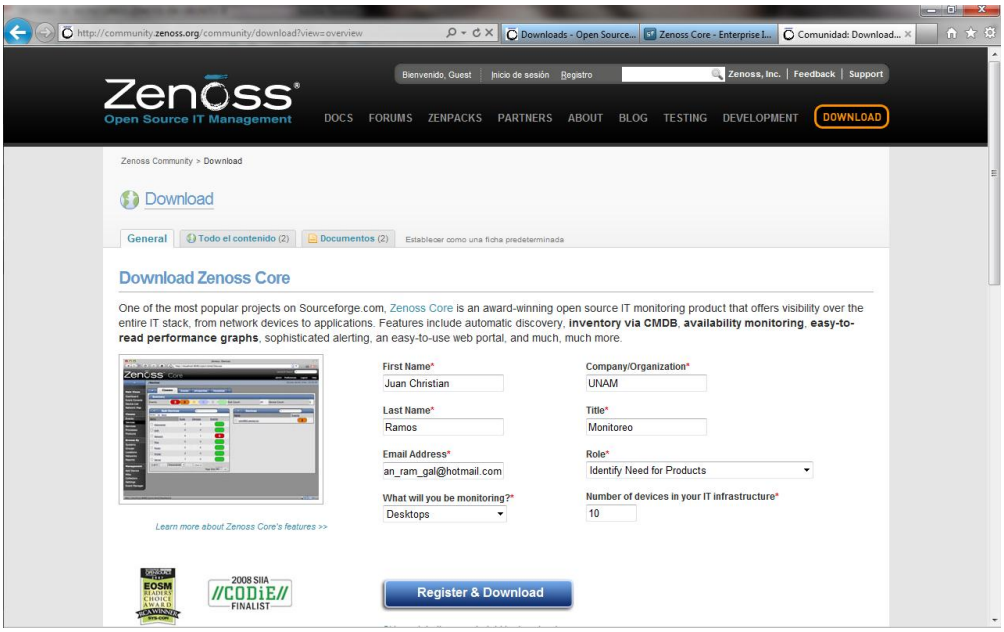


Fig 2.17 Pagina oficial de Zenoss

En esta página puede elegir las opciones de descarga para equipos de cualquier característica con sistema Linux, además de maquinas virtuales e información.

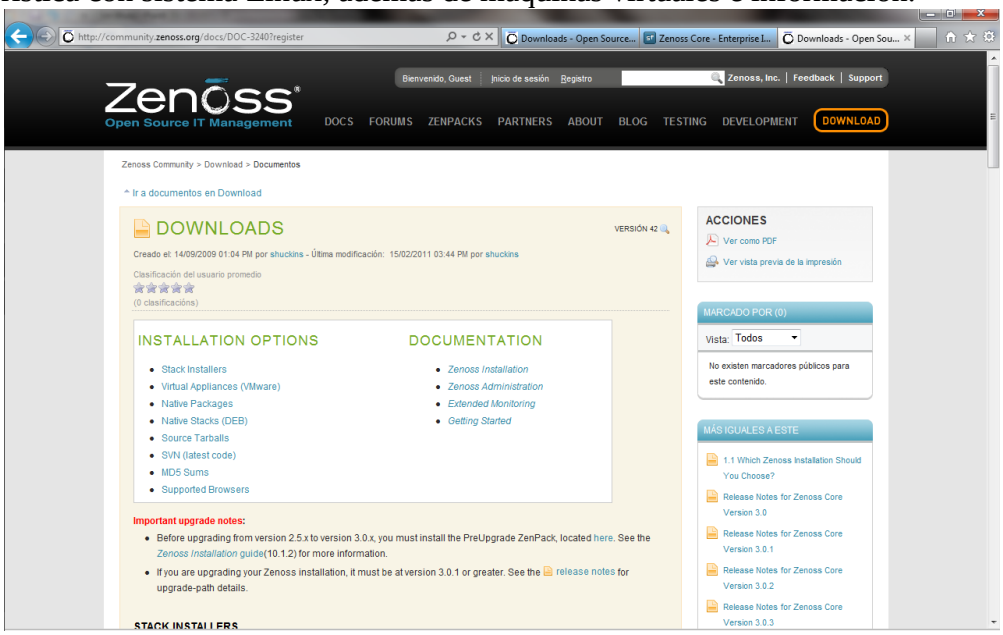


Fig 2.18 Página de descarga de Zenoss

2.- http://sourceforge.net/projects/zenoss/files/

Ésta es la otra página, se pueden encontrar varias versiones de zenoss (desde la 2.4 a la más actual)

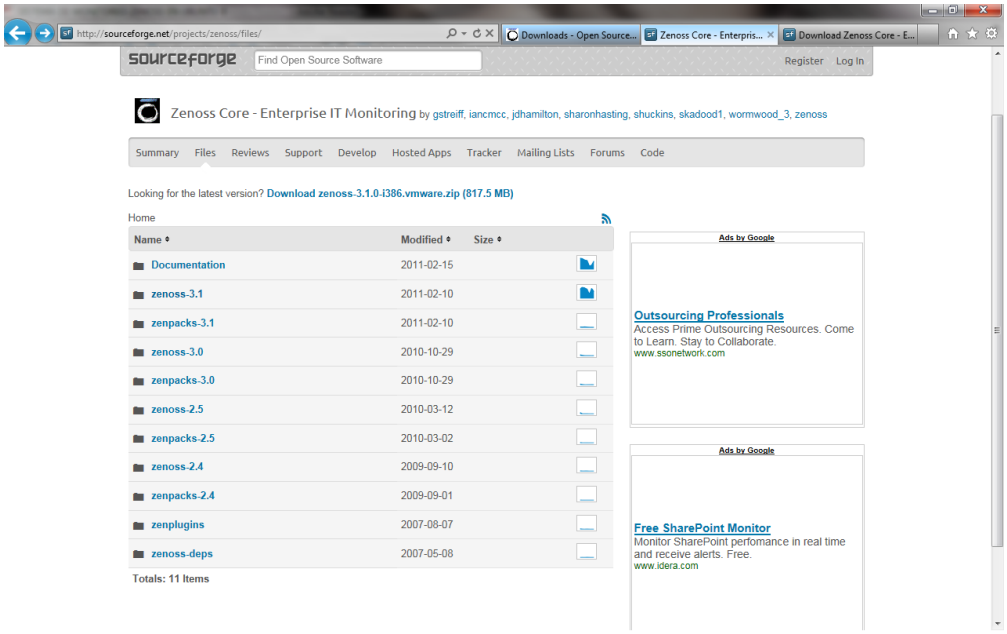


Fig 2.19 Página 2 de descarga de Zenoss

Se elige la versión requerida y se descarga, en este caso se eligió un archivo con extensión tar.gz versión 3.1. La descarga se realizo guardando el archivo en el escritorio y de forma gráfica.

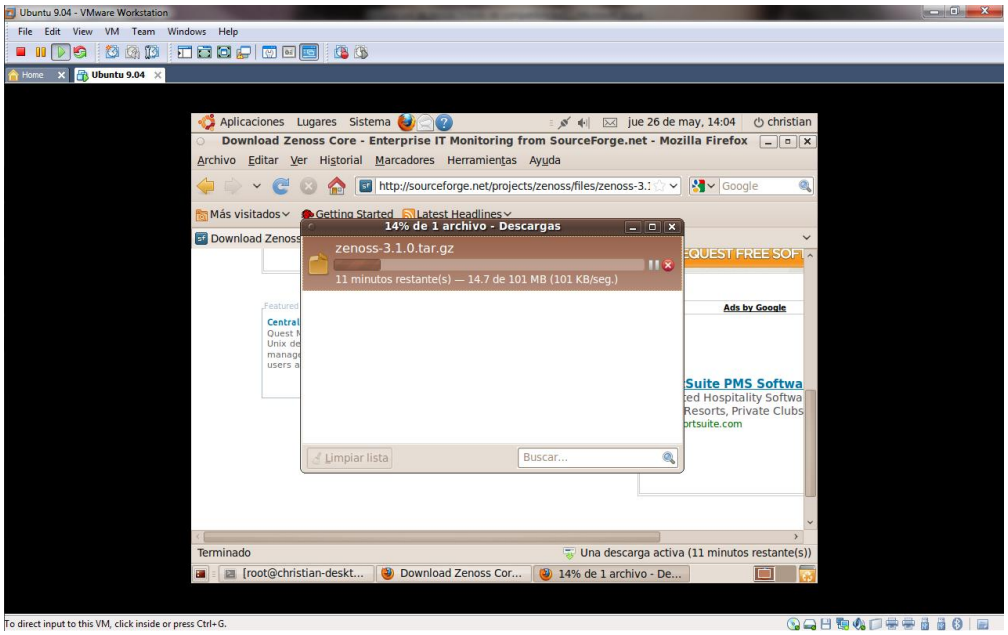


Fig 2.20 Descarga de Zenoss en forma gráfica

Se copia el paquete zenoss-3.1.0.tar.gz descargado en el escritorio a la ruta del directorio zenoss que anteriormente se había creado con el comando:

```
#cp /home/Christian/Escritorio/zenoss-3.1.0.tar.gz /usr/local/zenoss/
```

En ese comando se menciona primero la ruta donde se encuentra el archivo que se quiere mover en este caso zenoss-3.1.0.tar.gz, y luego la ruta a donde se quiere mandar, estas dos rutas separadas por un espacio.

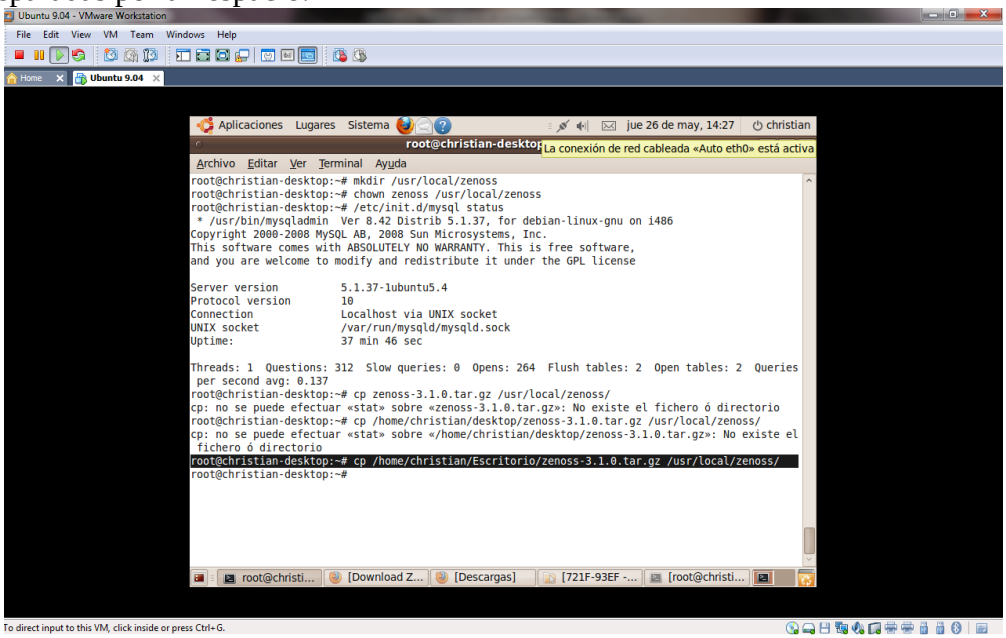


Fig 2.21 Copia del archivo descargado al directorio Zenoss

Se le da los permisos para los diferentes usuarios desde root, y después se posiciona en el directorio zenoss, con el comando:

```
#cd /usr/local/zenoss/
```

Posicionados en este directorio se le dan los permisos con el comando:

```
#chmod 755 zenoss-3.1.0.tar.gz
```

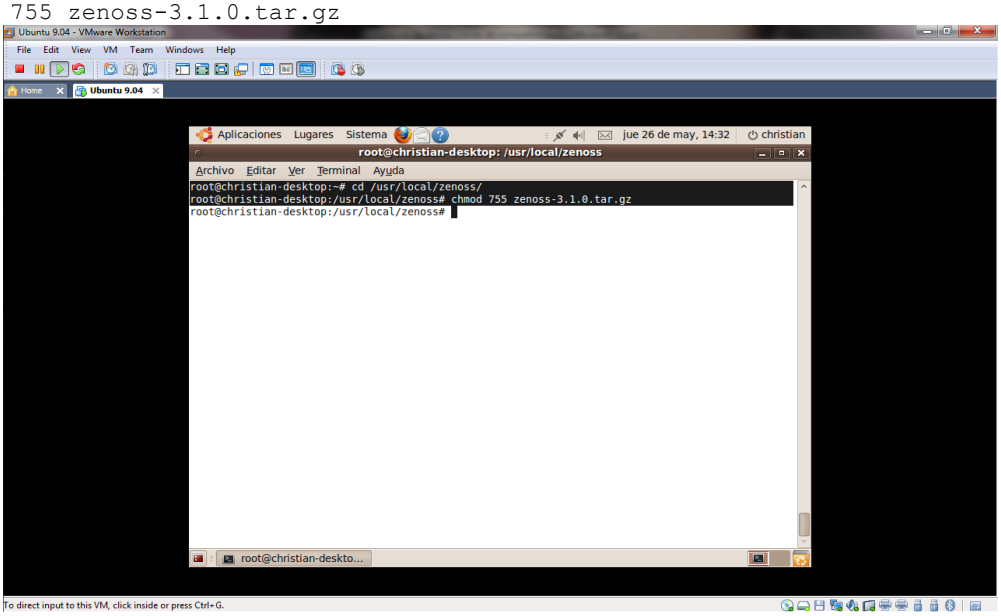


Fig 2.22 Permisos para los usuarios

Teniendo los permisos se descomprime y se compila el archivo zenoss-3.1.0.tar.gz, desde el usuario zenoss con los comandos:

```
#su zenoss
$cd /usr/local/zenoss/
$tar -zxvf zenoss-3.1.0.tar.gz
```

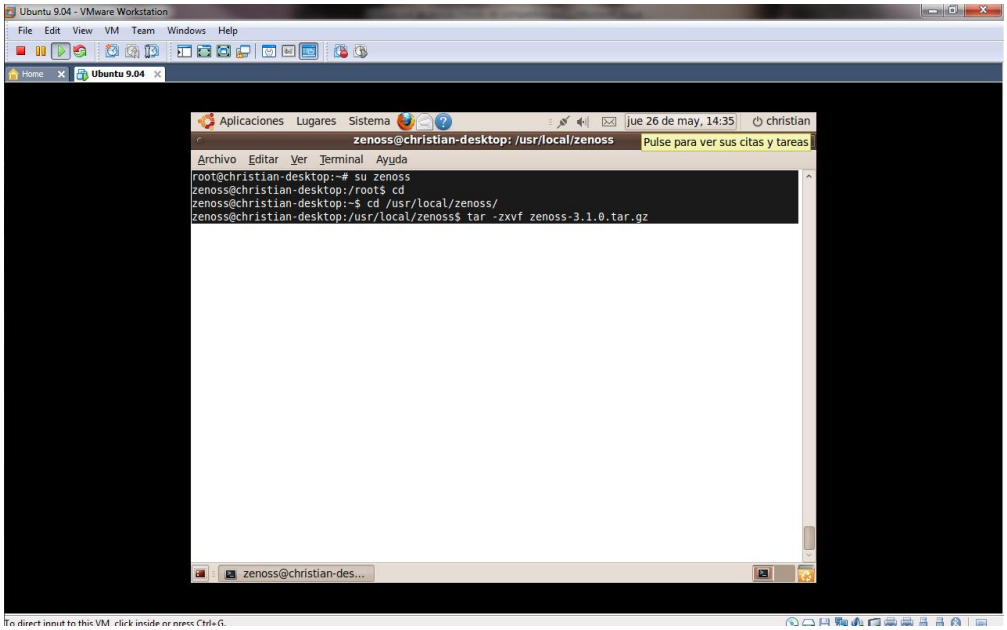


Fig 2.23 Comando para descomprimir el archivo

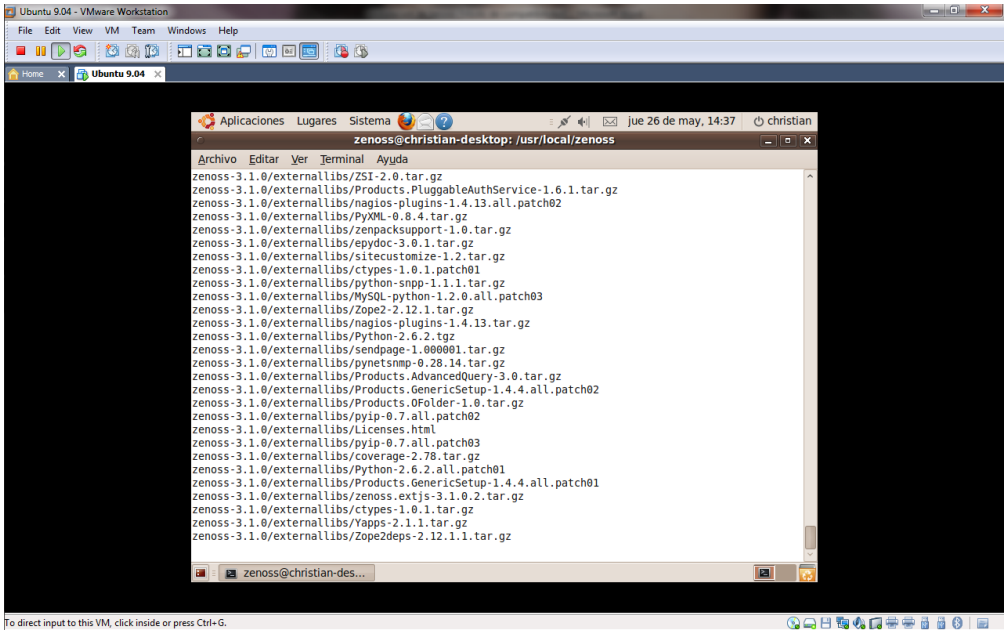


Fig 2.24 Archivo descomprimido

Después de esta larga preparación, es momento de instalar Zenoss entrando al directorio que se descomprimió, verificando su nombre de este nuevo directorio con el comando que muestra lo que contiene el directorio en el que estamos colocados:

```
$ls
```

En este caso aparece en la imagen de color azul y con el nombre de zenoss-3.1.0, es necesario moverse hacia el interior de este directorio con el comando:

```
$cd zenoss-3.1.0
```

Ya dentro se aplica el comando para instalarlo:

```
$./install.sh
```

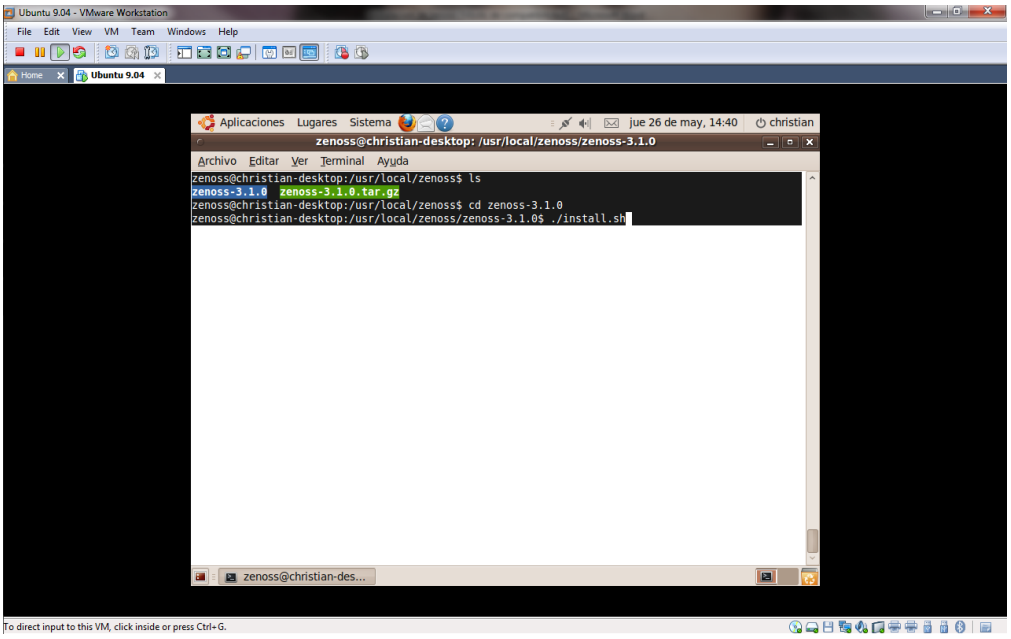


Fig 2.25 Comando de instalación

Otro error que se presento fue el del siguiente mensaje "*svn make is not in the path*", lo cual cancelo la instalación como se muestra en la imagen.

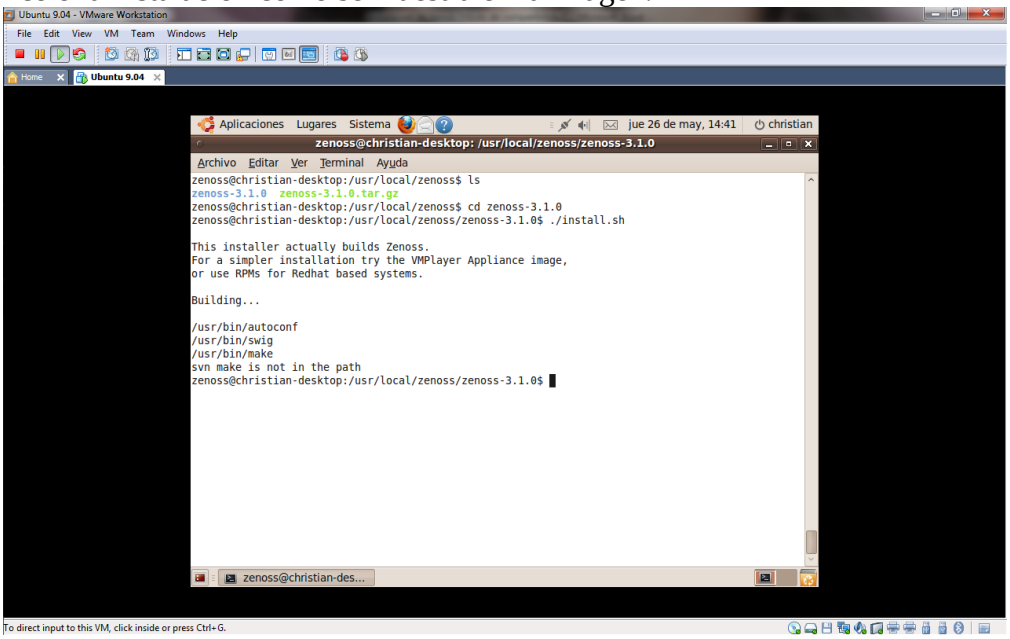


Fig 2.26 Error por falta de instalación de un paquete

Esto se debió, porque faltaba instalar el paquete "svn-buildpackage". Este es una herramienta para construir y mantener paquetes Debian utilizando un repositorio subversion.

La instalación de este paquete, se realiza como usuario root y con este comando:

```
$apt-get install svn-buildpackage
```

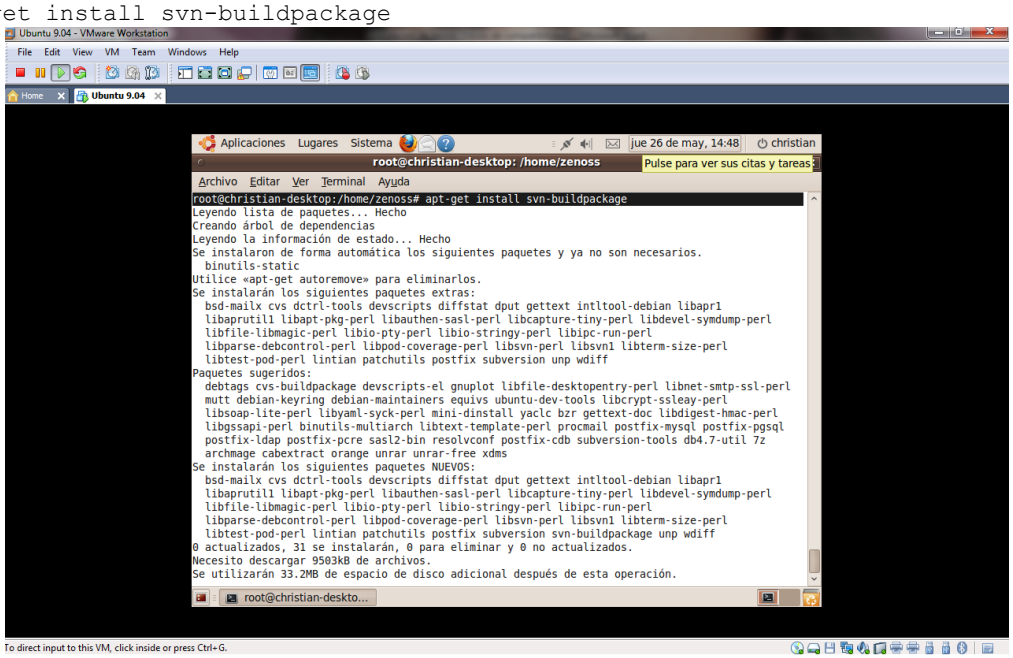


Fig 2.27 Instalación del paquete svn-buildpackage

Como es una prueba virtualizada y no se tiene un servidor de correos, cuando aparece la siguiente ventana azul con gris, se selecciona la opción "sin configuración", como en la imagen.

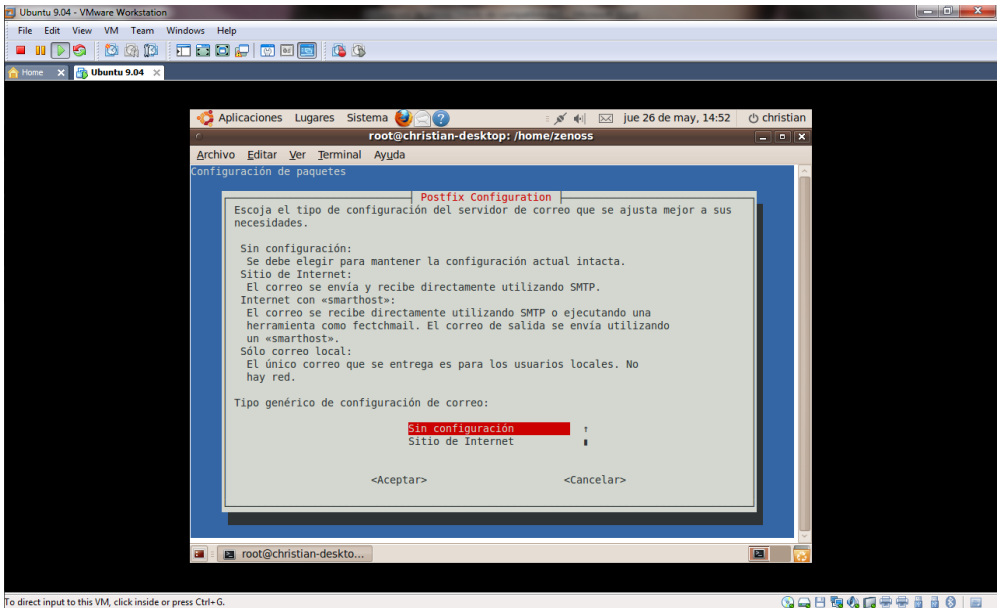


Fig 2.28 Elección de la opción "Sin configuración"

Después de instalar este paquete se puede comenzar a instalar Zenoss sin problemas. En la primera línea pide el servidor, donde se colocará la base de datos, presionamos Enter, pues se colocará en el servidor local.

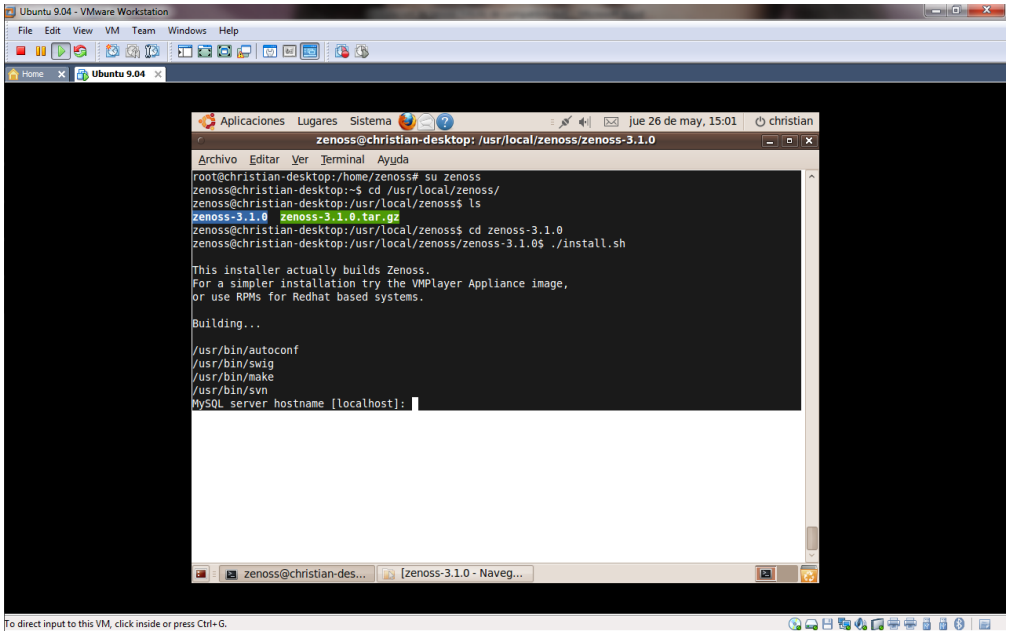


Fig 2.29 ubicación del servidor MySQL

En esta parte se coloca el password que se había puesto al usuario root de MySQL para la conexión de la base de datos.

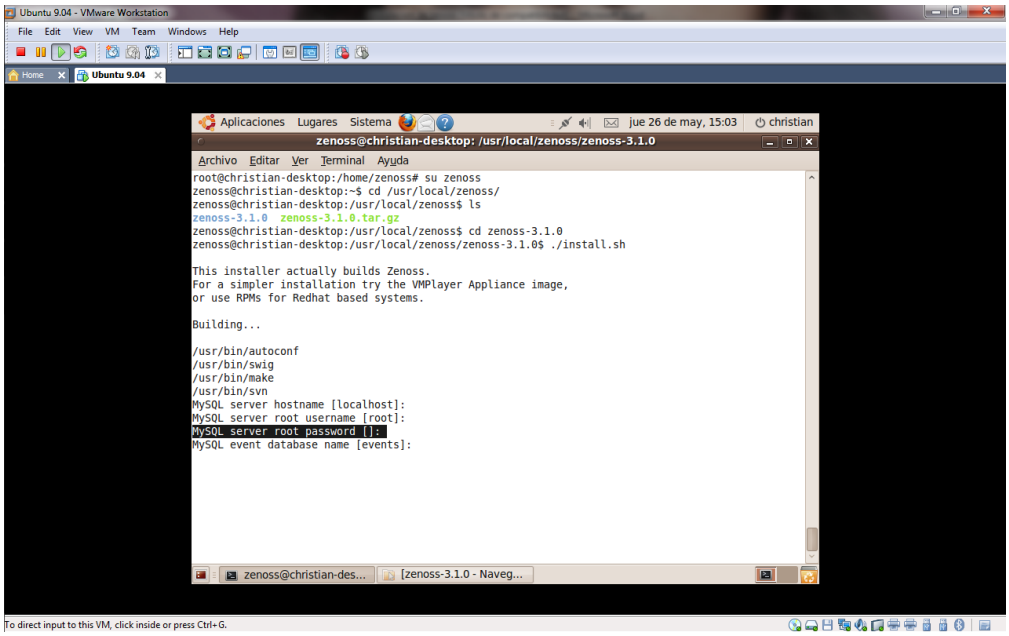


Fig 2.30 Contraseña del servidor MySQL

Se deja el usuario con el nombre de zenoss y se coloca de contraseña "zenoss" de nuevo como contraseña para la base de datos de Zenoss.

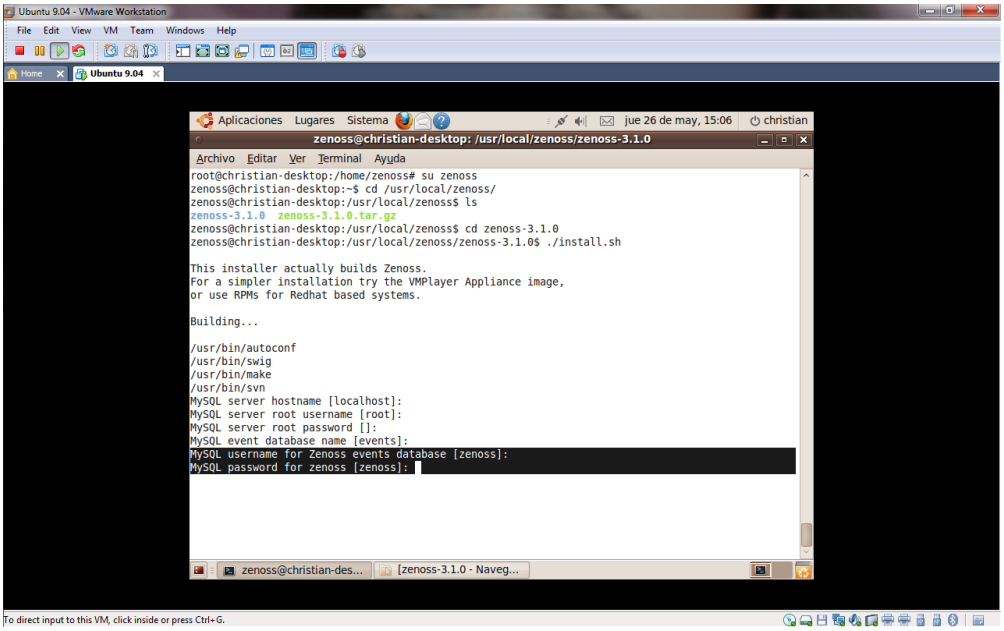


Fig 2.31 Usuario y contraseña para la base de datos de zenoss

La instalación tarda bastante dependiendo del ancho de banda de la red y de los recursos del equipo físico.

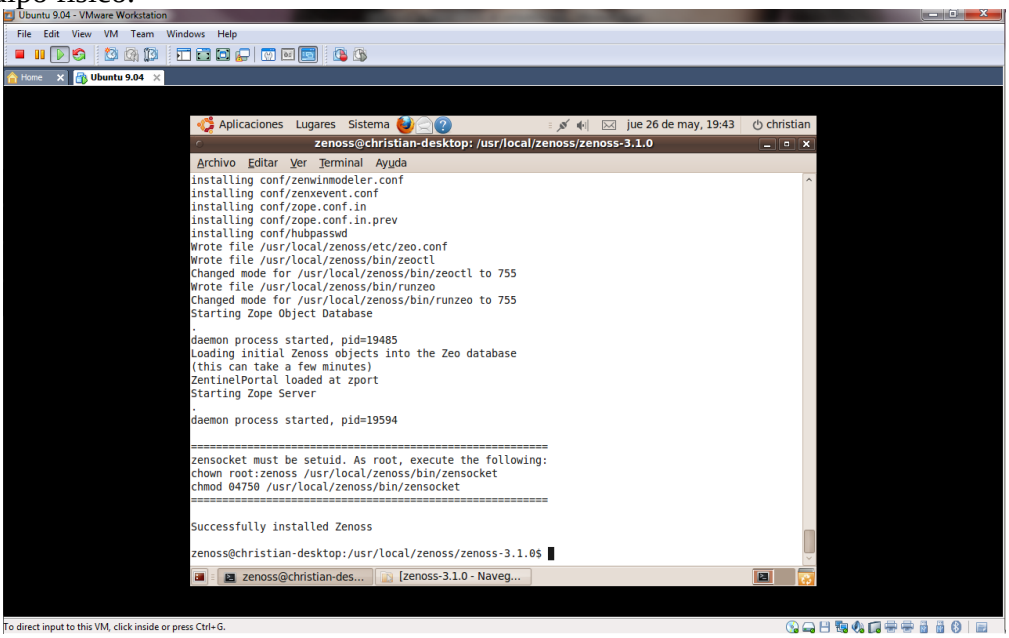


Fig 2.32 Fin de la instalación

Si la instalación llega a tener alguna falla, se puede deshacer los cambios hechos en el proceso, ejecutando el comando:

```
$make clean
```

Al finalizar la instalación, se cambia de propietarios y se asignan nuevos permisos al archivo zensocket, esto es para que el usuario zenoss pueda ejecutar ciertos binarios, y así tener un correcto funcionamiento de zenoss, realizando esto con los comandos:

```
#cd /usr/local/zenoss
#chown root:zenoss /usr/local/zenoss/bin/zensocket
#chmod 84750 /usr/local/zenoss/bin/zensocket
```

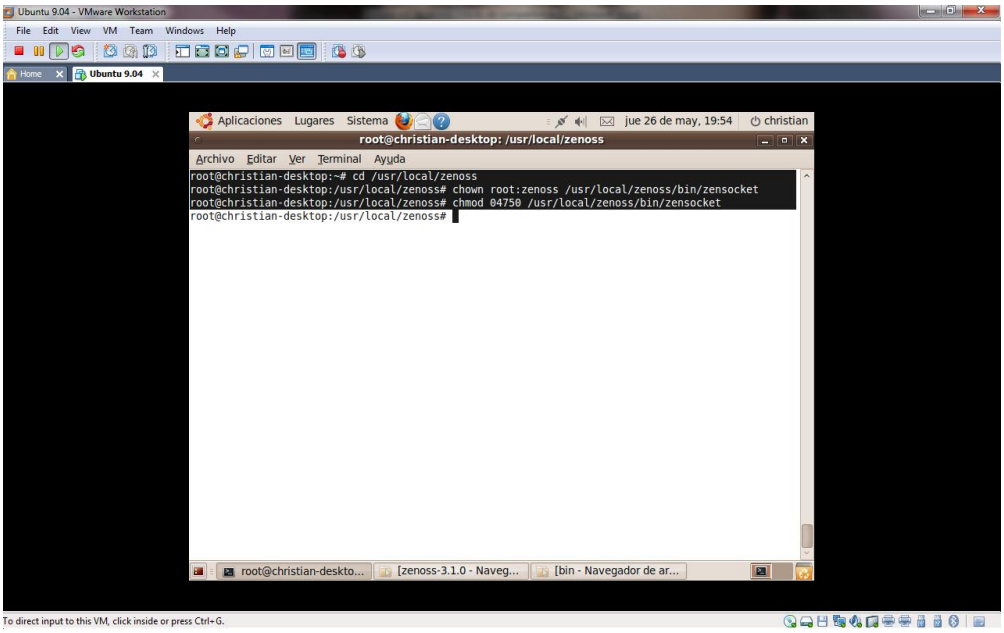


Fig 2.33 Permisos y nuevos servicios del archivo zensocket

Utilizando el usuario zenoss, se pueden inicializar los demonios del software para comenzar el monitoreo de la red, con el comando:

```
$zenoss start
```

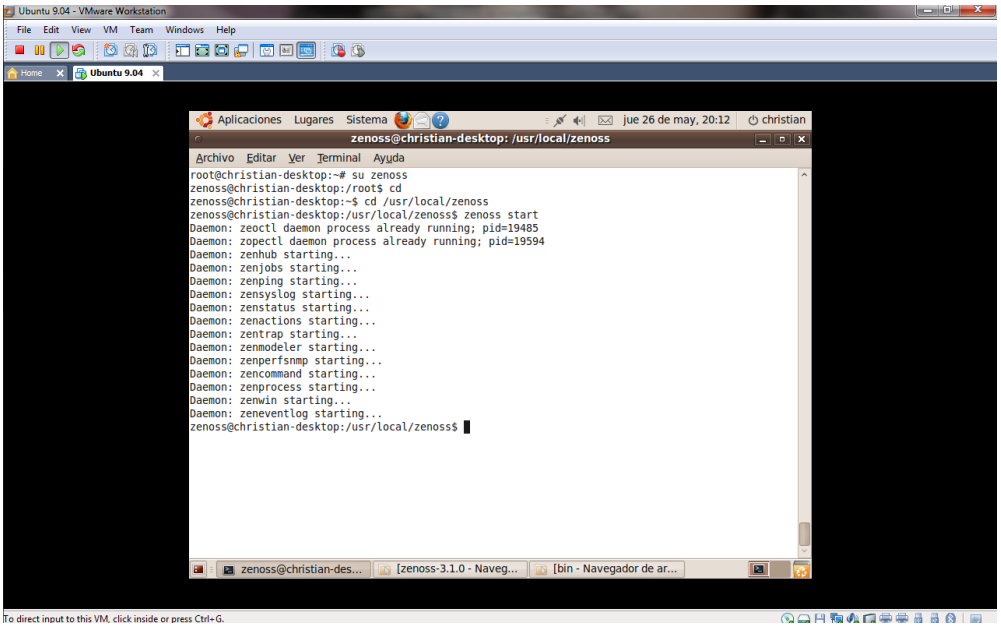


Fig 2.34 Inicio de zenoss

Para asegurarse de que los demonios de zenoss se encuentran corriendo correctamente se aplica el comando:

```
$zenoss status
```

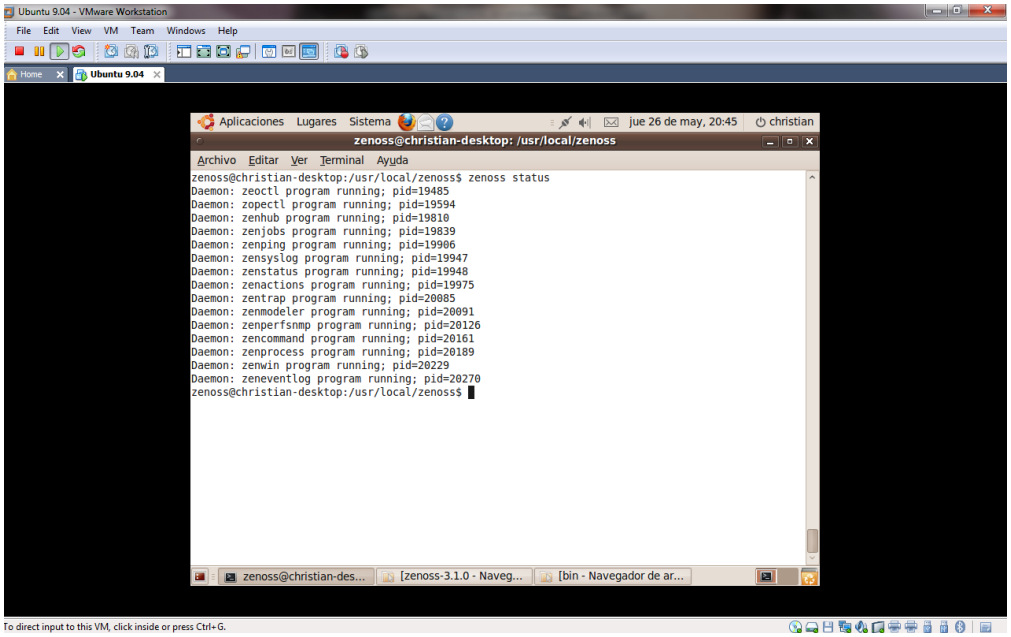


Fig 2.35 Verificación del estado de los servicios

Si en esta verificación del estado de zenoss llegase aparecer que el demonio "zenhub" se encuentra en "not runing" lo que provocria este error es impedir la conexión de zenoss con los dispositivos de la red, esto se puede resolver al ingresar a la carpeta de los archivos caches del usuario zenoss (/usr/local/zenoss/var/) y borrar el archivo cache de arranque de zunhub y posteriormente proceder a reiniciar zenoss.

```
zenoss@christian-desktop:/usr/localzenoss/var$ rm –rf zenhub-1.zec
zenoss@christian-desktop:/usr/localzenoss/var$ zenoss restart
```

Al conectarse por primera vez a la interfaz web de zenoss colocando la siguiente línea en la barra de direcciones:

```
http://localhost:8080/sport/dmd/
```

Se muestra la siguiente pantalla, en la cual oprimimos "Get Started" para continuar.

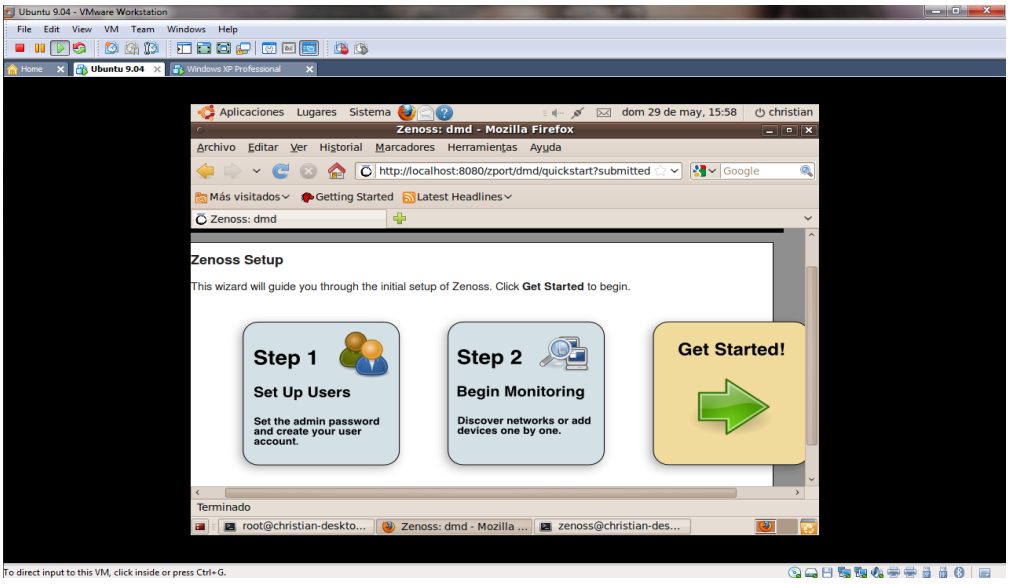


Fig 2.36 Pantalla inicial de la interfaz web

En la siguiente ventana se coloca la contraseña de administrador de **zenoss** y se crea un usuario del lado derecho, la diferencia de la segunda cuenta es que no tiene tantos privilegios como la primera.

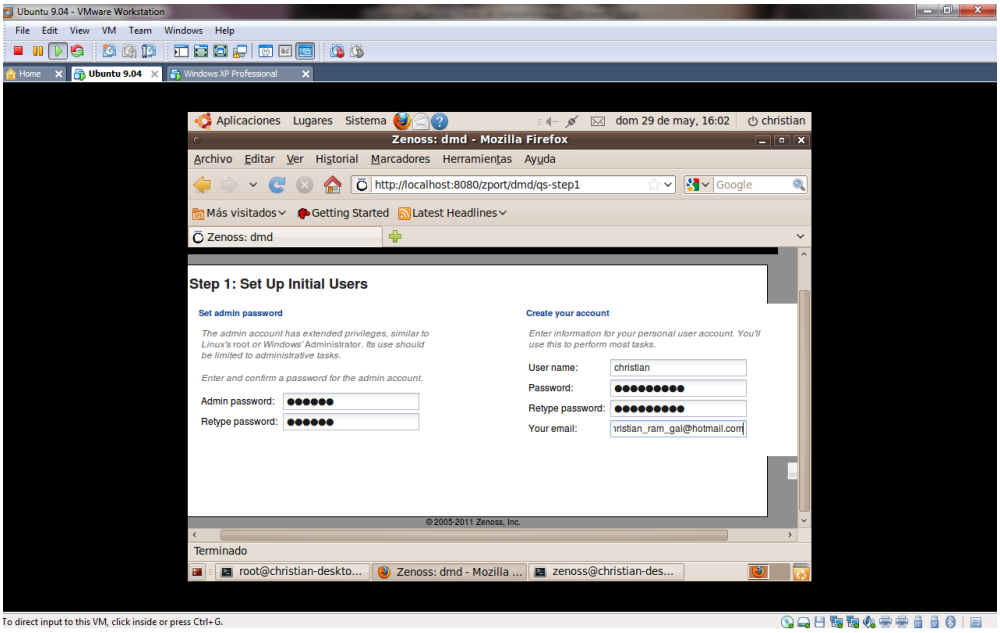


Fig 2.37 Establecimiento de usuarios iniciales

En la ventana para agregar una red solo damos en "***skip to the dasboard***" para después agregar los equipos, para empezar a familiarizarse con el software.

2.2 CONFIGURACION DE LOS EQUIPOS CLIENTES CON AGENTES SNMP

2.2.1Agente SNMP en Linux Ubuntu

Como se mencionó en tema1 este tipo de software de gestión de redes, necesita que los equipos clientes tengan instalado un agente, el cual recolecta la información y la envía al gestor o administrador. Es así como funciona Zenoss, por lo cual después de instalar el gestor, se procederá con la instalación del agente en cada uno de los equipos administrados. Como primer paso se necesita descargar e instalar el paquete del demonio "**snmpd**" desde los repositorios, además de descargar el paquete cliente de snmp para realizar pruebas internas de monitoreo.

Con los comandos:

```
#apt-get install snmpd
#apt-get install snmp
```

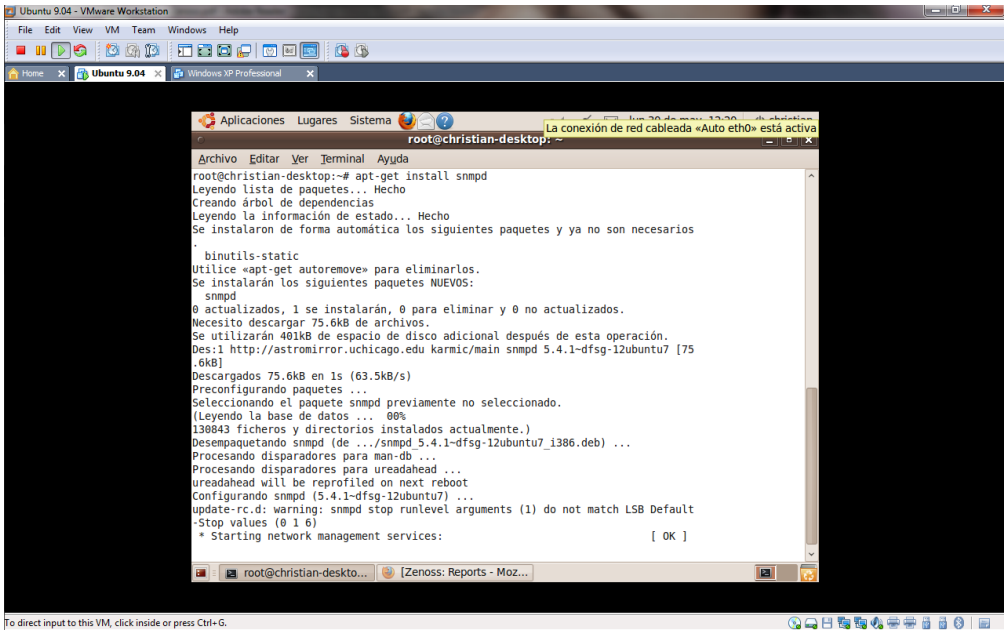


Fig 2.38 Instalación de snmpd

Despues de la instalcación, se abre el archivo *snmpd.conf* como usuario root y en las primeras líneas se definirán la relación entre comunidades y modelos de seguridad, creando una comunidad a la que se llamará "*práctica*", con permisos de lectura y escritura para permitir el escaneo completo del equipo y realizar diferentes pruebas. Este paso se representa en la línea remarcada de la imagen).

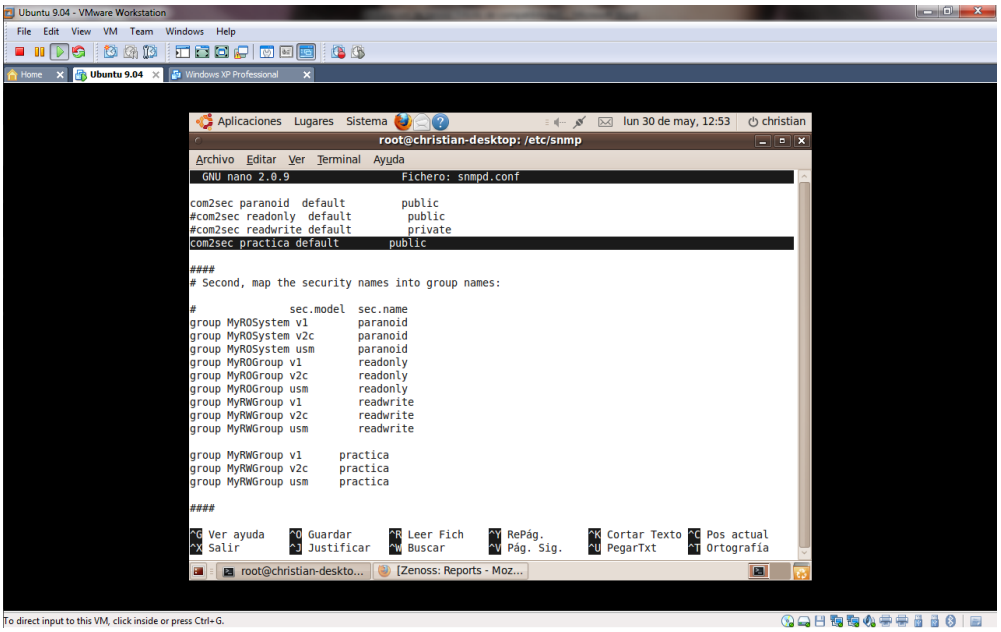


Fig 2.39 Comunidad práctica en archivo snmpd.conf

Después de colocar estas líneas, se define la relación entre modelos de seguridad y grupos, agregando en este mismo archivo las variables para los permisos de lectura y escritura de la comunidad "*practica*", los cuales se aplicarán a los agentes snmp de esta comunidad en específico que requieran información, este paso se representa en las 3 líneas seleccionadas en la imagen.

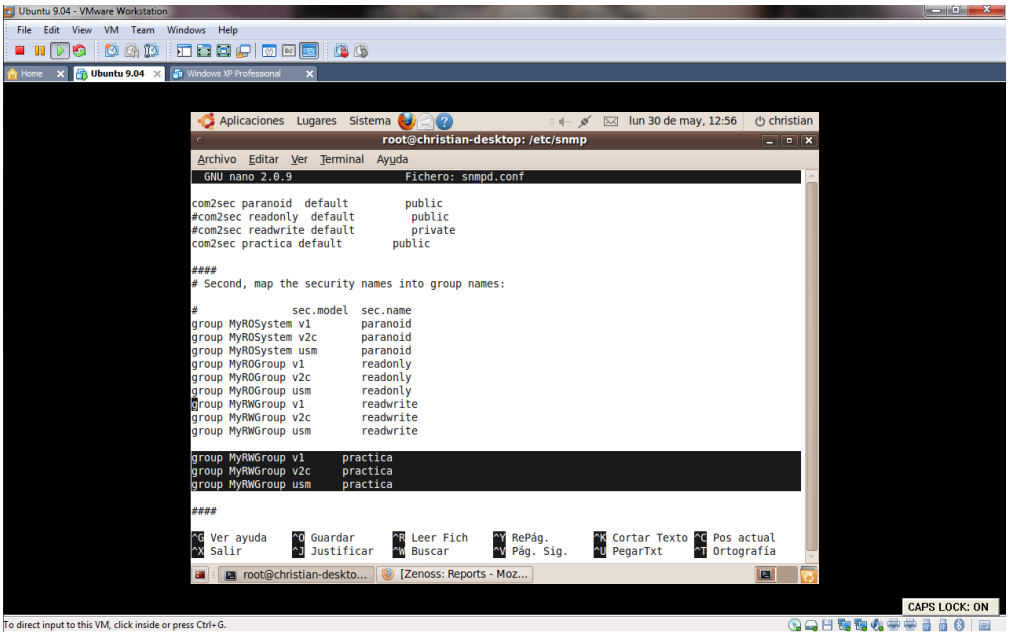


Fig 2.40 Relacion entre modelos de seguridad, grupos y variables

Es muy importante agregar la línea **rocommunity public** para activar las versiones SNMP 1, 2 de solo lectura y tener acceso de SNMP desde todos los host remotos con el nombre de comunidad public, permitiendo con esta configuración graficar los recursos en el equipo.

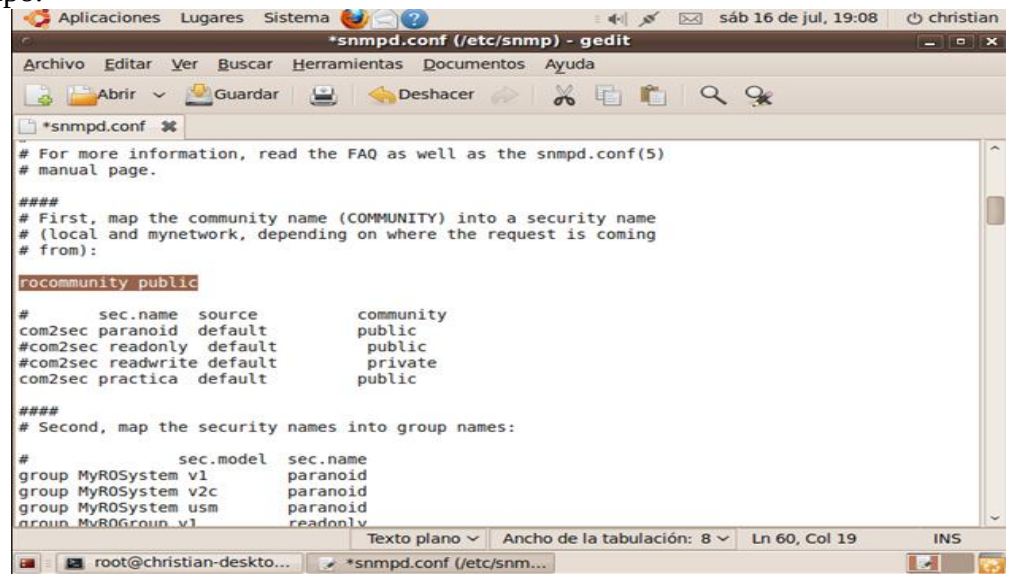


Fig 2.41 Agregado de la línea "rocommunity public"

Finalmente en el archivo "*snmpd*" se especificará que el equipo recibirá peticiones snmp de cualquier IP en la red. Este archivo "snmpd" se puede modificar y editar con el siguiente comando:

```
#nano /etc/default/snmpd
```

Abierto el archivo snmpd que se encuentra en el directorio */etc/default*, se borra de la línea seleccionada en la imagen, la IP de localhost (127.0.0.1), observándose exactamente como en la imagen 2.42. Realizado esto se guarda y se sale del archivo.

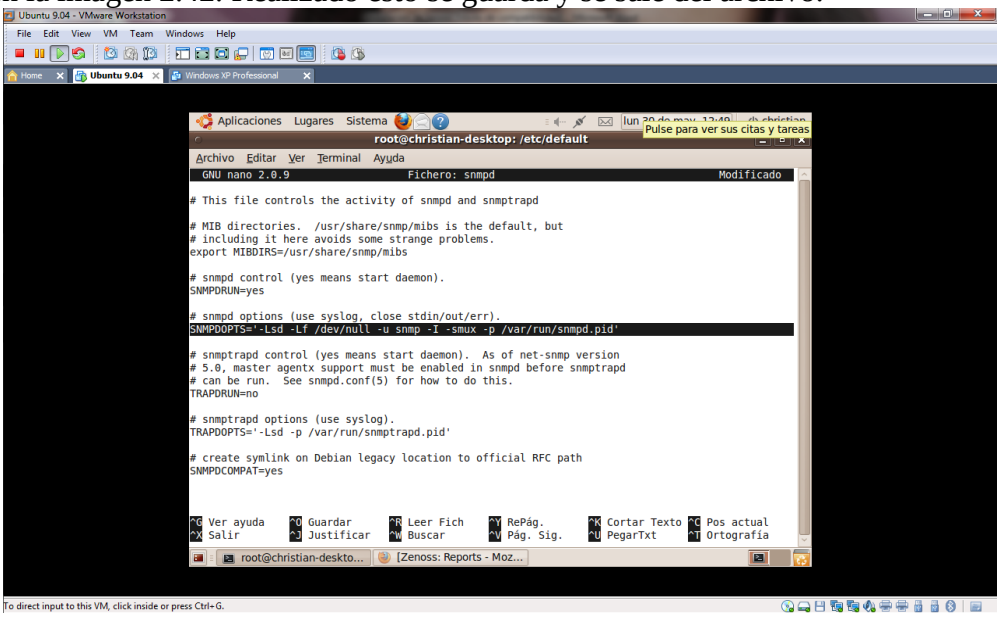


Fig 2.42 Borrado de localhost (127.0.0.1)

Para que se retomen los cambios efectuados reinicia el daemon de la siguiente manera:

```
#/etc/init.d/snmpd restart
```

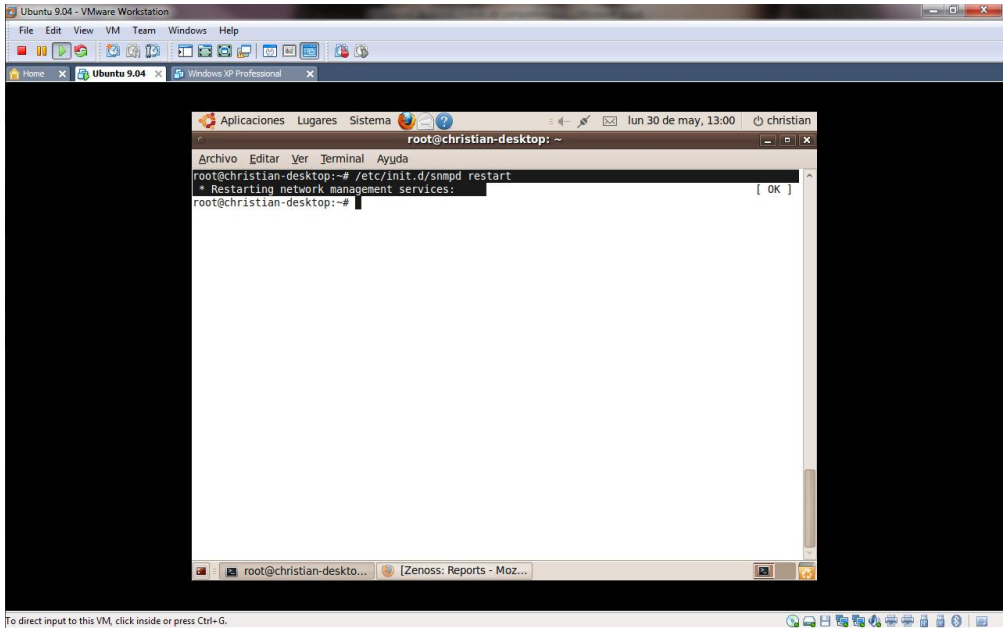


Fig 2.43 Reinicio de SNMP

Es necesario comprobar que el agente snmp esta correctamente configurado, para eso se utiliza el comando snmpwalk, especificando la versión, la comunidad y la IP del equipo a monitorear, en este caso el localhost.

```
# snmpwalk -c public -v2c 127.0.0.1
```

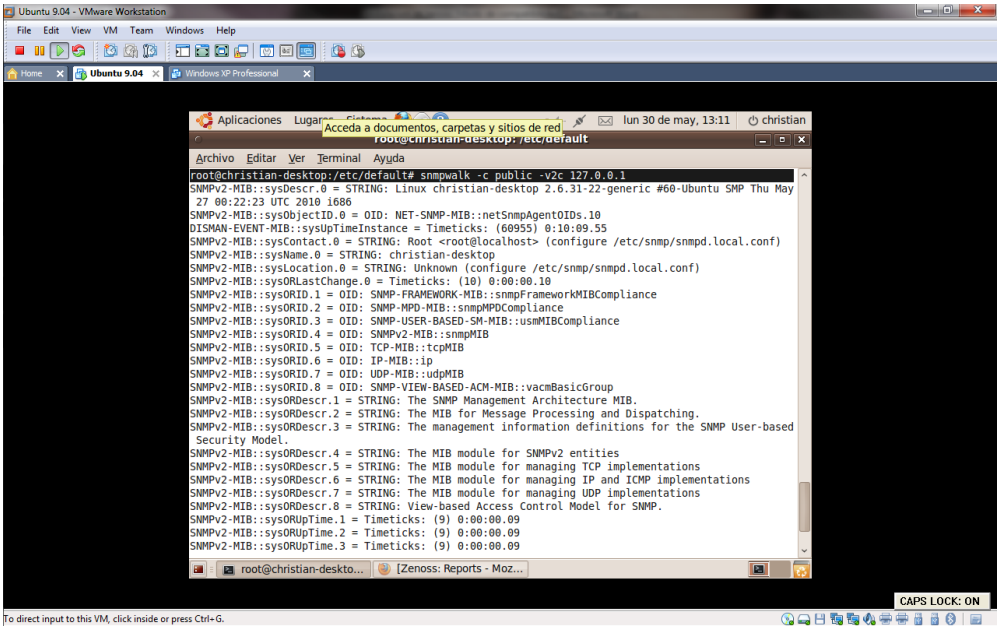


Fig 2.44 Comprobación del agente SNMP

2.2.2 Agente SNMP en Windows

Así como en Linux, Windows necesitan un agente SNMP que permita el monitoreo de su estado, dispositivos, aplicaciones, procesos y otros. Para su instalación se utiliza el CD de instalación de Windows, como se explica de la siguiente manera:

Para comenzar a instalar SNMP vamos a *inicio -> Panel de Control -> Agregar o quitar Programas*, la tabla muestra los programas instalados en el SO.

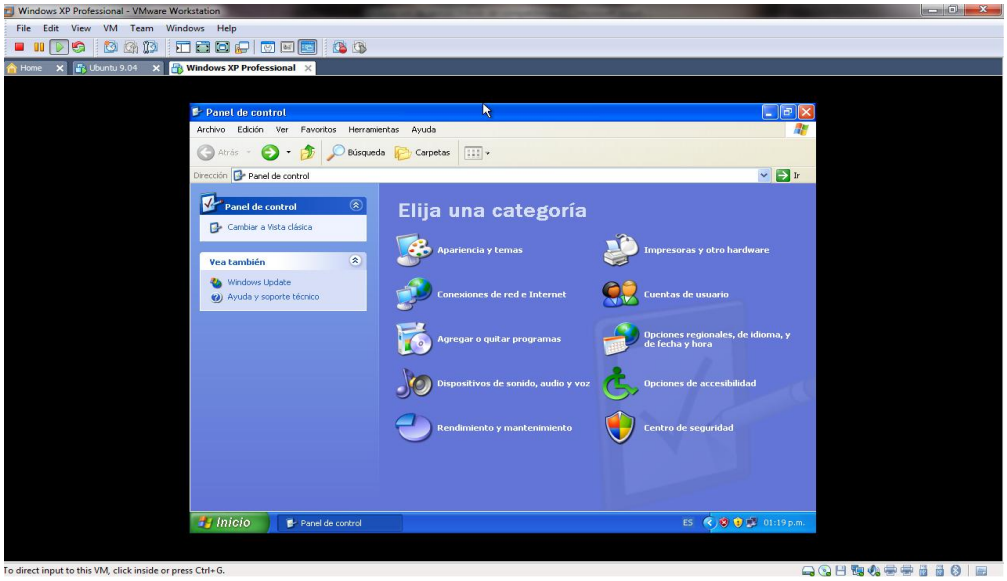


Fig 2.45 Panel de control

En la ventana que aparece, oprimimos el botón de "*Agregar o Quitar componentes de Windows"* localizado en el menú del lado izquierdo y aquí muestra los componentes para instalar desde el CD.Se selecciona y activa "*Herramientas de administración y supervisión*" donde se encuentra la activación del agente SNMP.

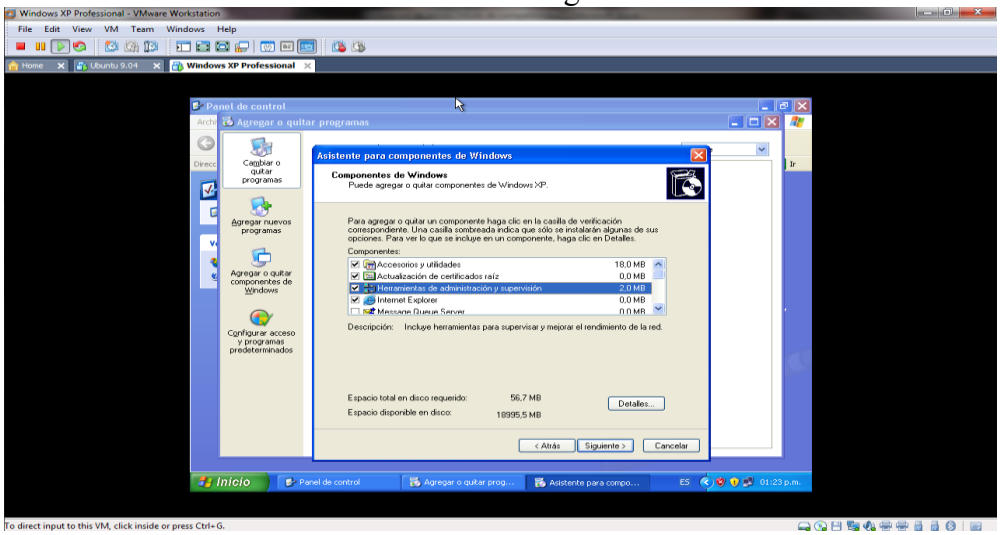


Fig 2.46 Herramientas de administración y supervisión

En detalles se pueden ver las líneas de activación de SNMP, se seleccionan y activan las dos que aparecen y se aceptan los cambios. Posteriormente el sistema pide el CD de instalación XP y se cargan los archivos seleccionados.

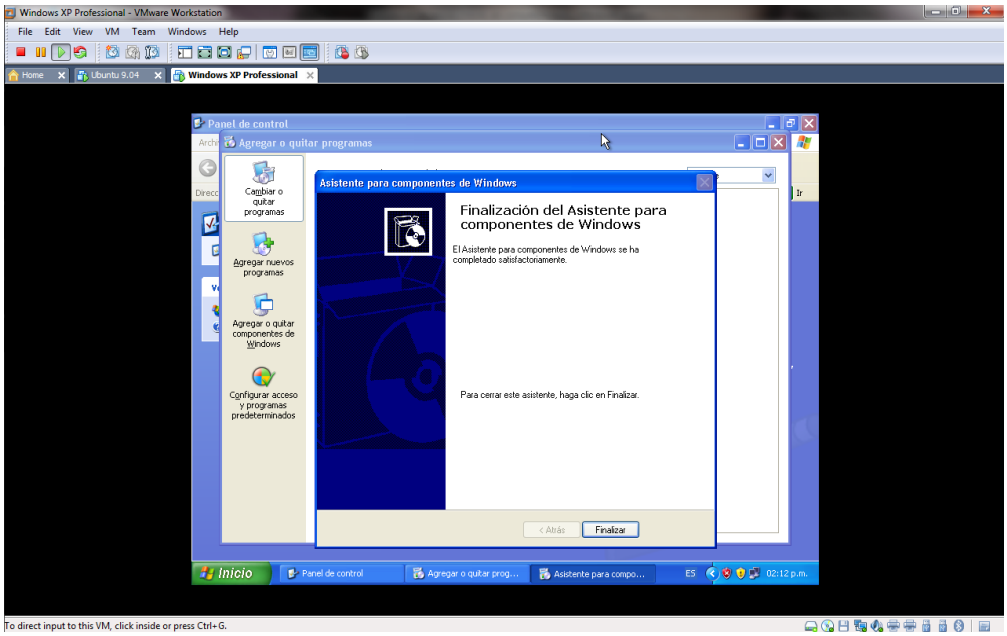


Fig 2.47 Fin de la instalación de los componentes SNMP

Después de que la instalación termina de manera correcta, se puede seguir con la configuración del agente para la entrega de datos.

Para lo cual se pasa a la interfaz de servicios de Windows dirigiéndose a *Inicio -> ejecutar -> y se teclea el comando services.msc*

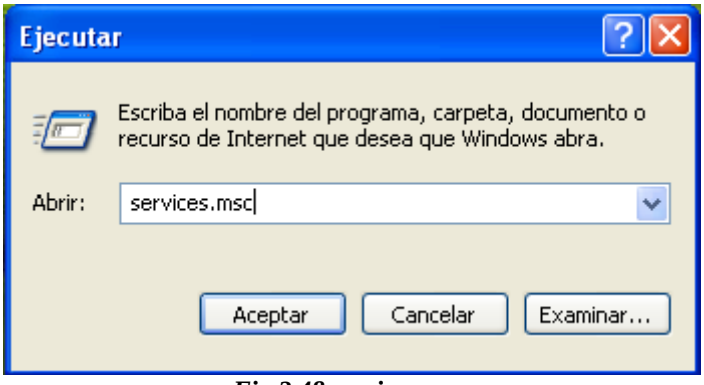


Fig 2.48 services.msc

Abierta la interfaz de servicios, se selecciona "*Servicio de captura SNMP*" el cual específica el envío de datos hacia el equipo que monitorea el sistema local.

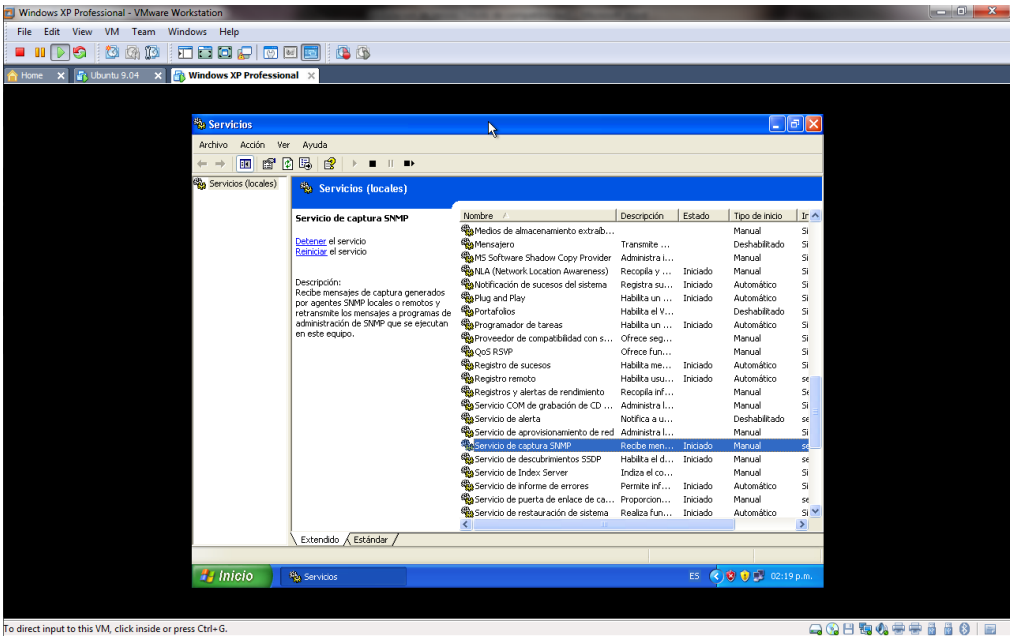


Fig 2.49 Selección del "Servicio de Captura SNMP"

Se habilita el inicio de servicio "*automático*" sin modificar los demás datos, se aceptan los cambios y se procede a reiniciar el servicio desde la opción superior izquierda.

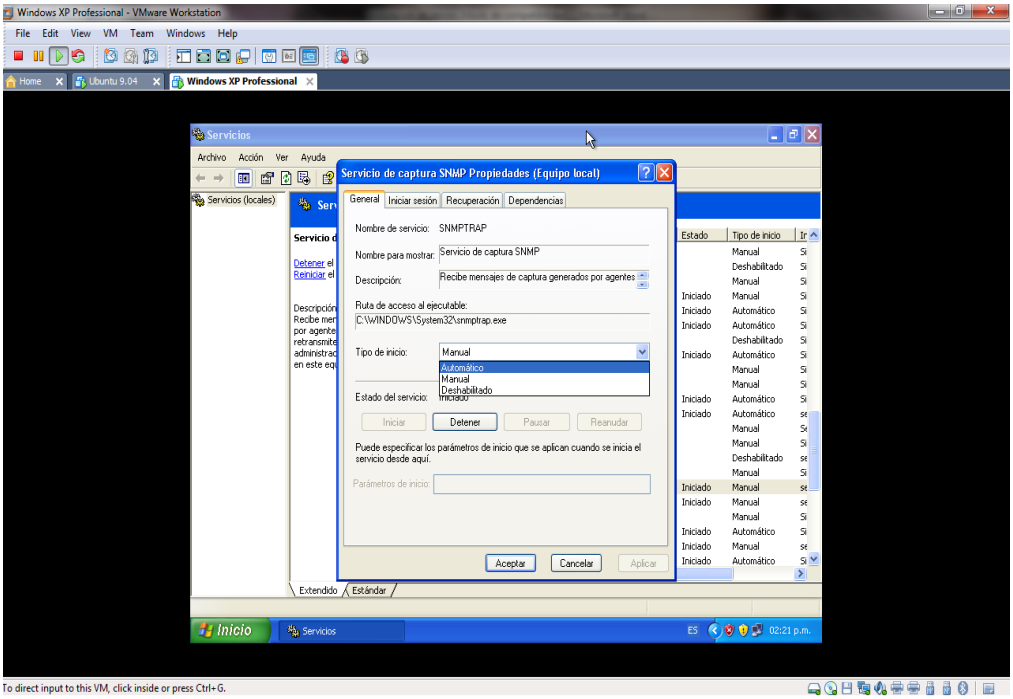


Fig. 2.50 Selección de inicio automático

Ahora se configura el "*Servicio SNMP*" como protocolo de entrega de datos de estado.

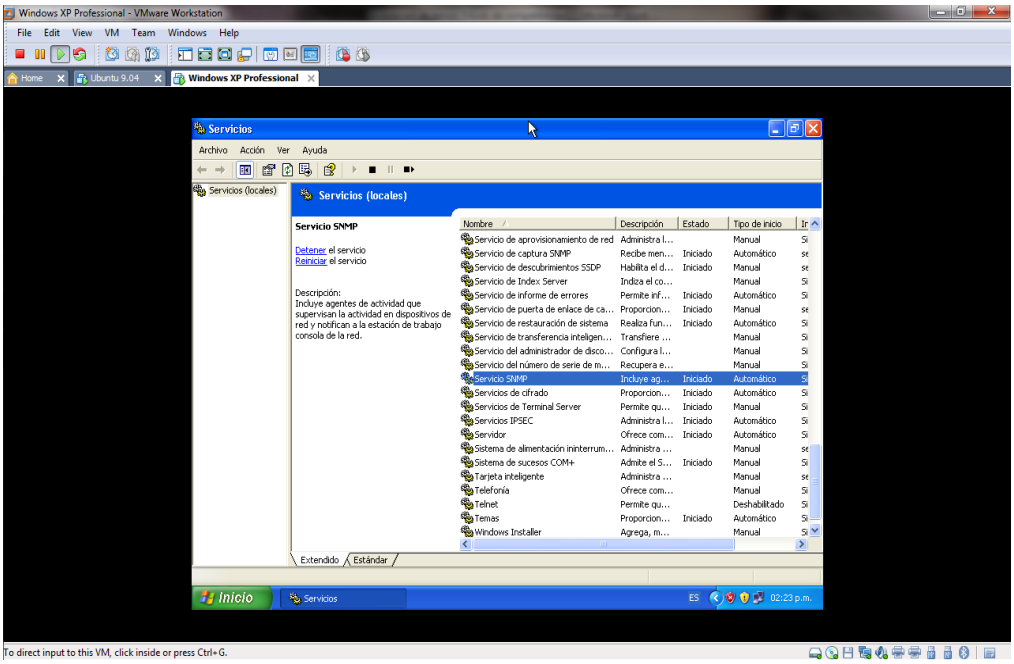


Fig 2.51 Selección del Servicio SNMP

Al abrir la ventana, se selecciona la pestaña **CAPTURAS** y se coloca la comunidad con la que se trabajará en los equipos que verán los datos, en este caso la comunidad es "*public*".

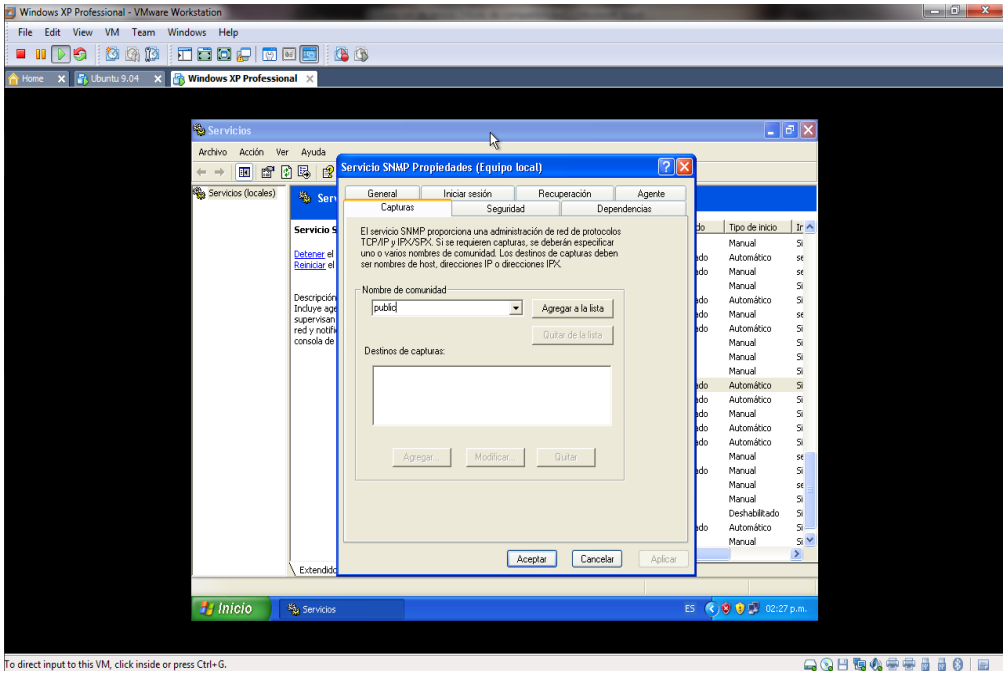


Fig 2.52 Se coloca la comunidad "Public"

En la pestaña *SEGURIDAD* se habilitan permisos que tendrán los agentes clientes que gestionan la red, se le darán permisos de lectura y escritura a la comunidad "*public*".

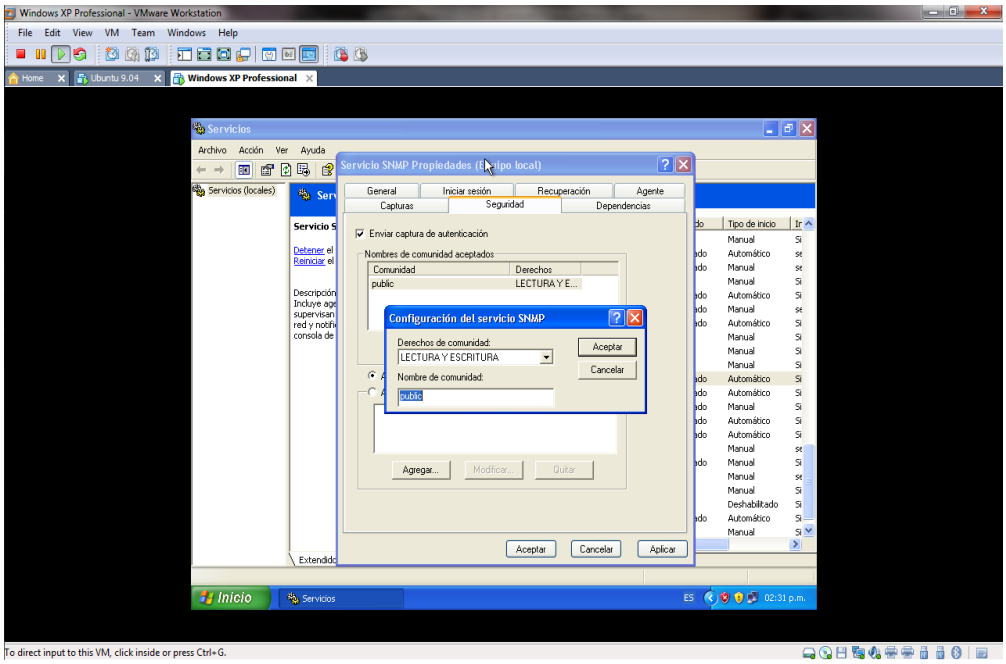


Fig 2.53 Permisos para la comunidad public

Posteriormente se habilita el inicio "*automático*" del servicio para no tener que iniciarlo cada que se prenda el equipo.

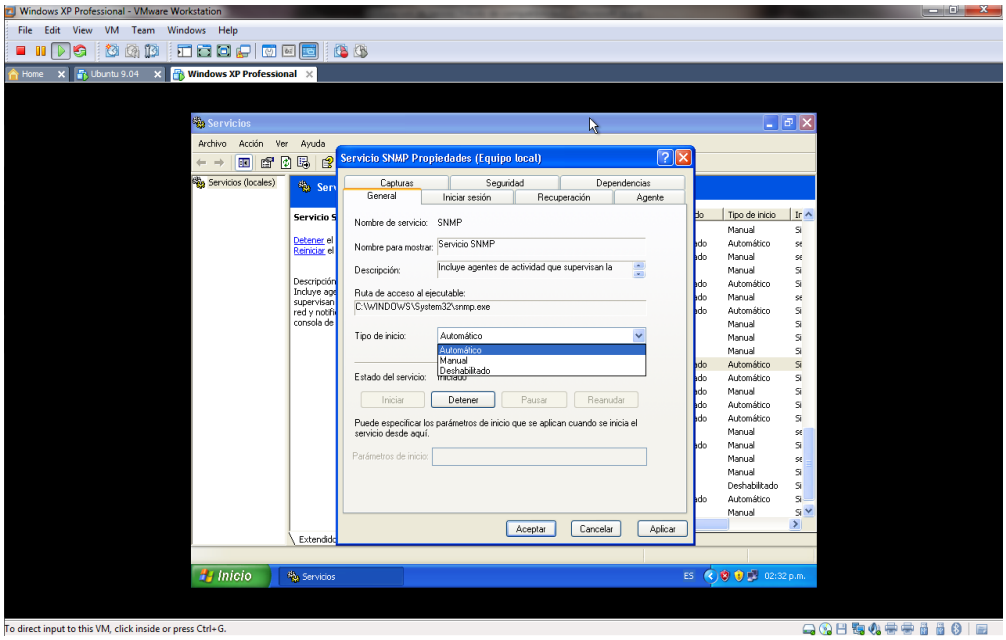


Fig 2.54 Inicio automático del servicio

Para finalizar la activación del servicio se reinicia desde la opción superior Izquierda, tomando los cambios realizados.

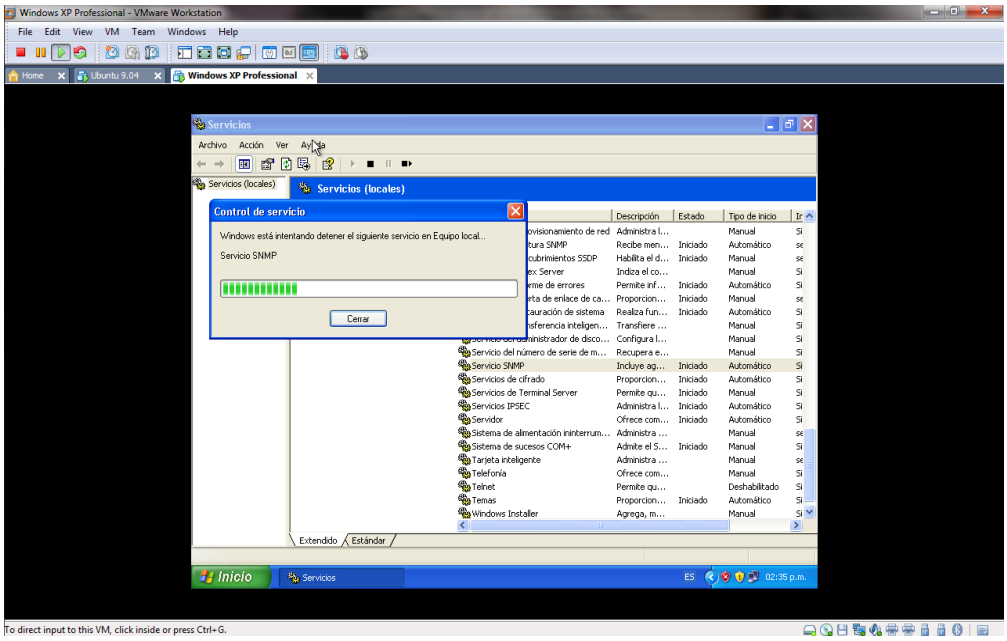


Fig 2.55 Reinicio de los servicios

Es necesario desactivar el firewall o abrir el puerto 161 para poder brindar los datos requeridos por el agente cliente utilizando SNMP.

Para cerciorarse que efectivamente el puerto de SNMP se encuentre abierto y el servicio se encuentre arriba, se utiliza el comando:

```
>netstat -an.
```

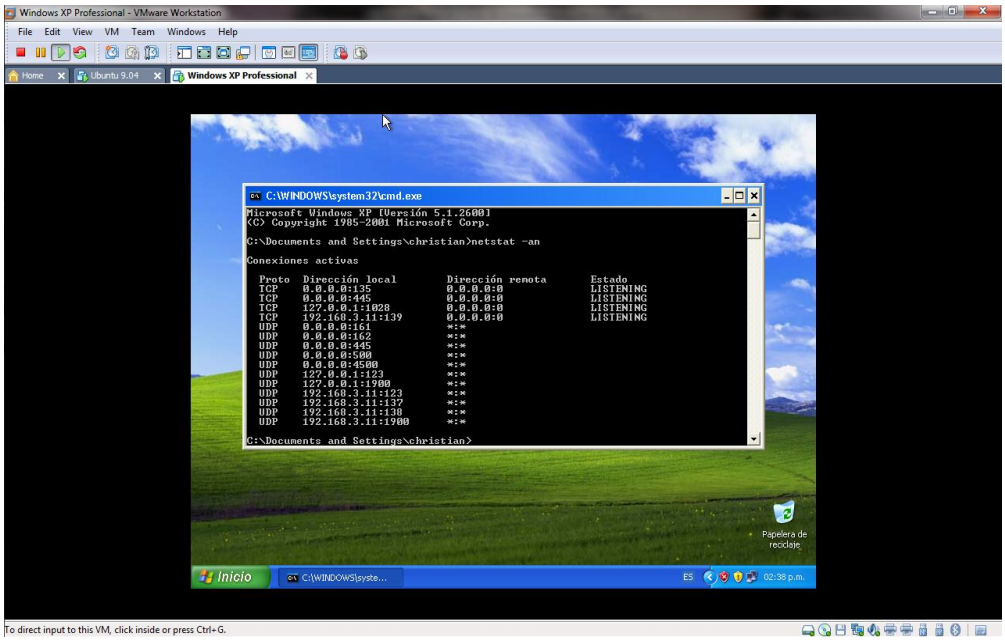


Fig 2.56 Comando netstat -an

Para poder observar las gráficas de rendimiento del SO Windows es necesario también la versión gratuita del software SNMP Informant que se puede obtener de la página:

http://www.snmp-informant.com

Para asegurarse que el software SNMP está funcionando correctamente, se aplica desde otro equipo en la red el comando:

```
#snmpwalk -v1 -cpublic 192.168.2.11 1.3.6.1.4.1.9600
```

Teniendo los agentes SNMP instalamos y configurados en Windows y Linux, se puede poner más atención en Zenoss y sus principales funciones, comenzando desde el menú de inicio y las diferentes interfaces que se muestran para su gestión.

2.2.3Agregar dispositivos a Zenoss por rango de IP´s

Existen 2 formas de agregar equipos a Zenoss:
1.- Por un rango de IP´s en el cual se abarcan varios equipos y
2.- Por equipo individual.

En esta parte se explicará cómo realizar el primer punto, el segundo se explicará posteriormente con un equipo Centos, en el cual cambia un poco su configuración en el agente SNMP, por lo cual se desea mostrar.
Para comenzar se sigue la siguiente ruta:

INFRASTRUCTURE>Add Devices>Add Multiple Devices…

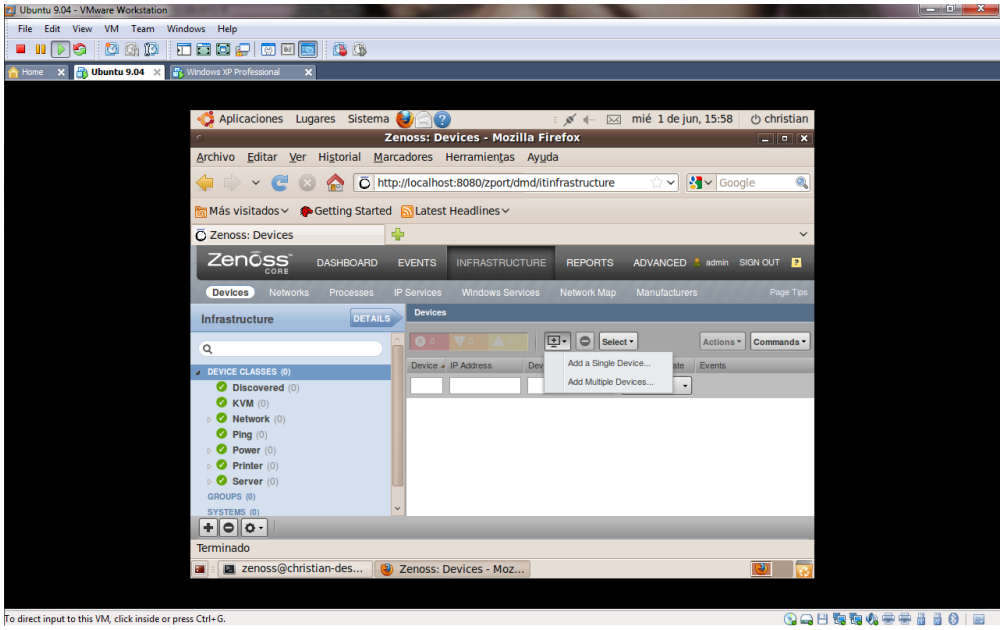


Fig 2.57 Agregado de multiples equipos para monitoreo

Ahí abrirá una ventana, en la cual se activa la opción "*Autodiscover devices*". En el recuadro blanco se colocará el rango de IP´s de nuestra red, ya sea especificándolo con la máscara de red o con el número del último octeto, como se muestra en las imágenes.

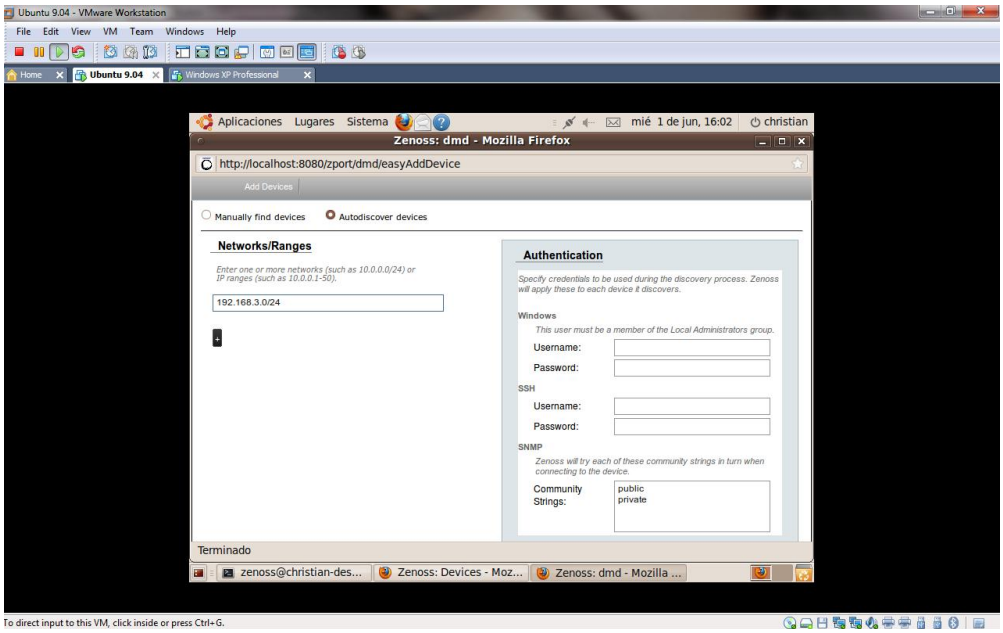


Fig 2.58 Forma uno de seleccionar un rango de IP´s

Un rango

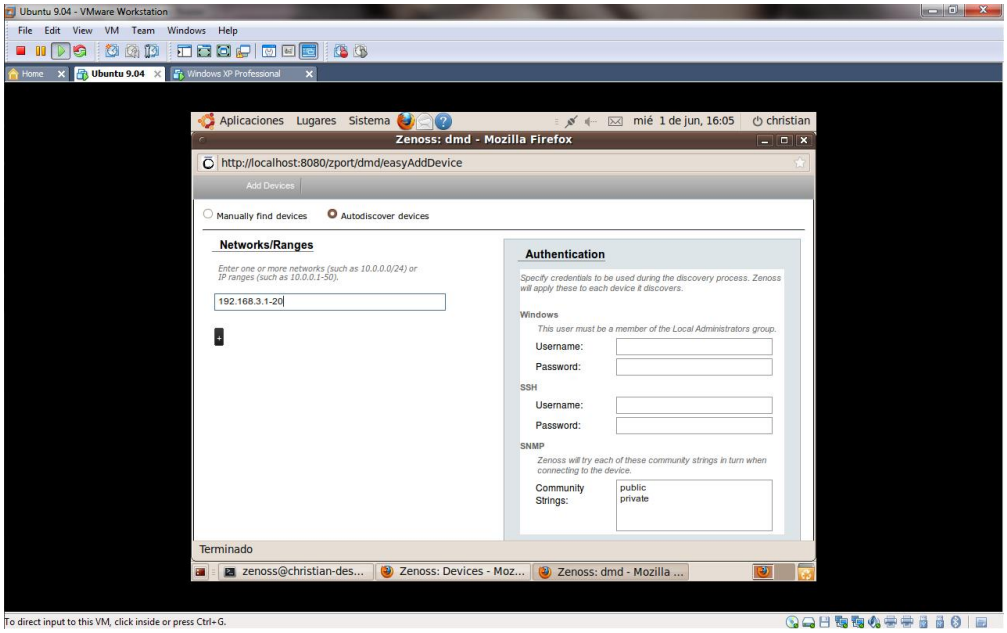


Fig 2.59 Forma dos de Seleccionar un rango limitado de IP´s

En el recuadro que se encuentra en la parte derecha, se coloca el nombre del usuario con el que se accederá a los datos y su contraseña, este debe ser un usuario con permisos de administrador en los equipos clientes.

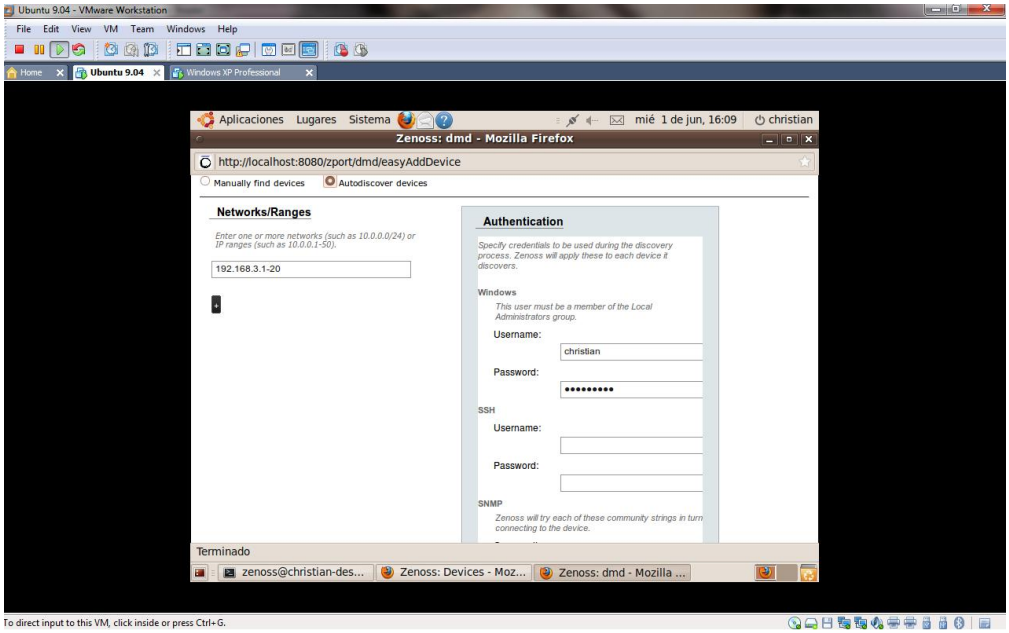


Fig 2.60 Agregado de usuario con permisos de administrador

Para terminar se le da click al boton *DISCOVER* para que comience a buscar los equipos.

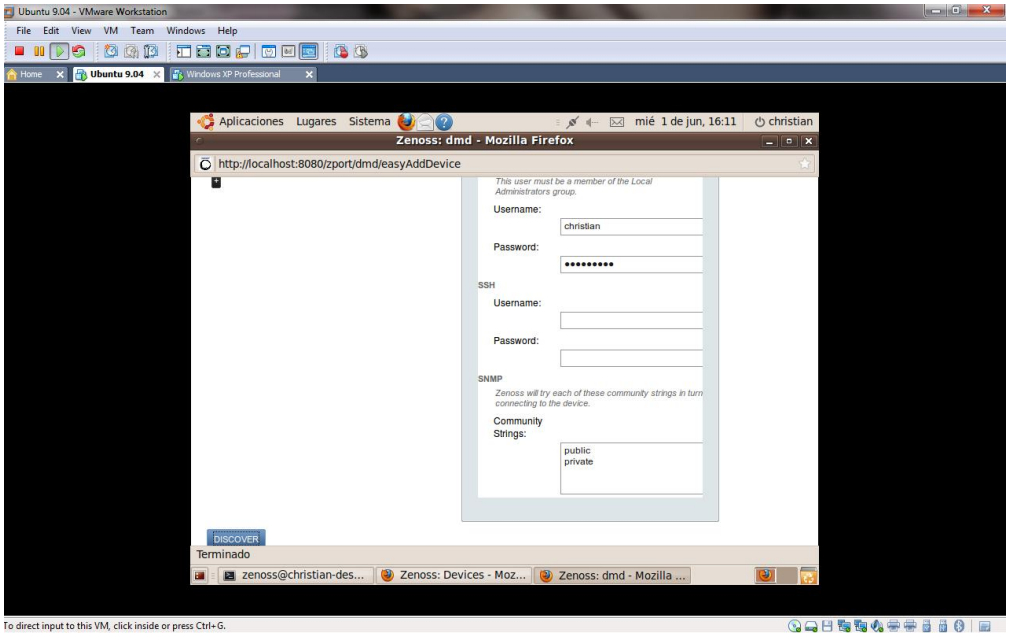


Fig 2.61 Localizacion del Boton DISCOVER

En esta imagen se puede observar un aviso en la parte superior, de que comenzó a descubrir nuevos equipos en este rango o red.

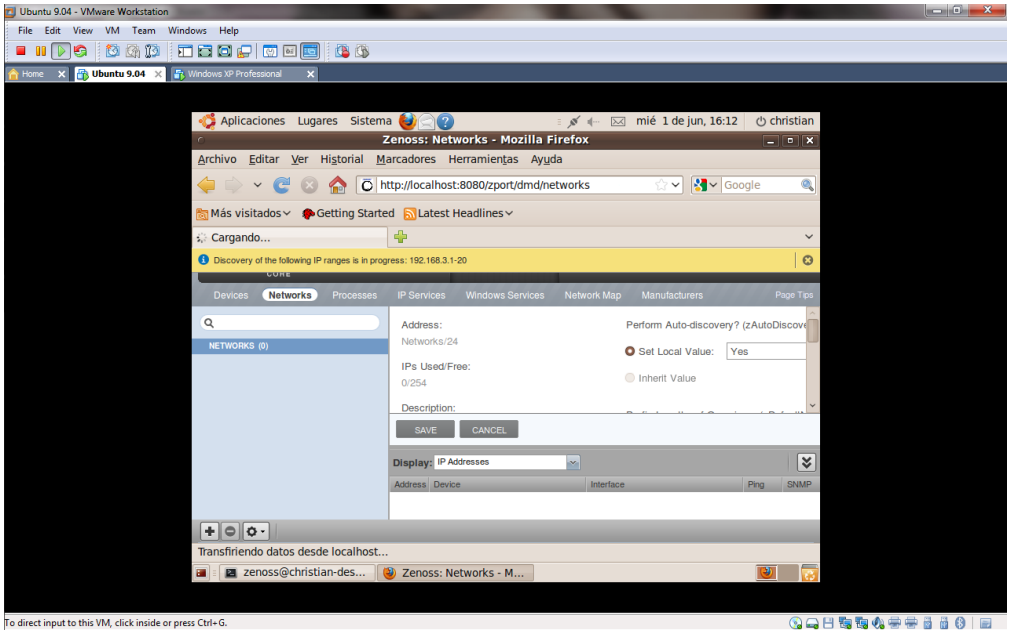


Fig 2.62 Descubrimiento de los equipos en el rango de IP´s

Y en esta imagen se puede apreciar los equipos descubiertos.

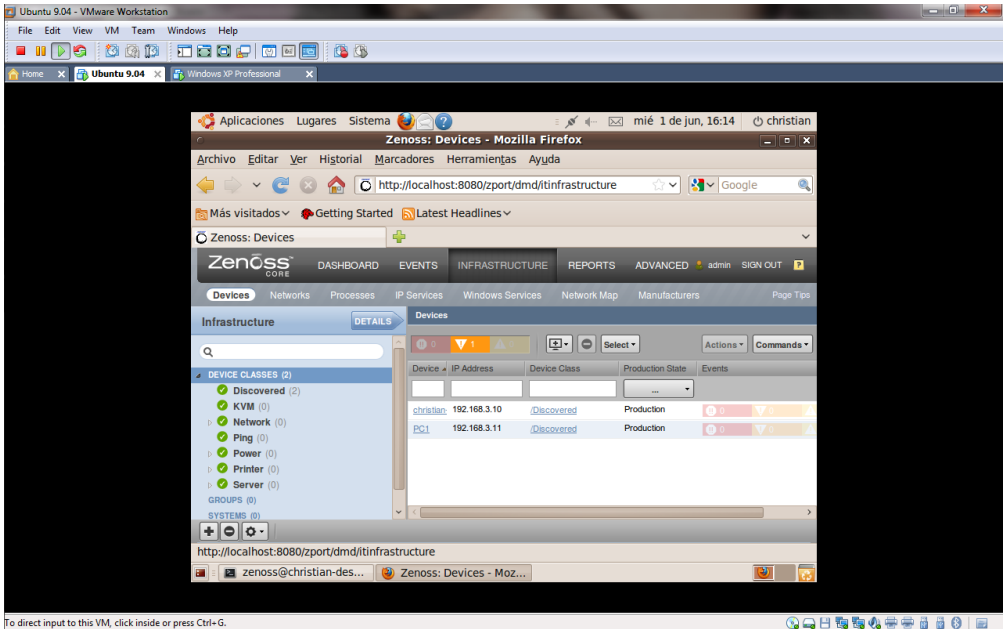


Fig 2.63 Equipos encontrados por Zenoss

Para que zenoss y el administrador tengan una mejor administración e identificación de los dispositivos, es necesario mover los dispositivos a la clase a la cual pertenecen, en este caso se distingue por el tipo de sistema operativo.

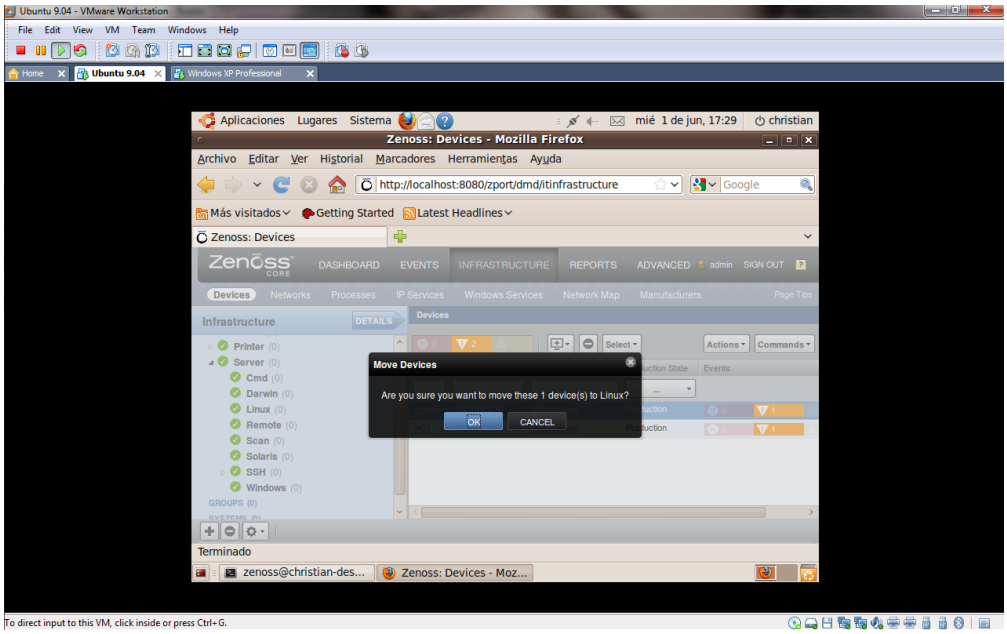


Fig 2.64 Equipo desplazado a la clase Linux

Se puede observar que ahora pertenecen los dispositivos encontrados, a la clasificación de equipos con SO Windows y Linux.

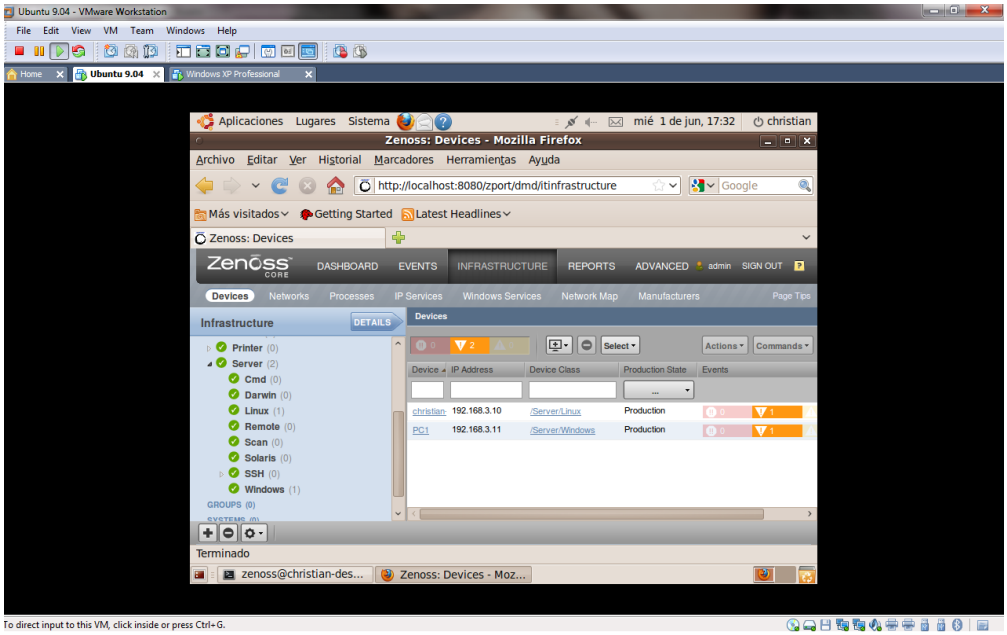


Fig 2.65 Equipos en una clasificación definida

2.2.4 Agregar por equipo, un equipo Centos

En éste se agregará una maquina virtual **Centos** a zenoss con la IP 192.168.3.3 primero hay que configurar SNMP para poder ser gestionada.
La Instalación de **Net-SNMP** en Centos es como usuario root y se realiza con el comando:

```
yum –y install net-snmp net-snmp-utils
```

Se instala junto con el paquete o archivo **/etc/snmp/snmpd.conf** el cual tiene muchos comentarios y opciones de muchos tipos que dependen de la configuración que se requiera. Se puede utilizar consultando el manual de dicho protocolo para ese SO, la configuración que se utiliza en esta prueba es la siguiente.

```
rocommunity public

com2sec local 127.0.0.1/32 public
com2sec pratica1 192.168.3.0/24 public

#grupos con acceso RW(Read/Write) version snmp 1, y 2c
group MyRWGroup v1 local
group MyRWGroup v2c local
group MyRWGroup usm local

# grupos con acceso modo RO(Read Only)
group MyROGroup v1 practica1
group MyROGroup v2c pratica1
group MyROGroup usm pratica1

#desplegar todo la info del arbol snmp
view all included .1 80

# Lista de control de acceso
access MyROGroup "" any noauth exact all none none
access MyRWGroup "" any noauth exact all all none

syslocation Linux Server on hostname #datos del host
syscontact Administrator jchristian_ram_gal@hotmail.com
```

Verificat bien en que archivo se coloca esta configuración, pues hay veces que se crean otros con el mismo nombre, pero con un signo más al final como por ejemplo: **snmpd.conf~** y puede llegar a confundir.

Teniendo esta configuración básica se inicia o reinicia el daemon **snmpd** con el comando:
`/etc/init.d/snmpd restart`

Se prosigue agregando el equipo con sistema Centos a zenoss.

Como se puede observar en Zenoss no se tiene el equipo con IP 192.168.3.33 que es la IP que tiene el equipo con Centos. Asi que se sigue la ruta: *INFRASTRUCTURE>Devices>Add Devices> Add Multiple Devices.*

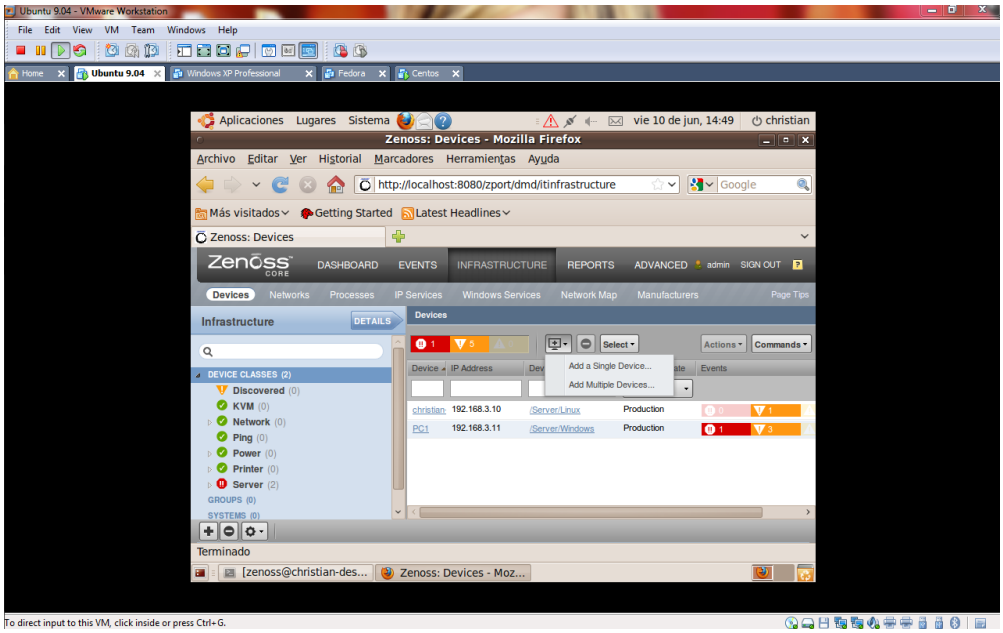


Fig 2.66 Agregado de un solo equipo a Zenoss

Se selecciona "*Manually find devices*" y en el recuadro, se coloca la IP del equipo que se requiere agregar y del lado derecho el tipo de dispositivo.

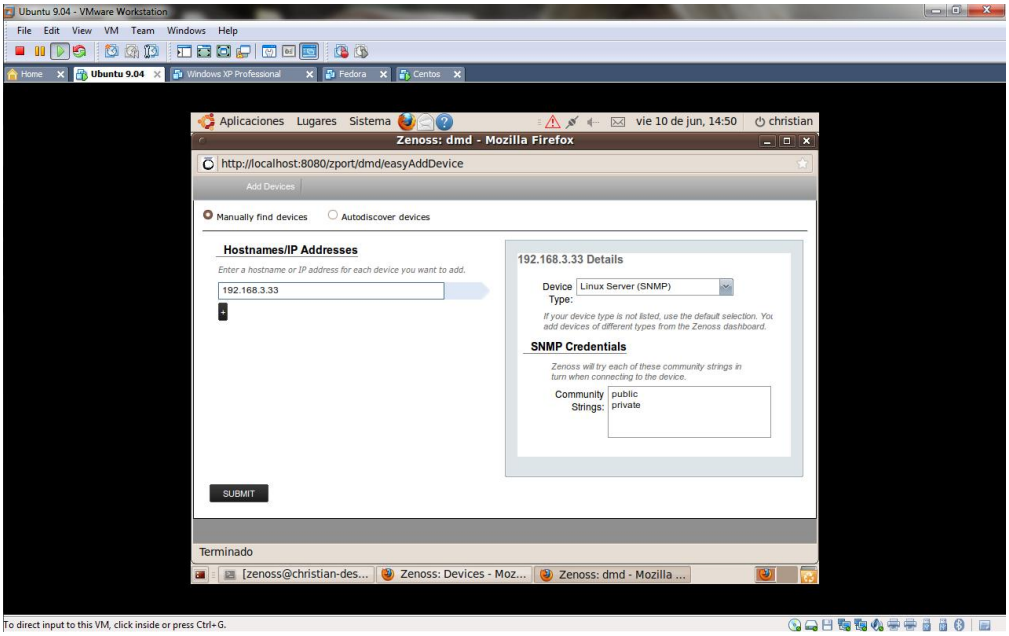


Fig 2.67 IP del equipo a agregar y tipo de dispositivo

Se espera un momento y observamos que se agregó.

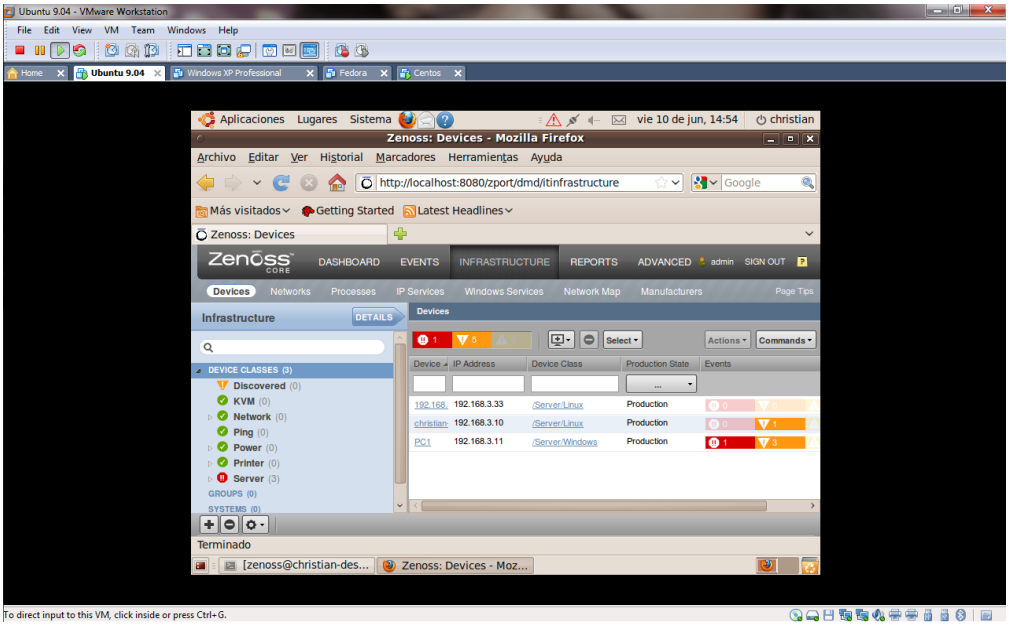


Fig 2.68 Equipo Centos agregado

Se prosigue dando doble click al dispositivo seleccionado y se configuran algunas características.

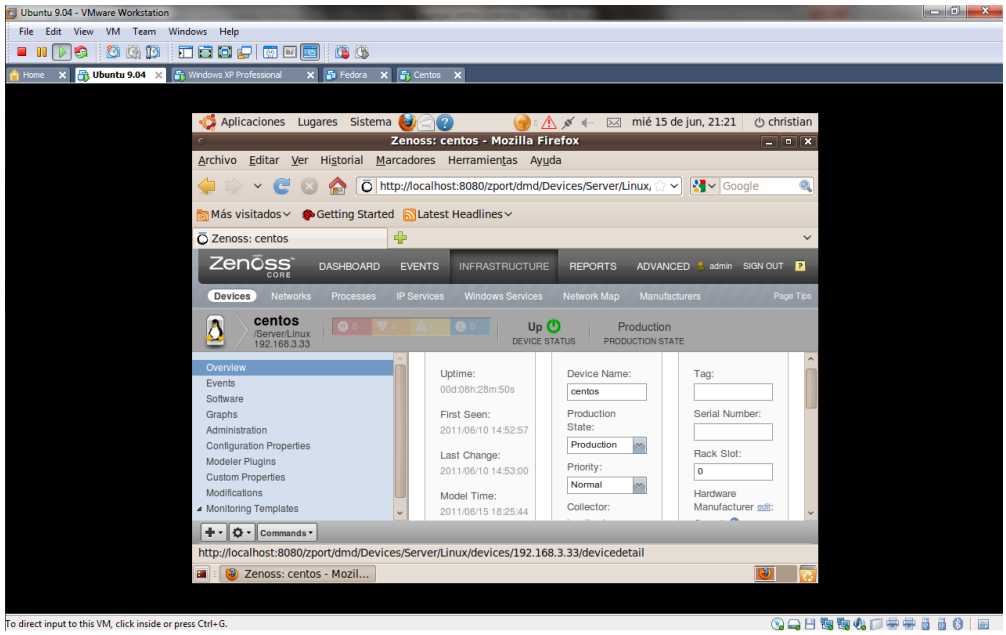


Fig 2.69 Vista general de configuración del equipo Centos

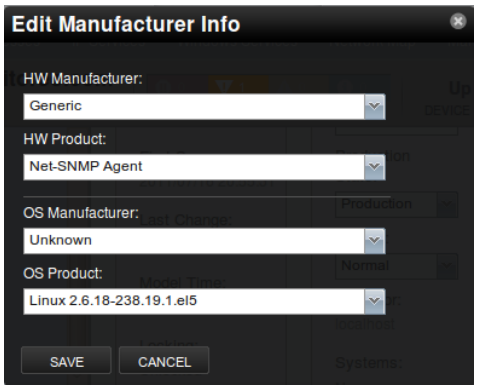


Fig 2.70 Información de la máquina Centos

Y en *"Configuration Properties"* se llenan los espacios de:

`zCommandPassword:` *`contraseña de root`*
`zCommandUsername:` *`root`*

Aquí se muestran algunas gráficas del rendimiento de la maquina virtual.

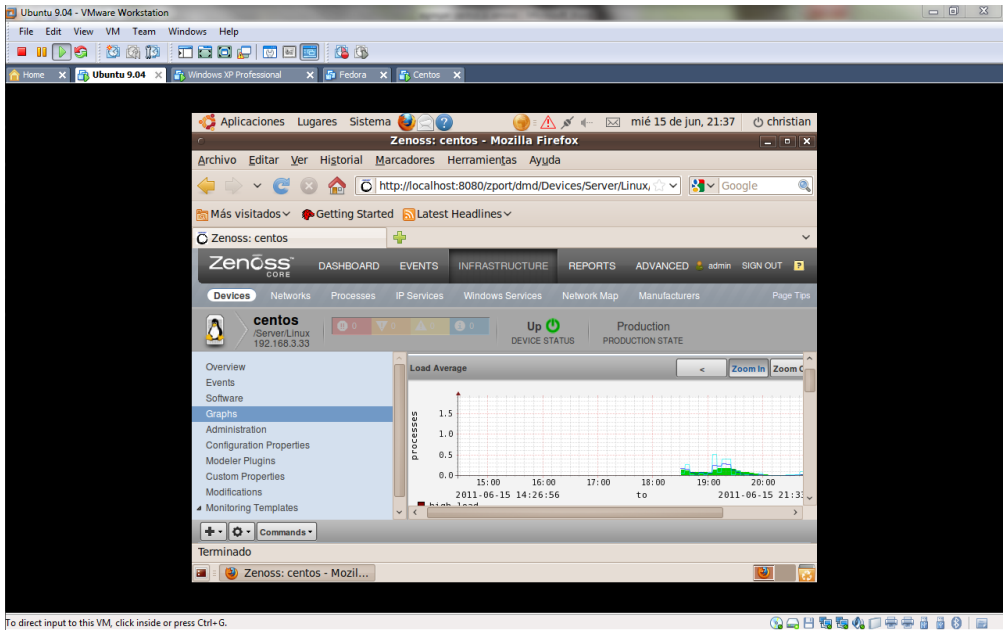


Fig 2.71 Gráfica de la carga promedio de la maquina virtual

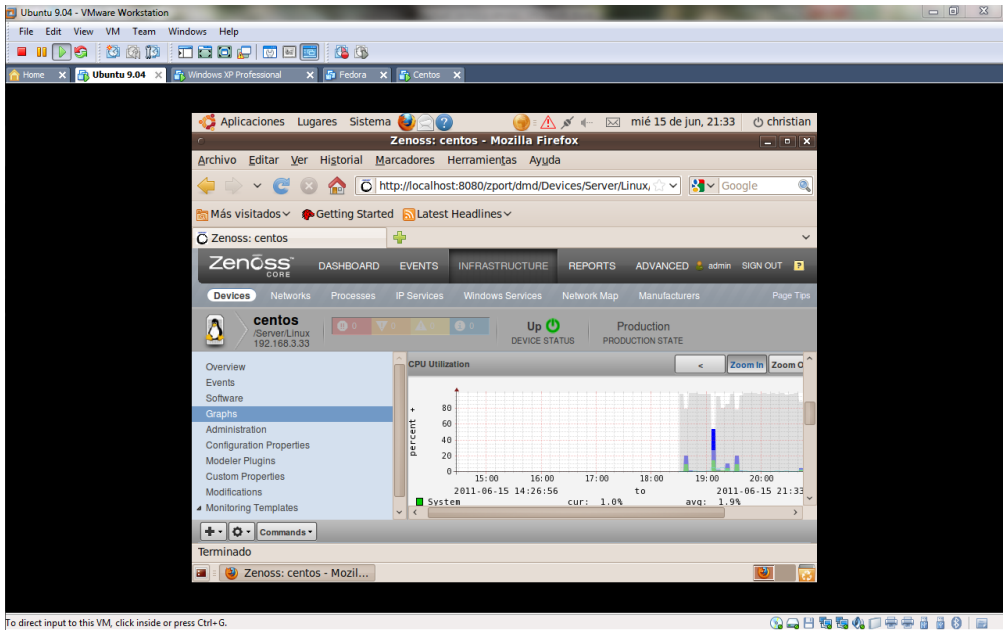


Fig 2.72 Gráfica del uso del procesador

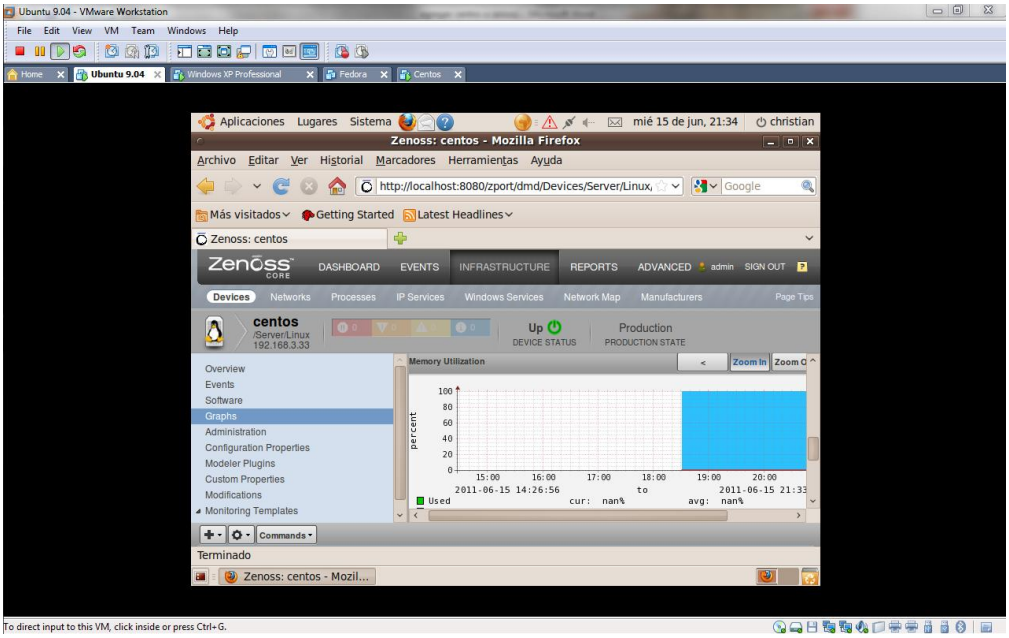


Fig 2.73 Gráfica de la memoria utilizada

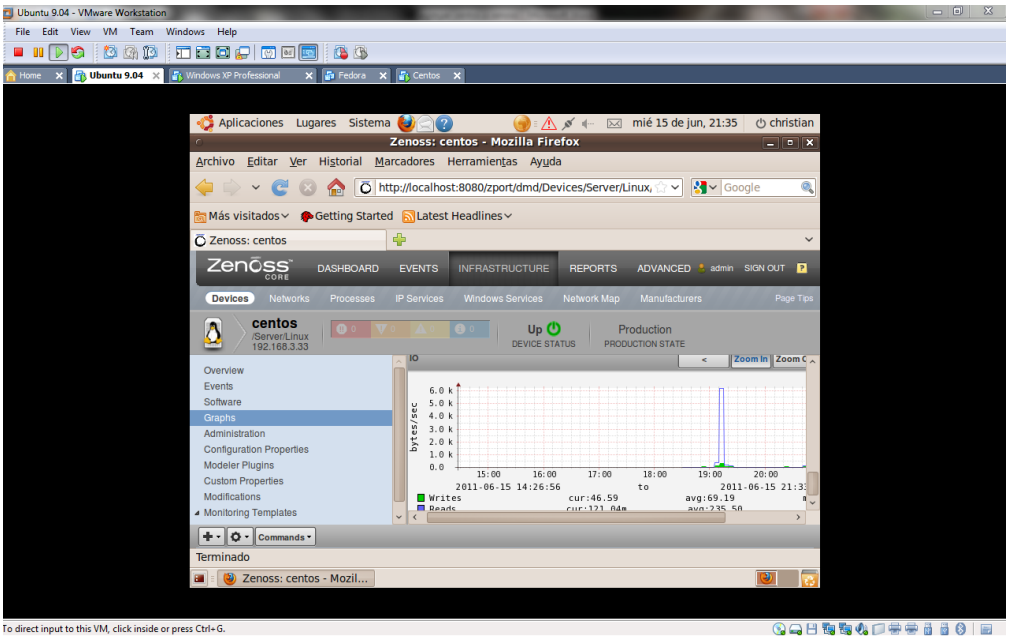


Fig 2.74 Grafica de lectura y escritura de datos en el equipo

Es necesario instalar *"flashplayer"* para algunas aplicaciones de zenoss esto se logra dirigiéndose a "*Centro de software*", se coloca en búsqueda "*extras"* y se instala el "*extras restringidos de Ubuntu"*

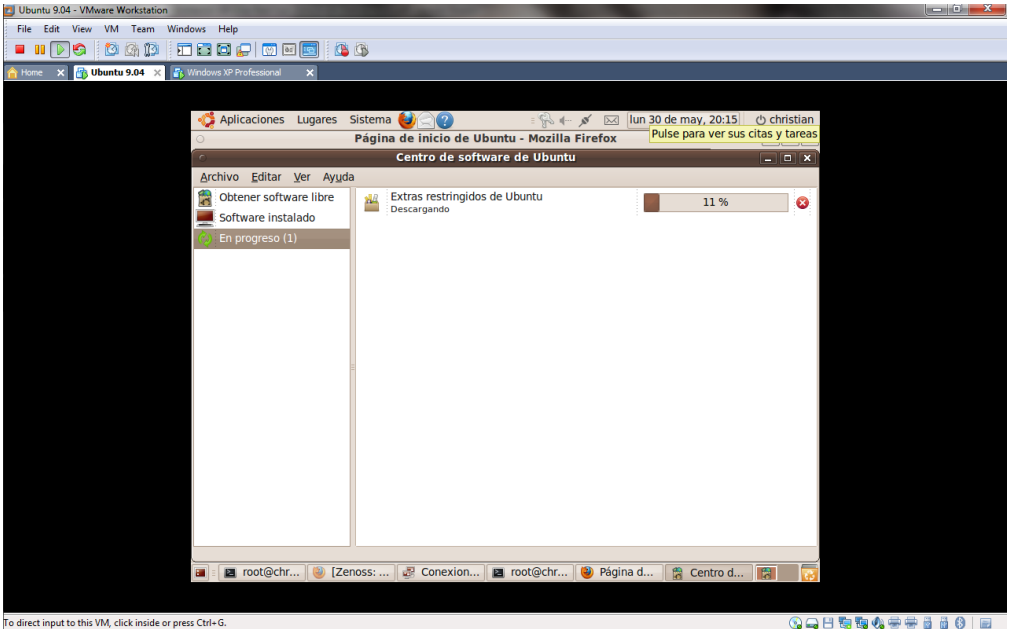


Fig 2.75 Instalación de flashplayer

Por ejemplo **Network Map**, es una de las herramientas de Zenoss que utiliza flashplayer.

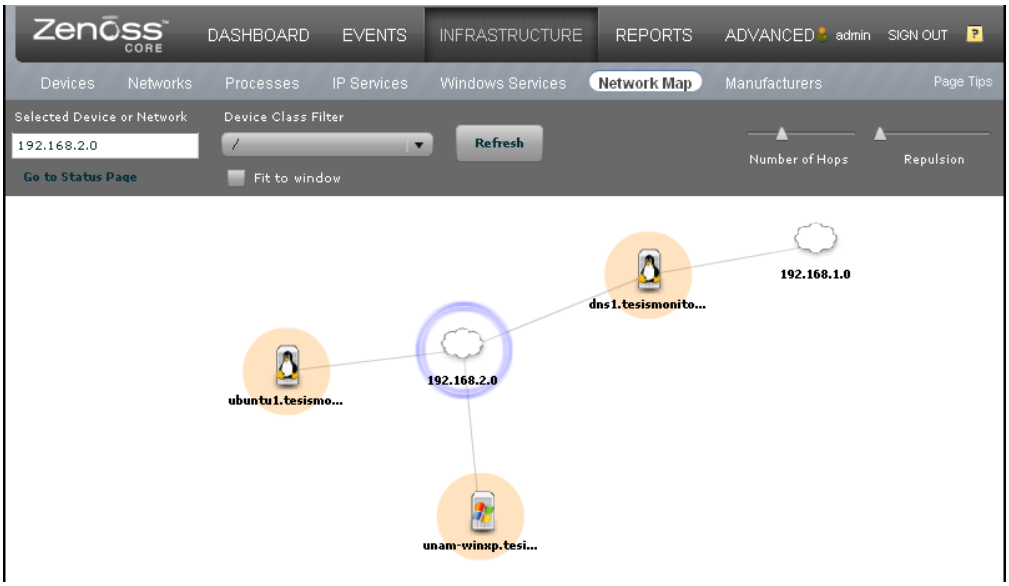


Fig 2.76 Infraestructura de la red virtual

2.3 GESTIÓN Y MONITOREO CON ZENOSS

Después de realizar la instalación completa de Zenoss en una red virtual, es necesario conocer las partes que conforman este software, así como su aplicación y la ventaja que se ofrece para una buena gestión y monitoreo de red, por lo cual en este tema se enfoca más a describir las partes más sobresalientes de Zenoss Core.

2.3.1DASHBOARD e integración con Google Maps

Al entrar a Zenoss el **DASHBOARD** es la primer ventana que aparece, está pagina provee un vistazo acerca del estatus de la Infraestructura IT.

La pestaña de DASHBOARD puede mostrar:

- Recursos de sistemas de información y páginas Web.
- El nivel de error de Eventos en los dispositivos.
- Vista geográfica general de la red.
- "Troubled" o conflictos en dispositivos.[46,PAG 101]

Cuando la red es demasiado grande y abarca un área geográfica, el sistema tiene la opción de localizar los equipos monitoreados utilizando Google Maps. Esta opción aparece en la primera vista de la ventana cuya pestaña se llama "DASHBOARD", cuando está configurada esta opción la localización seleccionada aparecerá en el mapa como un punto. El color del punto representa el nivel de importancia de algún evento o dispositivo en aquella localización. Las conexiones de red que abarcan grandes distancias, también son

representadas en el mapa por líneas con un color característico, dependiendo del estatus de la conexión.

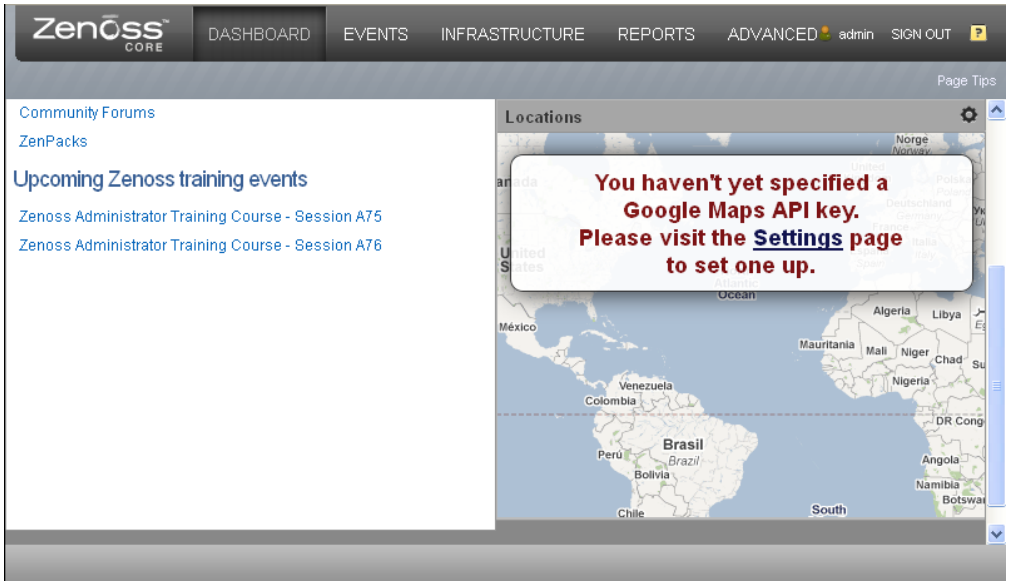


Fig 2.77 Interfaz web llamada DASHBOARD

Para realizar esta configuración se siguen los pasos indicados que aparecen en el recuadro sobre el mapa, como se ve en la imagen. Le damos click a "Settings" que redirecciona a las configuraciones del administrador de Zenoss, donde pide una clave con la que google posteará la API o interfaz de aplicaciones, para esto se abre el cuadro Google Maps API Key dándole click en HELP, que se encuentra al lado del campo donde se pide la clave.

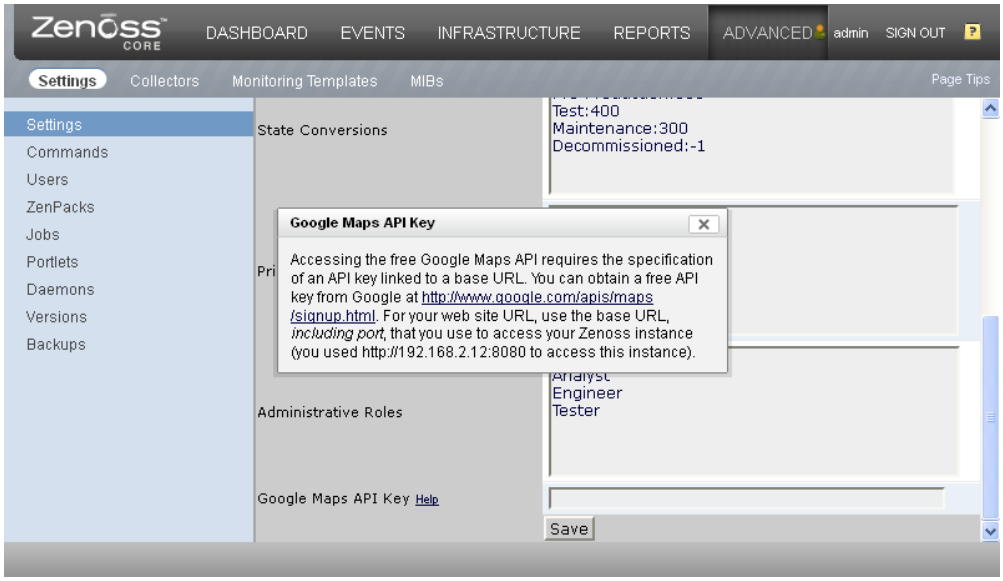


Fig 2.78 Ventana de Google Maps API Key

Se da click en la liga que aparece en la ventana, para obtener una clave de la API, y posteriormente se abre la página de obtención del mapa. Después de leer los requerimientos se pedirá la IP y el puerto de comunicación el cual es recomendable especificar desde ese

momento, en este caso es 8080, esto para prevenir que se ocupe el puerto por omisión de otro posible servidor web en producción que no recordemos.

La IP que Google solicita no es una IP privada, sino una IP pública que el ISP entrega al ofrecer el servicio de Internet.

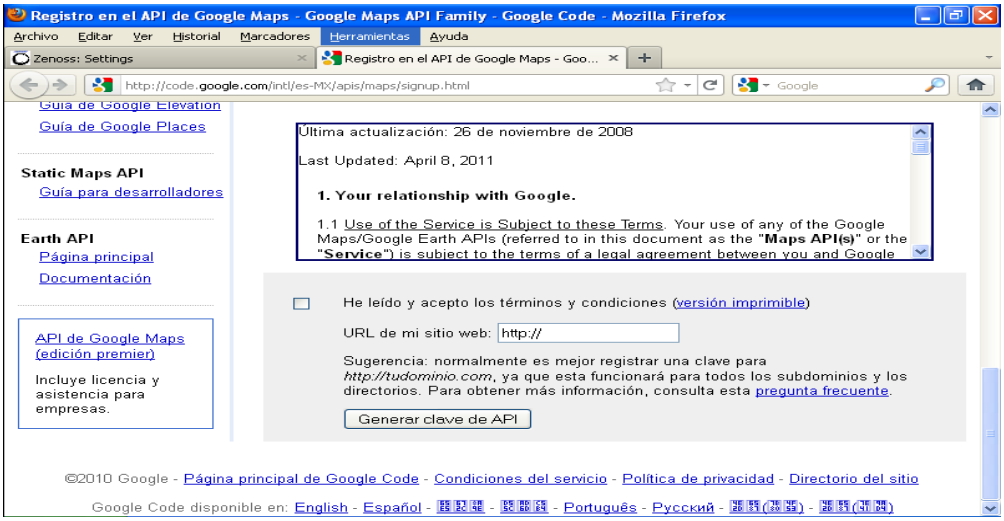


Fig 2.79 Generación de la clave de API

Para que se asigne el API es necesario contar con una cuenta de correo en google (gmail). En esta imagen podemos observar la clave asignada

Fig 2.80 Clave de API obtenida

Dicha clave se coloca en el campo correspondiente (Google Maps API Key) y se oprime **save** para guardar los cambios.

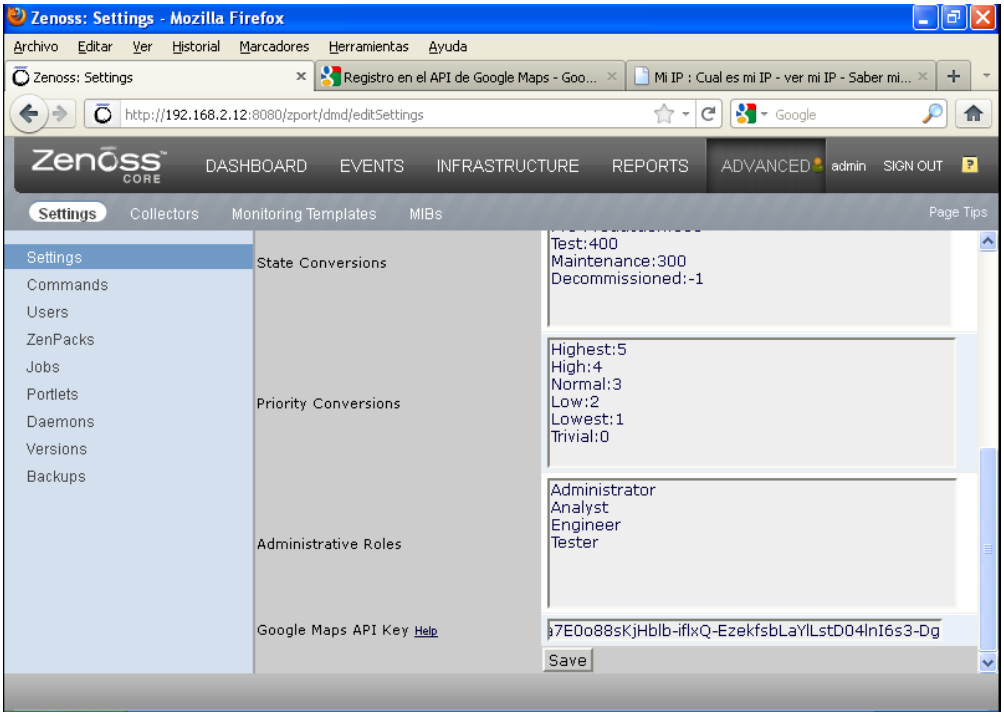


Fig 2.81 Guardado de la clave de API

Posteriormente, se puede observar dicho mapa en la pestaña **DASHBOARD** y configurarlo para la identificación y localizaciones de la red.

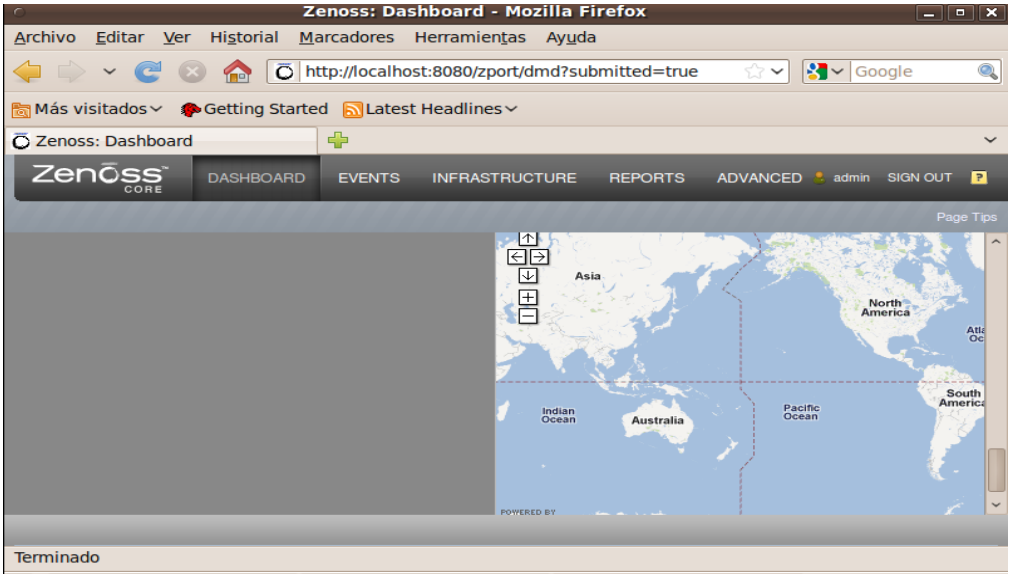


Fig 2.82 Mapa listo para configurarlo con una red WAN

2.3.2 INFRAESTRUCTURE

Esta pestaña muestra una lista de todos los dispositivos agregados en el sistema, también se puede buscar y ejecutar tareas de administración que abarque un rango o todos los dispositivos mostrados.

Para ver la lista de dispositivos, se debe seleccionar la pestaña **INFRASTRUCTURE** de la barra de navegación.

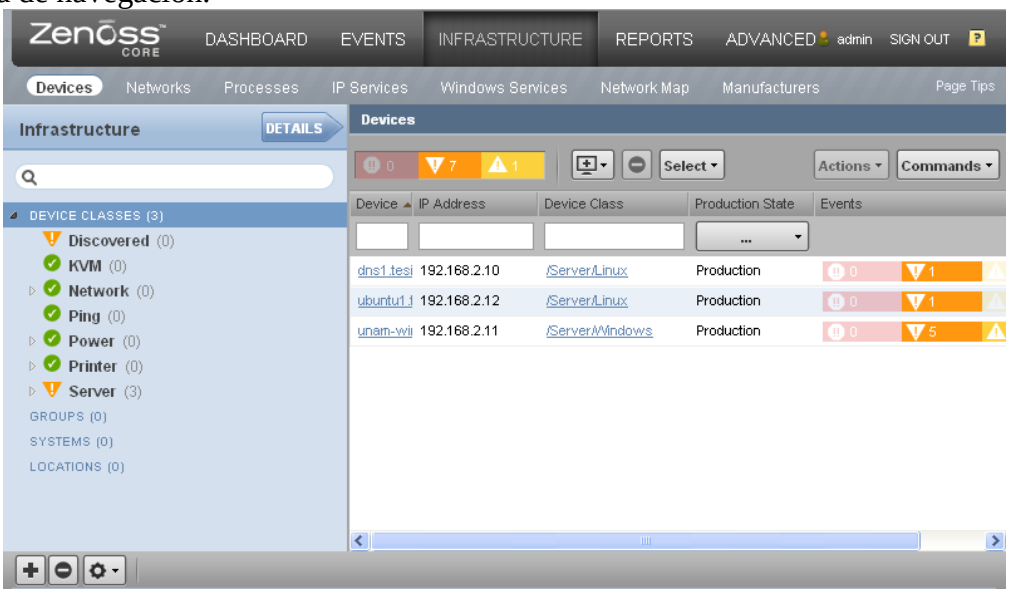


Fig 2.83 Ventana de la pestaña INFRASTRUCTURE

Esta lista se organiza en forma de árbol, con las siguientes divisiones o clasificaciones:

-DEVICE CLASSES
-GROUPS
-SYSTEMS
-LOCATIONS

Haciendo un click en alguna de las clasificaciones anteriores, se pueden observar los dispositivos que la componen o las subclases de esa clase.

En Zenoss se pueden ejecutar tareas de administración en más de un dispositivo a la vez;

Por ejemplo se puede:

-Mover dispositivos a diferentes clases.
-Asignar dispositivos a grupos, sistemas y localizaciones.
- Remover dispositivos
- Ejecutar acciones como; asignar prioridad y estados de producción.
-Asignar monitoreo para la colección de ciertos dispositivos seleccionados.
-bloqueos de dispositivos.
[46, pag 36]

2.3.3 Trabajando con dispositivos

Para ver los detalles específicos de un solo dispositivo, se da click en el nombre de dicho dispositivo que se encuentra en la lista.

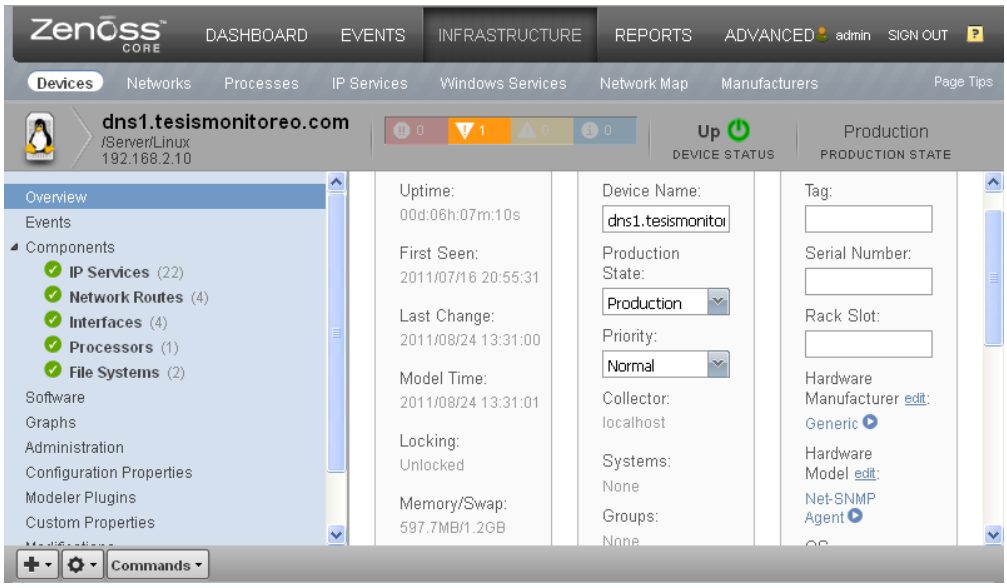


Fig 2.84 Vista de la configuración del equipo monitoreado

El estado de los eventos se puede observar en la parte superior de la página en donde se muestran 4 colores (rojo-critico, naranja-error, amarillo-advertencia, azul-informe, gris-depurar, green-limpio) además de otra información como:

- Nombre del dispositivo
- La IP usada para comunicarse con el dispositivo
- El Status del dispositivo (muestra si esta encendido o apagado)
- El estado de producción (Pre-producción,Producción, Test, Maintenance, o Decommissioned)

Al abrir la página, en la pestaña **Overview** se puede ver la información del dispositivo, aquí se puede editar su información rellenando los campos blancos de texto o editando los links.

[6]Del lado izquierdo del panel, la página permite acceder a otras vistas de administración, tales como:

- Event
- Components
- Software
- Graphs
- Administration
- Configuration Properties
- Modeler Plugins
- Custom
- Modifications
- Monitoring Templates

[46, pag 37,38]

2.3.3.1Events

En esta sección se muestra información detallada acerca de eventos del dispositivo seleccionado, para poder observarlos y administrarlos se oprime la pestaña **Events**. En esta sección se puede:

- Separar la información de los eventos por un rango de categorías.
- Clasificar y reconocer eventos.
- Filtrar eventos conforme a su severidad, estado, o por categorías.

2.3.3.2Components

La pestaña **Components** provee información acerca de los diferentes tipos de componentes de dispositivos, incluyendo.

- IPService
- WinService
- IpRouteEntry
- IpInterface
- CPU
- FileSystem
- Entre otros dependiendo del dispositivo que se esté gestionando y del sistema operativo que tenga.

Para tener acceso a la información de los componentes, se debe seleccionar el Componente en la parte izquierda del panel y también seleccionar el tipo de componente.

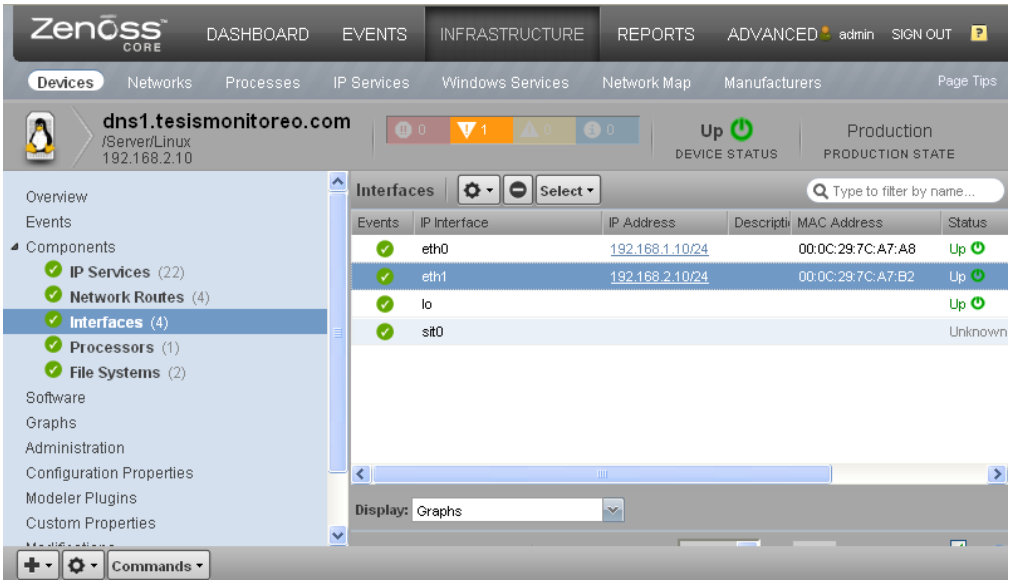


Fig 2.85 Interfaces con las que cuenta el equipo virtual

El status de cada tipo de componente del dispositivo, se muestra con el color del indicador (verde), este es determinado por el status del monitoreo general de componentes del mismo tipo. Por ejemplo, si el status del IP Services es verde, entonces todos los

IPServices monitoreados en el dispositivo están funcionando normalmente. Si hay un evento, relacionado a un componente IP Services, entonces el color del evento de mayor gravedad o más importante, asociado con ese componente es mostrado en el indicador, también muestra ciertas características en cada uno de los componentes como las IP, direcciones físicas MAC, velocidad y numero de procesadores, capacidades de los dispositivos de almacenamiento entre otros.

Si hay un evento sin relación a un componente conocido, entonces el sistema lo coloca en otros tipos de componentes. En esta lista se puede:

- Bloquear componentes
- Encender o apagar componentes monitoreados
- Borrar componentes.

2.3.3.3 Software

La pestaña software, enlista el software instalado en el dispositivo o equipo. Los detalles que se dan en esta pestaña dependen del método usado o por el modelo del dispositivo y clase.

Esta lista de software nos muestra un inventario muy completo de los programas instalados en cada uno de los equipos que conforman nuestra red o infraestrutura IT. Para tener acceso a la información del software, se selecciona la pestaña software en el árbol.

2.3.3.4 Graphs

La pestaña **Graphs,** muestra gráficamente el rendimiento del dispositivo o de sus componentes. Para tener acceso, solo se selecciona la pestaña **Graphs** del lado izquierdo del panel.

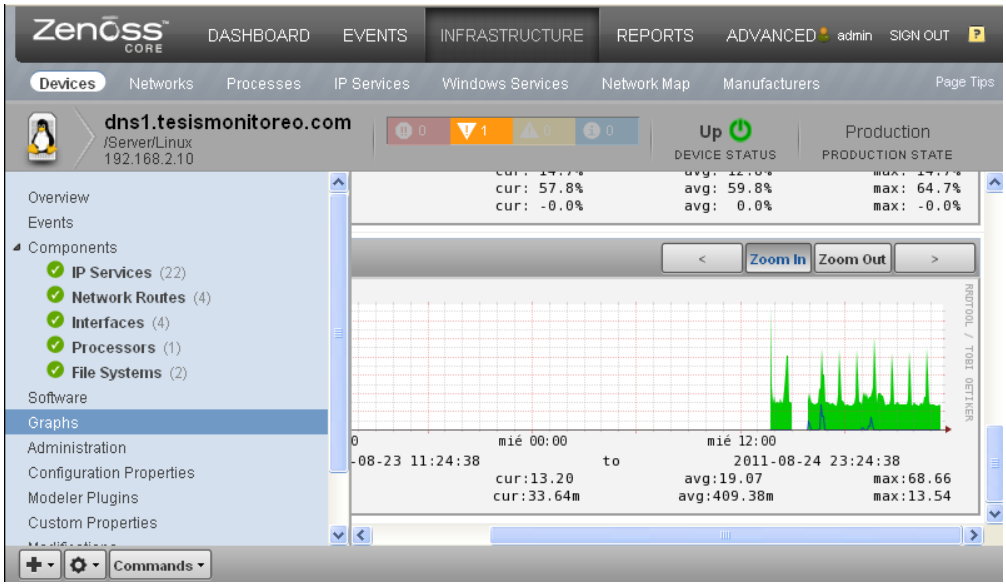


Fig 2.86 Imagen de la pestaña Graphs

Las flechas y botones que se encuentran sobre las graficas permiten maximizar o minimizar las vistas de las gráficas, deslizándose y controlando el zoom para verlas con más detalle.

Además también podemos personalizar el funcionamiento en las opciones de las graficas como:

- Range: Seleccionar la duración de tiempo mostrado en la grafica.
  -Hourly- pasando 36 horas
  -Daily – Pasando 10 Días
  -Weekly- Pasando 6 semanas
  -Monthly- Pasando 15 meses
  -Yearly- Pasando 2 años
- Reset: Si se le da click a esta opción se regresa a la vista inicial de las graficas.
- Links graphs: Por default todas las graficas se mueven juntas. Por ejemplo, si se hace click a la flecha hacia atrás entonces todas las graficas se moverán hacia atrás. Quita la opción Links graphs para controlar cada grafica individualmente.
- Stop/Start: palanca para desactivar o activar automáticamente la actualización de las graficas. Opcionalmente, modificamos el refrescar los valores (por default, 300 segundos), y también hacer click en Stop/Start para comenzar a refrescar las graficas en un nuevo intervalo.

[6, pag 40]

2.3.3.5Administration

Esta pestaña es utilizada para:

-Crear comandos personalizados para los usuarios y ejecutar los comandos.
-Administrar las ventanas de mantenimiento.
-Determinar quienes administran ciertos dispositivos, y sus roles.

Para el acceso a las opciones de administración, seleccionar **Administration** en el panel izquierdo.

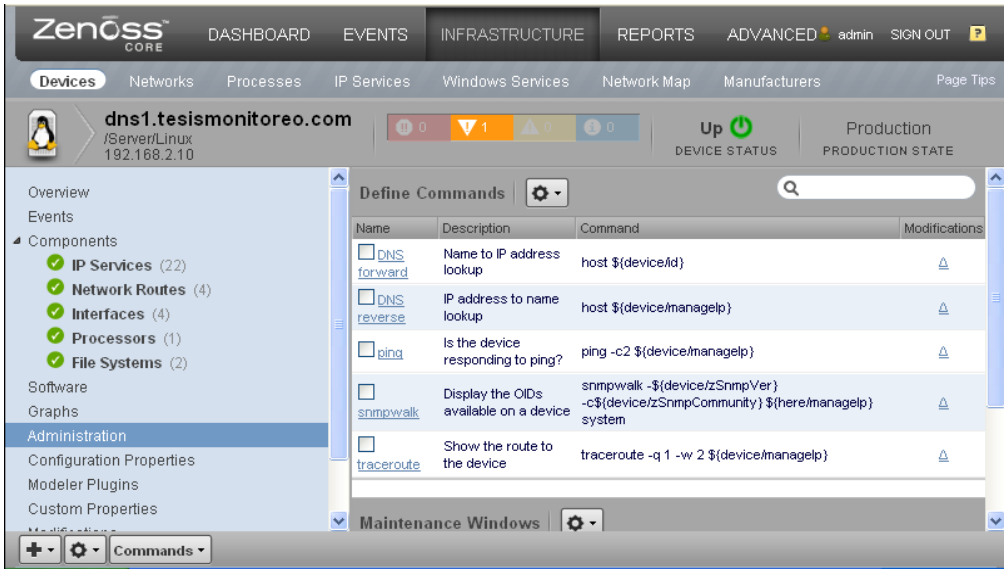


Fig 2.87 Se define los comandos que utilizan en Zenoss

2.3.3.6 Configuration Properties

En la pestaña **Configuration Properties**, se pueden configurar y agregar ciertas propiedades para un dispositivo y borrar otras.
La configuración de las propiedades y valores pueden ser agregados a un ZenPacks que sea creado o diseñado por el administrador, permitiendo personalizar esta pestaña al agregar dicho ZenPacks.

Para ver y editar las propiedades de configuración se da click en *INFRAESTRUCTURE***,** después en una de las divisiones del árbol que aparece del lado izquierdo, click en Details, y se selecciona *Configuration Properties***,** esto a nivel raíz pues estas modificaciones aplicarían para todos los equipos de esta clase.

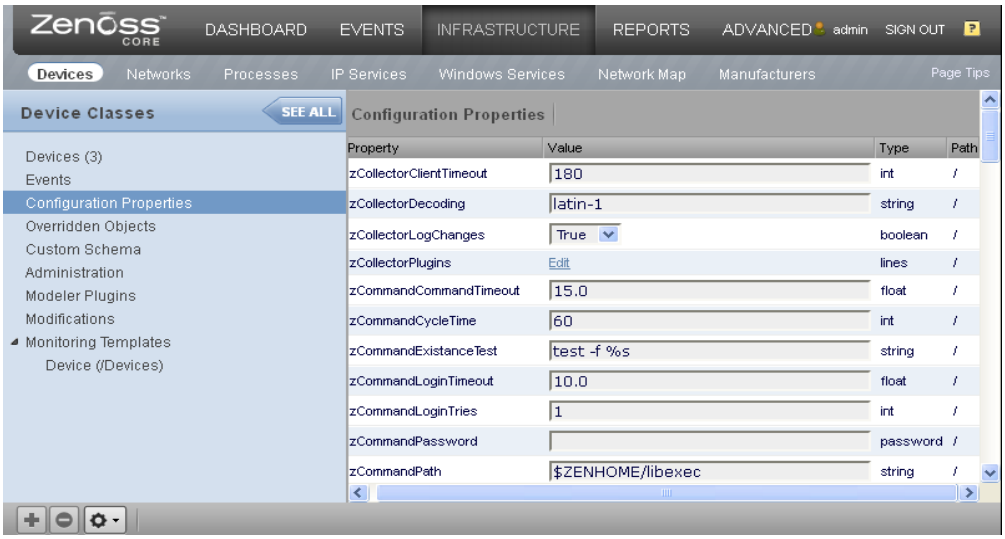


Fig 2.88 Configuration Properties de nivel raiz

Como las *Configuration Properties* a nivel raíz pasan por herencia y se estructura en forma jerárquica, si se necesita configurar un solo equipo con propiedades diferentes a las de los demás, se edita la configuración de dispositivo a nivel individual, esto seleccionando el dispositivo especifico de la lista y después se selecciona la pestaña *Configuration Properties* del panel izquierdo.

En éste caso se anularían los valores que se le había dado a nivel raíz, aplicando los del nivel individual. Todo esto debido al nivel de jerarquía, pues las propiedades definidas a nivel raíz aplican a todos los objetos que se encuentren esa clase o división, así como también se pueden aplicar por equipo, para anular las *Configuration Properties* por default que se aplican a todos.

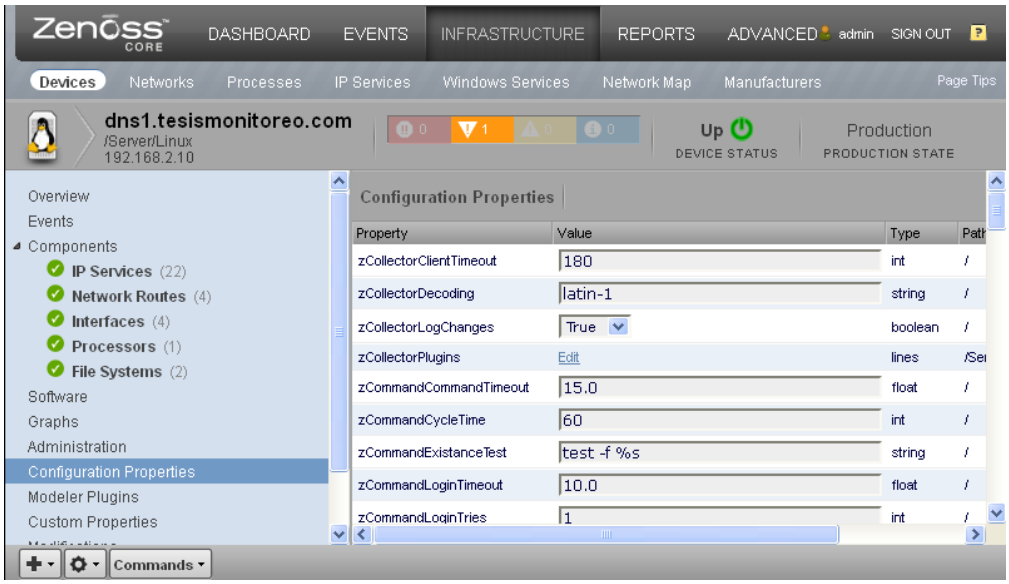


Fig 2.89 Opción "Configuration Properties" en el equipo virtual

2.3.3.7 Modeler Plugins

La pestaña *Modeler Plugins* es utilizada para administrar los plugins que están corriendo en un dispositivo. Para tener acceso a los plugins se debe seleccionar *Modeler Plugins* en el panel izquierdo.

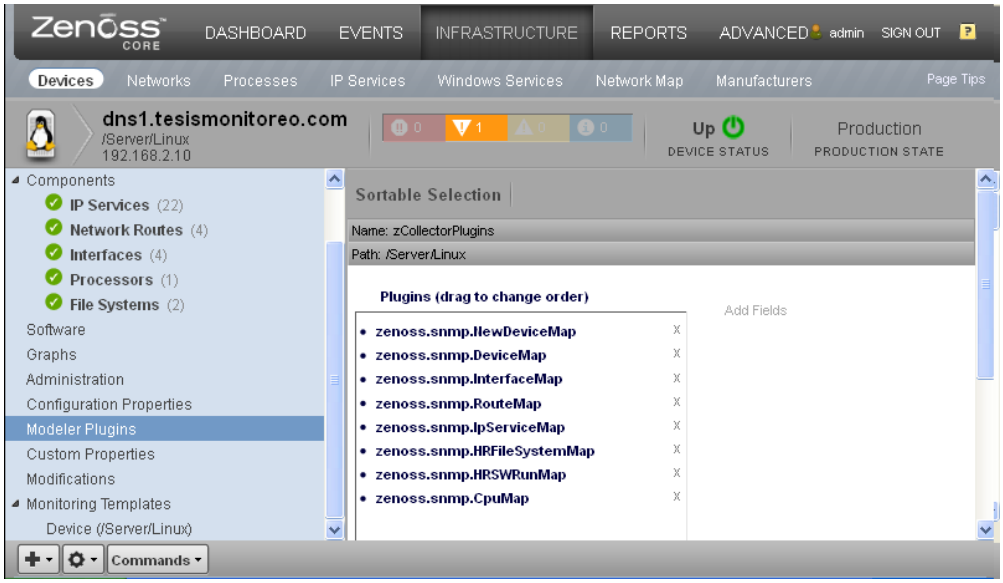


Fig 2.90 Ventana de la opción Modeler Plugins

2.3.3.8 Custom Properties

La pestaña **Custom Properties** es utilizada para editar los valores de las propiedades del cliente, aplicadas a un dispositivo.
No se puede definir las propiedades del cliente en un dispositivo individual.

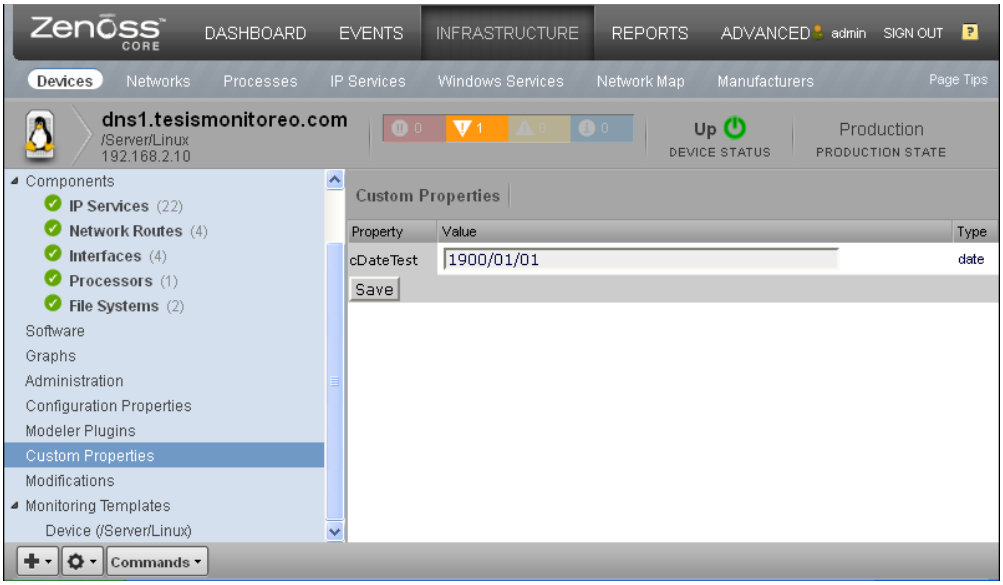


Fig 2.91 Ventana de la opción Custom Properties

2.3.3.9 Modifications

La pestaña muestra una lista de cambios hechos en un dispositivo, dando información de cuando, quien y la hora a la que se realizaron dichas modificaciones.

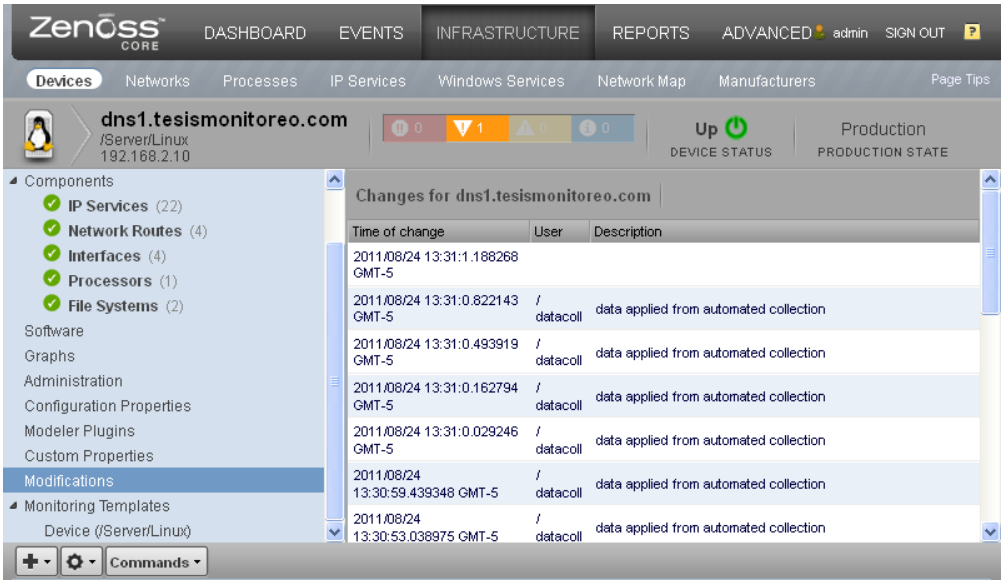


Fig 2.92 Ventana de la opción Modifications

2.3.3.10 Monitoring Templates

En la pestaña de Monitoring Templates se determina la forma en que el sistema recolecta los datos, de dispositivos y componentes. Para lograr tener acceso a las plantillas de monitoreo, se expande el Monitoring Templates en el panel izquierdo, y se selecciona Device. La página muestra todas las plantillas de monitoreo que están relacionados con el nombre del dispositivo.

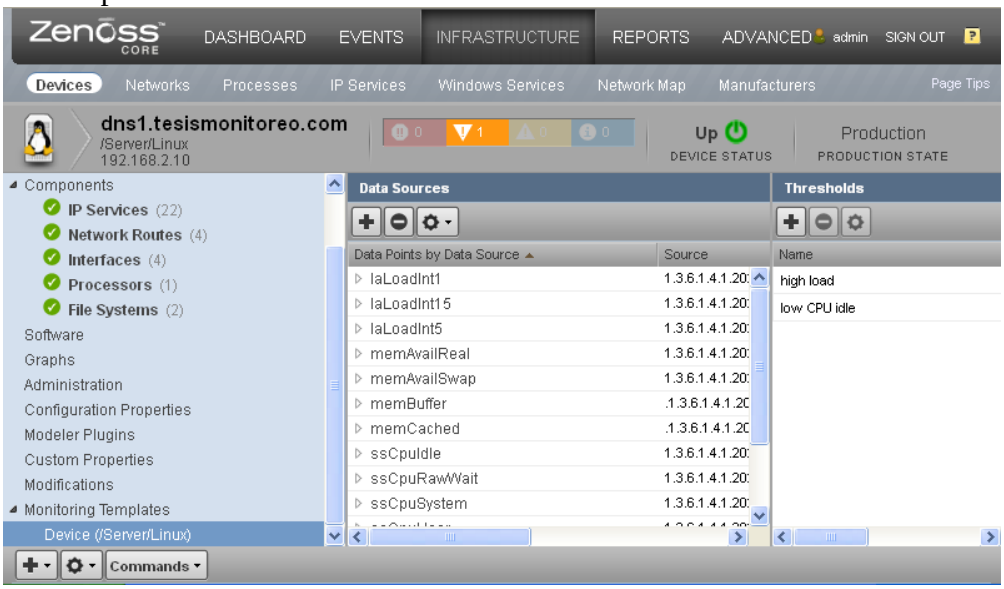


Fig 2.93 Ventana de la Opción Monitoring Templates

2.3.4 Monitoreo de Servicios IP

La pestaña de **IP Services** (INFRAESTRUCTURE > IP Services) permite monitorear los servicios IP que ejecutan en la red.

En el panel de la izquierda se selecciona el servicio, que muestra una ventana donde se puede introducir algunas de sus características como el nombre, su descripción, el puerto TCP por el que se comunica, entre otros. En la parte inferior de la ventana se muestra el estatus del servicio y el dispositivo en el que se encuentra dicho servicio.

Para activar los servicios hay que activar las secciones Enable Monitoring? (z Monitor) y Failure Event Severity (zFailSeverity) y guardar los cambios.

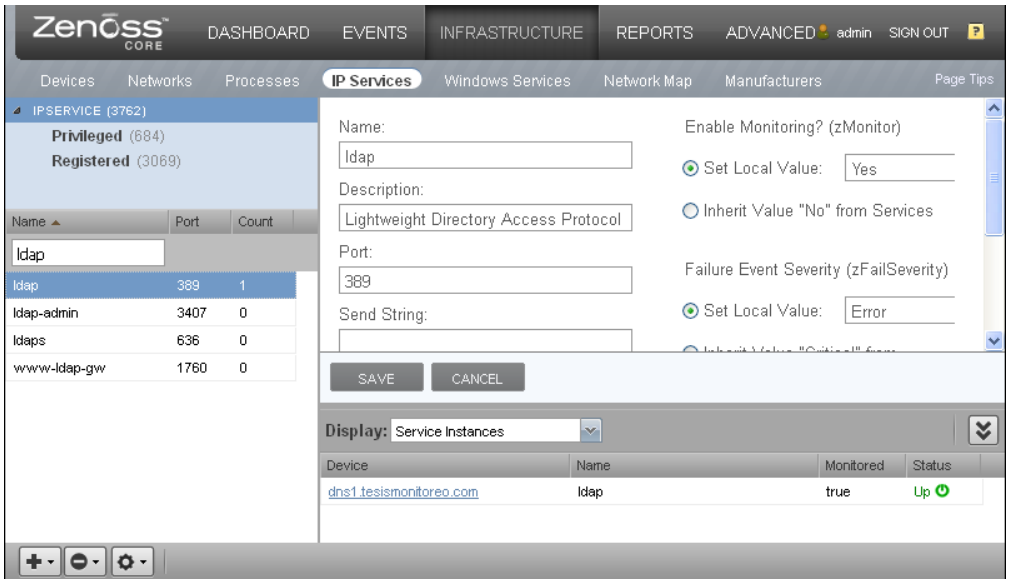


Fig 2.94 Ventana de la pestaña IP Services

2.3.5 Monitoreo de Servicios Windows

La pestaña Windows Services (INFRASTRUCTURE>Windows Services) permite administrar los servicios especiales para equipos Windows, teniendo las mismas características que la pestaña anterior y activándose cada servicio igual que en la pestaña IP Services. Es necesario activar los servicios de los equipos Windows para poder observar las gráficas además de instalar la versión gratuita del software SNMP Informant que se puede obtener de la página:
http://www.snmp-informant.com

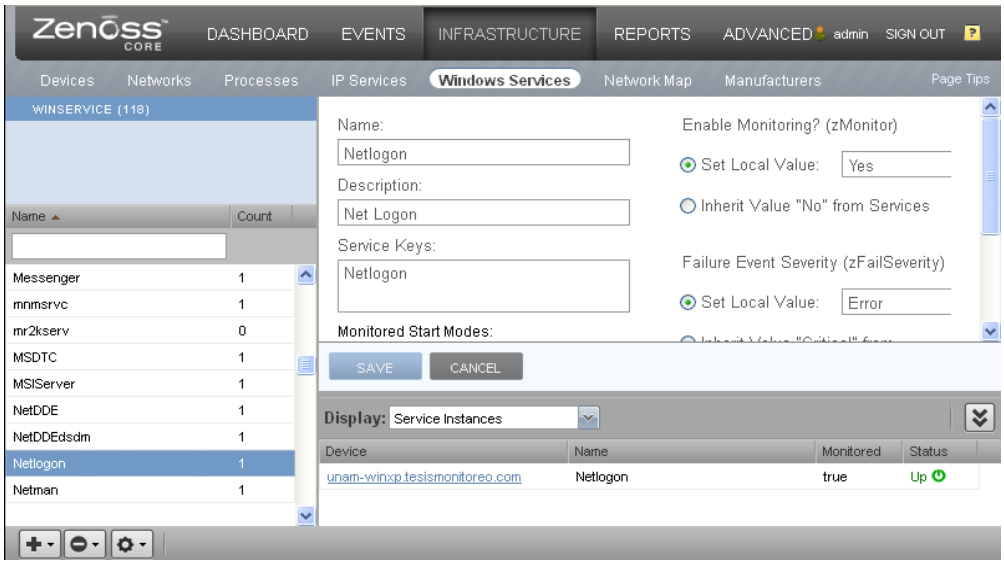


Fig 2.95 Ventana de la pestaña Windows Services

Para asegurarse que el software está funcionando correctamente se aplica desde otro equipo en la red el comando:

#snmpwalk –v1 –cpublic 192.168.2.11 1.3.6.1.4.1.9600

public = comunidad
192.168.2.11=dirección Ip

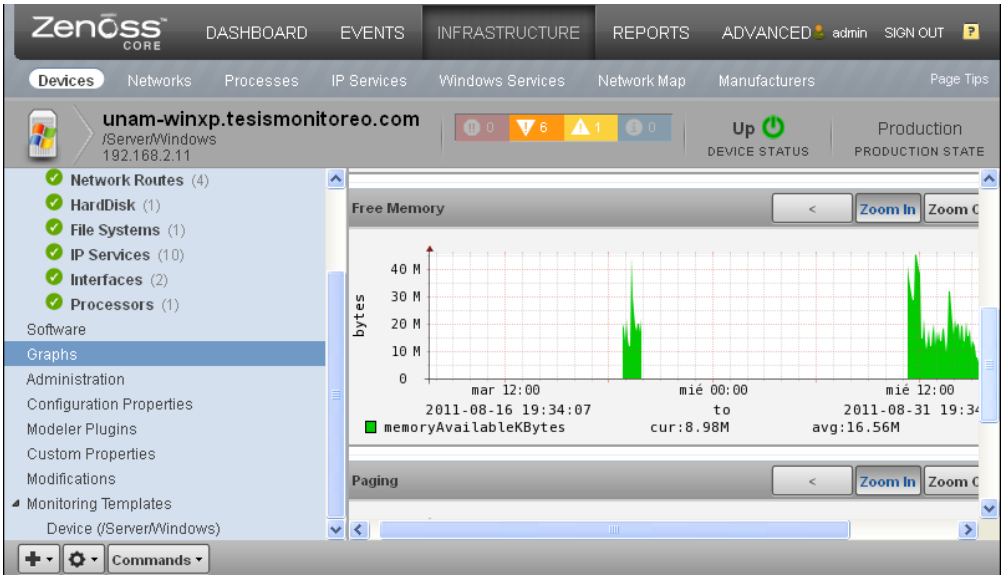


Fig 2.96 Imagen del monitoreo de un equipo virtual Windows

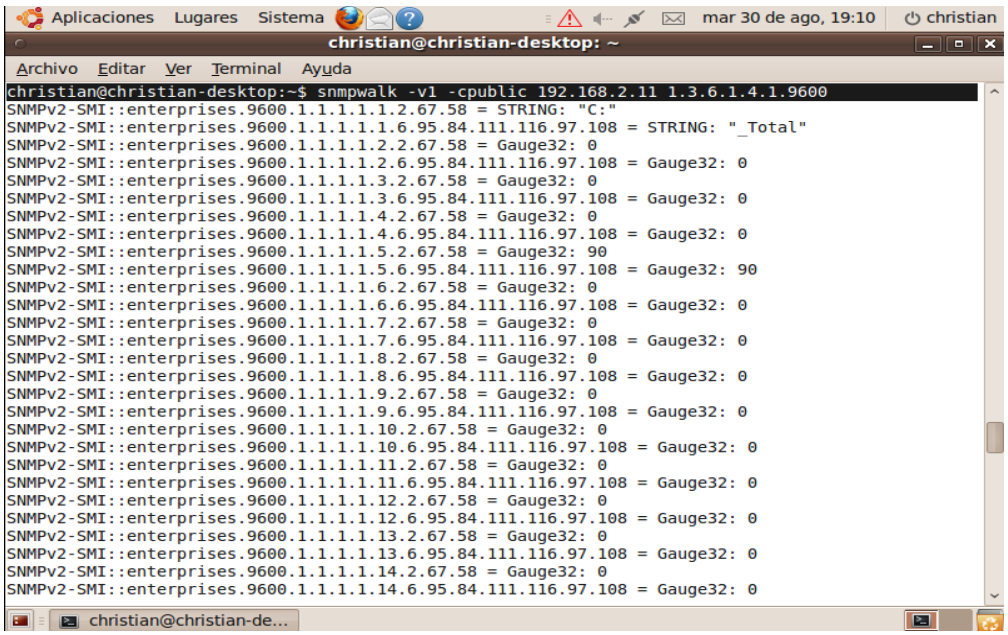


Fig 2.97 Confirmación de monitoreo SNMP a equipo Windows

2.3.6 EVENTS

La pestaña Events te permite ver y administrar los eventos de todos los dispositivos agregados al sistema. Cada consola muestra diferentes subcategorias de eventos.

Esté sistema central de eventos, muestra el repositorio de todos los eventos que han sido recogidos por el sistema, conteniendo las siguientes características:

Select, sort and filter events: Permite ordenar y filtrar de diferente forma los eventos, ya sea en conjunto o por evento.

Work with live search: Ayuda a localizar información relacionada con los eventos.

Save or refresh a view: Te permite guardar la vista en la que se encuentra la consola de eventos además de actualizarla (refrescarla) de manera manual o automática.

View event details Acknowledge events Return events to new status: Te permite observar más detalladamente los eventos además de que los puedes marcar como Acknowledging para identificarlos como reconocidos y saber que estas tomando alguna acción para resolverlo.

Classify events: Te permite asociar los eventos que se muestran como /Unknown con una clase de evento especifico o clasificarlos según el tiempo.

Move events to history or return them to active status: Esta opción se utiliza cuando no quieres mantener activos los eventos más antiguos o los quieres regresar a su estado activo.

Export Event Data: Sirve para exportar los eventos de la consola a un archivo que los separa por comas con extensión .csv o un archivo XML.

Create events. Sirve para crear eventos. Un evento se genera cuando los demonios detectan un fallo en el sistema.

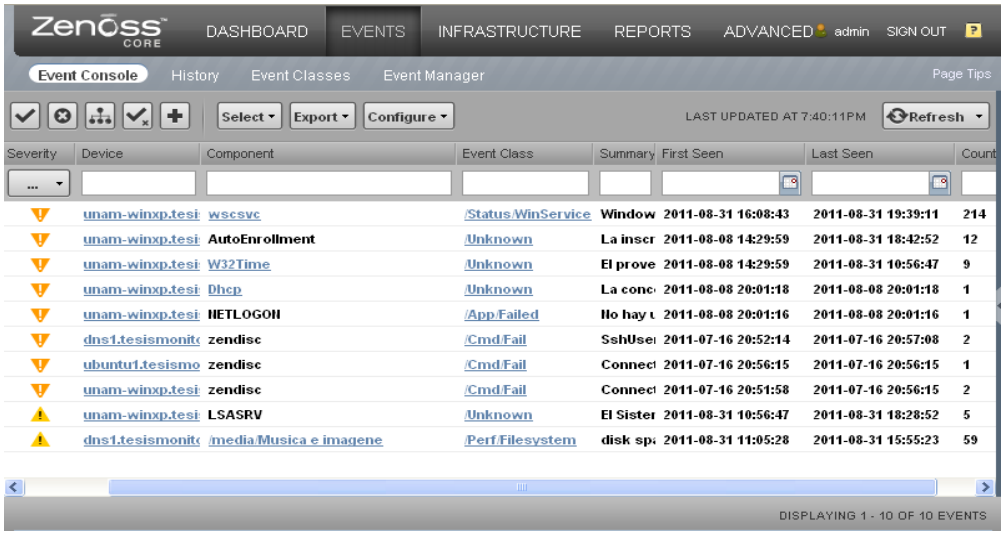


Fig 2.98 Eventos detectados en los equipos Virtuales

2.3.7 ADVANCED

2.3.7.1 Administración de Usuarios

En Zenoss se pueden crear diferentes usuarios con diferentes permisos de grupo y reglas de alertas únicas, con el objetivo de tener un acceso seguro del sistema. Para crear una cuenta de usuario administrador, se debe entrar al sistema con la cuenta de usuario llamada *"admin*" o como usuario con privilegios extendidos. Los pasos para crear una cuenta de usuario son los siguientes:

1.-Se abre la pestaña **ADVANCED**, aparece la página **Settings**.
2.-En el panel izquierdo se selecciona **Users**, aparecen los usuarios y grupos de administración que se crearon en zenoss.

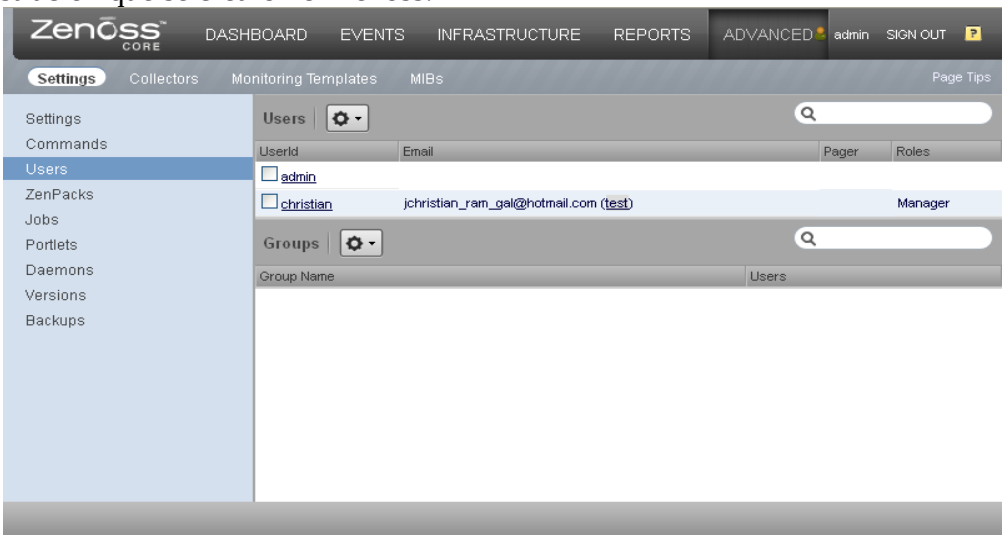


Fig 2.99 Usuarios registrados por Zenoss

3.-De el menú  (Add Menu), se selecciona Add New User y posteriormente aparecerá un cuadro de dialogo.

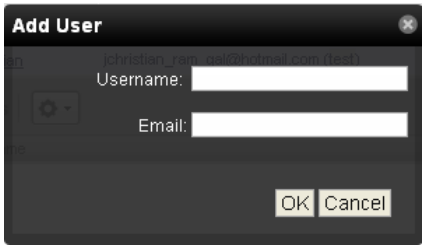


Fig 2.100 Ventana de datos para agregar un nuevo usuario a Zenoss

4.-En el campo de Username se coloca la cuenta de usuario que se utilizará y en el otro campo un correo electrónico, la utilidad de este último es para que se le envíen alertas.
5.-Y click en OK.

Las cuentas pueden ser editadas con características más particulares, seleccionando al usuario, también se pueden asociar objetos a usuarios específicos y asignarles un role especifico que aplica con respecto al objeto asignado e incluso hacerlo administrador de dicho objeto dándole más privilegios sobre él.

En esta sección se permite hacer clasificaciones por grupos de usuarios, ya que es de gran utilidad para un mejor control.

2.3.7.2 Roles

Un role en Zenoss es un grupo de permisos que pueden asignarse a los usuarios o grupos.

Los roles que existen en Zenoss son:

- ZenUser: Proporciona solo lectura global de acceso para el sistema de objetos.
- ZenManager: Proporciona lectura y escritura global de acceso para el sistema de objetos
- Manager: Provee una lectura y escritura global de acceso para el sistema de objetos. Adicionando que provee lectura y escritura de acceso para la base de datos de objetos Zope.
- ZenOperator: Instalado por el ZenPack ZenOperatorRole. Este ZenPack está disponible únicamente para clientes Enterprise. El role ZenOperator permite a los usuarios combinar el role ZenOperator con el role ZenUser para que los usuarios únicamente puedan leer el acceso al sistema, pero también permitiéndoles reconocer eventos, mover eventos al historiador, y agregar mensajes de logs a eventos.

[46,pag128]

2.3.7.3 ZenPacks

Los Zenpacks se extienden y modifican los sistemas para agregar nuevas funcionalidades, estos se pueden crear por medio de la interfaz de usuario, o si son más complejos se desarrollan en scripts usando diferentes lenguajes de programación. Su aplicación puede ser tan simple como agregar nuevas clases de dispositivos o plantillas de monitoreo, o tan complejo como extender el modelo de datos y proveer nuevas colecciones de demonios.

Con los Zenpack se pueden agregar nuevas funcionalidades como:

- Monitoreo de Plantillas
- Fuentes de Datos
- Gráficas
- Clases de Eventos
- Eventos y comandos de usuarios
- Reportes
- Extensiones de modelos
- Definiciones de productos

Instalación de ZenPacks

Los ZenPacks son distribuidos por archivos .egg, se pueden instalar por línea de comandos o por la interfaz gráfica del usuario.

Instalacion por linea de comandos

Se utilizan los siguientes comandos para realizar la instalación de un archivo ZenPack y para reiniciar.

zenpack - -install (filename o directoryname)
zenoss restart

Instalación desde la interfaz de usuario

Para instalar un archivo Zenpack .egg desde la interfaz de usuario.

1.-Selecciona la pestaña ADVANCED > Settings

2.- En el panel izquierdo seleccionar ZenPack

3.- De  (Action menu), seleccionamos install ZenPack, posterior mente aparece una ventana como la que se muestra en la imagen.

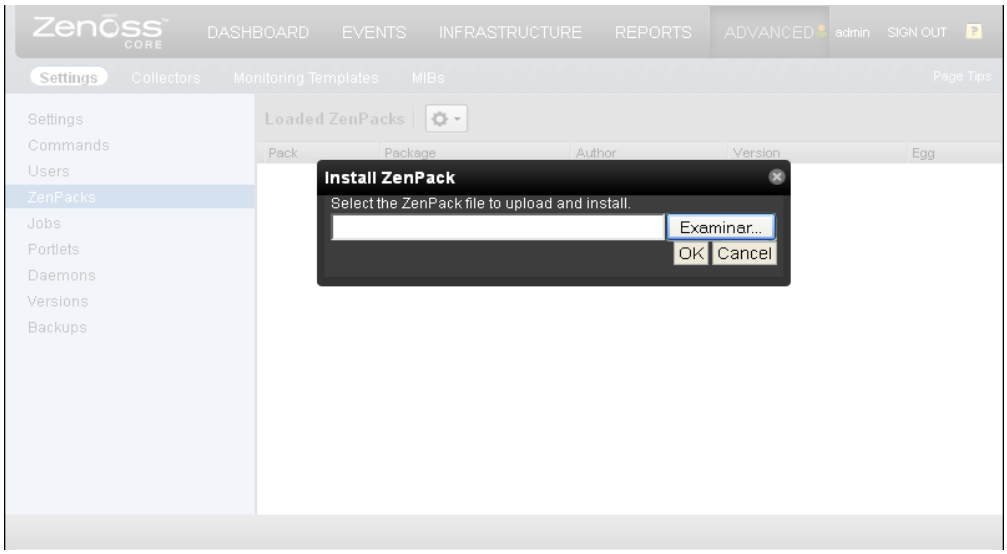


Fig 2.101 Ventana para agregar un nuevo ZenPack

4.-Se da click en Examinar para seleccionar el archivo .egg que se requiere instalar y OK. Este archivo es descargado al servidor Zenoss e instalado.

5.- Despues de instalar el ZenPack , es necesario reiniciar el sistema.

Los ZenPacks están disponibles para descargar de la siguiente página:

http://community.zenoss.org/community/zenpacks

Crear un Zenpack

Para crear un ZenPack se debe estar logueado como administrador.
1.-Seleccionar la pestaña **ADVANCED > Settings**
2.- En el panel izquierdo se selecciona ZenPacks
3.- De  (Action menu), seleccionamos Create ZenPack, posteriormente aparece una ventana como la que se muestra en la imagen.

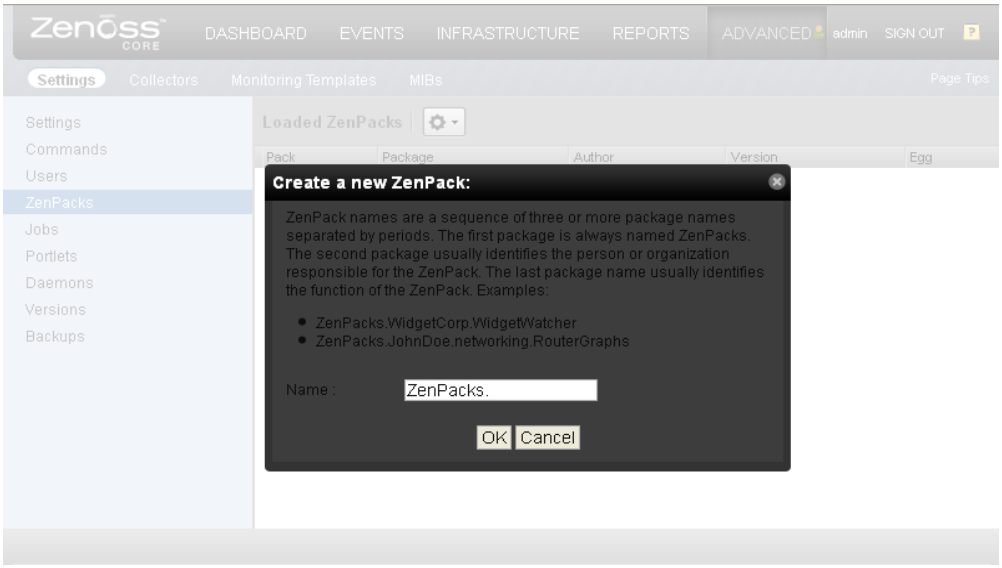


Fig 2.102 Ventana para la creación de un ZenPack

4.- Se coloca el nombre del ZenPack, el cual debe tener el formato:
ZenPacks.*Organization.Identifier*
5.- Y se hace click en OK.
El sistema crea el objeto ZenPack en la base de datos y un nuevo directorio en el sistema de archivos $ZENHOME/ZenPacks/*TUZenPackID*

Terminando todo esto, solo es necesario utilizar esta nueva funcionalidad de monitoreo.

2.3.8 REPORTS

Zenoss agrega y reporta, con tiempo, los datos que se crearon al monitorear los equipos, definiendo un rango y personalizando las diferentes opciones de reportes.

Para trabajar con reportes, se selecciona la pestaña REPORTS. Los reportes enlistados aparecen en forma de árbol en la sección del lado izquierdo de la ventana.

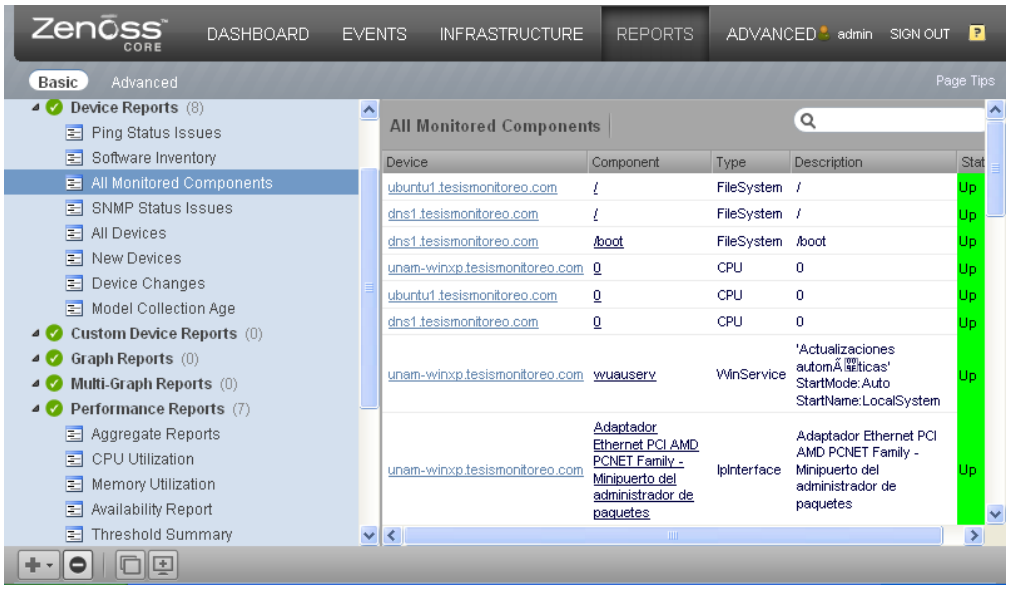


Fig 2.103 Ventana de la pestaña REPORTS

Los reportes se dividen en

- Device reports
- Custom Device Reports
- Graph Reports
- Multi-Graph Reports
- Performace Reports
- User Reports
- Event Reports

CAPÍTULO 3 *Gestión y Monitoreo de un Laboratorio de cómputo*

3.1 IMPLEMENTACIÓN DE UN SERVIDOR ZENOSS EN UN LABORATORIO

Posteriormente de realizar implementaciones en maquinas virtuales, se proseguirá a la implementación en un laboratorio con maquinas reales, para verificar la utilidad real de la herramienta y su funcionamiento en un ambiente de trabajo constante.

La implementación del servidor Zenoss en el laboratorio se realizó en un equipo con las siguientes características:

Memoria RAM de 512MB
Procesador: Pentium 4 a 2GHZ
Disco Duro de 40 GB
Un lector de cd

Las características de este equipo no fueron las más óptimas para un excelente funcionamiento, pero son útiles para el monitoreo en un laboratorio de computo pequeño, por lo que, para tener un rendimiento aceptable en el equipo al instalarse Zenoss, el sistema operativo sobre el cual se instalaría el sistema Zenoss sería "*Centos 5"*, pero sin Interfaz gráfica, para utilizar solo los recursos necesarios de la maquina y que estos sean aprovechados al máximo por el sistema Zenoss, además se manejará una instalación diferente que en la virtualización, esto con el objetivo de ampliar más el conocimiento de la herramienta.

A continuación se describirán los comandos y el procedimiento que se siguió para la implementación de zenoss en el laboratorio:

Para comenzar es recomendable aplicar comandos de actualización puesto que; tener la versión más actual del Sistema Operativo favorece a una mejor seguridad y funcionamiento estable, pero en este caso, debido a la falta de recursos en el equipo a utilizar no se realizó. De cualquier forma los comandos necesarios para esta acción son:

```
#yum –y upgrade
#yum –y update
```

La BDs que utiliza Zenoss es MySQL, por lo cual es necesario instalarla junto con algunas dependencias extras y necesarias para zenoss.

```
# yum -y install mysql-server net-snmp net-snmp-utils gmp libgomp libgcj
liberation-fonts
```

```
================================================================================
 Package              Arch       Version                    Repository     Size
================================================================================
Installing:
 mysql-server         i386       5.0.77-4.el5_6.6           base          9.8 M
 net-snmp             i386       1:5.3.2.2-14.el5_7.1       updates       702 k
 net-snmp-utils       i386       1:5.3.2.2-14.el5_7.1       updates       190 k
Installing for dependencies:
 mysql                i386       5.0.77-4.el5_6.6           base          4.8 M
 perl-DBD-MySQL       i386       3.0007-2.el5               base          148 k
 perl-DBI             i386       1.52-2.el5                 base          600 k

Transaction Summary
================================================================================
Install       6 Package(s)
Upgrade       0 Package(s)

Total download size: 16 M
Downloading Packages:
(1/6): perl-DBD-MySQL-3.0007-2.el5.i386.rpm               | 148 kB     00:01
(2/6): net-snmp-utils-5.3.2.2-14.el5_7.1.i386.rpm         | 190 kB     00:01
(3/6): perl-DBI-1.52-2.el5.i386.rpm                       | 600 kB     00:05
(4/6): net-snmp-5.3.2.2-14.el5_7.1.i386.rpm               | 702 kB     00:06
(5/6): mysql-5.0.77-4. (20%) 37% [====         ] 102 kB/s | 1.8 MB     00:29 ETA
```

Fig 3.1 Instalación de dependencias necesarias para Zenoss

Para configurar la base de datos de mysql se colocan los siguientes comandos

Agrega mysql en la secuencia de arranque

```
# /sbin/chkconfig --add mysqld
```

Sirve para mostrar los niveles actuales de ejecución

```
# /sbin/chkconfig --list mysqld
```

Ajusta los niveles de ejecución

```
# /sbin/chkconfig --level 2345 mysql on
```

Reinicia el servicio

```
# /etc/init.d/mysqld restart
```

Se colocan los password o se colocan comillas en lugar de contraseñas para después definirlas

```
# /usr/bin/mysqladmin -u root password ''

# /usr/bin/mysqladmin -u root -h localhost password ''
```

```
Alternatively you can run:
/usr/bin/mysql_secure_installation

which will also give you the option of removing the test
databases and anonymous user created by default.  This is
strongly recommended for production servers.

See the manual for more instructions.

You can start the MySQL daemon with:
cd /usr ; /usr/bin/mysqld_safe &

You can test the MySQL daemon with mysql-test-run.pl
cd mysql-test ; perl mysql-test-run.pl

Please report any problems with the /usr/bin/mysqlbug script!

The latest information about MySQL is available on the web at
http://www.mysql.com
Support MySQL by buying support/licenses at http://shop.mysql.com
                                                           [  OK  ]
Starting MySQL:                                            [  OK  ]
[root@localhost ~]# /usr/bin/mysqladmin -u root password ''
[root@localhost ~]# /usr/bin/mysqladmin -u root -h localhost password ''
[root@localhost ~]# _
```

Fig 3.2 Comando para definir contraseñas de MySQL

Se descarga el paquete zenoss-stack para su instalación:

```
#wget http://sourceforge.net/projects/zenoss/files/zenoss-3.2/zenoss-
3.2.0/zenoss-stack-3.2.0-linux.bin
```

```
enoss-stack-3.2.0-linux.bin/download [following]
--2011-10-09 13:44:50--  http://sourceforge.net/projects/zenoss/files/zenoss-3.2
/zenoss-3.2.0/zenoss-stack-3.2.0-linux.bin/download
Connecting to sourceforge.net|216.34.181.60|:80... connected.
HTTP request sent, awaiting response... 302 Found
Location: http://downloads.sourceforge.net/project/zenoss/zenoss-3.2/zenoss-3.2.
0/zenoss-stack-3.2.0-linux.bin?r=&ts=1318203807&use_mirror=cdnetworks-us-2 [foll
owing]
--2011-10-09 13:44:51--  http://downloads.sourceforge.net/project/zenoss/zenoss-
3.2/zenoss-3.2.0/zenoss-stack-3.2.0-linux.bin?r=&ts=1318203807&use_mirror=cdnetw
orks-us-2
Resolving downloads.sourceforge.net... 216.34.181.59
Connecting to downloads.sourceforge.net|216.34.181.59|:80... connected.
HTTP request sent, awaiting response... 302 Found
Location: http://cdnetworks-us-2.dl.sourceforge.net/project/zenoss/zenoss-3.2/ze
noss-3.2.0/zenoss-stack-3.2.0-linux.bin [following]
--2011-10-09 13:44:51--  http://cdnetworks-us-2.dl.sourceforge.net/project/zenos
s/zenoss-3.2/zenoss-3.2.0/zenoss-stack-3.2.0-linux.bin
Resolving cdnetworks-us-2.dl.sourceforge.net... 174.35.19.12
Connecting to cdnetworks-us-2.dl.sourceforge.net|174.35.19.12|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 97549773 (93M) [application/octet-stream]
Saving to: `zenoss-stack-3.2.0-linux.bin'

 4% [>                                       ] 3,978,215   84.1K/s  eta 14m 48s _
```

Fig 3.3 Descarga de Zenoss en modo consola

Después de descargar el paquete se le da permisos de ejecución con el siguiente comando:

```
# chmod +x zenoss-stack-3.2.0-linux.bin
```

Se inicia la instalación:

```
# ./zenoss-stack-3.2.0-linux.bin
```

```
install.log         zenoss-stack-3.2.0-linux.bin                          ▉
install.log.syslog
[root@localhost ~]# chmod +x zenoss-stack-3.2.0-linux.bin
[root@localhost ~]# ./zenoss-stack-3.2.0-linux.bin
-------------------------------------------------------------------------------
Welcome to the Zenoss Setup Wizard.

-------------------------------------------------------------------------------
Installation folder

Please, choose a folder to install Zenoss

Select a folder [/usr/local/zenoss]:

-------------------------------------------------------------------------------
MySQL Credentials

Please enter your database root user password

MySQL Server root password :
Re-enter password :
-------------------------------------------------------------------------------
Setup is now ready to begin installing Zenoss on your computer.

Do you want to continue? [Y/n]: _
```

Fig 3.4 Inicio de la instalación de Zenoss en el Servidor

La contraseña de MYSQL Server root es colocada.

En la instalación se permite elegir la ruta donde se instalará zenoss, dejando la ruta por default /usr/local/zenoss.

```
Welcome to the Zenoss Setup Wizard.
```

```
Installation folder
Please, choose a folder to install Zenoss
Select a folder [/usr/local/zenoss]:
```

Por default, Zenoss necesita los puertos 8080 para la aplicación y 8081 para Zenhub, si no se encontraran disponibles, debido a que son ocupados por otro servicio, es posible cambiarlos desde el instalador.

```
Zope Port Configuration
Please enter the Zope configuration parameters you wish to use.
Zope Server Port: [8080]:
Zope ZeoDB Server Port: [8100]:
```

Durante la instalación y la conexión con la BD en el equipo, se preguntará por la contraseña del administrador de MySQL.

```
MySQL Credentials
Please enter your database root user password
MySQL Server root password :
Re-enter password :
```

Zenoss pregunta si se quiere continuar e iniciar con la instalación.

```
Setup is now ready to begin installing Zenoss on your computer.
Do you want to continue? [Y/n]:
```

Al terminar los pasos anteriores comienza la instalación

```
Please wait while Setup installs Zenoss on your computer.
Installing
0% _______________ 50% _______________ 100%
########################################
```

Al finalizar se pregunta si deseamos iniciar zenoss y cómo se realiza el acceso a la web de administración

```
Setup has finished installing Zenoss on your computer.
Launch Zenoss [Y/n]:
Info: To access the Zenoss Application, go to [http://localhost:8080] from your
browser
Press [Enter] to continue:
```

```
--------------------------------------------------------------------------------
Setup is now ready to begin installing Zenoss on your computer.

Do you want to continue? [Y/n]: y

--------------------------------------------------------------------------------
Please wait while Setup installs Zenoss on your computer.

 Installing
 0% _______________ 50% _______________ 100%
 ########################################^[[B^[[A

#

--------------------------------------------------------------------------------
Setup has finished installing Zenoss on your computer.

Launch Zenoss [Y/n]:
Launch Zenoss [Y/n]:
y
Info: To access the Zenoss Application, go to http://localhost:8080 from your
browser.
Press [Enter] to continue :[root@localhost ~]#
[root@localhost ~]#
[root@localhost ~]# _
```

Fig 3.5 Fin de la instalación de Zenoss

3.1.1 SNMP EN LOS EQUIPOS DEL LABORATORIO

Para iniciar la implementación, se instaló y configuró SNMP en los equipos del laboratorio. Los Sistemas Operativos con los que contaban los equipos clientes del laboratorio eran; Windows XP y Fedora 4, estos SO se encontraban en todos los equipos, cada uno en una partición diferente del Disco Duro.

Para realizar dicha configuración en los equipos clientes, se debía instalar la versión SNMP para Fedora 4 pero existía un inconveniente; que los repositorios de esta versión ya no funcionaban, por lo cual se realizó una pequeña investigación para conseguir los paquetes net-snmp, net-snmp-utils y sus dependencias.

Posteriormente, con dichos paquetes se creó un archivo llamado: net-snmpfc4.tar.gz, el cual sirvió para la instalación del SNMP en cada uno de los equipos clientes, en la partición de Fedora.

La Instalación se realizó de la siguiente manera y con los siguientes comandos.

Para descomprimirlo se utilizó el comando

```
#tar –zxvf net-snmpfc4.tar.gz
```

Y después ubicados dentro de la carpeta descomprimida, se prosiguió a comenzar con la instalación del SNMP que en este caso el archivo para comenzar la instalación tiene el nombre de “instalar.sh” utilizando el siguiente comando para realizar dicha acción:

```
#sh instalar.sh
```

Para la instalación en equipos con SO Windows la instalación del SNMP es igual a la que se realizó en la red con Máquinas Virtuales en el capítulo anterior, en el tema 2.3.2 Agente SNMP en Windows, utilizando el CD de instalación.

Para poder revisar la aplicación web desde otro equipo de la red, se coloca la IP del servidor como se muestra en la siguiente imagen, en éste caso al servidor se le colocó la IP 192.168.3.70.

http:// 192.168.3.70:8080/zport/dmd/

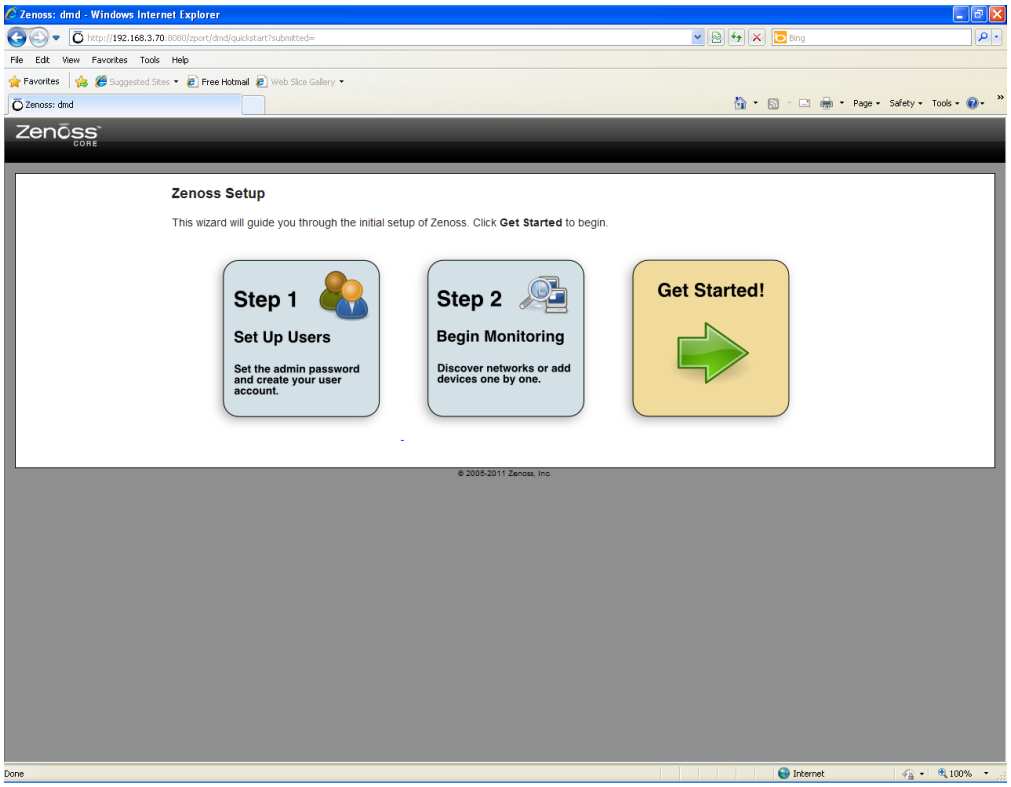


Fig 3.6 Primer imagen de la interfaz web

3.1.2 CONFIGURACIÓN DE ZENOSS PARA ADAPTARSE AL LABORATORIO

Como parte de la implementación en equipos reales, fue necesario configurar el servidor Zenoss, de tal forma que el sistema monitoreara dos Sistemas Operativos de manera automática cada que éste cambiara, sin que el administrador se estuviera preocupando de esta modificación, además de ser identificado cada equipo como uno solo, pero con 2 SO en este caso: Fedora 4 y Windows XP, encontrados en cada uno de los equipos en diferente partición de sus respectivos discos.

Esto se realizo con éxito al configurar el servidor Zenoss de la siguiente manera:

En la pestaña de **ADVANCED>Settings>Daemons,** buscamos el demonio llamado **zenmodeler** para detenerlo por unos momentos y poder modificarlo.

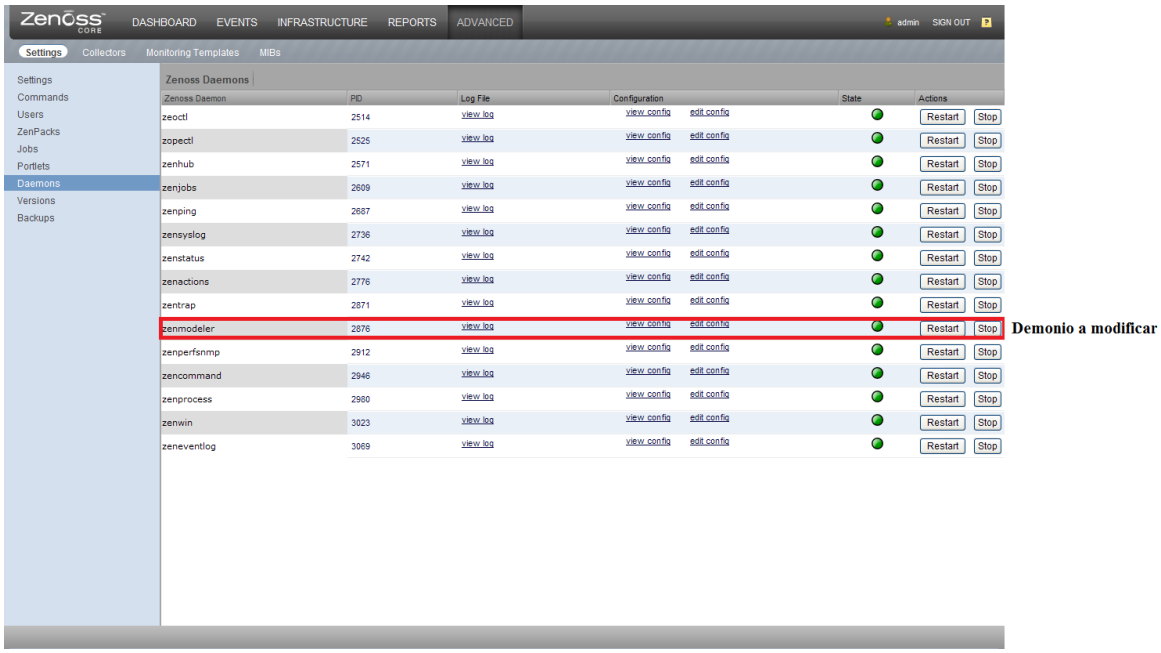


Fig 3.7 Daemon zenmodeler

Como se puede observar en la imagen, el demonio a modificar es "zenmodeler", la parte que se modifica es la de "cicletime 720" cambiando el 720 a 10, lo que provoca que se ejecute este proceso para recolectar la información cada 10 minutos, en lugar de esperar los 720 minutos (12 horas) que se tenían por default. Es así como se remodelan los dispositivos con más frecuencia, cambiando características monitoreadas dependiendo del SO que se encuentre en ejecución en ese momento. En redes grandes este cambio podría impactar en el rendimiento de la red, por lo cual se recomienda realizar antes una investigación y análisis del tráfico que se generaría o dejar los valores por default, otra opción sería; dar diferente IP a cada SO si se tienen varias particiones, todo depende del ambiente en el cual se trabaje.(pag 31 Modeling Devices)

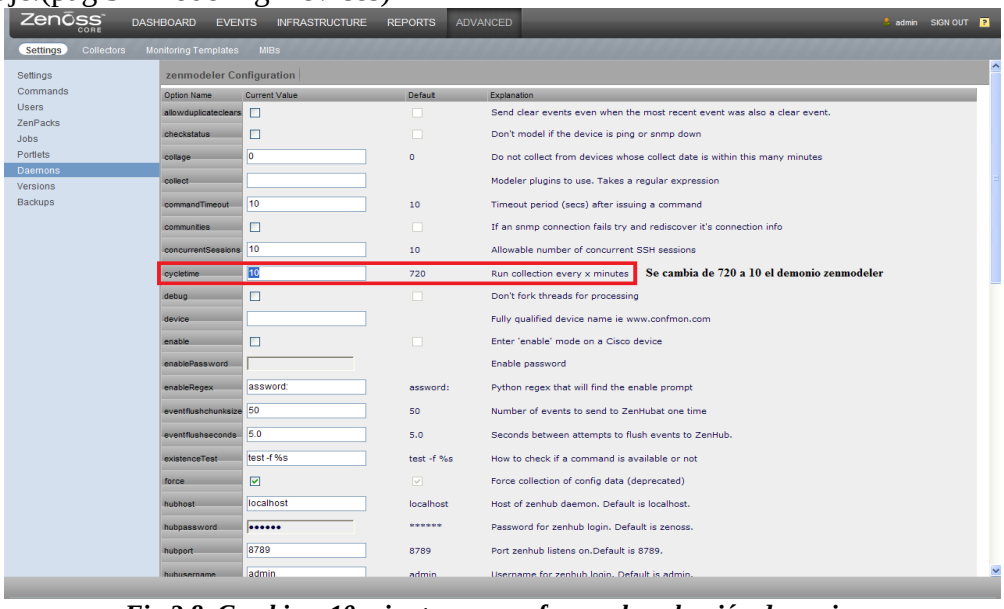


Fig 3.8 Cambio a 10 minutos para refrescar la colección de equipos

Existen clases de dispositivos estándar que se encuentran por default en Zenoss y que tienen Templates o plantillas ya predefinidas para cada tipo de dispositivo y/o SO, por lo cual los equipos clientes del laboratorio se colocaron en la clase o división "Server", que es una división o clase neutral para los diferentes SO. Ésta decisión se tomó debido a que si los colocamos en un tipo o clase, ya sea Windows o Linux y el equipo se encuentra trabajando en un SO diferente a la clase en el cual fue colocado, no se monitoreará, pues sus propiedades son diferentes y no corresponden a las Templates de esa clase o división. Y como se explicó con anterioridad, para cada dispositivo y SO existen diferentes Templates o plantillas, por eso para que el sistema monitoree tanto Windows como Linux que son los dos SO con los que cuentan los equipos clientes del laboratorio, se configuraron las Templates de cada SO en la clase Server de la siguiente manera.

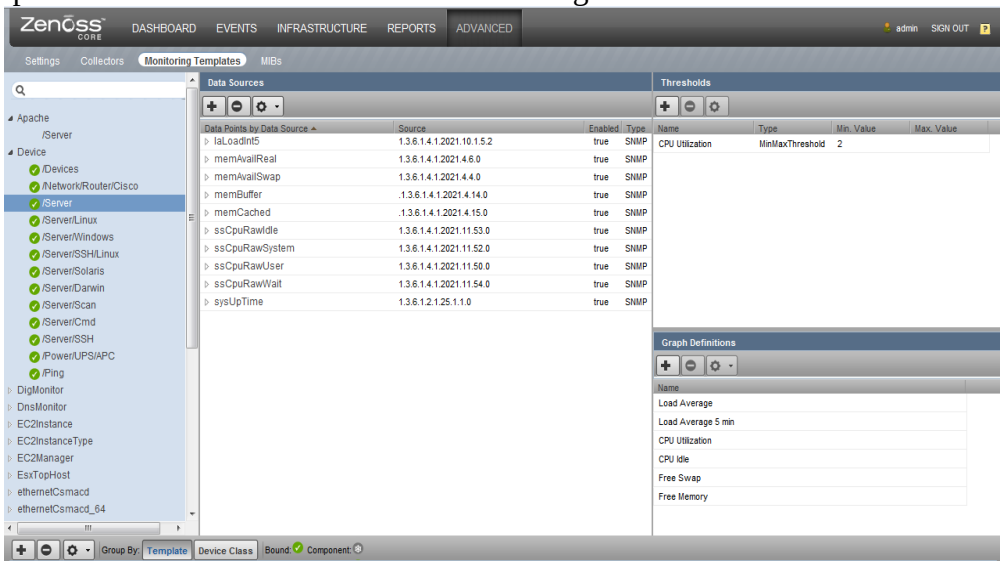


Fig 3.9 Templates de la clase server

Se verifican las Templates ya definidas en una división o clase para agregarlas en otra en la que se colocaran los dispositivos, en este ejemplo se utilizarán las Templates de Windows ya predefinidas para agregarlas a la sección de Server.

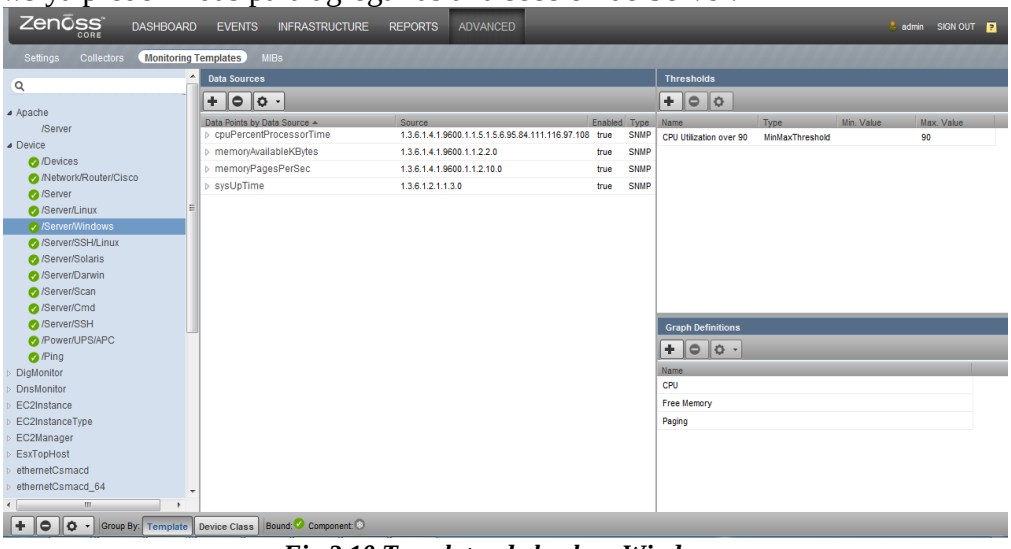


Fig 3.10 Templates de la clase Windows

Primero se agregan un Data Source con el icono  , apareciendo la siguiente ventana y dándole el mismo nombre que los Data Source mostrados en la Clase Windows, esto para evitar confusiones. Terminando se oprime "submit" para crearlo.

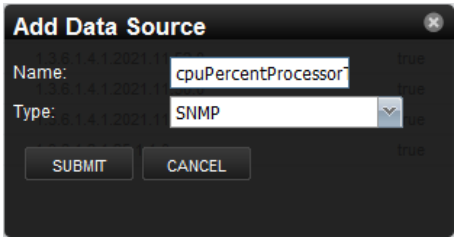
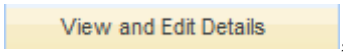


Fig 3.11Ventana para agregar un Data Source

Se selecciona el Data Source que se creó y se oprime  para seleccionar 

, apareciendo la siguiente imagen donde el nombre se encontrará por default, pero el OID se tendrá que copiar del Template en la división de Windows.

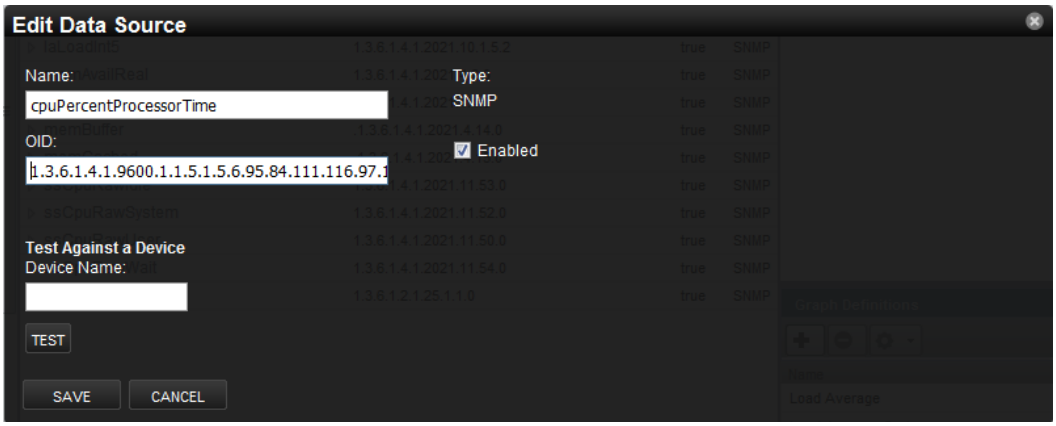


Fig 3.12 OID de la clase Windows a la clase Server

Se prosigue pasando a la sección de Thresholds o umbrales y se oprime  Add Threshold.

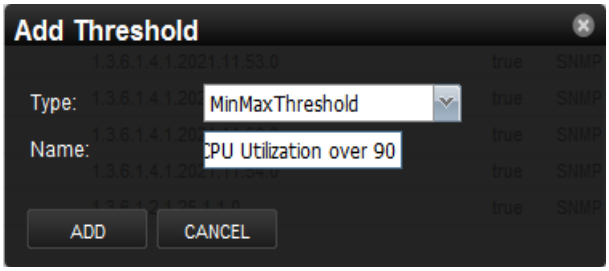


Fig 3.13 Agregado de Threshold

Posteriormente se da click a  , para editar el Threshold se pueden colocar y establecer las mismas características que las mostradas en la clase Windows dependiendo de las necesidades del laboratorio.

Threshold Server

Threshold Windows

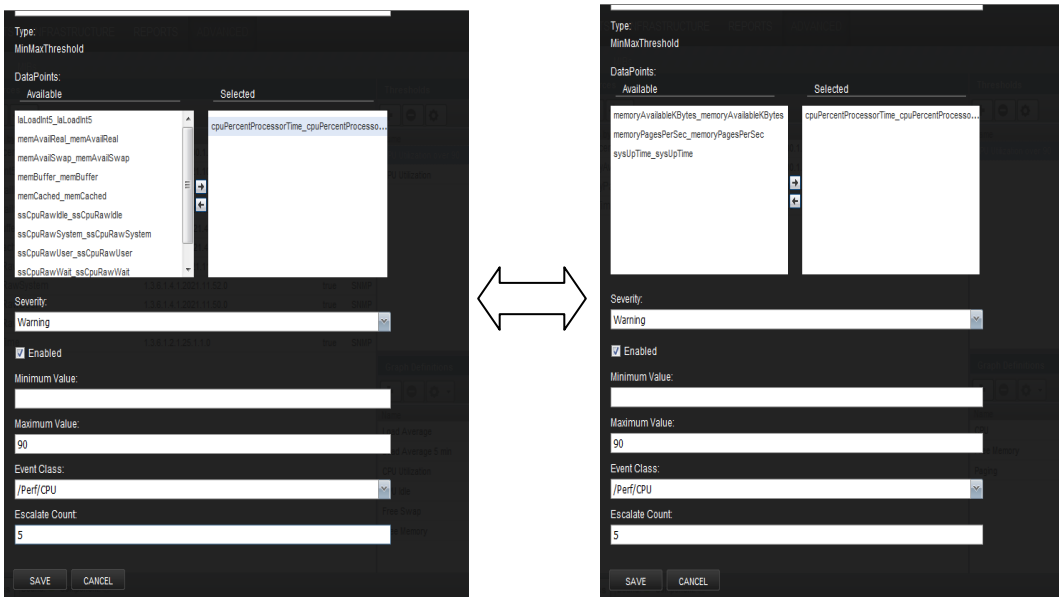


Fig 3.14 Configuraciones similares del Threshold

Despues de Editar el Threshold se pasa a la sección "Graph Definitions", donde al igual se oprime  Add Graph Definitions y se coloca el nombre de la gráfica, en este caso sí se puede cambiar el nombre para saber el SO al que pertenece la gráfica.

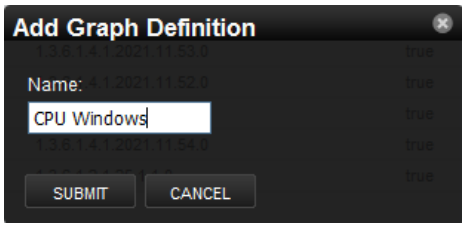
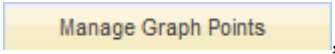


Fig 3.15 Nombre de la Gráfica que a crear

Posteriormente se selecciona el nombre que se le colocó a la grafica y se da click a  , eligiendo 

, lo cual muestra la siguiente ventana y se selecciona el Data Point que se había creado anteriormente (cpuPercentProcessors), agregando por default el Threshold del mismo Data Point.

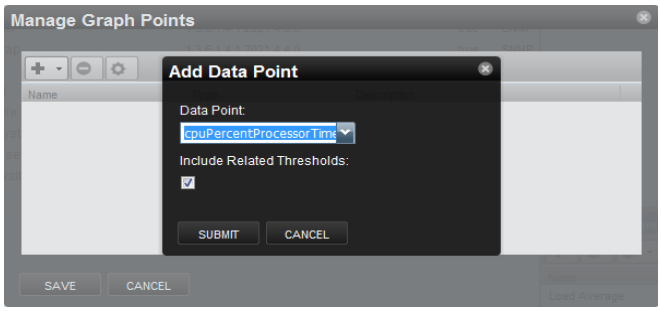


Fig 3.16 Selección del Data Point

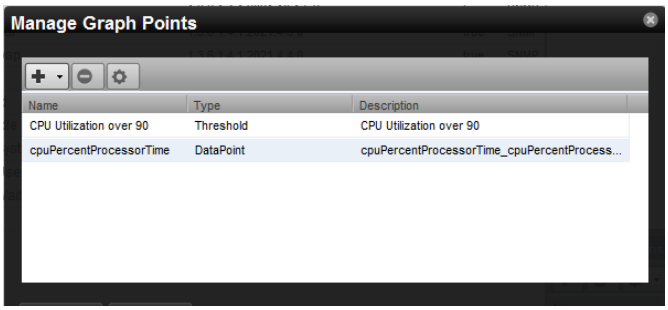
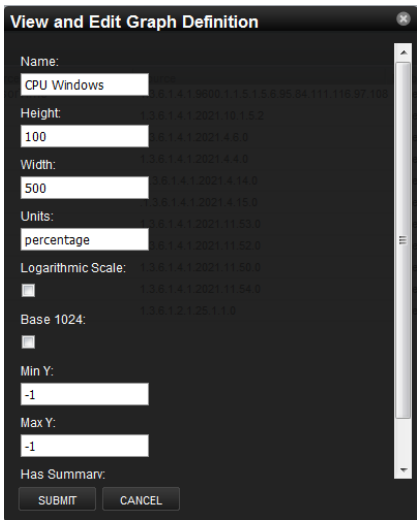


Fig 3.17 Configuraciones administrables de la gráfica creada

A continuación se oprime View and Edit Details, para agregar las siguientes configuraciones, siendo comparadas con la de la sección de las gráficas predeterminadas para Windows.

Server



Windows

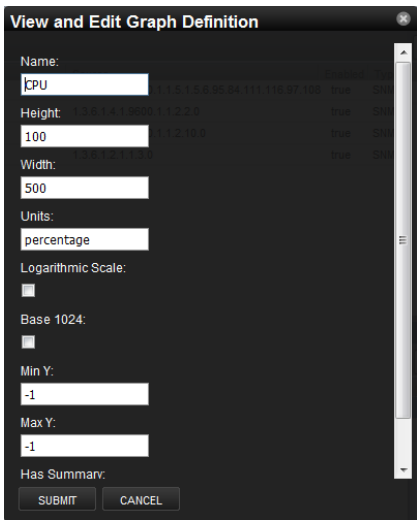
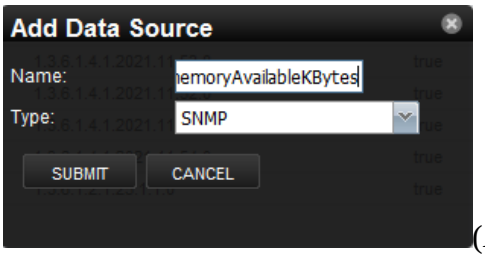


Fig 3.18 Valores con los que contará la gráfica

Así se van agregando las demás gráficas del sistema Windows.

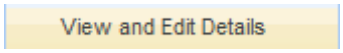
Para agregar los demás data Source "memoryAvailableKBytes, memoryPagesPerSec, sysUpTime" se da click en Add Data Source, colocamos el nombre



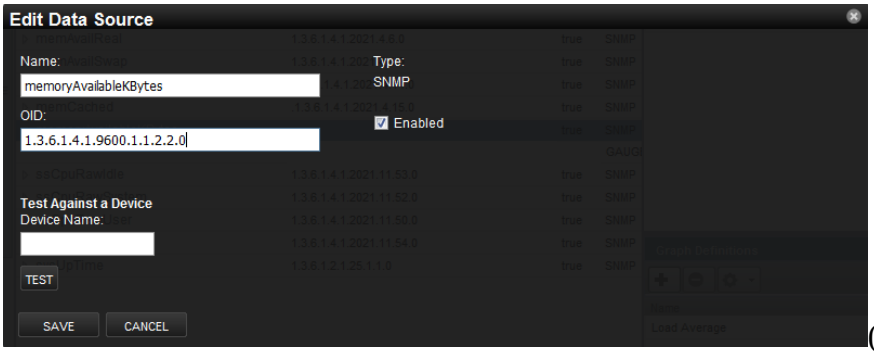
(A)

(B)

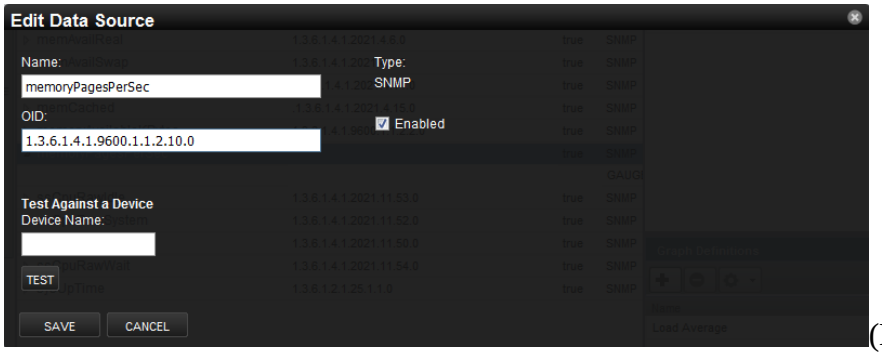
Fig 3.19 Agregado de nuevos Data Source

Se selecciona el Data Source que se creó y se oprime  para seleccionar 

apareciendo la siguiente ventana, donde el nombre aparecerá por default pero el OID lo tendremos que copiar del Template que se encuentra en las gráficas de la sección Windows.



(A)



(B)

Fig 3.20 Edición de los Data Source con su OID

Para que los datos que se recolecten sean graficados, se deben crear dichas gráficas en "Graph Definitions". Para lo cual en la gráfica de "Free Memory", solo agregamos el Data Source llamado "memoryAvailableKBytes", pues ya esta creada ésta grafica por default.

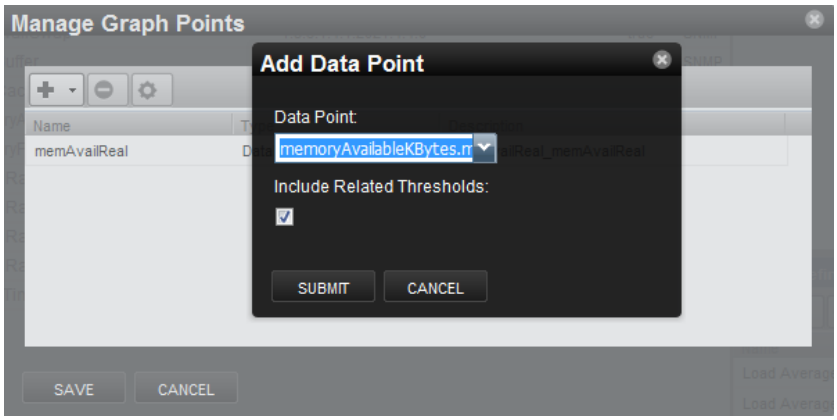


Fig 3.21 Agregar un Data Point ya existente

También se crea una gráfica llamada Paging Windows, que permite identificar el SO con el que trabaja dicha gráfica y el paginado que tiene dicho equipo.

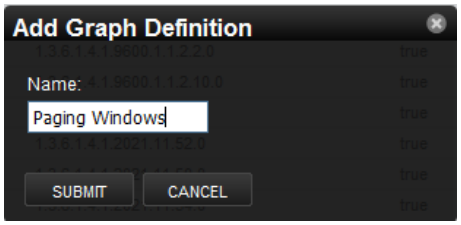


Fig 3.22 Grafica para el Paginado de equipos Windows

Se agrega el Data Source de "memoryPagesPerSec" a la gráfica

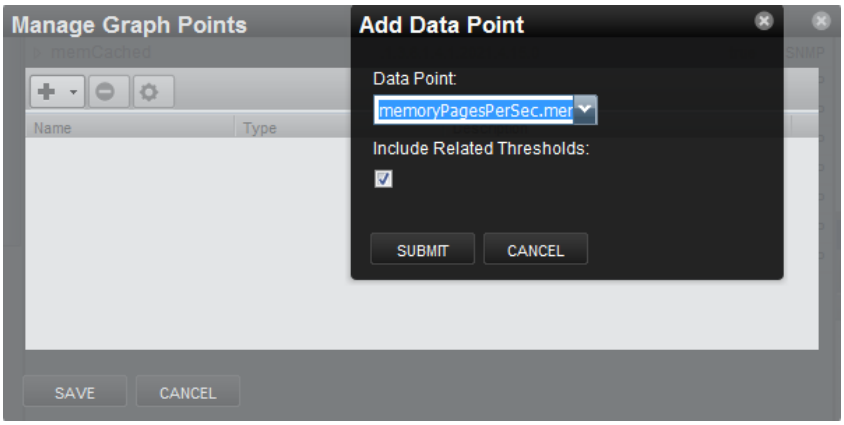
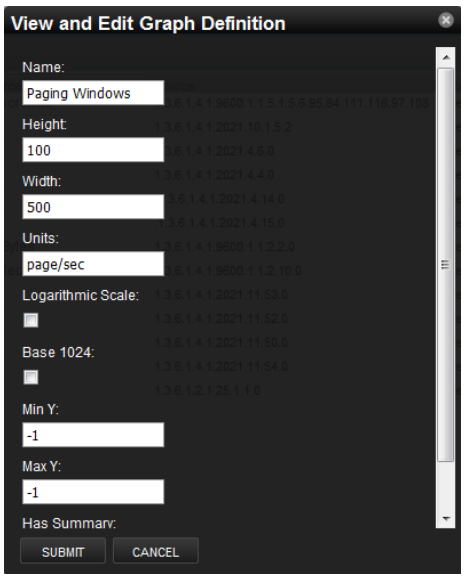


Fig 3.23Agregado del Data Point "memoryPagesPersec" para grafica

Recordando que las propiedades o definiciones de las graficas deben ser semejantes a las de la sección original de las gráficas para Windows, al menos que se requiera implementar un graficado diferente al estándar.

Gráfica Server



Gráfica Windows

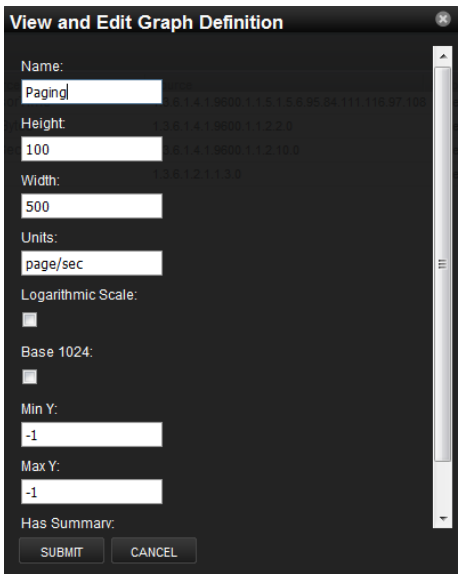


Fig 3.24 Intervalos y Valores para la gráfica

3.2 RESULTADOS DE LA GESTIÓN Y MONITOREO DEL LABORATORIO

En esta implementación se monitorearon 21 equipos con el Servidor como se muestra en la imagen, donde podemos observar su estatus, en este caso es de apagado por el cual se encuentran de color rojo, algo interesante es que se puede apreciar que el sistema detecta el último SO que utilizó en cada equipo.

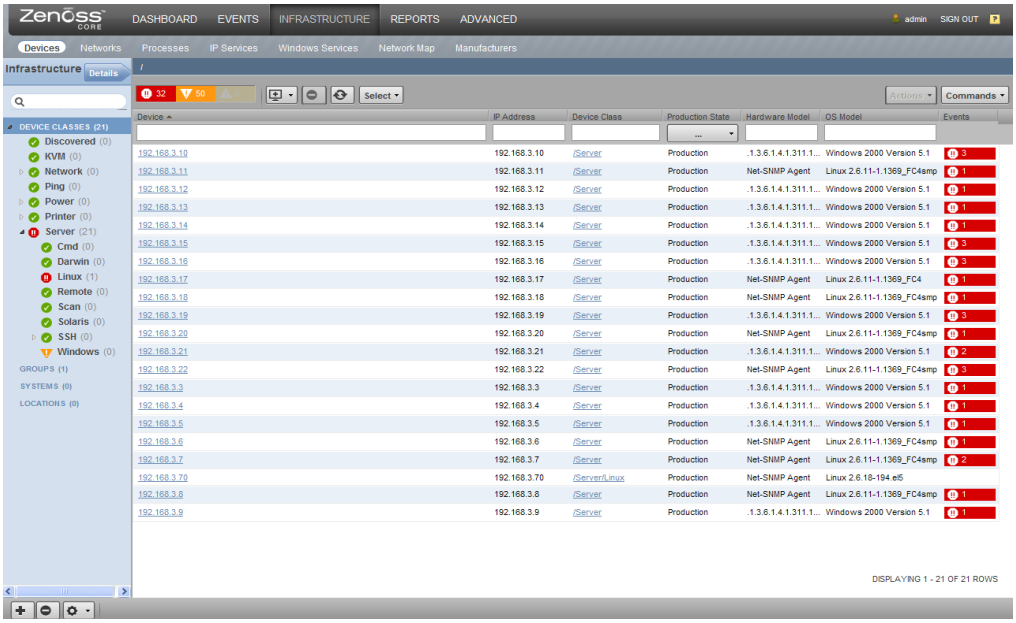


Fig 3.25 Equipos monitoreados en el laboratorio

En el monitoreo se recolectaron datos interesantes e importantes, que ofrecieron ayuda para mantener un correcto funcionamiento en la red por ejemplo; se obtuvo un inventario más completo de cada uno de los equipos, pues Zenoss muestra sus componentes tanto físicos y de software como en la siguiente imagen, en la cual se ofrece una vista general del equipo, el sistema operativo que se utilizó por última vez, la memoria ram y otros datos que ayudan a profundizar más y obtener información con mayor detalle.

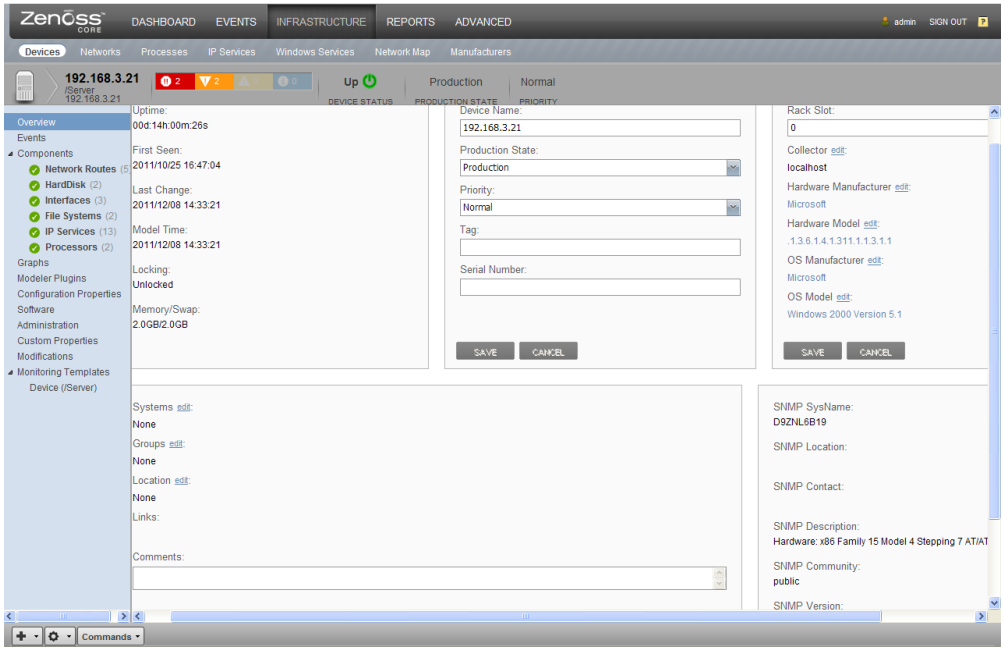


Fig 3.26 Configuración de uno de los equipos del laboratorio

Se puede observar la cantidad de disco utilizado y de espacio libre, así como su rendimiento y particiones en cada uno de los equipos que conforman la red.

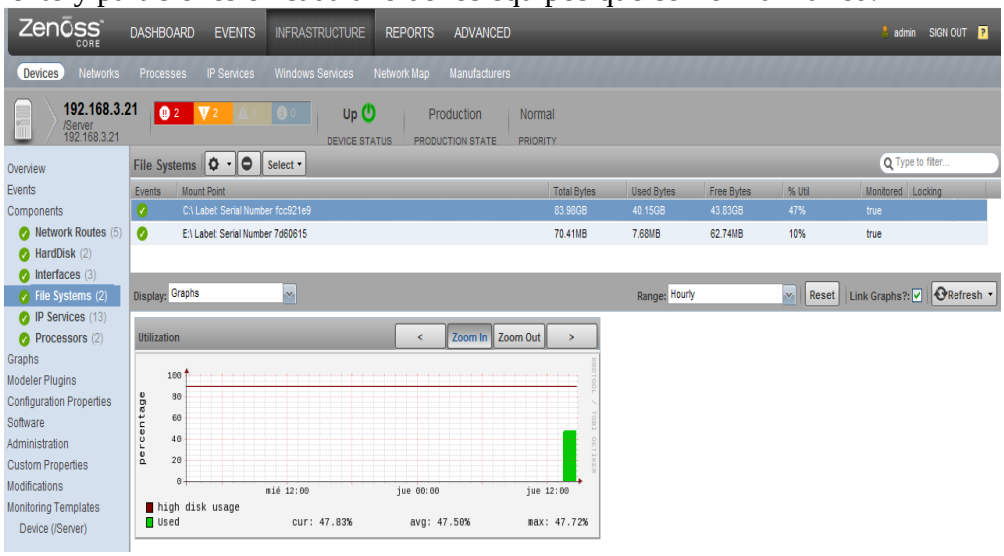


Fig 3.27 Características del Disco Duro

Se observan además, los eventos más importantes que se han presentado en el equipo, la fecha en que se presentaron, su severidad según el código de colores y muestra una pequeña leyenda del problema presentado.

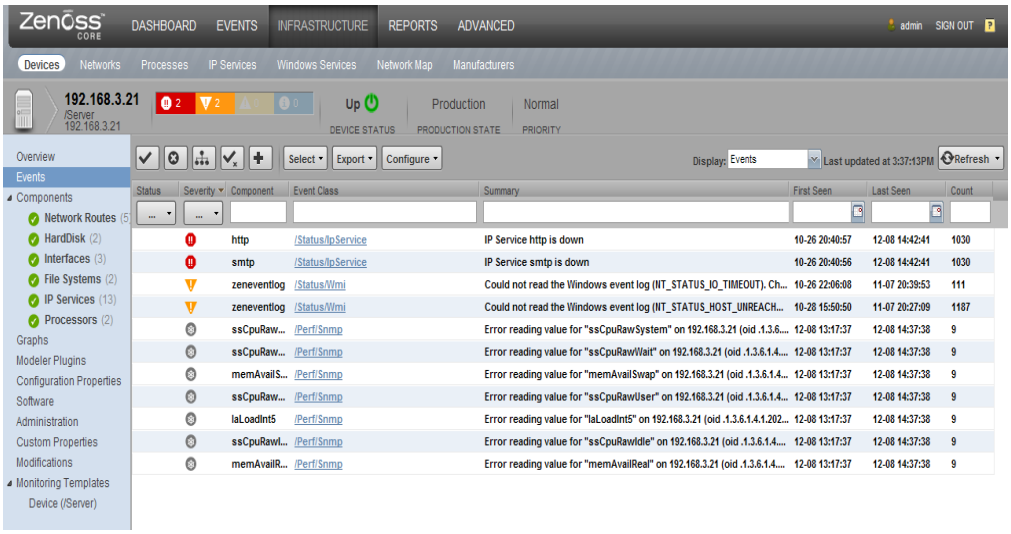


Fig 3.28 Eventos detectados en el equipo

Con esta herramienta se puede observar las gráficas de rendimiento de los componentes de cada uno de los quipos en la red. Las que se muestran a continuación fueron tomadas de un equipo con SO Windows, mostrando las graficas de rendimiento del procesador, el paginado y la memoria libre utilizada en esos momentos, el nivel de detalle se puede modificar ya sea por día e incluso horas dependiendo de cada administrador.

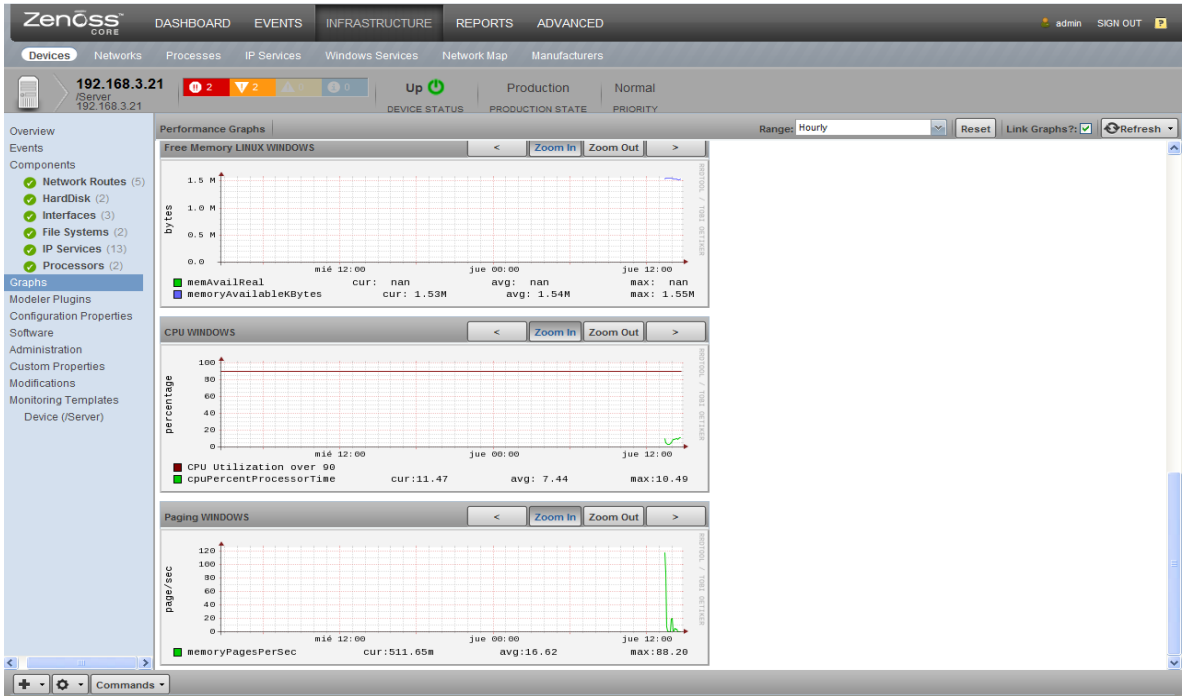


Fig 3.29 Gráficas de un equipo Windows

El tráfico que hay en las interfaces de red de cada uno de los equipos, es un elemento importante ya que, podemos verificar si el equipo trabaja de manera normal en la red o si hay algo diferente por lo cual su funcionamiento esta fuera de lo común.

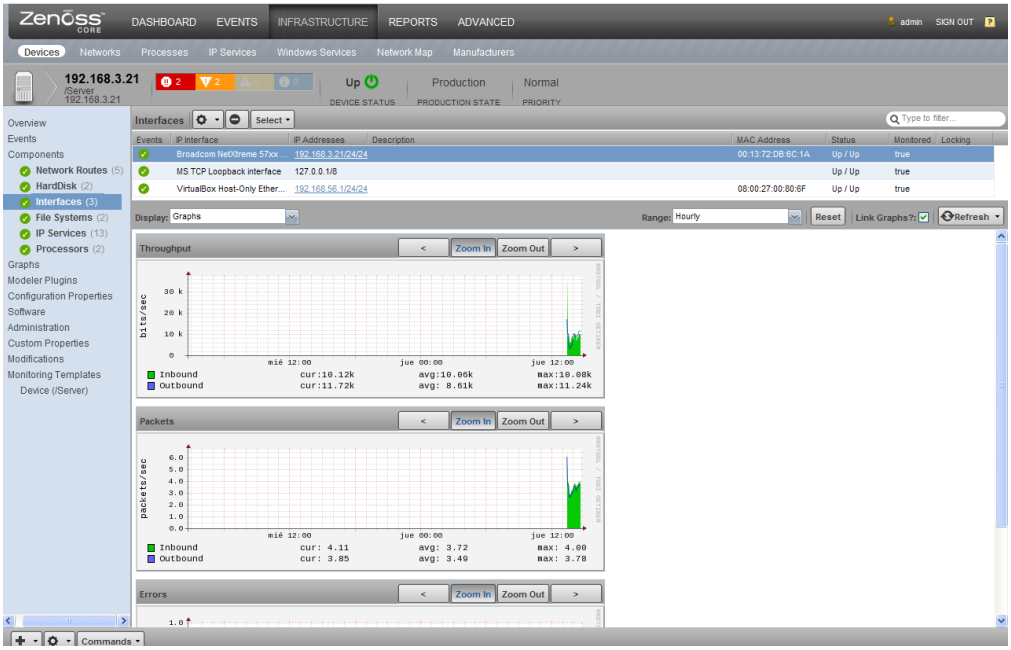


Fig 3.30 Graficas en interfaces de red

Con la gestión de esta herramienta se logra verificar los servicios funcionando correctamente y los que no en una red, así, se puede tener una gestión mejor y preestablecida para el laboratorio, por ejemplo servicios necesarios para un mejor rendimiento, o incluso identificar algunos que resulten ser una amenaza o no tan importantes en el uso del laboratorio.

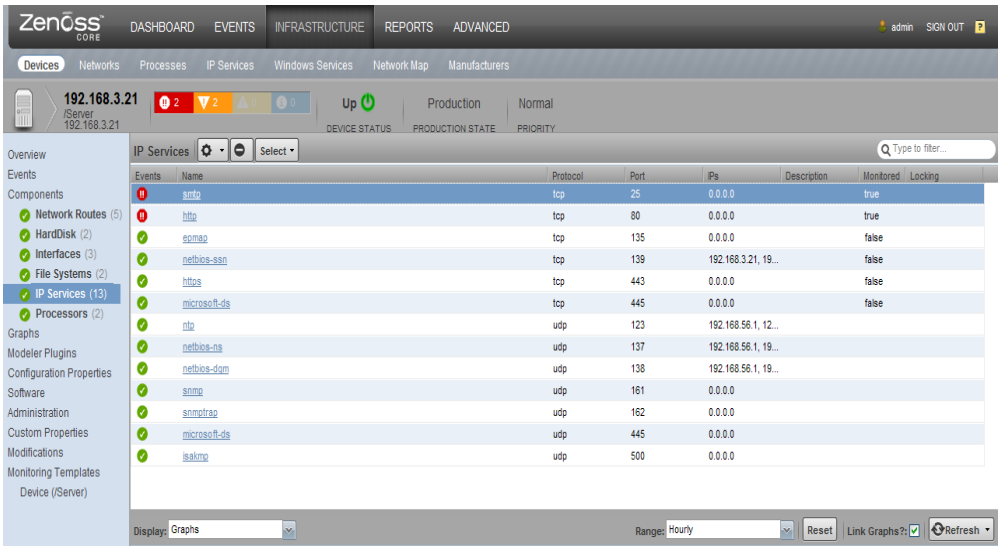


Fig *3.31Servicios IP monitoreados*

La obtención de los datos de funcionamiento general de la red son importantes, ya que ofrecen información valiosa que si se sabe aprovechar, puede ser da gran utilidad para prevenir problemas futuros y mejorar el funcionamiento y rendimiento. Entre la información más relevante que ofrece Zenoss está:

- El inventario de software con el que cuentan los equipos, para saber las herramientas más necesarias en el laboratorio y tener conocimiento de software malicioso o raro que podría llegar a perjudicar la eficiencia del laboratorio o del usuario.

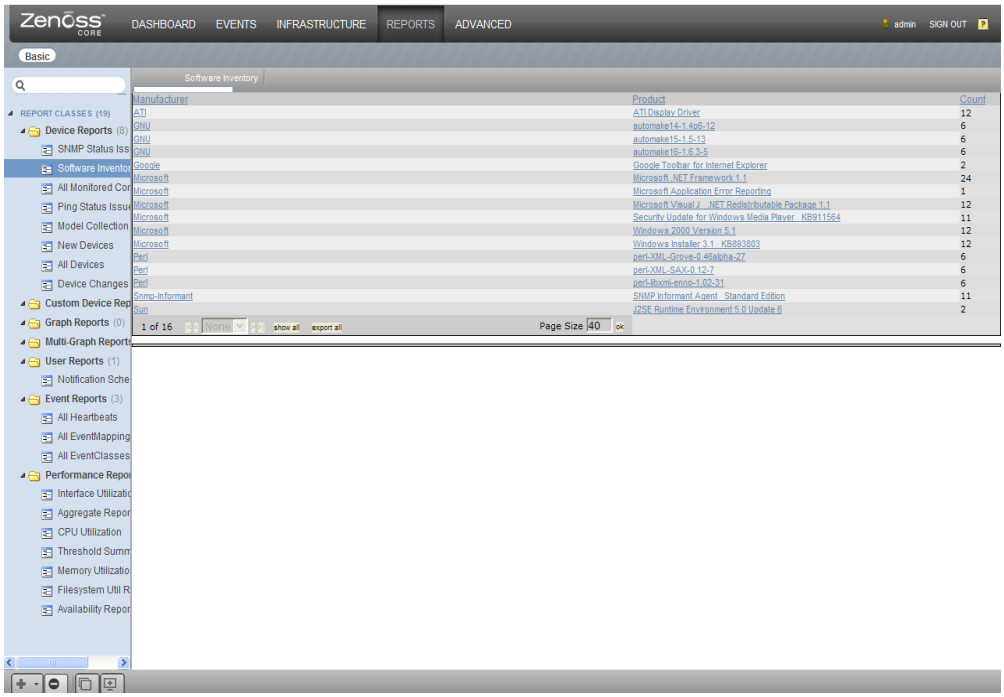


Fig 3.32 Software instalado en los equipos

- Los componentes con los que cuentan los equipos, ya que ayudan a identificar el tipo de sistema que tiene, entre otros.

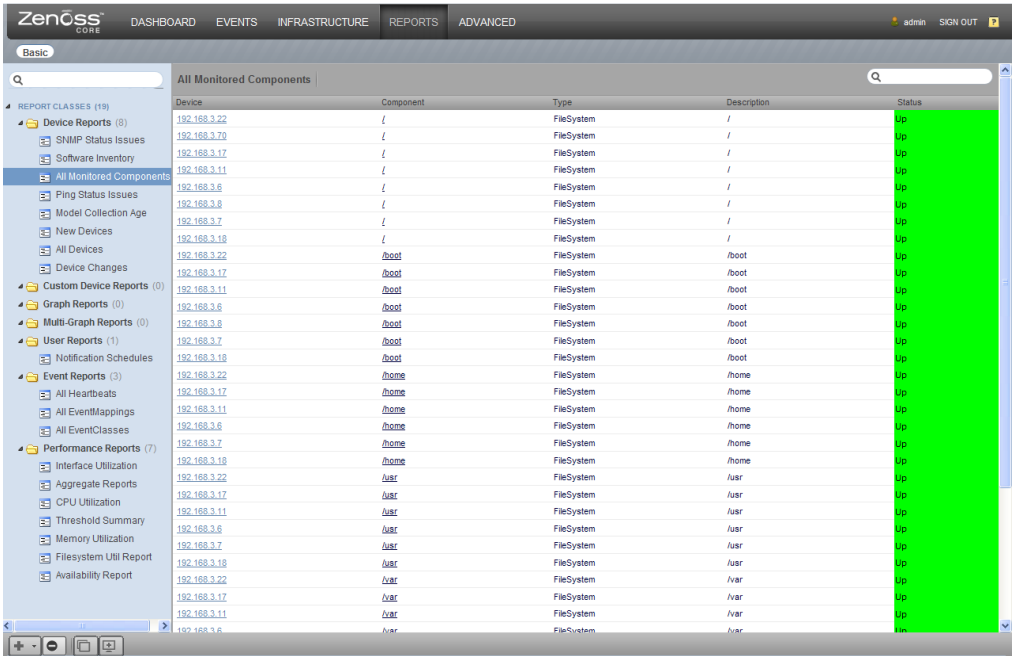


Fig 3.33 Monitoreo de los componentes y estatus del sistema

- El tener un reporte de los Discos de almacenamiento de cada uno de los equipos, así como sus particiones, puede ser importante, ya que, el saber su uso y espacio libre o estar enterados de cuales equipos necesitarán más capacidad de almacenamiento, permite hacer ver el trabajo como administrador de la red más eficiente, puesto que esta utilidad permitiría estar enterados mucho antes que el usuario de la falta de almacenamiento en su equipo.

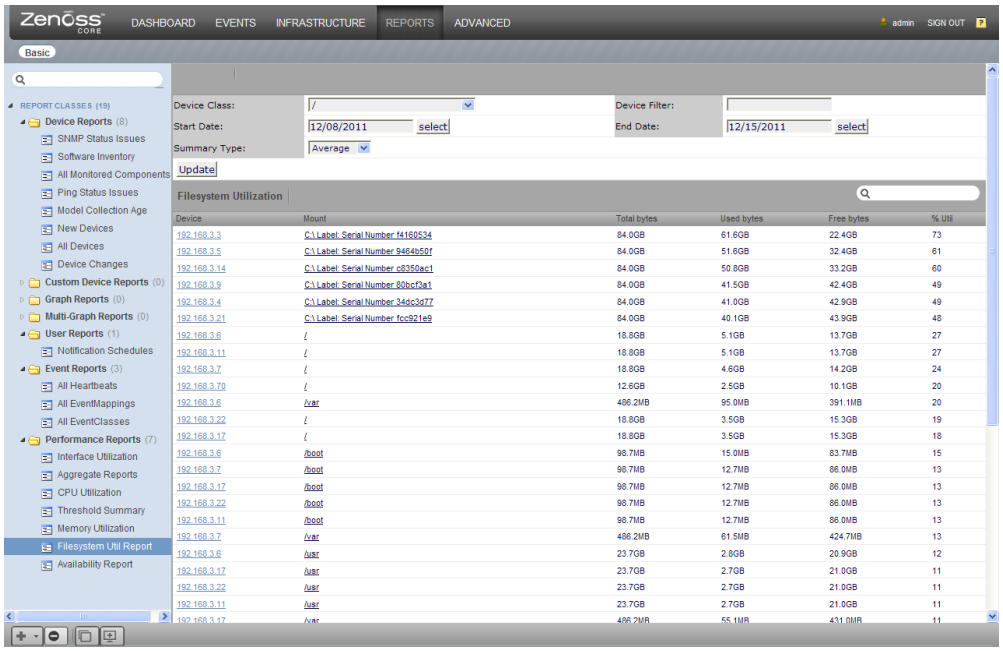


Fig 3.34 Inventario de los discos duros en la red

- Estar enterados de cuantas interfaces de red tienen los equipos y su funcionamiento; como el tráfico de entrada y salida, es también de gran utilidad para una buena gestión en la red del laboratorio, puesto que además del hardware que utiliza, podemos observar que usuarios son los que utilizan más la red e incluso que interfaces están fallando.

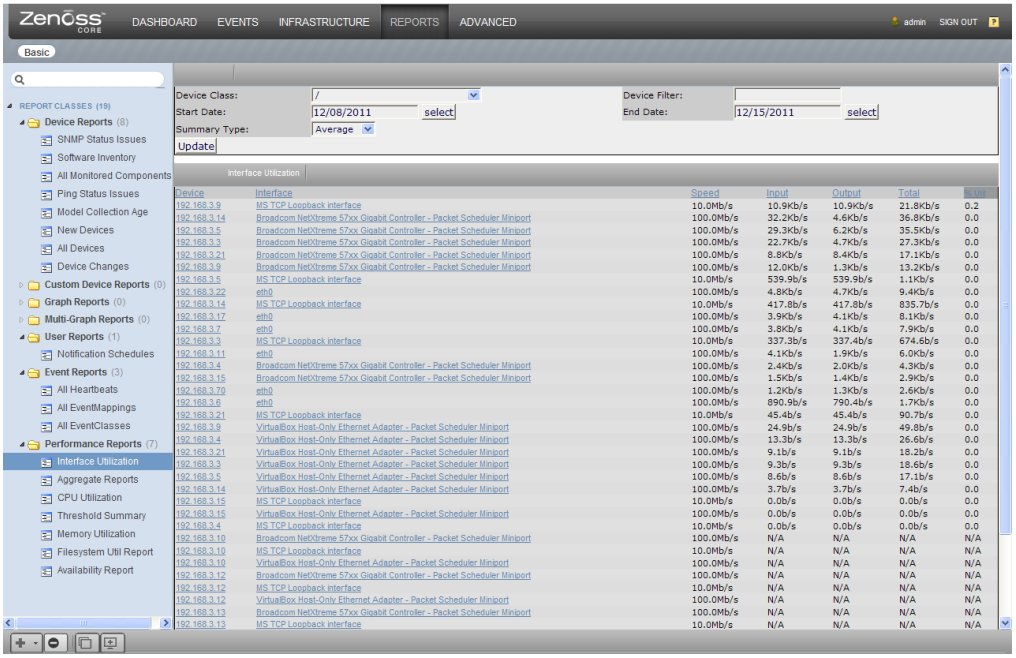


Fig 3.35 Inventario de las interfaces de red

- El saber del uso de la memoria RAM, su total y la memoria disponible para cada equipo, ofrece un inventario más completo e incluso seguridad física de los componentes en los equipos.

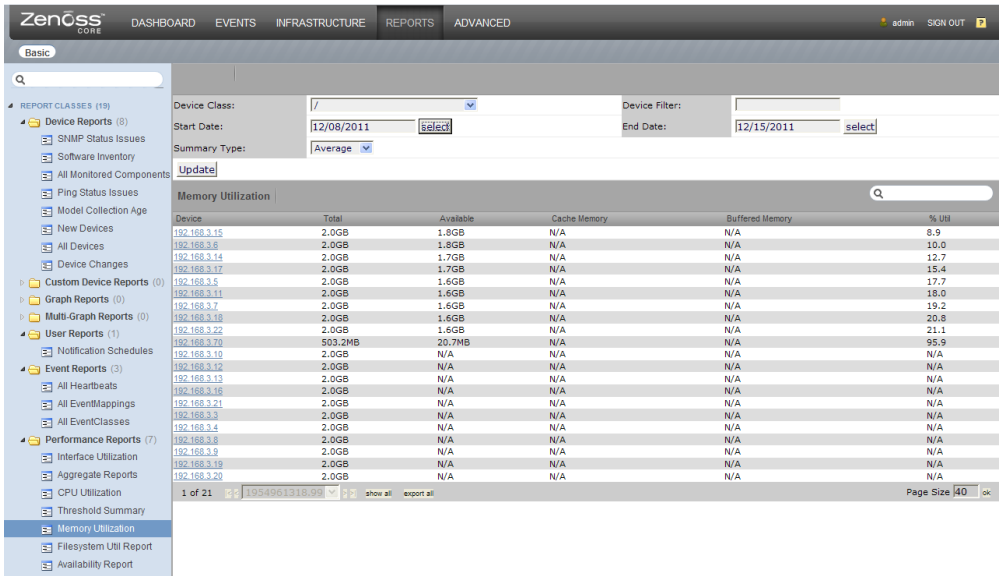


Fig 3.36 Memoria de los equipos monitoreados

A continuación se realizara un análisis detallado del monitoreo de el equipo con mayor funcionamiento en la red que es el mismo servidor Zenoss.

En esta gráfica podemos observar la carga que se presenta en el equipo contra el tiempo. Los diferentes colores muestran la cantidad de proceso que se realizó en a una determinada hora o intervalo de tiempo. En este caso el promedio de la cantidad de proceso que se realiza cada 5 min es de 0.12 ayudando a deducir que es un servidor, debido a la carga de trabajo todo el tiempo en comparación con graficas de estaciones de trabajo normales mostradas con anterioridad en las que muestran el funcionamiento del equipo en un lapso corto de tiempo.

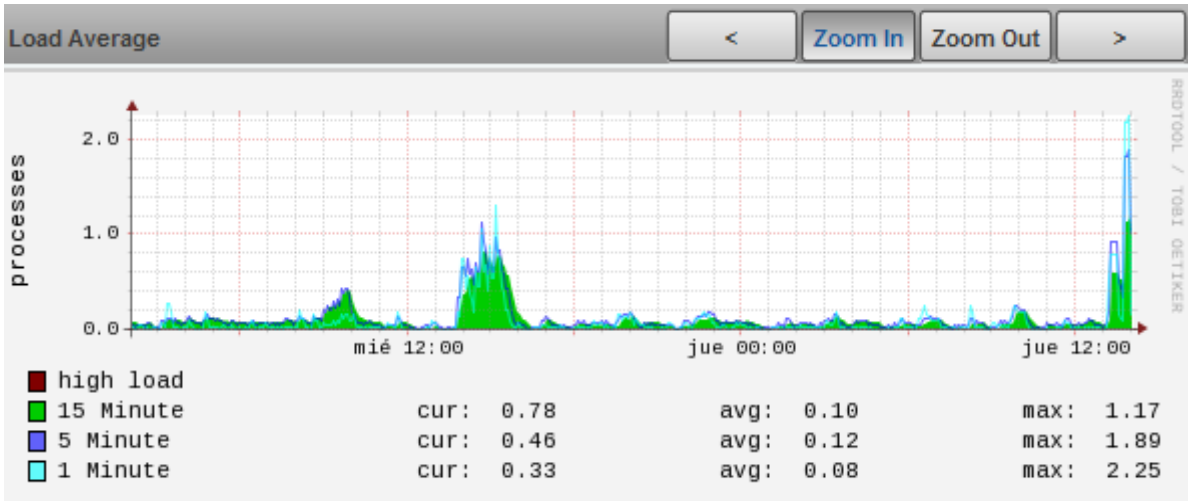


Fig 3.37 Gráfica de carga promedio en el servidor

La gráfica siguiente muestra el uso del CPU, con una simbología de cuatro colores que distinguen la utilización por sistema, usuario, cuando está en espera e inactivo; estas cuatro maneras diferentes de uso son medidas en forma de porcentaje. En esta imagen se observa que hay algunas espigas con un intervalo de tiempo constante de color azul, esto debido a que en esos intervalos se utilizaba el servidor para monitorear la red como usuario, provocando que el sistema ejecutara más procesos y llegase a un máximo del 61.5%.

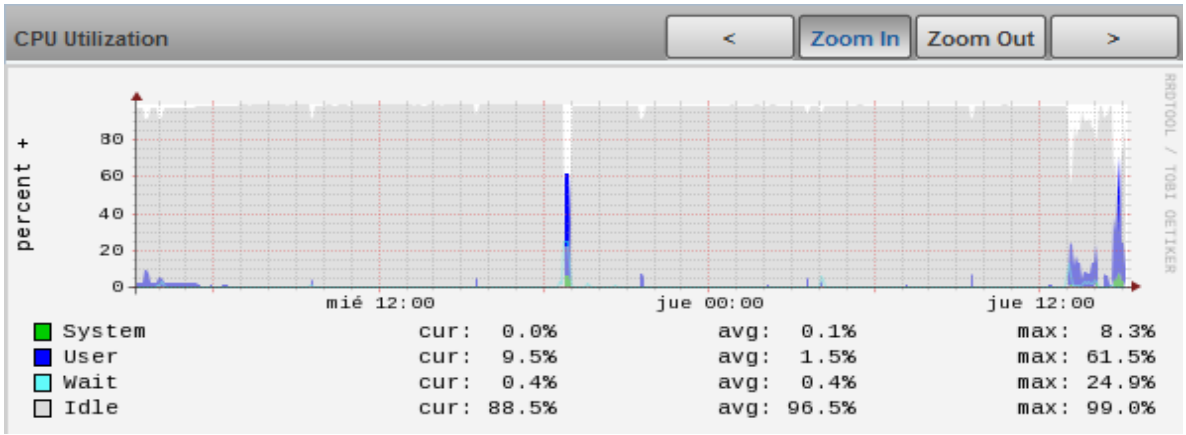


Fig 3.38 Gráfica del uso del CPU en el servidor

A continuación se muestra una gráfica en donde se puede observar el uso de la memoria, que en algunos momentos llega al 98.9% de la memoria utilizada (color verde) y el uso de la memoria volátil o swap con un promedio de 43% (color rojo), esto debido a que el equipo utiliza recursos muy limitados en (512 Ram).

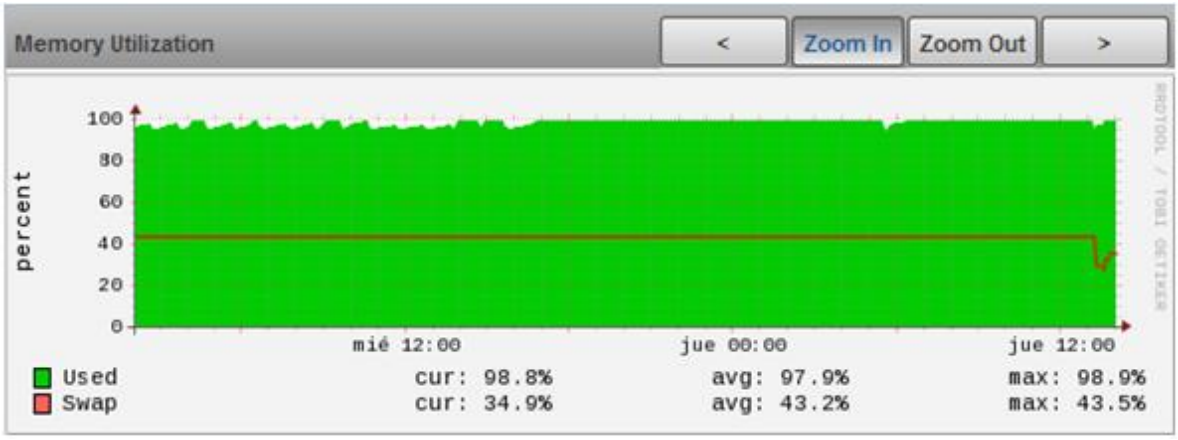


Fig 3.39 Gráfica de la memoria en el servidor

En esta gráfica se puede observar los bytes por segundo de escritura y lectura que realiza el servidor, mostrando varianza en estos procesos, pero un funcionamiento constante en el tiempo, ayudando a contemplar en que momentos se realizaron cambios o se trabajo más con el servidor.

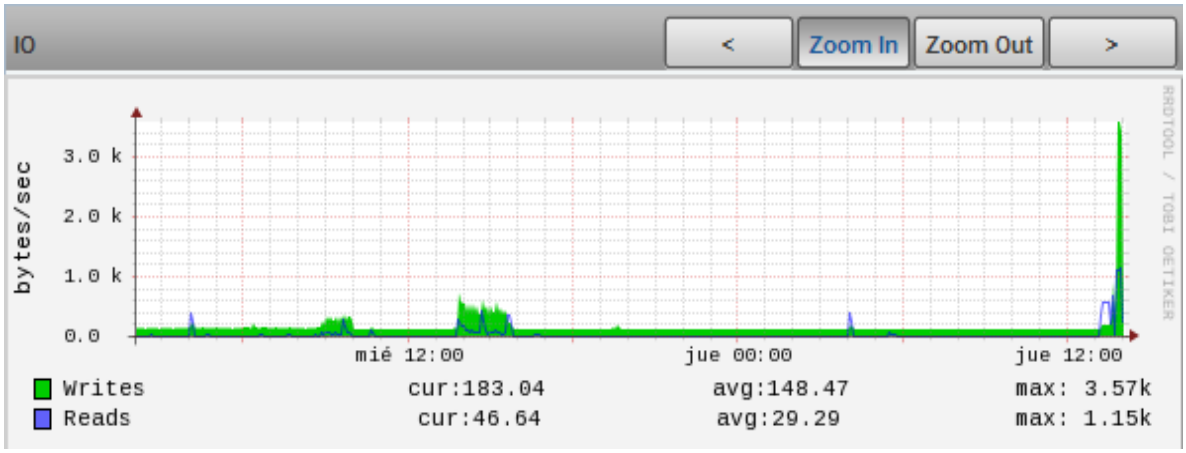


Fig 3.40 Grafica de la lectura y escritura del servidor

Zenoss también muestra en los reportes, las gráficas promedio del funcionamiento del total de la red, es decir haciendo un análisis y sacando un promedio de los valores de todos los equipos, para un análisis más completo y de manera general, basándose además en el tiempo, ya sea para verificar las gráficas promedio en la semana, al año o por mes, dependiendo del análisis necesario. Como las que se mostrarán a continuación, que fueron tomadas de forma semanal y que tienen relación con las graficas particulares.
La utilización del CPU o procesador. Aquí podemos observar el uso general de CPU en la red, es decir todos los CPU´s de los equipos que conforman la red en una sola gráfica, es por eso la diversidad de colores, pues estos representan al azar los diversos dispositivos que se agregan y son monitoreados.

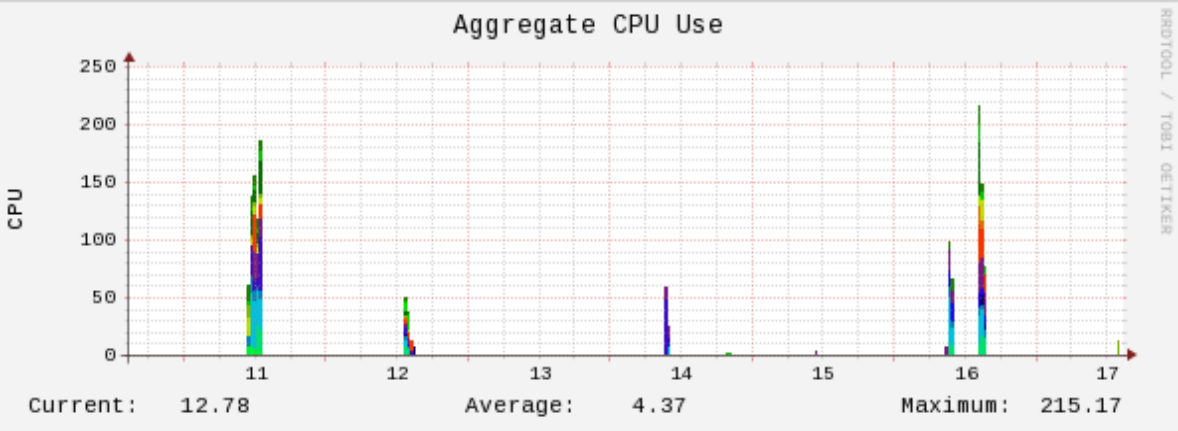


Fig 3.41 Grafica del uso promedio del CPU en la red

La memoria total libre. En la grafica siguiente se muestra la memoria libre total de los diversos equipos, teniendo un promedio de 6.70M por equipo a la semana, un máximo cuando se utilizan varios equipos de 192.69M y se muestra también la memoria libre en ese momento de 41.58 M pues no se ocupaban todos los equipos en ese momento pero si algunos.

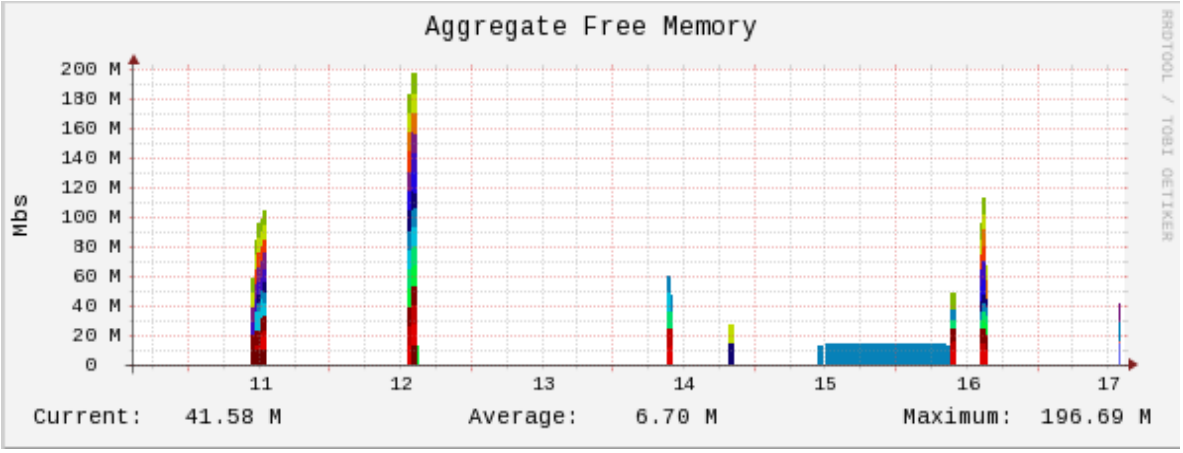


Fig 3.42 Grafica de la memoria libre promedio de la red

La memoria libre Swap. En esta gráfica, se puede observar que la memoria libre swap total, es decir que conforman todos los equipos, tuvo un promedio de 4.97M por día y llego a tener un máximo de 22.49M, el cual coincide con la memoria swap actual como se observa en los números y en la gráfica.

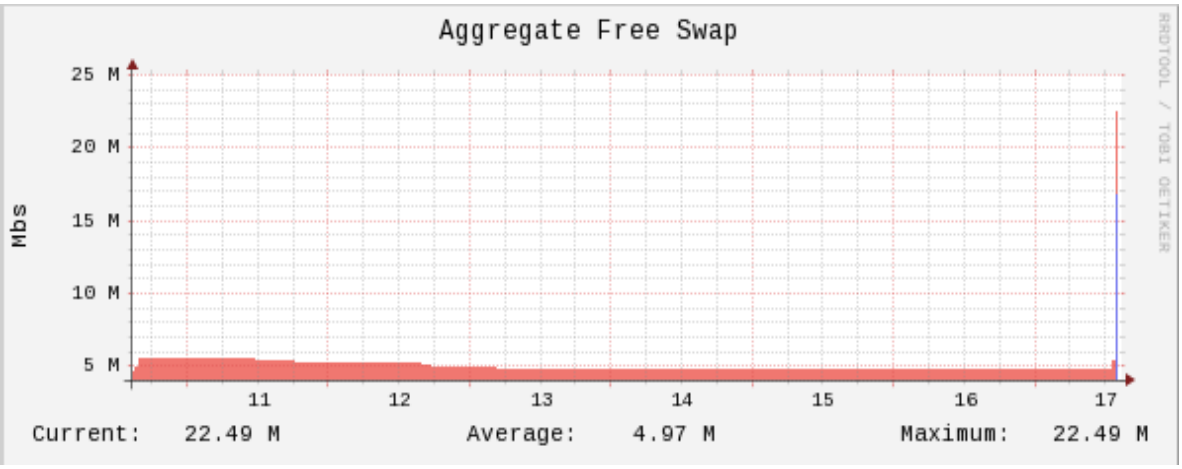


Fig 3.43Memoria Libre Swap de la red

Total de almacenamiento y su uso. Ésta gráfica muestra el total de espacio libre que se acumula al unir todos los discos de almacenamiento de los equipos en la red, el promedio de almacenamiento que abría en cada momento, e incluso el máximo almacenamiento libre que ha estado disponible cuando se encienden varios equipos.

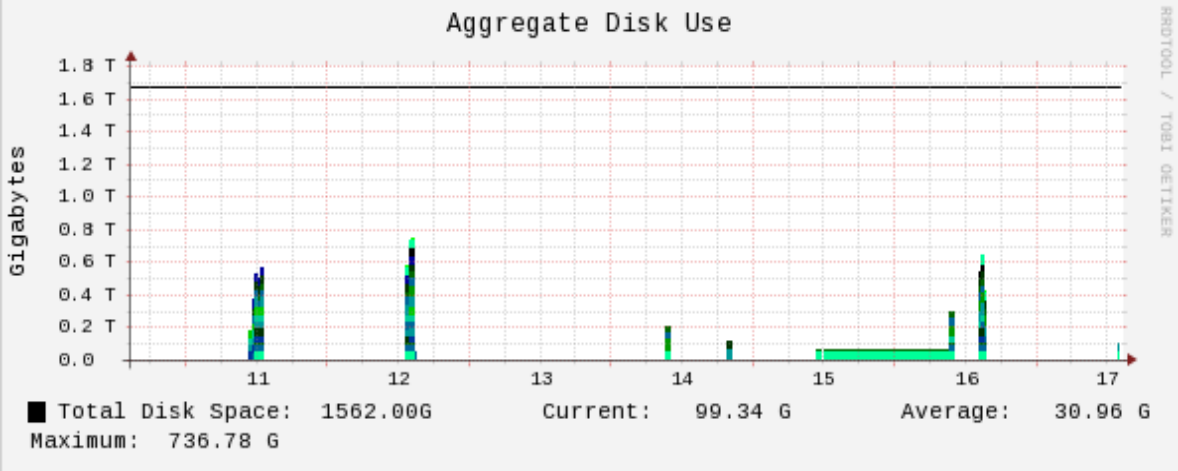


Fig 3.44 Grafica del almacenamiento total de la red

Red Entrante/ Saliente. En cuanto al tráfico promedio en las interfaces de red, tanto entrante y saliente, se puede mostrar esta grafica, en donde se observa que ha existido un máximo flujo de datos saliente de 1.47 M representados con un signo positivo y entrante de 5.67M representado con signo negativo, además, también se muestra el flujo de datos promedio y actual de todas las interfaces de red de los equipos en la semana.

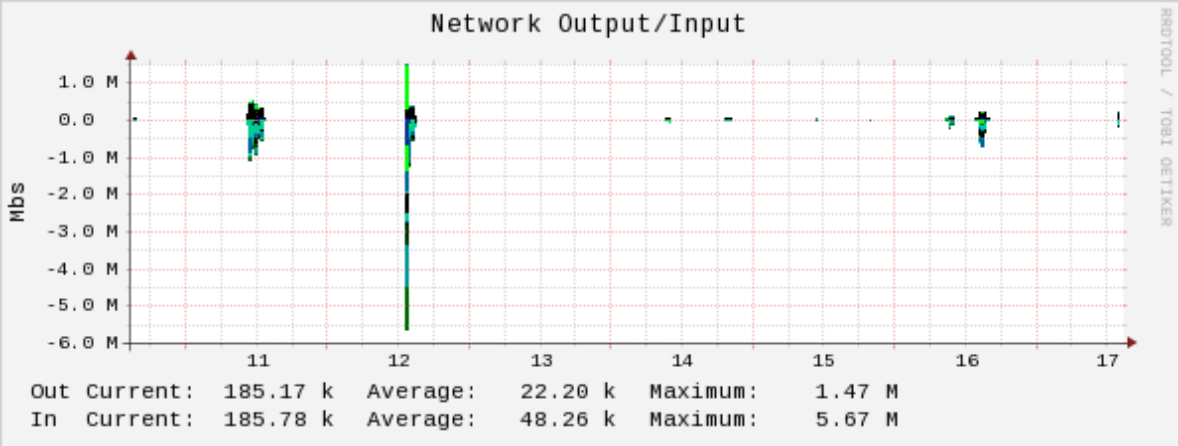


Fig 3.45 Gráfica del Flujo de datos entrante y saliente de la red

Con estos reportes, la herramienta muestra un monitoreo total del funcionamiento de la red tanto de forma particular, es decir, para cada equipo, como de manera general en la red, ayudando a mantener la seguridad y buen rendimiento en la red, manteniendo informados a los administradores de los problemas que se presenten o de anomalías que podrían llegar a suceder en el laboratorio.

Esta herramienta por ejemplo ayudo a identificar tarjetas de red que tenían fallas al desconectarse constantemente, a identificar servicios y puertos sin funcionar o cerrados en algunos equipos clientes, ha conocer la capacidad de disco duro de cada uno de los equipos y seguir su almacenamiento de manera continua, e incluso fue útil para la realización de un inventario general más exacto tanto de software como del hardware que contienen los equipos, actualizado constantemente la información de cada uno de los equipos que componen la red y sus características, para tomar acciones preventivas logrando un constante buen funcionamiento del Laboratorio al ser monitoreado.

CONCLUSIONES

Para alcanzar los objetivos propuestos fue importante la investigación y estudio de los temas mencionados, en los que se obtuvieron conclusiones importantes durante su desarrollo, las de mayor importancia se mencionan a continuación de forma más detallada.

El mencionar las bases teóricas como fueron los modelos de red, los protocolos y estándares, sirvió para recordar, para identificarlos en la implementación y para comprender mejor su uso y utilidad en la investigación, facilitando la comprensión y realización de temas posteriores, pues estos conceptos daban una visión más clara de los objetivos a lograr y de los problemas generales a resolver.

El tema de las Máquinas Virtuales fue importante, pues el conocer los tipos de virtualización que existen, sus ventajas y desventajas permitió estudiar los diferentes tipos de software existentes para este fin, observando los resultados que se obtenían y seleccionando el que tenía una mejor puntuación, eligiendo VMWare, todo con el objetivo de que la herramienta de virtualización seleccionada funcinara en el único equipo disponible el cual tenia recursos limitados tales como: 3Gigabyte en RAM, procesador de Doble núcleo AMD a 1.8 GHz y disco duro de 150 G. Esto para que la simulación a realizar fuera lo más parecida posible a la red real del laboratorio, con servicios, equipos con sistemas operativos Windows y Linux que tienen diferentes sistemas de archivos, provocando que los paquetes o programas para ser monitoreados cambie.

Antes de comenzar la simulación fue necesario conocer las caracteristicas y profundidad del monitoreo, la arquitectura de éste y técnicas existentes para elegir y realizar un análisis de la información obtenida que además ayudó al canalizarla correctamente para que sea de gran utilidad en la gestión del laboratorio, ofreciendo un panorama más claro y amplio del monitoreo en sí, lo que permitió y ayudo también para hacer la mejor elección de una de las tres herramientas con características sobresalientes en el monitoreo.

La herramienta seleccionada fue Zenoss pues cumplió con los requerimientos del laboratorio para ser monitoreado, mostrando lo importante que es el estudio y conocimiento de dichas herramientas de software para su selección y el cumplimiento de las necesidades o requerimientos que se solicitan antes de implementarla.

El desarrollar un ambiente virtual de monitoreo lo más parecido a uno real nos dio más experiencia para la implementación en el laboratorio y para solucionar problemas que se presentaron, lo más rápido y eficientemente posible, esto porque en el laboratorio se tenía que llegar con una solución directa debido al tiempo que se disponía para la implementación de la herramienta de monitoreo. Logrando incluso construir una red virtual con equipos clientes mixtos, es decir, con sistemas operativos diferentes como fueron Centos, Ubuntu y Windows que son las distribuciones más utilizadas en el laboratorio de cómputo, practicando la instalación y verificando su eficiencia y estabilidad en la red con la herramienta de monitoreo, aunque aprender a instalar la herramienta fue complicado y tardado en un ambiente virtual donde el equipo en el que se instaló contaba con pocos recursos fisicos, se logró con éxito debido a algunas configuraciones extras, aprendiendo

posteriormente el manejo de Zenoss para conocerlo mejor, lo que permitió crear una guía lo más eficiente posible, para su correcta y rápida instalación, utilizando comandos para familiarizarse con el sistema, tratando de solucionar los problemas más comunes que se iban encontrando en el camino.

Por otra parte en los equipos clientes se realizó la instalación de Agentes SNMP. Este protocolo permitió monitorear los recursos de los equipos, pero la forma en que se configura es de diferente manera en Windows y Linux para que la herramienta logré realizar un correcto monitoreo, comprendiendo con la práctica técnica lo estudiado en el capítulo del marco teórico.

Éste tema, además de ser complicado e interesante, ayudo a la motivación en la investigación, para así entender y aclarar conceptos de redes y virtualización, que posteriormente se fortalecieron con la práctica al realizar la implementación pues en la cual se tuvo que enfrentar a nuevos retos y problemas que al final fueron superados y resueltos, sirviendo de experiencia para la futura gestión con Zenoss que se realizaría en el laboratorio.

En esta parte se muestra los resultados que se obtienen al monitorear los equipos, como fueron: inventarios más completos de la red, alertas de problemas que enfrenta la infraestructura y son necesarios resolver, como fallas en las interfaces de red de algunos equipos de cómputo que se desconectaban con frecuencia, problemas de almacenamiento pues las particiones de los equipos para ciertos sistemas operativos ya se encontraban al límite, el tráfico en la red que comúnmente se genera en horas de clase y que nos permitiría saber si hay acciones raras cuando el trafico aumenta más de lo normal en los equipos. Todo esto con la intención de que el laboratorio sea gestionado y monitoreado para ofrecer un mejor servicio a los usuarios.

Los datos gráficos que se obtuvieron fueron de gran importancia ya que permitieron una interpretación fácil y rápida del monitoreo de la red, provocando un conocimiento constante del funcionamiento de ésta en torno a los equipos que la conforman y a sus características y servicios.

En general la experiencia de la realización de ésta tesis dejó gran aprendizaje y un mejor entendimiento de conceptos ya conocidos y nuevos, además de un conocimiento más amplio de la importancia en cuanto a la gestión y monitoreo de redes, como es la seguridad de la información, y la resolución de problemas en la red. El manejar la teoría y posteriormente la implementación, tanto virtual como de manera real nos deja una experiencia técnica para el manejo de herramientas como Zenoss y VMware, que con la información estadística que proporcionan se aprovechan para pasar de una cultura reactiva en donde solo se actúa ya que sucede algún problema o error a pasar a una cultura preventiva en la cual se está preparado para evitar que sucedan dichos problemas o errores y finalmente cumplir de esta manera con el objetivo que se planteó.

Como proyectos futuros se podrían realizar algunas adaptaciones, como cambiar el servidor dedicado Zenoss a un servidor virtual con mejores recursos físicos. Ya que como se pudo observar en el estudio realizado, las ventajas que ofrece la virtualizacion de servidores son mayores. Además de que se podrían adaptar equipos de red más especializados como switches y routers que vaya adquiriendo el laboratorio, pues Zenoss es escalable y se adapta a los cambios de infraestructura que llegasen a existir.

Otro de los proyectos que se podrían realizar es que la interfaz web de Zenoss sea visualizada en la página del laboratorio desde cualquier lugar con internet, permitiendo a los administradores estar al pendiente del funcionamiento del laboratorio en cualquier momento y lugar. Estas son futuras adaptaciones que se podrían realizar para mejorar el monitoreo y gestión del laboratorio en un futuro con Zenoss y que podrían ser extensiones de esta implementación.

ABREVIATURAS

ACK	Acknowledgement
API	Application Programming Interface (Interfaz de Programación de Aplicaciones)
ARPA	Advanced Research Projects Agency
ASN	Notación de Sintaxis Abstracta
BIT	Binary Digit
CISC	Complex Instruction Set Computer
CLNS/DECNet	Connectionless Network Service
CPU	Unidad de Procesamiento Central
DARPA	Defense Advanced Research Projects Agency
DLL	*Dynamic Link Library (*biblioteca de enlace dinámico*)*
DNS	Sistema de Nombre de Dominio
DoS	*Denial of Service (*DENEGACIÓN DE SERVICIO*)*
FTP	***F****ile* ***T****ransfer* ***P****rotocol*, (Protocolo de Transferencia de Archivos)
GCC	Compiler Collection (Colección de Compiladores GNU)
HEMS	High-Level Entity Management System
HTTP	*Hypertext Transfer Protocol*
ICMP	Protocolo Internet de Mensajes de Control
IHL	Longitud del Campo IP
IMAP	*Internet Message Access Protocol*
IP	Internet Protocol
ISO	Organización Internacional de Estándares
LDAP	Lightweight Directory Access Protocol
MAC	Access Control address

MILNET	MILitary NETwork
MTU	Unidades de Transmisión Máxima
NetBEUI	NetBIOS Extended User Interface (Interfaz extendida de usuario de NetBIOS
NFS	Network File System
NIC	Tarjetas de Interfaz de Red
NNTP	Network News Transport Protocol
OSI	Open System Interconexión (Interconexión de sistemas abiertos)
PDUs	Protocol Data Units (Unidades de Datos de Protocolo)
PKI	Public Key Infraestructura (Infraestructura de Claves Públicas)
QOS	*Quality of Service (*CALIDAD DE SERVICIO*)*
RAM	Random Access Memory (Memoria de Acceso Aleatorio)
RFC	Requests for Comments
RISC	Reduced Instruction Set Computer
RPC	*Remote Procedure Call* (Llamada de Procedimiento Remoto)
RTT	*Real Time Timer*
SCP	Secure CoPy
SGMP	Simple Gateway Monitoring Protocol
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SO	Sistema Operativo
SSH	Protocolo Secure Shell
SSL	Secure Sockets Layer
TCO	Total Cost of Ownership
TCP	Transmission Control Protocol

GLOSARIO

ABSTRACCIÓN DEL HARDWARE: Es un elemento del sistema operativo que funciona como una interfaz entre el software y el hardware del sistema, proveyendo una plataforma de hardware consistente sobre la cual correr las aplicaciones.

ACK: En comunicaciones entre computadoras, es un mensaje que se envía para confirmar que un mensaje o un conjunto de mensajes han llegado. Si el terminal de destino tiene capacidad para detectar errores, el significado de ACK es "ha llegado y además ha llegado correctamente", en español es conocido como acuse de recibo.

ALPARGATA (sneakernet): Proceso de copiar archivos en disquetes y dárselos a otras personas para copiarlos en sus equipos. Def : Libro Microsoft Fundamentos de redes plus.

API: Es el conjunto de funciones y procedimientos (o métodos, en la programación orientada a objetos) que ofrece cierta biblioteca para ser utilizado por otro software como una capa de abstracción. Son usadas generalmente en las bibliotecas (también denominadas comúnmente "librerías").

APLIACIÓN: Programa informático que permite a un usuario utilizar una computadora con un fin específico. Las aplicaciones son parte del software de una computadora, y suelen ejecutarse sobre el sistema operativo.

APPLETALK: AppleTalk es una pila de protocolo diseñado para proporcionar a los grupos pequeños de computadoras capacidades de red básica. // AppleTalk es una red de banda base que transfiere información a una velocidad de 230 kilobits por segundo y enlaza hasta 32 dispositivos (nodos) en una distancia de aproximadamente 300 metros mediante un conductor doble trenzado blindado denominado LocalTalk. La red utiliza un conjunto jerarquizado de protocolos similar al modelo de la ISO/OSI (Organización Internacional de Normalización/Interconexión de Sistemas Abiertos), transmitiendo la información en forma de paquetes llamados tramas. AppleTalk no es compatible con las comunicaciones por Internet, sin embargo, que es la razón principal que se está abandonando en favor de TCP/IP.

AUTENTICACIÓN: La autenticación es el proceso de detectar y comprobar la identidad de una entidad de seguridad mediante el examen de las credenciales del usuario y la validación de las mismas consultando a una autoridad determinada.

BASH: es un programa informático cuya función consiste en interpretar órdenes.

BIT: Abreviatura de *binary digit,* es la unidad más pequeña de datos en una computadora. Un bit tiene un único binario de valor, 0 o 1

BYTE: Un byte es la unidad fundamental de datos en los ordenadores personales, un byte son ocho bits contiguos. El byte es también la unidad de medida básica para memoria, almacenando el equivalente a un carácter.

CHECKPOINTS: Un método en el cálculo por el cual el estado de un programa se guarda.// Para la recuperación de la gestión de datos

CISC: (complex instruction set computer) Computadoras con un conjunto de instrucciones complejo.

CLNS/DECNet: Un servicio no orientado ala conexión que envía los datos directamente sin preguntar antes. Si la comunicación no es posible los datos se perderán. Ejemplo: servicio postal y telegráfico.

CLUSTERING: El término clúster se aplica a los conjuntos o conglomerados de computadoras construidos mediante la utilización de componentes de hardware comunes y que se comportan como si fuesen una única computadora.

DATAGRAMA: Es la estructura interna de un paquete de datos. // Paquetes de datos que se transfieren en una conexión

DLL: Es el término con el que se refiere a los archivos con código ejecutable que se cargan bajo demanda de un programa por parte del sistema operativo.

DoS: Es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.

ESTÁNDAR**:** Permite que productos de diferentes distribuidores se comuniquen entre sí, ofreciendo al comprador mayor flexibilidad en la selección y uso de los equipamientos.

EXTENSIBILIDAD: Es la cualidad que permite a un hipertexto ir de lo secuencial a lo reticular, de la línea a la red con ramificaciones no jerárquicas ni lineales, sino asociativas y multilineales. Esta cualidad se aplica tanto a una red hipertextual cerrada como a su salida a la World Wide Web. El texto se va ampliando y extendiendo a medida que optemos por seguir un enlace sea éste interno o externo al propio hiperdocumento. Y así, podemos hablar de extensibilidad interna y extensibilidad externa.// Extensibilidad.- Determina si el sistema puede extenderse y re implementado en diversos aspectos (añadir y quitar componentes). La integración de componentes escritos por diferentes programadores es un autentico reto.

FLUCTUACIÓN: Término que se refiere a la cantidad de variación de retardo que introduce la red. Una red con fluctuación cero tarda exactamente el mismo tiempo en transferir cada paquete, mientras que una red con fluctuación alta tarda mucho más en entregar algunos paquetes que otros. La fluctuación es importante al enviar audio o vídeo, que deben llegar a intervalos regulares.

FRAMES: fotograma o cuadro, una imagen particular dentro de una sucesión de imágenes que componen una animación.

GATEWAY: Una pasarela o puerta de enlace es un equipo que permite interconectar redes con protocolos y arquitecturas completamente diferentes a todos los niveles de comunicación

GCC: Es un conjunto de compiladores creados por el proyecto GNU. GCC es software libre y lo distribuye la FSF bajo la licencia GPL.

GET-RESPONSE: Este mensaje es usado para recorrer una tabla de objetos. Una vez que se ha usado un mensaje GetRequest para recoger el valor de un objeto, puede ser utilizado el mensaje GetNextRequest para repetir la operación con el siguiente objeto de la tabla. Siempre el resultado de la operación anterior será utilizado para la nueva consulta. De esta forma un NMS puede recorrer una tabla de longitud variable hasta que haya extraído toda la información para cada fila existente.

GET-REQUEST: A través de este mensaje el NMS solicita al agente retornar el valor de un objeto de interés mediante su nombre. En respuesta el agente envía una respuesta indicando el éxito o fracaso de la petición. Si la petición fue correcta, el mensaje resultante también contendrá el valor del objeto solicitado. Este mensaje puede ser usado para recoger un valor de un objeto, o varios valores de varios objetos, a través del uso de listas.

HTTP: Protocolo de transferencia de hipertexto, se diseñó específicamente para el World Wide Web: es un protocolo rápido y sencillo que permite la transferencia de múltiples tipos de información de forma eficiente y rápida.

HYPER THREADING: Es una marca registrada de la empresa Intel, para nombrar su implementación de la tecnología Multithreading Simultáneo también conocido como SMT. Permite a los programas preparados para ejecutar múltiples hilos (multi-threaded) procesarlos en paralelo dentro de un único procesador, incrementando el uso de las unidades de ejecución del procesador. Esta tecnología consiste en simular dos procesadores lógicos dentro de un único procesador físico.

IMAP: Permite a un usuario acceder remotamente a su correo electrónico como si este fuera local, con lo cual se entiende que los buzones se almacenan en el servidor

INSTANCIA DE OBJETO: es una variable

INTERFAZ: En software, parte de un programa que permite el flujo de información entre un usuario y la aplicación, o entre la aplicación y otros programas o periféricos. Esa parte de un programa está constituida por un conjunto de comandos y métodos que permiten estas intercomunicaciones.// Interfaz también hace referencia al conjunto de métodos para lograr interactividad entre un usuario y una computadora. Una interfaz puede ser del tipo GUI, o línea de comandos, etc. También puede ser a partir de un hardware, por ejemplo, el monitor, el teclado y el mouse, son interfaces entre el usuario y el ordenador. //En electrónica, un interfaz es el puerto por el cual se envían o reciben señales desde un sistema hacia otros. Por ejemplo, el interfaz USB, interfaz SCSI, interfaz IDE, interfaz puerto paralelo o serial, etc.

INTRANET: es una red de ordenadores privados que utiliza tecnología Internet para compartir de forma segura cualquier información o programa del sistema operativo para evitar que cualquier usuario de Internet pueda ingresar.

IP: es un número que identifica de manera lógica y jerárquica a una interfaz de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red del protocolo TCP/IP.

LOGS: son registros de eventos que ocurren dentro de los sistemas de información de una organización. Prácticamente todos los sistemas, servicios, aplicaciones y dispositivos en la empresa tienen capacidades de registro. Originalmente el registro de datos se utilizan para solucionar problemas de sistemas, así los sistemas y los requerimientos del negocio pueden evolucionan o actualizarse al realizar un análisis de registros.

LOOPBACK: Es una interfaz de red virtual. Las direcciones del rango 127.0.0.0/8 son direcciones de loopback, de la cual la que se utiliza de forma mayoritaria es la 127.0.0.1 por ser la primera de dicho rango.

MAC: En redes de computadoras la dirección MAC es un identificador hexadecimal de 48 bits que se corresponde de forma única con una tarjeta o interfaz de red. Es individual, cada dispositivo tiene su propia dirección MAC determinada y configurada por el IEEE (los primeros 24 bits) y el fabricante (los últimos 24 bits).

MALWARE: Cualquier programa creado con intenciones de molestar, dañar o sacar provecho en las computadoras infectadas.

MODULARIDAD: Concepto aplicado en el contexto de la informática, especialmente en la programación. Un módulo es un componente de un sistema más grande y opera dentro del sistema independientemente de las operaciones de otros componentes. La modularidad es una opción importante para la escalabilidad y comprensión de programas, además de ahorrar trabajo y tiempo en el desarrollo.

MONITOR REMOTO: se refiere a un dispositivo en una red LAN, que observa todo el tráfico en ésta y reúne información acerca de éste tráfico.

MULTICAST O MULTIDIFUSIÓN*:* es aquel que tiene un punto de origen y múltiples destinos**.**

MULTIPLEXAR: Circular mensajes destinados a distintos receptores y procedentes de fuentes distintas por la misma línea de transmisión de datos. // Técnica que permite transmitir diferentes comunicaciones a través de un único canal.

MULTIPROGRAMACIÓN: Es la técnica que permite que dos o más programas ocupen la misma unidad de memoria principal y que sean ejecutados al mismo tiempo.

NetBEUI: Protocolo de nivel de red simple que era utilizado en las primeras redes de Microsoft como LAN Manager o en Windows 95.

NETWORKING: Interconexión de cualquier grupo de computadores, impresoras, routers, switches y otros dispositivos con el propósito de comunicarse a través de algún medio de transmisión.

NODO: Un nodo es el punto de unión entre varias redes. En Internet, un nodo es un host con un solo nombre de dominio y dirección que le han sido asignados por el InterNIC (Internet Network Information Center) o ICANN (Internet Corporation for Assigned Names and Numbers).

NORMA: Una Norma con frecuencia comprende la interrelación de muchos protocolos diferentes, como es el caso del TCP/IP. Las reglas por ejemplo son un conjunto de Normas con las que se lleva a cabo un juego. Las Normas impiden que surja una situación donde dos sistemas, al parecer compatibles, en realidad no lo sean. Éstas se establecieron debido a que existen muchos fabricantes y suministradores de redes de computadoras, cada uno con sus propias ideas de cómo deben funcionar las comunicaciones.

PAQUETE: Son cada uno de los bloques en que se divide la información que se envía a través de una red en el nivel de red del modelo OSI. Cada paquete transporta la información que le ayudará a llegar a su destino – básicamente la dirección IP del que envía el paquete

PDUs: Se utiliza para el intercambio entre unidades parejas, dentro de una capa del modelo OSI.

PROCESADOR: circuito electrónico integrado que actúa como unidad central de proceso de un ordenador, proporcionando el control de las operaciones de cálculo.

PROGRAMACIÓN: Acción de programar. En computación, la programación es el proceso de escribir en un lenguaje de programación el código fuente de un software. Un término más amplio de programación puede incluir no sólo a escribir, sino a analizar, probar, depurar y mantener el código programado.

PROTOCOLOS: Son reglas y procedimientos para la comunicación. Si dos equipos están conectados entre sí (en red), a las reglas y procedimientos que dictan su comunicación son a lo que llamamos protocolos.

PROXY: Es un medio para proveer funcionalidad de gestión sobre dispositivos o elementos no compatibles mediante conversión de protocolos

QOS: Son las tecnologías que garantizan la transmisión de cierta cantidad de información en un tiempo dado (*throughput*). Calidad de servicio es la capacidad de dar un buen servicio. Es especialmente importante para ciertas aplicaciones tales como la transmisión de vídeo o voz.

REBOOT: Reiniciar el ordenador o computadora es el proceso de recargar el sistema operativo de una computadora. Por lo general se asocia al proceso de reiniciar (voluntaria o involuntariamente) la computadora cuando ya está encendida e iniciada.//Al reiniciar una computadora comienza un mecanismo llamado boot (booting).

REPOSITORIO: Depósito o archivo es un sitio centralizado donde se almacena y mantiene información digital, habitualmente bases de datos o archivos informáticos.

REPOSITORIO SUBVERSION: Es un sistema de control de versiones diseñado específicamente para reemplazar al popular CVS. Es software libre bajo una licencia de tipo Apache/BSD y se le conoce también como svn por ser el nombre de la herramienta utilizada en la línea de órdenes.
Una característica importante de Subversión es que, a diferencia de CVS, los archivos versionados no tienen cada uno un número de revisión independiente, en cambio, todo el repositorio tiene un único número de versión que identifica un estado común de todos los archivos del repositorio en un instante determinado

RFC: Son un conjunto de informes, propuestas de protocolos y estándares de protocolos utilizados por la comunidad de Internet

RISC: Computadoras con un conjunto de instrucciones reducido.

ROUTERS O RUTEADORES: Es un dispositivo o, en algunos casos software en una computadora, que determina el punto de la red por el cual un paquete debe ser enviado hacia su destino.

RPC*:* Es un protocolo que permite a un programa de ordenador ejecutar código en otra máquina remota sin tener que preocuparse por las comunicaciones entre ambos.// RPC es la transferencia sincrónica de datos y control entre dos partes de un programa distribuido a través de espacios de direcciones disjuntas.

RRDTOOL: es el acrónimo de *Round Robin Database tool*. Se trata de una herramienta que trabaja con una base de datos que maneja planificación según Round-Robin. Esta técnica trabaja con una cantidad de datos fija, definida en el momento de crear la base de datos, y un puntero al elemento actual.

SCP: Es un medio de transferencia segura de archivos informáticos entre un host local y otro remoto o entre dos hosts remotos, usando el protocolo Secure Shell (SSH).

SISTEMAS DISTRIBUIDOS: se define como una colección de computadores autónomos conectados por una red, y con el software distribuido adecuado para que el sistema sea visto por los usuarios como una única entidad capaz de proporcionar facilidades de computación.

SMTP: El objetivo del Simple Transfer Protocol (SMTP) es el transferir correos de forma fiable y eficiente.

SNIFFER: También conocido como analizador de red, analizador de protocolos o sniffer, software o hardware que puede interceptar y registrar tráfico que pasa a través de una red digital

SNMP: Protocolo básico de gestión de red, utilizado en internet para el control de redes y componentes de redes.

SOFTWARE DE APLICACIÓN: Es aquel que hace que el **computador** coopere con el usuario en la realización de tareas típicamente humanas, tales como gestionar una contabilidad o escribir un texto.

SSH (Secure Shell): Es un protocolo de acceso remoto seguro a otros servicios de red a través de una red insegura.

SSL(Secure Sockets Layer): Proporciona autenticación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía. Habitualmente, sólo el servidor es autenticado (es decir, se garantiza su identidad) mientras que el cliente se mantiene sin autenticar.// El objetivo principal del protocolo SSL es proveer privacidad y fiabilidad entre dos aplicaciones que se comunican.

SUPERÁMBITOS: es un agrupamiento administrativo de ámbitos que se puede utilizar para admitir varias subredes con IP lógicas en la misma subred física. Los superámbitos resultan útiles para volver a numerar o ampliar el rango de direcciones IP sin que afecte a los ámbitos activos.

STREAM: Es una especie de canal a través del cual fluyen los datos. Técnicamente, un stream es el enlace lógico utilizado por el programador, para leer o escribir datos desde y hacia los dispositivos estándar conectados a la PC.

SYN: Es un bit de control dentro del segmento TCP, que se utiliza para sincronizar los números de secuencia iniciales ISN de una conexión en el procedimiento de establecimiento de tres fases (*3 way handshake*). Se usa para sincronizar los números de secuencia en tres tipos de segmentos: petición de conexión, confirmación de conexión (con ACK activo) y la recepción de la confirmación (con ACK activo).

TOKEN: Un token es una serie especial de bits que viajan por las redes token-ring. Cuando los token circulan, las computadoras de la red pueden capturarlos. Los token actúan como tickets, permitiendo a sus dueños enviar un mensaje por la red. Existe sólo un token por cada red, por lo tanto no hay posibilidad que dos computadoras intenten transferir mensajes al mismo tiempo.

TRAMA: Una trama de datos es una estructura lógica y organizada en la que se pueden colocar los datos.\\ el PDU de la capa de enlace de datos.

FUENTES DE INFORMACIÓN

LIBROS

[1] Titulo: Aprendiendo TCP/IP en 14 días (segunda edición) *Autor: Tim Parker Editorial: PRICE-HALL HISPANOAMERICANA, S.A.*

[2] Titulo: Libro Microsoft de Fundamentos de redes Plus Curso oficial de certificación de MCSE, *Autores: Antonio Vaquero Sánchez, Gerardo Quiroz Vieyra. Editorial.McGraw-Hill/Interamericana de España, S. A. U. Edicion Original Inglesa 2000 por Microsoft Corporation, Aravaca Madrid, 623 páginas.*

[3] Título: Redes Globales de Información con Internet y TCP/IP Principios básicos, protocolos y arquitectura (Tercera Edición), *Autor: DOUGLAS E. COMER, Editorial: Prentice-Hall Hispanoamericana, S. A.*

[4] Titulo: CCENT/CCNA ICND1 Official Exam Certification Guide Second Edition. Autor. Wendell Odom, CCIE No.1624 Editorial: Cisco Press

[5] Titulo: Tecnologías de interconectividad de redes *Autor: Merilee Ford, H. Kim Lew, Steve Spanier, Tim Stevenson Editorial: Prentice Hall Hispanoamericana, S.A.*

[6] Titulo: Sistemas Operativos Una visión aplicada *Autor: Jesús Carretero Pérez, Félix García Carballeira, Pedro de Miguel Anasagasti, Fernando Pérez Costoya. Editorial McGraw-Hill/ Interamericana de España, S.A.U fecha: marzo 2004*

[7] Titulo: Seguridad en Microsoft Windows XP y Microsoft Windows 2000 Running+, *Autor: Bott, Ed; Siechert, Carl Editorial: McGraw-Hill/ Interamericana de España, S.A Edición 1*

[8] Titulo: Informática para cursos de Bachillerato, *Autor: Gonzalo Ferreyra Cortés. Editorial: Alfaomega*

[9] Título : SNMP, SNMPv2, SNMPv3, and RMON 1 y 2 Third Edition Autor: William Stallings Editorial: ADDISON-WESLEY No TK5105.5 S737 1999 G.-185136

[10] Título: Network Management - Problems, Standards and Strategies Autor: Franz-Joachim Kauffels Editorial: ADDISON-WESLEY PUBLISHING COMPANY No TK5105.5 K421 G-122472

[11] CCNA Exploration / Accesso a la WAN / 8 Resolución de problemas de red / 8.1 Establecimiento de base de rendimiento de la red / 8.1.3 ¿Por qué es importante establecer una línea de base de red? (8.1.3.1).

[12] CCNA Exploration / Aspectos básicos de networking / 1 La vida en un mundo centrado en la red / 1.4 Arquitectura de internet / 1.4.1 Arquitectura de red (1.4.1.1)

PDF´s

[13] TÍTULO: El modelo OSI y los protocolos de red, Capitulo 2, *sin autor.*
http://blyx.com/public/docs/pila_OSI.pdf
(pila_OSI) (20/05/2012)

[14] TÍTULO: Fundamentos de comunicaciones y redes de datos. Versión 0.2. *Autores:Diego A. López García, Manuel Sánchez Raya. Escuela Politécnica Superior Universidad de Huelva*
http://www.uhu.es/diego.lopez/redes0607/NT1-REDES-06.pdf
(NT1-REDES-06.pdf) (20/05/2012)

[15] TÍTULO: Capas de sesión, presentación y aplicación. *Autor:Danielle Romero*
http://www.elrinconcito.com/articulos/Sesiones/sesiones.pdf
(sesiones.pdf) (10/11/2011)

[16] TÍTULO: Apuntes de Redes de Datos. *Autor: Jorge E. Pezoa Núñez Universidad de Concepción Facultad de ingeniería, Depto. De Ingeniería Eléctrica*
ftp://ftp.puce.edu.ec/Facultades/Ingenieria/Sistemas/Network%20news/redes.pdf
(redes.pdf) (10/11/2011)

[17] TÍTULO: Laboratorio de Redes. Diseño y configuración de redes de computadoras. Capitulo 2: Capa Física. *Autor: Ing. Mauricio Bísaro, Ing. Eduardo Danizio.*
http://traficoweb.googlecode.com/files/Capitulo_02_Capa_Fisica.pdf
(Capitulo_02_Capa_Física.pdf) (20/05/2012)

[18] TÍTULO: REDES. TEMA 2: LA CAPA FÍSICA. *Autor: Universidad de Oviedo. Ingeniería de Sistemas y Automática*
http://www.isa.uniovi.es/docencia/redes/Apuntes/tema3.pdf
(tema3.pdf) (20/05/2012)

[19] TÍTULO:Análisis de seguridad de la familia de protocolos TCP/IP y sus servicios asociados. TCP/IP Security (Primera Edición) *Autor: Raúl Siles Peláez*
http://www.arcert.gov.ar/webs/textos/Seguridad_en_TCP-IP_Ed1.pdf
(Seguridad_en _TCP-IP_Ed1.pdf).(10/11/2011)

[20] TÍTULO: Interconexión de redes (Internetworking) Sistemas operativos *Autor: Vanesa Solange Roffé. Uniersidad Nacional del Nordeste. Facultad de Ciencias Exactas y Naturales y Agrimensura.Licenciatura en Sistemas de Información.*
http://200.45.54.90/depar/areas/informatica/SistemasOperativos/Informe_SO_08.pdf
(Informe_SO_08.pdf) (20/05/2012)

[21] TÍTULO: Analisis de la virtualización de sistemas operativos. *Autor: Albert López Medina. Universidad de Barcelona, Facultad de Matemáticas, Ingeniería Técnica en Informática de Sistemas.*
http://www.maia.ub.es/~sergio/pfcs/An%C3%A1lisis%20de%20la%20virtualizaci%C3%B3n%20de%20sistemas%20operativos.pdf
(Tesis de virtualizacion) (15/01/2012)

[22] TÍTULO: Maquinas Virtuales. *Autor: Jairo Hidalgo Róman UTPL(Universidad Técnica Particular de Loja), Escuela de Electrónica y Telecomunicaciones Sistemas operativos "C" UTPL(Universidad Técnica Particular de Loja), Escuela de Electrónica y Telecomunicaciones Sistemas operativos "C"*
http://blogs.utpl.edu.ec/sistemasoperativos/files/2010/01/maquinas-virtuales-centos.pdf
(maquinas-virtuales-centos.pdf) (20/05/2012)

[23] TÍTULO: Virtualización corporativa con VMware *Autor: Irochka, Josep Ross, vExpert. Ncora Information Technology S.L. Av. Catalunya 7 2° 4° - 43830 Torredembarra (Spain) http://www.libro-vmware.com/muestra.pdf*
(muestra.pdf) (20/05/2012)

[24] TÍTULO: Máquinas Virtuales (Virtualización de Hardware) *Autor: Sofía Ramos Ortiz*
http://www.jeuazarru.com/docs/Maquina_virtual.pdf
(Maquina_Virtual.pdf) (20/05/2012)

[25] TÍTULO: Sistemas operativos, Maquinas Virtuales *Autor: Andrea Leonor Jaramillo Armijos Escuela de Electrónica y Telecomunicaciones*
http://blogs.utpl.edu.ec/sistemasoperativos/files/2010/01/maquinas-virtuales3.pdf
(PDF Maquinas_virtuales3) (20/05/2012)

[26] TÍTULO: Ventajas y consideraciones sobre la virtualización Infraestructura de Hardware *Autor: M.C. Rodrigo Morteo Ortiz*
http://morteo.isotecmexico.com/Publications/whitepapers/wp_virtuaizacion.pdf
(wp_virtualización.pdf) (20/05/2012)

[27] TÍTULO: Maquinas virtuales: Una alternativa para PYMES, Soluciones para empresas *Autor: Daniel García revista LINUX+ 5/2009*
http://www.iniqua.com/wp-content/uploads/2009/04/18_19_20.pdf
(18_19_20.pdf) (20/05/2012)

[28] TÍTULO: Sistemas Operativos *Autor: Pablo Ruiz Múzquiz Un libro libre de Alqua.madeincommunity Versión 0.5.0*
http://forja.rediris.es/frs/download.php/1922/SSOO-0_5_0.pdf
(SSOO-0_5_0.pdf) (20/05/2012)

[29] TÍTULO: Sistemas Operativos *Autor: Magister David Luis la Red Martínez. Profesor Titular por Concurso de "Sistemas Operativos". Licenciatura en sistemas de Información. Departamento de Informática. Universidad Nacional Del Nordeste U.N.N.E-Argentina*
http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/sistope2.PDF

(sistope2.pdf) (20/05/2012)

[30] TÍTULO: El Sistema Operativo Windows Capitulo II *Autor: Marcelo Romo Proaño, M.Sc. Escuela Politécnica del Ejercito – Ecuador.*
http://publiespe.espe.edu.ec/librosvirtuales/informatica-basica/informatica-basica/informatica-basica02.pdf
(SO Windows.pdf) (20/05/2012)

[31] TÍTULO: Accesibilidad de los sistemas operativos Windows y Linux *Autor: Joaquim Fonoll y Antonio Sacco. Departamento Educación Generalitat de Cataluña, España. Universidad Abierta Interamericana de Buenos Aires, Argentina.*
http://publiespe.espe.edu.ec/librosvirtuales/informatica-basica/informatica-basica/informatica-basica02.pdf
(Informatica-basica02) (20/05/2012)

[32] TÍTULO: Curso Open LDAP Autor: Jose Manuel Suárez COA Sistemas Informáticos Avanzados Versión 1.0
http://www.redes-linux.com/manuales/openldap/curso_openldap.pdf
(curso_openldap.pdf) *(20/05/2012)*

[33] TÍTULO: ANÁLISIS Y DETERMINACION DE PATRONES DE TRÁFICO DE PROTOCOLOS EN REDES LAN. *Autor: Santiago Pérez, Higinio Pacchini, Gustavo Mercado. Facultad Regional Mendoza, Universidad Tecnológica Nacional.*
http://gridtics.frm.utn.edu.ar/docs/POSTER%20WICC07%20TRAFICO.pdf
(POSTER WICC07 TRAFICO.pdf) (20/05/2012)

[34] TÍTULO: Interfaz para monitoreo de redes de comunicaciones mediante una aplicación web *Autor: Hugo Solano Vera. Universidad de las Américas Puebla*
(portada) http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/solano_v_h/portada.html
(capítulo) http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/solano_v_h/capitulo1.pdf
(Monitoreo de red.pdf) (20/05/2012)

[35] TÍTULO: Cap.24 Seguridad de redes de computadoras *Autor: Alcocer Carlos*
http://biblioteca.pucp.edu.pe/docs/elibros_pucp/alcocer_carlos/24_Alcocer_2000_Redes_Cap_24.pdf
(Seguridad en redes de datos.pdf) (20/05/2012)

[36] TÍTULO: Resumen Protocolos de Monitorización por Mz v1-0 Autor: Mario Zalzar
http://docente.ucol.mx/al986138/public_html/MARIO/adm_redes/Resumen%20Protocolos%20de%20Monitorizacion%20por%20Mz%20v1-0.pdf
(Resumen Protocolos de Monitorizacion por Mz v1-0) *(20/05/2012)*

[37] TÍTULO: Seguridad Perimetral "Monitoreo de recursos de red" Autor: Ing. Carlos Alberto Vicente Altamirano. Universidad Nacional Autónoma de México- DGSCA.
http://juliorestrepo.files.wordpress.com/2011/04/monitoreo.pdf
(monitoreo.pdf) (20/05/2012)

[38] TÍTULO:Una Herramienta de Gestión de Redes Virtuales *Autor: Abraham Jorge Jiménez Alfaro. Universidad Autónoma Metropolitana. Tesis para Obtener el Grado de Maestro en Ciencias de la Computación.*
http://newton.azc.uam.mx/mcc/01_esp/11_tesis/tesis/terminada/jimenez_alfaro_abraham_jorge.pdf
(jimenez_alfaro_abraham_jorge.pdf) (20/05/2012)

[39] TÍTULO: Notas sobre TMN (Telecomunications Management Network)*Autor: Sin Autor*
http://www.eie.fceia.unr.edu.ar/ftp/Tecnologias%20de%20banda%20angosta/Notas_sobre_TMN.pdf
(Notas_sobre_TMN.pdf) (15/01/2012)

[40] TÍTULO: Redes de Computadoras II Administración de redes *Autor: Sin Autor*
http://www.ciudadranelagh.com.ar/unlz/unocursada/Redes%20de%20Computadoras/ClaseAdmRedes_unlz.pdf
(ClaseAdmRedes_unlz.pdf) (10/11/2011)

[41]TÍTULO: Sistema de Monitoreo Zenoss en Ubuntu 8.04 *Autores: Alejandro Arboleda, Andrés López, Andrés Restrepo, Eder García, Joman Robledo, Daniel Valencia, Rodolfo Herrera, Alejandra Gutiérrez.*
http://es.scribd.com/doc/63100607/Manual-Sistema-de-Monitoreo-Zenoss-en-Ubuntu-8
(Manualsistema-de-Monitoreo-Zenoss-en-Ubuntu-8.pdf) (20/05/2012)

[42]TITULO: MOMITOREO, ADMINISTRACIÓN Y GESTION EN LINUX (Titulación Administración en Redes) *Autores: Erica Uribe, Andres Deossa, Ana Carrilo, Danilo Gutierrez, Vanessa Valenzuela, Lina Marcela, Sandra Viviana.*
http://www.slideshare.net/andreslds/gestion-y-monitoreozenoss-presentation
(Gestion y Monitoreo con Zenoss.pdf) (20/05/2012)

[43]TÍTULO: Monitoreo. Administración y Gestión Integral de una red en Linux Proyecto II *Autores: Marcelo Esteban Henao, Carlos Córdoba , Jenny Gonzáles, Luisa ernanda Arias, Luz Dary Tequia, Luisa Fernanda Rave, Katerine Luna Ruiz, Yenith Maritza Rodríguez. Centro de Servicio y Gestión Empresarial Medellin.*
2008http://es.scribd.com/doc/8761567/3/Zenoss
(Monitoreo- Gestion-y-Administracion-de Una-Red-Con-Zenoss-en-Debian-Etch.pdf)
(20/05/2012)

[44]TÍTULO: Manual de Monitoreo y gestión Zenoss core, Bajo el Sistema Operativo : Debian lenny betta2, *Autores: Natalia Valencia Gallego, Fernanda Orozco Pineda, Cristina Piedrahita, Roger Olarte. Instituto Nacional de Aprendizaje Sena, Admon de redes 2008.*
http://es.scribd.com/doc/8756072/Manual-de-Monitoreo-de-Zennos
(monitoreo-Zenoss.pdf) (20/05/2012)

[45]TÍTULO: GETTING STARTED Autor: Zenoss, Inc
http://iweb.dl.sourceforge.net/project/zenoss/Documentation/Getting%20Started/Getting_Started_01-092010-3.0-v02.pdf
(Getting_Started_01.pdf) *(20/05/2012)*

[46]TÍTULO: ADMINISTRATION *Autor: Zenoss. Inc*
http://community.zenoss.org/community/documentation/official_documentation/zenoss-guide
(Zenoss_Administration_06.pdf) (20/05/2012)

[47]TÍTULO: INSTALLATION *Autor: Zenoss. Inc*
http://iweb.dl.sourceforge.net/project/zenoss/Documentation/zenoss-3.0.x-docs/zendocs-3.0.3/Zenoss_Core_Installation_04-102010-3.0-v05.pdf
(Zenoss_Core_Installation_04.pdf) (20/05/2012)

[48]TITULO: EXTENDED MONITORING *Autor: Zenoss. Inc(http://iweb.dl.sourceforge.net/project/zenoss/Documentation/zenoss-3.0.x-docs/zendocs-3.0.3/Zenoss_Extended_Monitoring_07-102010-3.0-v04.pdf*
(*Zenoss_Extended_ Monitoring_07.pdf) (20/05/2012)*

[49] TITULO: VIRTUALIZACIÓN DE HARDWARE PARA PRUEBAS Autor: Ing. MSc. René Fernández Guzmán, Ing. Karina Carrasco Torrejón, Ing. MSc. Iván Claros Beltrán.
http://www.univalle.edu/publicaciones/journal/journal20/pagina11.pdf
(20/05/2012)

RECURSOS ELECTRÓNICOS

[50] Página del Instituto Tecnológico de la Paz. Departamento de Sistemas y Computación.
Temas:"1.2 Modelo OSI" e "Historia de las Redes Locales"
http://sistemas.itlp.edu.mx/tutoriales/redes/tema12.htm
http://sistemas.itlp.edu.mx/tutoriales/redes/tema11.htm
(10/11/2011)

[51] Página Instituto Tecnológico de Chetumal. Curso de Redes de Computadoras.
Webmaster:Bernardo Villegas Alonzo
Temas:"Unidad 10 Capa de Aplicación"
http://www.itchetumal.edu.mx/paginasvar/Maestros/redes1/unidad10/unidad10.htm
(20/05/2012)

[52] Página de Adrformacion. ADR Infor S.L. Av/ Vara de Rey nº 41 Bis -1º, Oficina 6, 26002 Logroño (La Rioja) España *Curso de Redes y Windows 2003 Server*
Tema:"Capa 3 del modelo OSI: La capa de red, Importancia de la capa de red, Segmentación, Comunicación entre redes, Dispositivos de capa 3, Determinación de ruta, Direccionamiento de capa de red, La Capa 3 y la movilidad de los ordenadores, Comparación entre direccionamiento plano y jerárquico"

http://www.adrformacion.com/cursos/wserver/leccion2/tutorial4.html
(20/05/2012)

[53] Página de Adrformacion. ADR Infor S.L. Av/ Vara de Rey nº 41 Bis -1º, Oficina 6, 26002 Logroño (La Rioja) España *Curso de Redes y Windows 2003 Server*
Tema:"El Modelo TCP/IP: El modelo de referencia TCP/IP, Capa de aplicación, Capa de transporte, Capa de Internet, Capa de Acceso de Red, Comparación entre el modelo OSI y TCP/IP".
http://www.adrformacion.com/cursos/wserver/leccion1/tutorial5.html
(20/05/2012)

[54] Página de VMware Copyright @ 2011, Inc. All rights reserved. *Tema:Aspectos básicos de la Virtualización*
http://www.vmware.com/es/virtualization/virtualization-basics/what-is-virtualization.html
(20/05/2012)

[55] Página de techWEEK.es *Autor: Isabel Martín, consultor preenta de Software de Servidores Críticos de HP*
TITULO: Ventajas y desventajas de la virtualización (Ventajas y desventajas de la virtualización - Tech Labs - Virtualización - techWEEK_es)
http://www.techweek.es/virtualizacion/tech-labs/1003109005901/ventajas-desventajas-virtualizacion.1.html
(20/05/2012)

[56] Página: Historia de Linux y sus distribuciones *Autor: Guillermo García García*
TITULO: Historia De Linux Y Sus Distribuciones
http://www.cdlibre.org/clase/0506amaya/0506_7l/guillermo_garcia/enlaces1/linux.html
(10/11/2011)

[57] Página: Solo ciencia El portal de la Ciencia y la Tecnología Autor: Jorge L. Castillo
TITULO: Historia de LINUX y UNIX.
http://www.solociencia.com/informatica/computador-historia-linux-unix.htm
(20/05/2012)

[58] Página: Computación Aplicada al Desarrollo SA de CV. Adelfa 213-A, Villa de las flores, León Guanajuato.
TITULO: Historia de Linux
http://www.cad.com.mx/historia_de_linux.htm
(20/05/2012)

[59] Página: Red Hat Linux9 Manual de referenciade Red Hat Linux *Autor: Colophon*
TITULO: Red Hat Linux 9:Berkeley Internet Name Domain (BIND)
http://www.linux-cd.com.ar/manuales/rh9.0/rhl-rg-es-9/s1-bind-features.html
(20/05/2012)

[60] Página: Profesional Linux Consulting & Training Av. Ing. Eduardo Molina #5609 Desp.303 Col. Gertrudis Sánchez

TITULO: Servidor DNS
http://www.plct.com.mx/node/9
(20/05/2012)

[61] Página: TechNet Microsoft
TITULO: Biblioteca TechNet Windows Server TechCenter Autor: Microsoft TechNet
http://technet.microsoft.com/es-es/library/cc787920(WS.10).aspx
http://technet.microsoft.com/es-es/library/cc753635(WS.10).aspx
http://technet.microsoft.com/es-es/library/cc783848(WS.10).aspx
http://technet.microsoft.com/es-es/library/cc784698(WS.10).aspx
http://technet.microsoft.com/es-es/library/cc770392(WS.10).aspx
http://technet.microsoft.com/es-es/library/cc784707(WS.10).aspx
http://technet.microsoft.com/es-es/library/cc780906(WS.10).aspx
http://technet.microsoft.com/es-es/library/cc778368(v=ws.10).aspx
http://technet.microsoft.com/es-es/library/cc757978(WS.10).aspx
http://technet.microsoft.com/es-es/library/cc779033(WS.10).aspx
http://technet.microsoft.com/es-es/library/cc787057(WS.10).aspx
(20/05/2012)

[62] PáginaConfigurar un servidor Controlador de Dominio con Samba y OpenLDAP en Ubuntu Server Hardy 8.04 Autor: Jorge Armando Medina, Alejandro Gabriel Sánchez Martínez, Computación Gráfica de México Documentación Técnica
http://tuxjm.net/docs/Configurar_Servidor_Controlador_de_Dominio_con_Samba_y_OpenLDAP/Ubuntu/html-onechunk/
(20/05/2012)

[63] Página: Oreilly Online Catalog
TITULO: Using Samba Autor: Robert Eckstein, David Collier-Brown, Peter Kelly 1st Edition November 1999
http://oreilly.com/catalog/samba/chapter/book/index.html
(20/05/2012)

[64] Página: Scribd *Autor: Ing. Alexis Wol*
TITULO: Cátedra de Telemática
http://es.scribd.com/doc/49816497/112/Base-de-informacion-de-administracion-SNMP-MIB
(20/05/2012)

[65] Página: Proyecto de Gestión de red: Protocolo SNMP Autores: José Ramon Carrasco Cuadrado, Juan Espino Campos, Carlos Ruiz Carrasco.
TITULO: Gestión de red: Protocolo SNMP
http://ceres.ugr.es/~alumnos/gder/html/SNMP1.htm
(10/11/2011)

[66] Página: Aplicaciones Empresariales.com Autor: Junior Leo
TITULO: Zenoss, monitorización de tecnología en la empresa

http://www.aplicacionesempresariales.com/zenoss-monitorizacion-de-tecnologia-en-la-empresa.html
(20/05/2012)

[67] Página: Tenea Tecnologías SL Madrid España
TÍTULO:Servicios Nagios Autor:
http://www.tenea.com/servicios/nagios.html
(20/05/2012)

[68] TÍTULO: Monitoria y análisis de Red con Nagios
Autor: Sergio Cayuqueo
http://cayu.com.ar/files/manuales-nagios.pdf
(manuales-nagios.pdf)
(10/11/2011)

[69] Página: Nagios
TÍTULO: Nagios Features
http://www.nagios.org/about/features
(20/05/2012)

[70]Página; TCOMM Network Services
TÍTULO: Nagios Control
http://www.tcomm.es/joomla/index.php/es/products-menu/nagios-products-menu.html
(20/05/2012)

[71] Blog Cerebro en la sombra TITULO: Monitorizando Servidores con Cacti Autor: osus~~EN~~osusnet.com
http://blog.osusnet.com/2008/04/23/monitorizando-servidores-con-cacti/
(20/05/2012)

[72] Pagina: Cacti
TÍTULO: Features
http://www.cacti.net/features.php
(20/05/2012)

[73] Pagina: Scribd
TITULO: Manual de Cacti
http://es.scribd.com/doc/7399275/Proyecto-2-Manual-Cacti
(20/05/2012)

[74] Página:MCL Smart Solutions
TÍTULO: Cacti
http://mclsolution.com.ve/MCL-Solutions/cacti.html
(10/11/2012)

[75] Pagina:Wikispaces Maestría en Ciencias de la computación Mención redes de computadoras.
Autor: Msc. Luzneida, Matute
TITULO: Administración de redes
http://administracionderedes2010.wikispaces.com/cacti_nestrada_ryepez
(20/05/2012)

[76] Pagina: Taringa Autor: Marco Antonio Alvarez Iglesias
TÍTULO:Cacti solución de graficado en red
http://www.taringa.net/posts/linux/1077025/Cacti_Solucion-de-Graficado-en-Red.html
(10/11/2011)

[77] Página: El programador Hereje *TÍTULO: Cuando el cache de APT Sufre un Desbordamiento Autor: Jose Diaz*
http://josediaz.web.ve/blog/2010/08/23/cuando-el-cache-de-apt-sufre-un-desbordamiento/
(10/11/2011)

[78] Página: Alcance libre *TÍTULO: Como configurar SNMP Autor: Joel Barrios Dueñas*
http://www.alcancelibre.org/staticpages/index.php/como-linux-snmp
(20/05/2012)

[79] Página: Bitácora personal de un SysAdmin Gnu/Linux, Windows, BSD
TÍTULO: Como Instalar y configurar SNMP Autor: Sin Autor Noviembre 18, 2008
http://rm-rf.es/como-instalar-y-configurar-snmp/
(20/05/2012)

[80] LINUX BLOG: Monitoreando con Zenoss Autor: *Sin Autor 11de Abril del 2007*
http://www.rz0r.net/2007/04/monitoreando-con-zenoss-parte2/
(20/05/2012)

[81] BanPe: The Blog: Instalacion de Zenoss3.0.3 en Debian 5.0.2.1 *Lenny Autor: tobias 13 dic,2010 http://theblog.banpe.com.mx/?p=557*
(20/05/2012)

[82]Página Vmlogía soluciones virtuales soluciones reales TÍTULO: Virtualización de servidores http://www.vmlogia.com/vdeservidores.aspx
(20/05/2012)

[83]Página WIKI-LATAM Proyecto Fedora TÍTULO: Tipos de virtualización
http://proyectofedora.org/wiki/Tipos_de_virtualizaci%C3%B3n
(20/05/2012)

[84] Pagina SNMP Research International TITULO: Secure Internet Management and SNMP http://www.snmp.com/
(20/05/2012)

[85] Pagina RFC del protocolo RMON http://tools.ietf.org/html/rfc3577
(20/05/2012)

[86] Pagina CISCO sobre MIB (Base de Información de Administración)
http://www.cisco.com/en/US/docs/ios/12_0t/12_0t1/feature/guide/isdn_mib.pdf
(20/05/2012)

[87] RFC de MIB (Base de Información de Administración)
http://www.ietf.org/rfc/rfc1213.txt
(20/05/2012)

[88] RFC de SMTP http://www.ietf.org/rfc/rfc2821.txt
(20/05/2012)

[89] RFC de RPC http://tools.ietf.org/html/rfc1831
(20/05/2012)

[90] RFC de SSH http://www.normes-internet.com/normes.php?rfc=rfc4462&lang=es
(20/05/2012)