IMPLEMENTACION DE UNA HERRAMIENTA BAJO SOTFWARE LIBRE PARA MONITOREO DE REDES INFORMATICAS

LUZ ELENA DIAZ TABERA

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERIAS FISICOMECANICAS
ESCUELA INGENIERIA ELECTRICA, ELECTRONICA Y TELECOMUNICACIONES
ESPECIALIZACION EN TELECOMUNICACIONES
BUCARAMANGA
2011

IMPLEMENTACION DE UNA HERRAMIENTA BAJO SOTFWARE LIBRE PARA MONITOREO DE REDES INFORMATICAS

LUZ ELENA DIAZ TABERA

Monografía presentada como requisito para optar al título de Especialista en Telecomunicaciones

Director:
JORGE HERNANDORAMON SUAREZ
Ingeniero Electricista, MsC.

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERIAS FISICOMECANICAS
ESCUELA INGENIERIA ELECTRICA, ELECTRONICA Y TELECOMUNICACIONES
ESPECIALIZACION EN TELECOMUNICACIONES
BUCARAMANGA
2011

AGRADECIMIENTOS

Expreso mis agradecimientos a:

A mi Dios padre, porque me guía en todos los momentos de mi vida. Gracias, por permitirme este nuevo logro en mi vida profesional.

A mi familia, especialmente a mi madre. Gracias, por brindarme su cariño, comprensión y apoyo incondicional.

Al ingeniero Jorge Hernando Ramón Suarez. Gracias, por su dirección y colaboración en la realización del presente trabajo de grado. También, gracias alequipo administrativo y docente de la especialización y a todas las personas, que de alguna u otra forma contribuyeron para que este sueño se hiciera realidad.

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

GLOSARIO

- **Cgi (Common Gateway Interface)**: Interfaz Común de Pasarela, tecnología compuesta por un protocolo de comunicación que fija una interfaz que permite el intercambio de información entre el servidor de web y programas que ya existían en el sistema.

  El interfaz CGI permite comunicar el servidor de web con otros programas que realizan tareas diversas, estos programas se ejecutan como tareas independientes del servidor de web. Con el nombre de "cgi-bin" nos referimos a los programas que el cliente web ejecuta a través del servidor de web.

- **Dashboard**: Es una pantalla principal completamente configurable, con varias solapas y diversos marcos configurables con información acerca del sistema y los equipos monitorizados. Los marcos se pueden mover por la pantalla con el ratón, arrastrándolos y soltándolos. Cada usuario define su propio Dashboard.

- **Gestión de Traps**: Los agentes snmp en dispositivos como routers, switches, printers, servidores, etc. pueden enviar alarmas (traps) cuando ocurren ciertos eventos:- Se “cae” una interfaz, - Se estropea el ventilador de un router, - La carga de procesos excede un límite, - Se llena una partición de disco, - Un UPS cambia de estado.

  Es necesario un mecanismo inteligente para notificar al administrador sólo cuando interesa.

- **Licencia GNU/GPL**: Es una licencia creada por la Free Software Foundation en 1989 (la primera versión), y está orientada principalmente a proteger la libre distribución, modificación y uso de software. Su propósito es declarar que el

software cubierto por esta licencia es software libre y protegerlo de intentos de apropiación que restrinjan esas libertades a los usuarios.

- **Hosts:**Se trata del objeto básico de monitorización, puede ser cualquier dispositivo de una red IP con el agente instalado o SNMP activo para su monitorización. En la monitorización activa, el servidor irá a estos hosts de forma periódica a buscar la información requerida. En la comunicación pasiva, será el host quien conectará con el nodo servidor.

- **Ipmi**: El estándar IPMI (Intelligent Platform Management Interface) permite gestionar servidores y blades con independencia de sistemas operativos y tipos de CPU, se trata de un chipset que permite en forma remota obtener información del estado de diferentes componentes hardware, temperaturas, voltajes, etc. El alcance del protocolo es bastante amplio, pero en la práctica le permite a una organización implementar *lights-out management* utilizando medios secundarios de acceso a un equipo cuando todo lo demás falla. En tal sentido, esta tecnología permite reducción de costos, en particular cuando se deben administrar centros de datos geográficamente distribuidos.
  Implementada entre otros por HP, Dell, Intel y Toshiba [1], esta herramienta escucha peticiones en los puertos UDP 663 y 664 y actúa en forma independiente al sistema operativo instalado. La sesión comienza con un `Ping de Presencia' al puerto 663, cualquiera puede enviarlo y si la máquina soporta IPMI devuelve información sobre la misma.

- **Ítems**: También llamados monitores, engloban aquella información específica que se desea conocer sobre un host. Son bastante flexibles y heterogéneos, pues tenemos desde consultas SNMP, a agentes predefinidos que recogen información local, scripts personalizados que corren localmente en el Host y que permiten recoger información, ítems que trabajan sobre información ya recibida, solicitudes de ejecución de scripts por Telnet o ssh, etc.

- **Log:** Archivo habitualmente en texto plano donde se dejan las trazas de un sistema operativo o de una aplicación concreta.

- **Monitorización Wmi**: Windows Management Instrumentation o Windows Management Interface, WMI es un standard de Microsoft para obtener información del sistema operativo y aplicaciones de entornos Microsoft Windows, permite implementar la gestión integrada de sistemas llamado Web Based Enterprise Management -WBEM (gestión basada en la web). Dicha información incluye información sobre el estado de la memoria del sistema, inventarios de todas las aplicaciones instaladas en un equipo o en un dominio, rendimiento y mucha otra información de cliente adicional. La mejor manera de utilizar WMI es integrarlo en los scripts de administración.

- **Nms (Network Management System)**: Son sistemas definidos y diseñados, para realizar gestión sobre las redes de operación, realizando una combinación entre hardware y software para la gestión, administración, O&M (Operación & Manteamiento) y el monitoreo de los diferentes Elementos de Red (NE's), mediante SNMP. Desde los equipos NMS, se pueden extraer las estadísticas y las alarmas de los equipos operacionales que conforman una red de servicio (voz, datos, video).Algunos NMS, permiten gestionar umbrales de utilización en indicadores, y accionar alarmas sobre el comportamiento de nodos de la red.

- **RRDtool**: RRDtool es un sistema gráfico basado en round-robin databases (RRDs). Este se utiliza para guardar y crear los gráficos de la base de datos.

- **Servidor zope**: Es un servidor de aplicaciones web de código abierto escrito en el lenguaje de programaciónPython. Para las funciones de edición de contenidos, así como personalizaciones básicas, puede ser usado mediante un navegador web. La programación avanzada así como el desarrollo de nuevas

funcionalidades requiere la edición de componentes en «file system». Un sitio web de Zope está compuesto de objetos en lugar de archivos, como es usual con la mayoría de los otros sistemas de servidores web.

- **Smi (Structure of Management Information)**: Es un conjunto de estructuras y esquemas de identificación para acceder a la MIB. Define la estructura lógica de la información de gestión OS. Establece las reglas para nombrar a los objetos gestionables y a sus atributos, define un conjunto de subclases y tipos de atributos que son en principio aplicables a todos los tipos de clases de objetos gestionables.

- **SNMP:** Acrónimo de Simple Network Transfer Protocol. Protocolo de Internet que permite la gestión de dispositivos en redes IP.

- **Template**: (plantillas), permiten definir item, trigger, y graph de forma conjunta para todos los hosts que estén vinculados (linked) a ella. Es una forma fácil de desplegar objetos para hosts nuevos, sirven para facilitar la gestión de los administradores ya que una vez hechas se pueden asignar de forma sencilla a los agentes necesarios. Los templates se pueden exportar/importar de forma sencilla en XML, de manera que la comunidad puede compartir templates ya creadas para un sistema operativo concreto.

- **Trigger**: Los triggers o iniciadoresson condiciones que disparan una alerta en el sistema ante el estado de un cierto ítem.

RESUMEN

TITULO: IMPLEMENTACIÓN DE UNA HERRAMIENTA BAJO SOFTWARE LIBRE PARA MONITOREO DE REDES INFORMÁTICAS[*]

AUTORA: LUZ ELENA DIAZ TABERA[**]

PALABRAS CLAVES: MONITOREO, GESTOR, AGENTE, TRAPS, SNMP, GNU/GPL, UBUNTU SERVER.

DESCRIPCION:

Las redes informáticas se hacen cada vez más grandes y complejas como consecuencia de las aplicaciones y servicios quesoportan, lo que conlleva a que las tareas de gestión que implica monitoreo y control, sea un elemento importante y de carácter pro-activo para evitar posibles fallos y mejorar su operatividad. Esto se puede lograr con la automatización, mediante software que aporta la posibilidad de monitorizar de forma centralizada y desde una única interfaz, un gran número de dispositivos y servicios, en plataformas heterogéneas.

La implementación de herramientas para monitoreo bajo software libre, es una oportunidad para las pequeñas y medianas empresas (pymes), por ser software de altas prestaciones además por el factor económico que representa frente a las herramientas comerciales.El presente trabajo aborda el estudio y comparación de tres herramientas bajo software libre para monitoreo de redes informáticas, previamente seleccionadas dentro de una gran variedad de herramientas open source, que existen en la red para este propósito y que se investigó mediante una amplia bibliografía consultada, como resultado de esta comparación se puede recomendar una, la cual se escogió para su posterior instalación e implementación bajo el sistema operativo Linux con la distribución de Ubuntu 9.1 server Karmic Koala, la selección de la herramienta de monitoreo se hizoen consideración a las características ofrecidas como soporte de comunidad, facilidad de configuración, amigabilidad y alto desempeño.

[*] Trabajo de grado

[**] Facultad de Ingenierías Fisicomecánicas. Escuela de Ingeniería Eléctrica, Electrónica y Telecomunicaciones. Director: Msc. Jorge Hernando Ramón Suarez

SUMMARY

TITLE: IMPLEMENTATION UNDER FREE SOFTWARE TOOL FOR MONITORING COMPUTER NETWORKS*

AUTHOR: LUZ ELENA DIAZ TABERA**

KEY WORDS: MONITORING, MANAGER, AGENT, TRAPS, SNMP, GNU/GPLUBUNTU SERVER.

DESCRIPTION

Computer networks are becoming larger and more complex as a result of applications and services that support, leading to management tasks involving monitoring and control is an important and proactive in nature to prevent malfunction and improve its operation. This can be achieved through automation, through software that provides the ability to monitor centrally from a single interface, a large number of devices and services across heterogeneous platforms.

The implementation of tools for monitoring under free software is an opportunity for small and medium enterprises (SMEs), because high-performance software besides the economic factor is off the shelf tools. This paper deals with the study and comparison of three free software tools under monitoring computer networks, previously selected in a variety of open source tools that exist on the network for this purpose, which was investigated by an extensive bibliography, as a result of this comparison may be recommended, which was chosen for subsequent installation and implementation under the Linux operating system with Ubuntu 9.1 Server distribution Karmic, the selection of the monitoring tool was made in consideration of the features offered and community support, easy customization, user-friendliness and high performance.

* Work Degree

** Faculty of Engineerings Fisicomecánicas. School of Electrical, Electronic Engineering and Telecomunications. Directress: Msc. Jorge Hernando Ramón Suarez

INTRODUCCION

A medida que aumenta la expansión y con ello la complejidad de las redes informáticas como consecuencia de los recursos y servicios que soporta, las tareas administrativas enfocadas a mantener la operatividad y disponibilidad de la infraestructura tecnológica, se han convertido sin duda alguna en un componente crítico y de gran importancia para el logro de los objetivos propuestos y calidad de servicios ofrecidos desde TI.

Las herramientas de monitoreo, son un componente a la gestión de redes, que han sido desarrolladas con el fin de vigilar y controlar el normal funcionamiento de la plataforma tecnológica, permitiendo la entrega a los usuarios finales, de los niveles de disponibilidad y rendimiento mediante parámetros de calidad previamente definidos.

A partir de lo anterior, considerando las dificultades que conlleva para las PYMES[1] la implementación de este tipo de tecnologías, debido a los costos de licencia y soporte de las herramientas existentes en el mercado,se propone la utilización de herramientas de software libre, por sus altas prestaciones y beneficios con respecto al factor económico que representan frente a las comerciales.

Este documento presenta una revisión de los conceptos relacionados con la gestión de redes, los fundamentos del protocolo snmp y del tema de monitorización. Con respecto al tema central motivo del presente trabajo, se hace la presentación y comparación de tres herramientas de monitoreo bajo software libre, las cuales fueron previamente seleccionadas bajo una extensa bibliografía consultada y herramientas encontradas, mediante la exploración exhaustiva en la Internet y foros sociales. Posteriormente, con base en la comparación realizada, se selecciono una y se finaliza con la instalación e implementación.

[1] Pequeñas y Medianas Empresas. http://openpyme.osl.ull.es/GI/applications

1. PLANTEAMIENTO DEL PROBLEMA

1.1 SITUACION PROBLEMA

Los grandes avances tecnológicos, en donde las redes de computadoras han tenido una expansión y crecimiento sostenido,caracterizadas por la complejidad y heterogeneidad de los recursos que la componen,han propiciado un ambiente globalizado que demanda cada vez, nuevas exigencias enla operatividady calidad delos servicios ofrecidos desde TI.

Los principales problemas relacionados con la expansión de las redes son la gestión de su correcto funcionamiento día a día y la planificación estratégica de su crecimiento. De hecho más se estima que más del 70 % del coste de una red corporativa se atribuye a su gestión y operación.[2]Cuando fallan las redes, se interrumpen los servicios de comunicación, el acceso a la información, servicios básicos de impresión, correo electrónico, todo esto conllevando a pérdidas de productividad y buen desempeño.

Por lo anterior, la gestión de red integrada, como un conjunto de actividades dedicadas al control y monitoreo de recursos y servicios informáticos bajo el mismo sistema de gestión, se ha convertido en un aspecto de mucha importancia en el mundo de las telecomunicaciones,gracias a los beneficios que dichas redes representan para el éxito de los negocios.

Para la gestión de las redes informáticas, el mercado ofrece varias herramientas comerciales las cuales tienen un costo significativo generalmente asequible por las

[2] MILLAN TEJEDOR Ramón Jesús. Publicado en Windows NT/2000 Actual nº 12, Prensa Técnica S.A. http://www.com/tutoriales/gestionred.php#plataformas

grandes empresas pero difícilmente para las pequeñas y medianas empresas las cuales no cuentan en muchas ocasiones con los recursos y presupuesto apropiado para la inversión en este tipo de herramientas, lo que conlleva a una desigualdad de oportunidades con respecto a una adecuada infraestructura tecnológica para el desarrollo del negocio.

Frente a esta situación, sería importante considerar la implementaciónde otras opciones como las herramientas de software libre y lograr mejorar ese nivel de desarrollo y competitividad frente al tema tecnológico.

La formulación del problema a resolver en este proyecto es la siguiente:

.

Qué herramienta de software libre, implementar para monitoreo de redes informáticas que entregue altas prestaciones y relación costo-beneficio?

1.2 OBJETIVOS

1.2.1 Objetivo General.

Realizar el estudio e implementación de una herramienta bajo software libre para monitoreo de redes inalámbricas como solución a pymes.

1.2.2 Objetivos Específicos.

* Investigar y estudiar las diferentes herramientas bajo software libre para monitoreo de redes informáticas.

*Seleccionar y describir tres herramientas para monitoreo de redes informáticas.

* Realizar la instalación e implementación de una herramienta para monitoreo de redes informáticas.

* Evaluar el funcionamiento y describir las consideraciones sobre desempeño de una herramienta bajo software libre para monitoreo de redes.

1.3 JUSTIFICACION.

El monitoreo y control son los aspectos básicos de la gestión de redes. Una de las tareas importantes que corresponden a un administrador de red es la monitorización del sistema, es imprescindible conocer en todo momento qué está ocurriendo en la red y atajar así cualquier problema que pueda surgir, esto es posible mediante la utilización de software para monitoreo de redes.

El monitoreo de redes informáticas a través de la implementación de herramientas de software libre para este propósito, es una propuesta para las pequeñas y medianas empresas quienes difícilmente cuenta con un presupuesto apropiado para la inversión en este tipo tecnología, que se requiere para lograr el soporte de una infraestructura tecnológica para su operatividad y disponibilidad, componente crítico y de gran importancia para el desarrollo del negocio.

El uso de tecnología de código abierto es una de las acciones que reduce costos empresariales, además ofrece altas prestaciones y potencialidades. Las pymes tienen distintas necesidades y expectativas de administración de redes debido a que la experiencia técnica y el equipo de trabajo son limitados. Ellos necesitan herramientas de bajo costo, fáciles de instalar y utilizar.

Mediante este trabajo se propone el estudio y la implementación de una herramienta para el monitoreo de redes informáticas para que sirva como base para la aplicación y solucióna las necesidades actuales de la gestión eficiente de los servicios y recursos soportados mediante las redes de computadoras enfocado hacia las pequeñas y medianas empresas, para la conformación e integración de una plataforma sustentable para el desarrollo de competencias.

Este proyecto se realizará en tres partes la primera de ellas consiste en investigar y estudiar las herramientas de software libre para monitoreo de redes. Luego se escogerá tres herramientas para describirlas y realizar la instalación e implementación. Se finalizará con las respectivas conclusiones sobre los resultados arrojados del estudio y la práctica realizada.

Al desarrollo de este proyecto se cumple con el requisito para optar al título de especialista en telecomunicaciones de la Escuela de Ingeniería Eléctrica, Electrónica de la Universidad Industrial del Santander UIS.

1.4 ESTADO DEL ARTE

Los servicios de tecnologías de la información, la plataforma tecnológica, los departamentos de sistemas, la conectividad y las líneas de comunicaciones se están convirtiendo cada vez más en la base y columna vertebral sobre la que las

organizaciones ya sea de tipo educativa, empresarial, comercial, etc, gestionan y realizan sus procesos. Dicha infraestructura crece y se vuelve más compleja a medida que se introducen nuevos servicios con el objeto de expandirse, ofrecer nuevos productos y servicios o mejorar la calidad, lo que conlleva a que la exigencia de la operación sea cada vez más demandante, convirtiendo las tareas de análisis y monitoreo en una labor cada vez mas importante y de carácter pro activo para evitar posibles problemas con la infraestructura de red.

Por todo ello, el nivel de servicio, de profesionalidad y de disponibilidad que se exige a los empleados de tecnologías de la información y a las plataformas quemantienen es cada vez mayor. Sin embargo, el gran número de dispositivos, tecnologías, plataformas, lenguajes e interfaces con las que deben enfrentarse en el día a día aumenta proporcionalmente. Además, se requiere actuar de forma rápida y pro-activa ya que cualquier tiempo de parada de la plataforma tecnológica repercute en forma negativa la calidad de los servicios soportados bajo su infraestructura.

En este escenario, cualquier acción o solución encaminada a monitorizar la totalidad de la plataforma tecnológica supone una inversión de rápido retorno dado que no se trata de reaccionar ante simples dificultades, sino ante un sistema de control y monitorización que escala los problemas detectados de manera instantánea, para soporte en la toma de decisiones y optimización del desempeño de la red.

La solución que cumpla con los requisitos especificados debe ser de arquitectura abierta y debe respaldarse en protocolos estándares. De esta manera, podrán monitorizarse plataformas de cualquier tipo y de cualquier fabricante: dispositivos de comunicaciones, estaciones de trabajo, servidores y hosts críticos, impresoras de red, dispositivos de seguridad, PLCs, aplicaciones críticas, etc. ¿Dónde reside el límite? En estar conectado a la red, disponer de una dirección IP y, a ser

posible, habilitar el protocolo SNMP. ¿Dónde llega el límite de monitorización de la solución? Dado que es basada en protocolos estándares (TCP/IP y SNMP) depende de la información que proporcione cada fabricante sobre sus productos. Dicha información reside en ficheros de tipo MIB (Management Information Base) que describen los productos, las alarmas que pueden generar y las consultas sobre rendimiento, descripción del producto y disponibilidad que pueden realizarse por ejemplo a un router, sobre el ancho de banda utilizado; a un switch le pediremos información de cada una de sus conexiones activas; a una aplicación de copias deseguridad, el resultado de la copia diaria.

Las herramientas de administración gestionan sus dispositivos a través de interfaces e incluso sistemas diferentes. Una misma herramienta difícilmente servirá para generar usuarios, detectar intrusos, analizar protocolos y administrar el correo electrónico, sin embargo, integrar a dichas herramientas la solución de monitorización de manera que cada dispositivo responda a un cierto tipo de acciones y nos conduzca a las herramientas y utilidades necesarias para gestionarlo o solucionar los problemas detectados en el mismo, resultaría algo muy ventajoso.

2. GESTION DE REDES

La gestión de redes incluye el despliegue, integración y coordinación del hardware, software y los elementos humanos para monitorizar, probar, sondear, configurar, analizar, evaluar y controlar los recursos de la red para conseguir los requerimientos de tiempo real, desempeño operacional y calidad de servicio a un precio razonable.[3]

La gestión en redes tiene dos funciones fundamentales: la monitorización y el control. **La monitorización**, está relacionada con funciones de lectura, esto implica observar y analizar el estado y comportamiento de la configuración de red y sus componentes. Sus áreas de trabajo abarca: prestaciones, fallos y costes. **El control**, abarca funciones de escritura, relacionado con la alteración de los parámetros de los diferentes componentes de la configuración de la red y causan acciones predefinidas para ser ejecutadas por estos componentes. Esto implica cambiar la configuración de los dispositivos desde la estación de gestión. Tiene dos áreas de trabajo que son el control de configuración y el control de seguridad.

2.1 ELEMENTOS DE UN SISTEMA DE GESTION DE RED

Un sistema de gestión de red es una colección de herramientas para monitorizar y controlar la red, el cual debe estar integrado por:

- Una interfaz de operador única con comandos potentes pero agradables.

[3] T.Saydam and T. Magedanz, "From Networks and Network Management into Service and Service Management",
Journal of Networks and Systems Management, Vol 4, No. 4 (Dic 1996).

- Una cantidad mínima de equipamiento, separado del sistema de gestión. Generalmente el hardware y software de gestión están incorporados en los equipos.

Figura 1. Elementos de un sistema de gestión

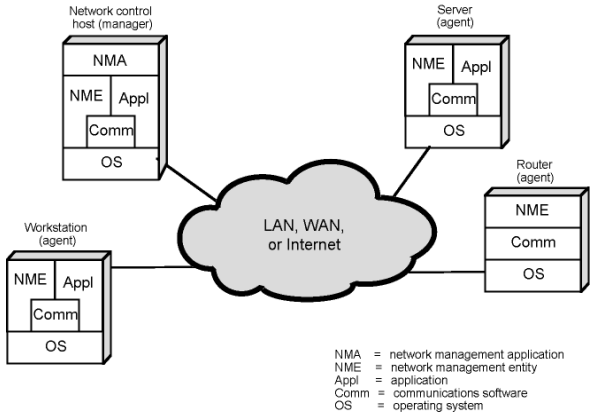


Figure 17.1 Elements of a Network Management System

Fuente: William Stallings.

El software de gestión se ejecuta en estaciones desde las cuales se controla y actúa sobre los elementos de red. Suelen ser estaciones de trabajo de altas prestaciones.

El software de agente localizado en los elementos de red como hosts, routers, terminales X. servidores de terminales, etc., se encargan de actualizar información, responder a las solicitudes del agente y comunicar problemas.

La Estación de Gestión o NMS (Network Monitoring System - Sistema de Monitoreo de Red) sirve como interfaz entre el Administrador de red humano y el sistema de gestión de red, y tiene una base de datos de información de gestión de red extraída de las bases de datos de todas las entidades gestionadas en la red.

2.2 PROTOCOLOS PARA LA GESTION DE REDES

Existen distintos protocolos de gestión de red, dentro de los cuales destaca SNMP (Simple Network Management Protocol), perteneciente al conjunto de protocolos TCP/IP. Este es el protocolo a utilizar en redes empresariales, pues todos los equipos lo soportan, y de hecho, SNMP puede ser considerado el estándar de facto. Otro protocolo estándar, es el CMIP (Common Management Information Protocol), de la familia de protocolos OSI (Open Systems Interconnection) de la ISO (International Organization for Standarization), que si bien no está muy implantado en la empresa, está presente en la mayoría de los operadores de los servicios de telecomunicación para su gestión de redes.

El crecimiento experimentado por las redes de área local y la aparición de sistemas distribuidos, ha generado nuevas técnicas y protocolos especializados en la gestión de redes. Lo que se busca, es conseguir que desde un único puesto de la red denominado consola, se pueda monitorizar toda la red. Estas tecnologías recogen información de cada uno de los nodos, observando el tráfico en cada uno de los segmentos de la red, avisando en el caso de que se llegue a situaciones que el administrador de la red defina como alarmantes.

Los dispositivos gestionados en una red disponen de un agente que envía alarmas si detecta problemas o situaciones anómalas en la red. Por otra parte, se instalan en la red otros programas denominados entidades de gestión, que recogen e interpretan estas alarmas disparando los mecanismos oportunos para informar al administrador de red o corregir los problemas. Además, las entidades de gestión interrogan periódicamente a los agentes de red sobre su estado.

De este modo, la entidad de gestión se hace una composición de lugar sobre el estado de la red en cada instante. Este sistema de pregunta/respuesta(polling) se

realiza mediante protocolos especializados como SNMP (Simple Network Management Protocol, protocolo básico de gestión de red). La información recogida se almacena en una base de datos denominada MIB (Management Informatión Base, base de datos de información de gestión).

A partir de los MIB, las aplicaciones de gestión elaboran estadísticas y otros informes que permiten al administrador tomar decisiones estratégicas sobre la funcionalidad y la seguridad de la red en cada uno de sus puntos.

2.3 INTERFACES DE GESTION

La gestión de un dispositivo puede ser llevada a cabo a través de diferentes formas, vía consola, vía web o a través de un software de administración. Generalmente la administración por consola y vía web permite la configuración del dispositivo y la revisión de sus características, pero dificulta el control y la monitorización continua del mismo, así como del sistema de red completo. Para llevar a cabo la gestión de un sistema que involucre más de un dispositivo se hace necesario la utilización de una herramienta de gestión que permita la realización de las tareas de administración básicas por medio de la utilización de un protocolo de gestión, por ejemplo SNMP.

2.4 MODELO DE GESTION OSI

El modelo de gestión ISO clasifica las tareas de los sistemas de gestión en cinco áreas funcionales. La tarea del encargado de gestionar una red empresarial será

evaluar la plataforma de gestión a utilizar en cuanto a la medida en que dicha plataforma resuelva la problemática de gestión en cada una de estas áreas:

- Gestión de Fallos
- Gestión de La Configuración
- Gestión del Rendimiento
- Gestión de La Seguridad
- Gestión de Contabilidad

2.4.1 Gestión de configuración.

El objetivo de la gestión de configuración es obtener datos de la red y utilizarlos para incorporar, mantener y retirar los distintos componentes y recursos a integrar. Consiste en la realización de tres tareas fundamentales:

- Recolección automatizada de datos sobre el inventario y estado de la red, tales como versiones software y hardware de los distintos componentes.
- Cambio en la configuración de los recursos.
- Almacenamiento de los datos de configuración.

2.4.2 Gestión de rendimiento.

La gestión de prestaciones o del rendimiento tiene como objetivo principal el mantenimiento del nivel de servicio que la red ofrece a sus usuarios, asegurándose de que esté operando de manera eficiente en todo momento.

Algunas cuestiones que atañen al gestor de la red son: ¿Cuál es la utilización de la red? , ¿Hay un tráfico excesivo?, ¿Se ha reducido la productividad a niveles

inaceptables?, ¿Existen cuellos de botella?, ¿Está aumentando el tiempo de respuesta?. Para ello, la gestión de prestaciones se basa en cuatro tareas:

- Recogida de datos o variables indicadoras de rendimiento, tales como el througtput de la red, los tiempos de respuesta o latencia, la utilización de la línea, etc.
- Análisis de los datos para determinar los niveles normales de rendimiento.
- Establecimiento de umbrales, como indicadores que fijan los niveles mínimos de rendimiento que pueden ser tolerados.
- Determinación de un sistema de procesado periódico de los datos de prestación de los distintos equipos, para su estudio continuado.

Los tipos de indicadores que puede usar el administrador de la red, está dentro de dos categorías:

- Medidas orientadas al servicio. Permiten mantener los niveles de determinados servicios a satisfacción de los usuarios. Son los más importantes:

  Disponibilidad: Porcentaje de tiempo que una red, un dispositivo o una aplicaciónestá disponible para el usuario.
  Tiempo de respuesta: Cuanto tarda en aparecer la respuesta en el terminal delusuario cuando éste realiza una acción.
  Exactitud: Porcentaje de tiempo en el que no ocurren errores en la transmisión yentrega de información

- Medidas orientadas a la eficiencia. Permiten mantener los niveles de satisfacción anteriores al mínimo coste posible.

Throughput: La tasa a la que ocurren eventos a nivel de aplicación (p.e. Transacciones, mensajes, transferencia de archivos).

Utilización: Porcentaje de la capacidad teórica de un recurso (p.e. Un concentrador, una línea de transmisión, un conmutador) que se está utilizando.

2.4.3 Gestión de contabilidad.

La gestión de contabilidad tiene como misión la medida de parámetros de utilización de la red que permitan a su explotador preparar las correspondientes facturas a sus clientes. Entre las tareas que se deben realizar en esta área, están:

- Recolección de datos sobre la utilización de los recursos.
- Establecimiento de cuotas.
- Cobro a los usuarios con las tarifas derivadas de la utilización de los recursos.

Los recursos que son objeto de gestión de costos suelen ser:

- **Recursos de comunicación**: LANs, WANs, líneas alquiladas, líneas conmutadas alquiladas, conmutadores PBXs, etc.
- **Hardware de computació**n: Servidores, estaciones de trabajo.
- **Sistemas y software**: Utilidades software y aplicaciones en servidores, un centro de proceso de datos.
- **Servicios**: Todos los servicios de información y servicios de comunicaciones comerciales disponibles.

2.4.4 Gestión de fallos.

La gestión de fallos tiene por objetivo fundamental la localización y recuperación de los problemas de la red. La gestión de problemas de red implica las siguientes tareas:

- Determinación de los síntomas del problema.
- Aislamiento del fallo.
- Resolución del fallo.
- Comprobación de la validez de la solución en todos los subsistemas importantes de la red.
- Almacenamiento de la detección y resolución del problema.

2.4.5 Gestión de seguridad.

La misión de la gestión de seguridad es ofrecer mecanismos que faciliten el mantenimiento de políticas de seguridad (orientadas a la protección contra ataques de intrusos). Entre las funciones realizadas por los sistemas de gestión de seguridad, están:

- Identificación de recursos sensibles en la red, tales como ficheros o dispositivos de comunicaciones.
- Determinación de las relaciones entre los recursos sensibles de la red y los grupos de usuarios.
- Monitorización de los puntos de acceso a los recursos sensibles de red.
- Almacenamiento de los intentos de acceso no autorizados a estos recursos, para su posterior análisis.

3. SNMP

El Protocolo Simple de Administración de Red o SNMP es un protocolo de la capa de aplicación, no orientado a conexión, que facilita el intercambio de información de administración entre dispositivos de red que se ejecuta sobre los niveles del protocolo IP y UDP. Es parte de la familia de protocolos TCP/IP. SNMP permite a los administradores supervisar el funcionamiento de la red, buscar y resolver sus problemas, y planear su crecimiento.

Fue diseñado por el IETF (Internet Engineering Task Force). Las versiones de SNMP más utilizadas son SNMP versión 1 (SNMPv1) y SNMP versión 2 (SNMPv2). SNMP en su última versión (SNMPv3) posee cambios significativos con relación a sus predecesores, sobre todo en aspectos de seguridad, sin embargo no ha sido mayoritariamente aceptado en la industria.

3.1 ARQUITECTURA DEL PROTOCOLO SNMP

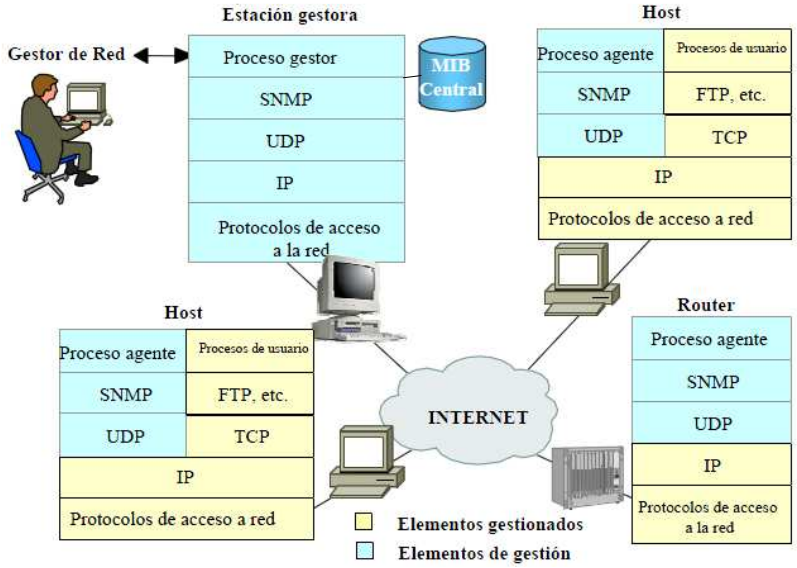
El protocolo SNMP está compuesto por dos elementos: el agente (agent), y el gestor (manager). Es una arquitectura cliente-servidor, en la cual el agente desempeña el papel de cliente y el gestor hace el de servidor, es decir, utilizan una estructura básica, conocida por paradigma gestor-agente.

El principio de funcionamiento reside en el intercambio de información de gestión entre nodos gestores y nodos gestionados. Habitualmente, los agentes mantienen en cada nodo gestionado información acerca del estado y las características de funcionamiento de un determinado recurso de la red. El gestor pide al agente, a

través de un protocolo de gestión de red, que realice determinadas operaciones con estos datos de gestión, gracias a las cuales podrá conocer el estado del recurso y podrá influir en su comportamiento.

Cuando se produce alguna situación anómala en un recurso gestionado, los agentes, sin necesidad de ser invocados por el gestor, emiten los denominados eventos o notificaciones que son enviados a un gestor para que el sistema de gestión pueda actuar en consecuencia.

Figura 2. Arquitectura SNMP



Fuente: Grupo de Ingeniería Telemática, Udc.

Una red administrada a través de SNMP consiste de cuatro componentes principales:

- Estación de gestión.
- Agente de gestión.
- Base de Información de Gestión.
- Protocolo de gestión de redes.

3.1.1 Estación de gestión.

Dispositivo dedicado a las tareas de gestión, es la interface del administrador de red en el sistema. Contiene el gestor SNMP, software que interacciona con los agentes mediante operaciones SNMP y mantiene una base de datos denominada MIB con formato SMI. Los dispositivos administrados, a veces llamados elementos de red, pueden ser routers, servidores de acceso, switches, bridges, hubs, computadores o impresoras.

3.1.2 Agente de gestión.

Es un módulo de software de administración de red que reside en un dispositivo administrado. Un agente posee un conocimiento local de información de administración (memoria libre, número de paquetes IP recibidos, rutas, etcétera), la cual es traducida a un formato compatible con SNMP y organizada en jerarquías. Soporta dos tipos de transacciones:
Petición por parte del gestor, y respuesta por parte de agente.
Notificaciones no solicitadas (traps) desde el agente al gestor.

3.1.3 Base de información de gestión MIB.

Una base de datos relacional (organizada por objetos (o variables) y sus atributos (o valores)) que contiene información del estado y es actualizada por los agentes. La monitorización se hace leyendo el valor de los objetos de la MIB, el control se realiza modificando el valor de ciertas variaciones SNMP.

Existe otro estándar que define e identifica las variables MIB, llamado "Structure of Management Information" (SMI). SMI especifica las variables MIB, éstas se declaran empleando un lenguaje formal ISO llamado ASN.1 (Abstract Syntax Notation One), que hace que tanto la forma como los contenidos de estas

variables sean no ambiguos. Las MIB tienen 126 áreas de información sobre el estado del dispositivo, el desempeño, sus conexiones y su configuración.

El espacio de nombres ISO (árbol) está situado dentro de un espacio de nombres junto con otros árboles de otros estándares de otras organizaciones. Dentro del espacio de nombres ISO hay una rama específica para la información MIB. Dentro de esta rama MIB, los objetos están a su vez jerarquizados en subárboles para los distintos protocolos y aplicaciones, de forma que esta información puede representarse unívocamente.

Para facilitar el acceso a la información, se establece la estructura en forma de árbol jerárquico. Las ramas del árbol son los objetos gestionados, cada uno de los cuales representa algunos recursos del dispositivo, estadísticas de uso, o cualquier tipo de información de gestión.

En esencia, el SNMP es un protocolo muy sencillo puesto que todas las operaciones se realizan bajo el paradigma de carga-y-almacenamiento (load-and-store), lo que permite un juego de comandos reducido. Un gestor puede realizar sólo dos tipos diferentes de operaciones sobre un agente: leer o escribir un valor de una variable en el MIB del agente. Estas dos operaciones se conocen como petición-de-lectura (get-request) y petición-de-escritura (set-request). Hay un comando para responder a una petición-de-lectura llamado respuesta-de-lectura (get-response), que es utilizado únicamente por el agente.

La posibilidad de ampliación del protocolo está directamente relacionado con la capacidad del MIB de almacenar nuevos elementos. Si un fabricante quiere añadir un nuevo comando a un dispositivo, como puede ser un encaminador, tan sólo tiene que añadir las variables correspondientes a su base de datos (MIB).

3.2 MENSAJES SNMP

Cinco tipos de mensajes son definidos en SNMP que permiten a un administrador interrogar o establecer el valor de una variable, permitir a un agente contestar con el valor de una variable solicitada o permitir que un agente indique cierto evento relacionado a su objeto manejado. Cada mensaje incluye un número de versión, un nombre de comunidad que será usado para intercambio y uno de los cinco tipos de unidades de datos.

Se definen cinco unidades de datos de protocolo, PDU (Protocol Data Unit).

3.2.1 GetRequest.

Con esta PDU se puede solicitar el valor de una o varias variables. Las variables de las cuales se requiere conocer su valor se listan en variable-bindings. Como respuesta se recibe una PDU de tipo GetResponse, con los valores de las variables solicitadas establecidos en variable-bindings o en caso de que hubiese algún error éste se identificaría con error-index para saber qué variable falló, y error-status para saber cuál fue el fallo. El campo request-id de la PDU GetResponse tendrá el mismo valor que en GetRequest, de esta manera la aplicación puede asociar la respuesta con la petición

3.2.2 GetNextRequest.

Con esta PDU se solicita el valor de la siguiente variable a la indicada o indicadas, suponiendo un orden léxico. Pueden darse las siguientes situaciones de error:

- No hay un sucesor léxico para alguna variable de las indicadas en variable-bindings. En este caso se devuelve en error-status el valor "noSuchName" y error-index indicará qué nombre de variable falló.
- La respuesta recibida es demasiado grande, como en la PDU anterior se devolverá la respuesta con el campo error-status indicando "tooBig" y error-index a 0.
- No se puede obtener el valor de la variable sucesora a alguna de las indicadas en variablebindings. Se enviará la respuesta con error-index indicando qué variable.

3.2.3 GetResponse.

Esta PDU se genera como respuesta a las PDUs de tipo GetRequest, GetNextRequest y SetRequest.

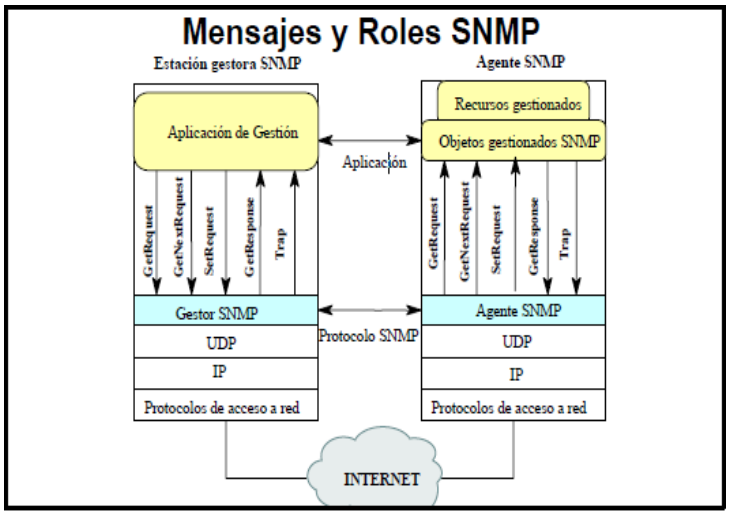
3.2.4 SetRequest.

Con esta PDU se solicita el establecimiento del valor de la variable o variables que indiquemos en variable-bindings. En caso de no haber errores el receptor devuelve una PDU de tipo Response con el campo error-status establecido a NoError y error- index a 0.

3.2.5 Traps.

Permiten a los agentes comunicar de manera asíncrona a los gestores cualquier evento que haya sucedido al objeto gestionado y en el cual el gestor tiene interés de ser informado.

Figura 3. Mensajes y Roles SNMP



Fuente: William Stallings.

Estos cinco tipos de mensajes SNMP son encapsulados en datagramas UDP. Los mensajes de petición y respuesta son enviados al puerto 161, mientras que las notificaciones de eventos usan el puerto 162.[4]

[4]JIMENEZ ALFARO Abraham Jorge, Herramienta de Gestión de Redes Virtuales. México DF Julio 2005.

4. MONITORIZACION

La monitorización de una red es el aspecto principal de la gestión. Aunque muchos de los sistemas administrables de redes no incluyen control de características de la red, todos si incluyen un componente de monitorización. El propósito de ésta es reunir información acerca del estado y comportamiento de los elementos de la red.

La información a ser reunida incluye información estática, relacionada con la configuración; información dinámica, relacionada con los eventos en la red; e información estadística, obtenida de la información dinámica. Cada dispositivo administrable en la red incluye un modulo agente responsable de recolectar localmente la información de gestión y trasmitirlo a una o más estaciones gestoras. Cada estación gestora incluye un software de administración de red para comunicarse con los agentes.Existen dos alternativas para recolectar esta información:

- Sondeo o polling, en donde el gestor solicita información al agente, que responderá a la petición.

- Informe de eventos o notificaciones, la iniciativa de la comunicación es tomada por el agente, teniendo que estar por tanto el gestor a la espera de información de este tipo.

Para abordar el proceso de monitorear una red, existen dos puntos de vista: el enfoque activo y el enfoque pasivo. Aunque son diferentes ambos se complementan.[5]

[5] VICENTE ALTAMIRANO Carlos Alberto. MONITOREO DE RECURSOS DE RED, Primera Edición, Universidad autónoma de México, 2005.

4.1 SONDEO O POLLING

Interacción petición/respuesta iniciada por el gestor. El gestor puede pedir información sobre:

- El valor de uno o varios elementos de información. El agente devolverá valores almacenadosen su MIB local. Este tipo de petición puede ser dos tipos:**específica**, pidiendo el valor de una o varias variables concretas y **genérica o de búsqueda**, solicitando información que cumpla ciertos criterios debúsqueda.

- Información sobre la estructura de la MIB del agente. Se utiliza para mantener actualizada la información que el gestor tiene de los elementos de la red, para lo cual sehace un sondeo periódico; también, para conocer la configuración de la red (y sus elementos) que está gestionando, investigar un área en detalle ante un problema y para soporte a usuarios, generando informes solicitados.

4.2 INFORME DE EVENTOS

El agente toma la iniciativa de enviar información al gestor. Se utiliza para:

- Comunicar la ocurrencia de eventos relevantes (Un cambio de estado) oinusuales (Un fallo).

- Generar un informe periódico al gestor del estado actual de los elementosgestionados por el agente.

Este sistema de comunicación es útil, sobre todo, para detectar problemas tan pronto como se producen y/o monitorizar objetos que cambian con poca frecuencia de estado (en este caso es máseficiente que el sondeo).

4.3 MONITOREO ACTIVO

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

Las técnicas para monitoreo activo son: basado en ICMP, basado en TCP, basado en UDP.

4.4 MONITOREO PASIVO

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

Como una de las técnicas, se utiliza SNMP, 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.

4.5 ESTRATEGIAS DE MONITOREO

Hay gran cantidad de motivos por los cuales un administrador necesita monitorizar entre otros : la utilización del ancho de banda, estado físico de las conexiones, la detección de cuellos de botella, detectar y solventar problemas con el cableado, administrar la información de encaminamiento entre máquinas, el consumo de cpu,consumo de memoria, tipo de tráfico, alarmas, servicios etc. La monitorización de la red es también un buen punto desde el que comenzar el estudio de los problemas de seguridad.

4.5.1 Métricas.

La definición de métricas permitirá establecer patrones de comportamiento para los dispositivos que serán monitoreados. Las métricas deben ser congruentes con los objetos a monitorear. A cada métrica sele asigna un valor promedio, el cual identifica su patrón de comportamiento.

4.5.2 Alarmas.

Las alarmas son consideradas comoeventos con comportamiento inusual. Las alarmas más comunes son las que reportan cuando el estado operacional de un dispositivo o servicio cambia. Existen otros tipos de alarmas basado en patrones previamente definidos en nuestras métricas, son valores máximos como umbrales o threshold. Cuando estos patrones son superados se producen una alarma, ya que son considerado como un comportamiento fuera del patrón. Algunos tipos de alarmas son:

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

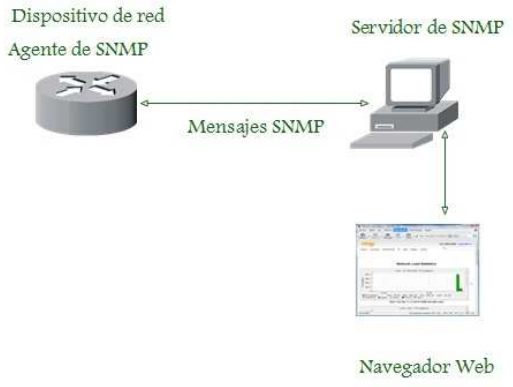
4.5.3 Elección de herramientas.

Existe un gran número de herramientas para resolver el problema del monitoreo de una red. Las hay tanto comerciales como basadas en software libre. La elección depende de varios factores, tanto humanos, económicos como de infraestructura. Para el presente trabajo de investigación se expondrá tresherramientas mássignificativas.

4.6 TOPOLOGIA DEL SISTEMA DE MONITOREO.

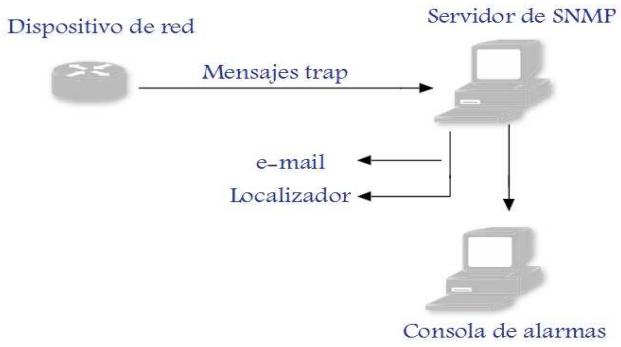
El sistema gestor/agente, consiste de un servidor que hace las solicitudes mediante el protocolo SNMP a los dispositivos de red, el cual a través de un agente de snmp envía la información solicitada. También puede ser que el dispositivo envíe mensajes trap al servidor de snmp anunciando que un evento inusual ha sucedido.

Figura 4. Monitoreo mediante solicitudes SNMP



Fuente: Autor.

Figura 5. Envío de trap



Fuente: Autor.

4.7 SISTEMA DE MONITOREO

El sistema de monitoreo incluye tres áreas: monitorización de estados, monitorización de rendimiento o tendencias, monitorización de registros o logs.[6]

La monitorización de estados, esta funcionalidad es la base de la mayoría de los sistemas de gestión de redes. Con este tipo de monitorización se responde a preguntas como "¿está activo el demonio?".

La monitorización de rendimientos, o tendencias, es la siguiente en popularidad, un ejemplo es la aplicación de monitorización RRDtool. Un monitor de rendimientos nos indica, por ejemplo, que nuestra CPU ha estado al 30% de carga durante los últimos seis meses y ha pasado a estar repentinamente al 90% en la última semana. Esta información es particularmente útil cuando se desea analizar elementos como el ancho de banda. La monitorización de registros o logs, virtualmente, toda aplicación genera logs para informar sobre qué está sucediendo y qué puede estar yendo mal.

[6]NALLEY David. Monitorización de la red con zenoss, www.Linux-magazine.es.

5. HERRAMIENTAS PARA MONITOREO DE RED

Hay tres valores técnicos fundamentales a la hora de elegir un sistema de monitorización adecuado para nuestro entorno, independientemente del precio o facilidad de instalación y de utilización. Estos tres valores son:

1. Forma de presentar los datos, las alarmas y gráficos para su estudio. Estos han de ser lo más eficientes posible y ofrecer una idea de los problemas de un solo vistazo.
2. Ubicación, distancia entre equipos y tipo de conexión (velocidad y rendimiento). A más distancia y cantidad de equipos, así como con conexiones lentas, es conveniente utilizar agentes locales que reporten a un servidor central.
3. Sistemas Operativos que se monitorizarán. Es más sencillo monitorizar únicamente máquinas basadas en Linux, aunque en la mayoría de los casos es fundamental hacerlo con Windows y conveniente utilizar WMI, (además de SNMP).

A continuación se presenta en detalle, la descripción de tres herramientas de monitorización bajo software libre con GNU Licencia Publica General, las cuales se han escogido con base en una amplia bibliografía consultada y estudiada, teniendo en cuenta también las discusiones de los foros de internet, los parámetros considerados son: soporte de comunidad activa, interfaz gráfica, plataforma, popularidad, desempeño.

5.1 NAGIOS

Originalmente llamado NetSaint (años 1999 a 2001), fue creado y es actualmente mantenido por Ethan Galstad. Nagios es un sistema de monitoreo de servidores y aplicaciones diseñado originalmente para informar fallos de una forma proactiva, reportándolos vía email, SMS, mensaje instantáneo. Esta escrito en C, es un sistema open source, publicado bajo la GNU General Public License.La potencia de Nagios viene dada por un sistema de “plugins” externos,encargados de enviar la información requerida.

Nagios proporciona supervisión de los servicios de red (SMTP, POP3, HTTP, NNTP, ICMP, SNMP, FTP, SSH) y recursos de host (carga del procesador, uso de disco, los registros del sistema), entre otros. El control remoto es manejado a través de túneles SSH o SSL cifrado. Nagios tiene un diseño simple que ofrece a los usuarios la libertad para desarrollar sus chequeos de servicio basado en las necesidades y mediante el uso de cualquiera de las herramientas de apoyo para detectar y diferenciar entre hosts que están abajo y los que son inalcanzables. Cuando los servicios o los problemas de acogida se plantean, la notificación será enviada a la persona que está a cargo de la red a través del correo electrónico, SMS.

Requisitos.Para la instalación de la herramienta NAGIOS se requiere:

- Apache 2
- PHP
- GCC: librerías de desarrollo y compilación
- GD: librerías de desarrollo

Características. Nagios proporciona funcionalidades como las siguientes:

- Monitorización de servicios de red (SMTP, POP3, HTTP, PING, etc.)
- Monitorización de recursos de los hosts (carga de procesador, uso de disco, etc.)
- Diseño simple de plugins que permiten crear monitorizaciones acordes a las necesidades especificas.
- Notificaciones a contactos cuando un servicio o un host presenta fallos (e-mail, SMS o definido por el usuario).
- monitorización del estado y disponibilidad de equipos, servicios y recursos.
- En cuanto a la interfaz gráfica, nagios permite varios tipos de mapas de visualización de red y de los recursos monitorizados.
- Monitorización remota, a través de túneles SSL cifrados o SSH.
- Visualización del estado de la red en tiempo real a través de interfaz web, con la posibilidad de generar informes y gráficas de comportamiento de los sistemas monitorizados, y visualización del listado de notificaciones enviadas, historial de fallos, archivos de registros.

5.2 ZENOSS

Erik Dahl comenzó el desarrollo de Zenoss en el 2002 y en agosto del 2005 fundó Zenoss, Inc., con Bill Karpovich. Zenoss, Inc. patrocina el desarrollo de Zenoss Core. Teniendo en cuenta que este proyecto open source también incluye dos versiones de esta herramienta: la enterprise y la profesional, para fines de este documento se hará referencia a la versión core.

Zenoss (Zenoss Core) es una herramienta de código abierto lliberado bajo la Licencia Pública General de GNU (GPL) versión 2, para monitoreo de redes y servidores basada en otras herramientas como cacti y nagios (ambas open source), utiliza diferentes tecnologías opensource basadas en el lenguaje Python como el servidor de aplicaciones Zope, las librerías Twisted, rrdtool para gráficos y la base de datos MySQL.Zenoss Core se basa en las siguientes tecnologías de código abierto:

- Zope Application server: servidor web orientado a objetos desarrollado en Python.
- Python: lenguaje de programación extensible.
- Net-SNMP: protocolo de monitoreo que recolecta información sobre el estado de los sistemas.
- RRDtool: grafica y guarda registros de series temporales de datos.
- MySQL: motor de base de datos muy popular de código abierto.
- Twisted: herramienta para interconexión de redes dirigida por eventos desarrollada en Python.

Zenoss se distribuye en rpm para su instalación automática bajo RedHat, CentOS y Fedora Core 6. Para Suse, Debian, Ubuntu, FreeBSD, Gentoo, Solaris 10 y Mac OS X, se distribuyen las fuentes para ser compilados en cada uno de los sistemas mencionados.

Zenoss no necesita agentes en las máquinas remotas, ya que con SSH puede ejecutar de forma segura cualquier comando que deseemos para extraer todo tipo de información. Para monitorizar máquinas Windows, utiliza un binario que conecta usando WMI para modelar y monitorizar sus servicios.

Características. Zenoss proporciona las siguientes funcionalidades:

- Monitoreo de sistemas operativos windows y linux sin necesidad de instalar agentes en los sistemas operativos, por medio de SNMP o WMI para los sistemas windows.
- Monitoreo de disponibilidad de dispositivos en la red utilizando SNMP.
- Monitoreo de servicios de red (HTTP,POP3,NNTP,SNMP,FTP).
- Monitoreo de recursos de máquinas anfitrionas (Microprocesador, utilización de disco) en la mayoría de los sistemas operativos de red.
- Monitoreo de rendimiento de dispositivos a través de series temporales de datos.
- Herramientas de gestión de eventos para anotar las alertas de un sistema.
- Detecta automáticamente recursos en una red y cambios en su configuración.
- Sistema de alertas que provee notificaciones basadas en un conjunto de reglas y calendarios.
- Soporta el formato de plugins Nagios.
- Administración y monitoreo de eventos: Mantener la disponibilidad y performance de su red. Obtener información de logs y eventos de diferentes fuentes como syslog, traps SNMP y el event log de Windows.
- Remediación automática: cuando ocurre un problema, Zenoss puede actuar tomando acciones correctivas basadas en reglas y políticas.
- Visualización de la red: a medida que su red crece Zenoss incluye mapeo de dependencias, visualización de topologías de red de capa 3 y la posibilidad de integrarse con Google Maps.
- Reportes comunitarios: le permiten a los usuarios finales de generar sus propios reportes en el momento en que lo necesiten dentro de los cuales se puede encontrar reportes históricos o en tiempo real de dispositivos, eventos, performance, usuarios y mucho más.

- Provee de una interfaz web que permite a los administradores de sistemas monitorear disponibilidad, inventario/configuración, desempeño y eventos.
- Ofrece posibilidad de utilizar la api de Google Maps para presentar en el dashboard de Zenoss un mapa con la ubicación de nuestros servidores.

5.3 ZABBIX.

Zabbix fue creado por AlexeiVladishev en el año 2001, actualmente se desarrolla y se soporta por la compañía Zabbix SIA, su última versión estable es zabbix 1.8.4. Es una solución Open Source con Licencia Publica General Versión 2, desarrollado en C++ y en PHP para su interfaz gráfica, requiere de Apache, MySQL (Postgress u Oracle), PHP y librerías PHP de gráficos o de SNMP, diseñada para controlar y rastrear el desempeño y la disponibilidad de servidores, aplicaciones, dispositivos y recursos que hacen parte de una red. Disponible en las plataformas: AIX, FreeBSD, HP-UX, Linux, Mac OS X, Novell Netware, Open BSD, SCO Open Server, Solaris, Tru64/OSF, Windows NT 4.0, Windows 2000, Windows 2003, Windows XP.

Zabbix es una herramienta de monitorización semi-distribuida, proporciona una administración centralizada y en tiempo real a través de una interfaz vía web browser, ofrece características de administración avanzada, soporta triggers, con los cuales se pueden realizar diversas alertas y/o notificaciones programadas vía e-mail, SMS e incluso a través de Jabber para usuarios de Google Talk.

Permite el uso de nodos de monitoreo remoto o proxy's. Además tiene soporte para traps SNMP en las versiones 1, 2 y 3 del protocolo, proporciona también extensa información sobre la máquina que monitoriza: disco, memoria, E/S, entre

otras; mediante un completo sistema de estadísticas históricas cuyos datos se guardan en bases de datos (oracle, mysql, postgreSQL, SQLite).

Requisitos. Los requisitos de software para utilizar zabbix son:

● apache 1.3.12 o superior (trabaja con 2.x)
● mysql 3.22 en adelante o PostgreSQL 7 o mayor
● PHP4 o superior (necesita modulo GD para generar las gráficas)

Las librerías NETSNMP, son necesarias para el server, para instalarlo a partir del código fuente es necesario GCC.

Características y arquitectura de zabbix. Se debe diferenciar entre el servidor y los agentes. El servidor recopila la información que generan los agentes, la muestra y almacena en la base de datos seleccionada durante su instalación y configuración. Este trabaja en el puerto 10051pero se puede cambiar. Los agentes se encargande enviar al servidor zabbix toda la información que se está monitoreando. Se destaca las siguientes características:

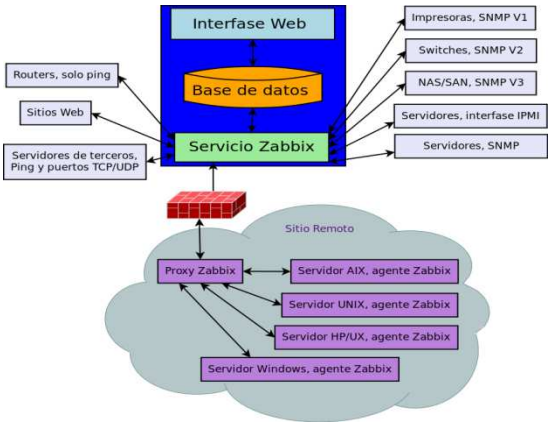
- El agente está disponible para cualquier variante de Unix, en la mayoría de distribuciones GNU/Linux se encuentra en repositorios oficiales y para la mayoría de sistemas operativos de Microsoft hay binarios precompilados de fácil instalación).
- Monitorización de dispositivos SNMP V1, 2 y 3.
- Monitorización de dispositivos con interfaces IPMI (como por ejemplo las ILO en servidores HP o DRAC en servidores Dell).
- Permite monitorear sitios web, URLS específicas y secuencias de acceso a sitios web.

- Permite el uso de plantillas (Templates) para facilitar el modelamiento de dispositivos a monitorear.
- Emite notificaciones o alertas, que permiten configurar niveles de escalamiento y opcionalmente también utilizar scripts para emitir tipos nuevos de alertas. Notificaciones vía e-mail, mensajería y localizador.
- monitorización de disponibilidad y rendimiento de redes, servicios y aplicaciones en tiempo real y en forma remota.
- Escalabilidad superior a 100000 dispositivos y con 1000000 de monitores.
- Visualización de mapas, gráficos, vistas personalizadas, etc. Generaciónde estadísticas.
- ZABBIX proporciona la funcionalidad de auto-descubrimiento, basado en la siguiente información.
    - rangos de IP
    - La disponibilidad de servicios externos (FTP, SSH, WEB, PO3, IMAP, TCP)
    - La información recibida de agente ZABBIX
    - La información recibida de agente SNMP
- Internamente Zabbix está integrado por tres componentes principales, a saber:

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

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

Figura 6. Arquitectura Zabbix



Fuente: Revista Linux.net

5.4 CUADRO COMPARATIVO

A continuación se presenta un cuadro comparativo de los principales parámetros considerados en una herramienta de monitoreo.

Tabla 1. Comparación de herramientas de monitorización

CARACTERISTICA	NAGIOS	ZENOSS	ZABBIX
LICENCIA	GNU/GPL	GNU/GPL	GNU/GPL
MANEJADOR DE DATOS	MySQL, RRDtool	ZODB, MySQL, RRDtool	Oracle,Mysql,Posgre SQL, SQLite
COMPLEJIDAD CONFIGURACION	Medio	Medio	Bajo
AUTODESCUBRIMIENTO	Vía Plugins	Si	Si
REPORTES	Vía Plugins	Si	Si
ALERTAS	Si	Si	Si
INVENTARIO	Vía Plugins	Si	Si
AGENTE	Soportado	No	Soportado
PROTOCOLO SNMP	Vía Plugins	Si	Si
PLUGINS	Si	Si	Si
AREA MONITORIZACION	Local/Remota	Local/Remota	Local/Remota

Fuente: Autora.

En resumen, una desventaja presentada de la herramienta Zenoss, se debe a que depende de servidor zope y la complejidad de su interfaz.La herramienta nagios, presenta gran popularidad a nivel de la red[7], sin embargo su funcionalidad depende o está basada en la configuración de plugins.

En cuanto aZabbix, posee las mismas funcionalidades de nagios, se le suma, la capacidad de guardar historial y su capacidad de monitorización en tiempo real.Zabbix es una solución de código abierto totalmente integrada que ofrece características de monitorización avanzadas, alertas, correlación de gráficas y visualización.

Zabbix, dispone de una interfaz gráfica amigable, desarrollada en **php**. Desde este punto, resulta relativamente sencillo el manejo de la aplicación, tanto para monitorizar como para configurar el entorno.

Para el cumplimiento de los objetivos propuestos, se opta por la instalación de la herramienta zabbix, en consideración a las características encontradas, a su amigabilidad en la interfaz web y a la forma de presentación de gráficas.

[7] http://www.google.com/trends.

6. INSTALACION DE UNA HERRAMIENTADE SOFTWARE LIBRE PARA MONITOREO

6.1 INSTALACION DE UBUNTU 9.1 SERVER

Para la instalación de la herramienta de monitoreo zabbix versión 1.8.4, se ha escogido la plataforma de software libre GNU/Linux Ubuntu 9.1 server Karmic Koala. Para el propósito del presente trabajo, la instalación del sistema operativo Linux será en forma virtualizada. Es de resaltar que el concepto de virtualización está orientado a la optimización de los recursos de hardware, mediante lo cual es posible habilitar un sistema de gestión.

En este escenario, la instalación de la plataforma Ubuntu 9.1 server i386.iso como sistema base para la implementación de la herramienta zabbix, se hará sobre VmwareWorkstation, alojadasobre un sistema operativo WINDOWS 7. Lo cual permite tener los dos ambientes (windows y linux) en el mismo equipo y para cambiar de ambiente de trabajo, simplemente se procede a cambiar de ventana activa.

Ubuntu, es una distribución GNU/Linux que ofrece una suite de repositorios para cualquier tipo de aplicación, no requiere de grandes capacidades computacionales para la instalación de su sistema base. Proporciona facilidad para la instalación de paquetes a través del Centro de software de Ubuntu o también desde una terminal de línea de comandos desde donde se puede instalar, actualizar, configurar y remover aplicaciones.Los requerimientos mínimos de máquina para trabajar con el sistema Windows 7 y la plataforma Ubuntu 9.1 server se detalla a continuación:

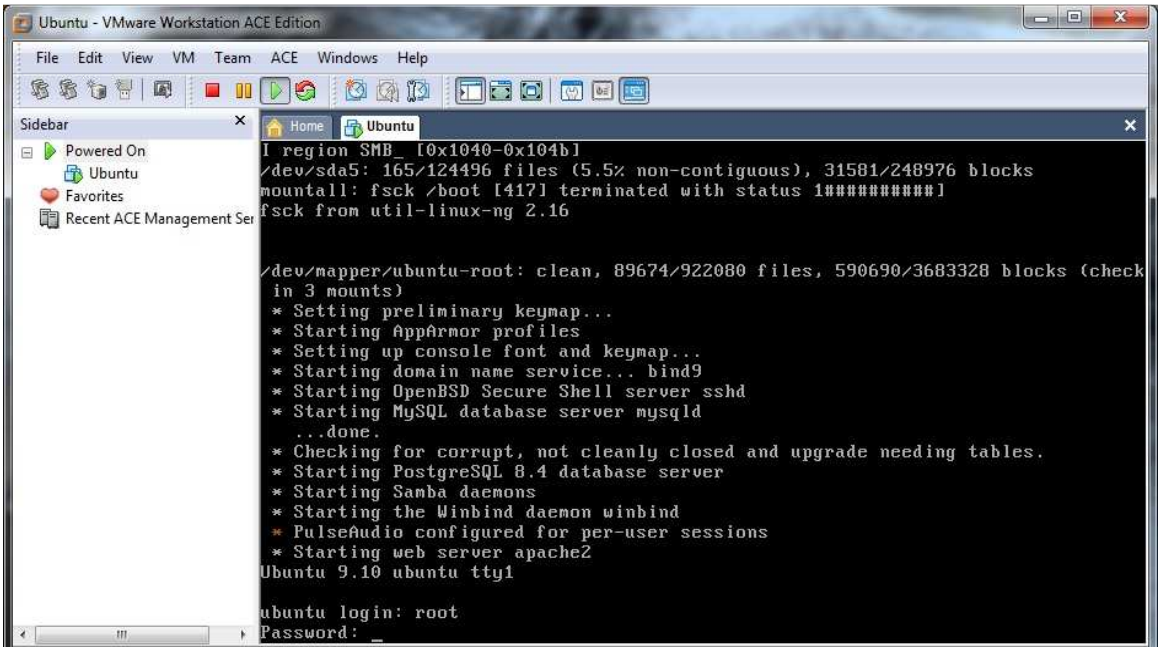
Tabla 2. Requerimientos mínimos de máquina

Plataforma	Memoria RAM	Procesador	Espacio en Disco
Ubuntu Linux 32 bits	1024 MB	1.0 GHz x86 32 bit	5GB
Windows 7 32 bits	1024 MB	2.0 GHz x86 32 bit	6GB

Fuente: Autora.

Una vez, realizada la instalación con las especificaciones mencionadas tenemos la siguiente ventana desde donde se carga la imagen iso de ubuntu server , se ingresa con el usuario configurado en la instalación de linux, usuario: **root** y password: **root2011**.

Figura 7. Instalación Ubuntu en maquina virtual Vmware



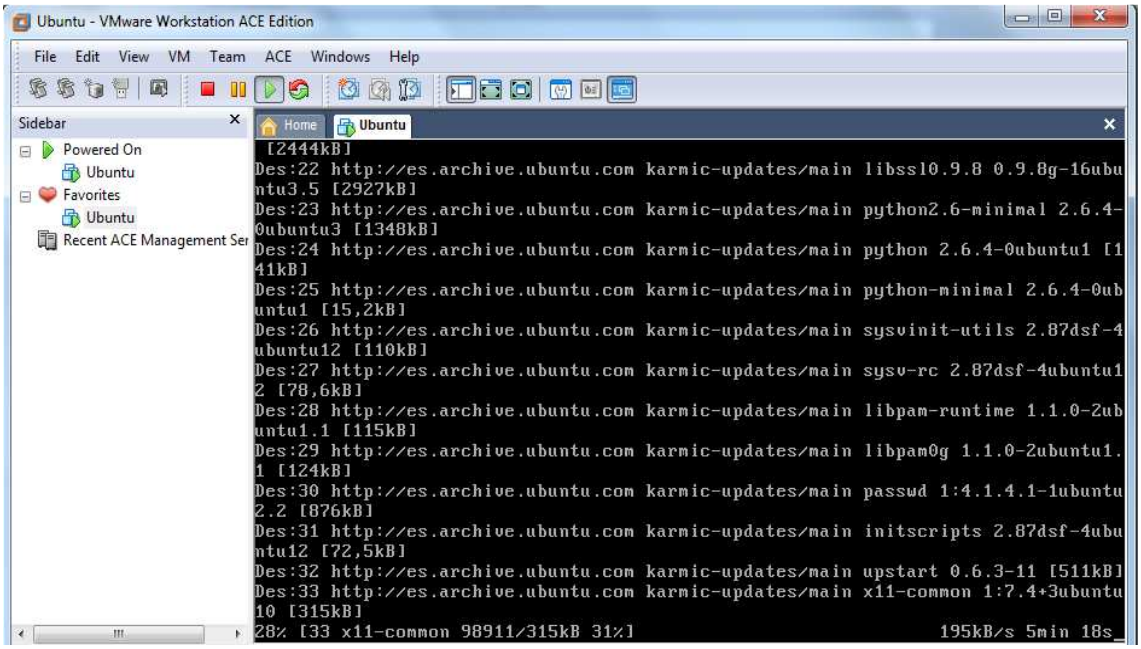
Fuente. Autora.

Ya instalada la distribución Ubuntu 9.1 server, el primer paso consiste en actualizar la información de los repositorios y de todos los paquetes que se

tieneinstalados para evitarnos problemas. Eso se consigue ejecutando el siguiente comando:

sudo apt-get update luego
Sudo apt-get upgrade

Figura 8. Actualización y descarga de repositorios

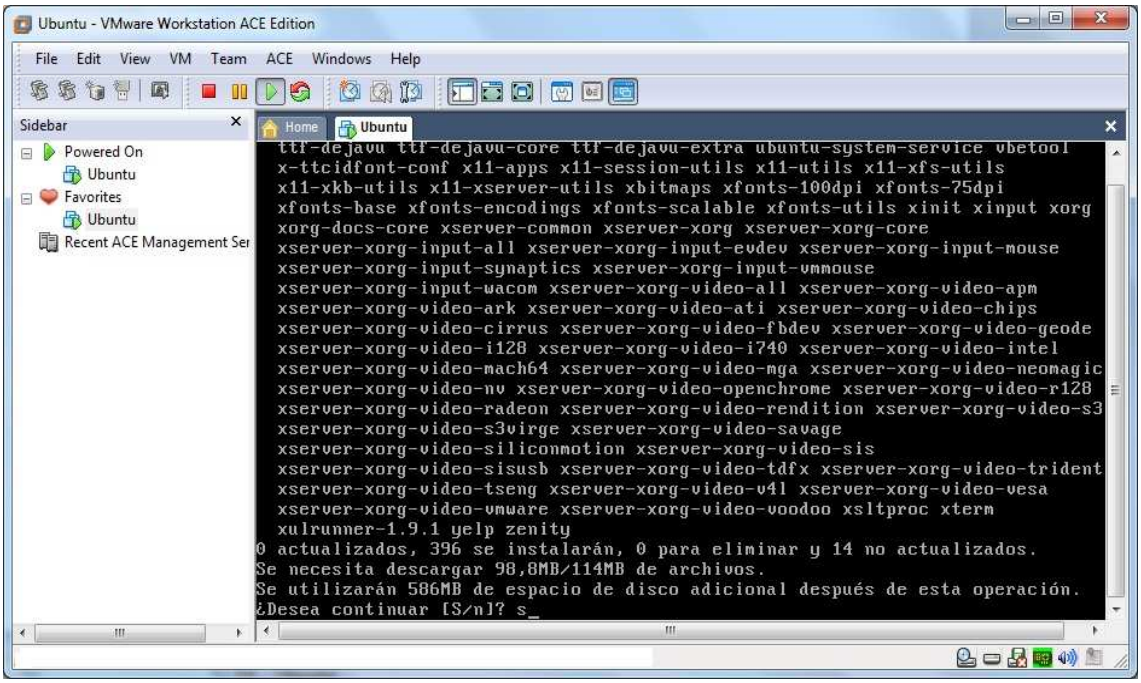


Fuente. Autora.

En efecto, como las versiones server de Ubuntu vienen sin entorno gráfico (normal, teniendo en cuenta que están destinadas a servidores) y considerando que posteriormente se necesitará hacer uso de un navegador para la administración de la herramienta zabbix, entonces se procedió con la descarga e instalación de un entorno gráfico mínimo, instalando los paquetes xorg y gnome-core con el siguiente comando:

sudo apt-get install xorg gnome-core

Figura 9. Instalación de entorno gráfico en Ubuntu server



Fuente. Autora.

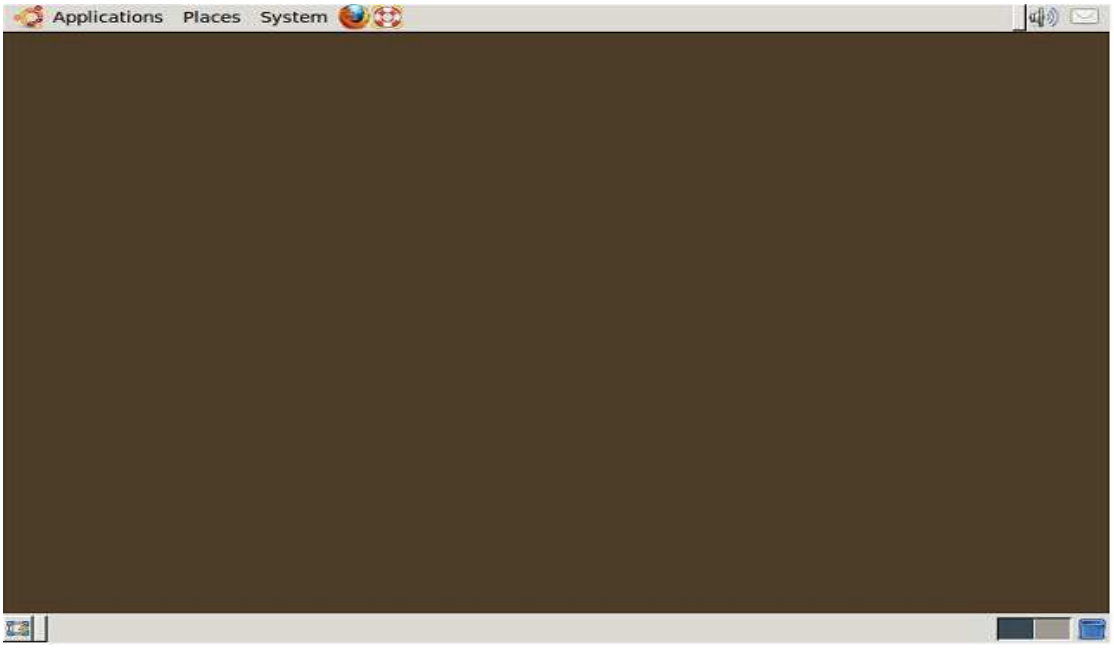
Luego, se procede con la instalación del navegador firefox, con el comando:

sudo apt-get install firefox

Ahora, ya se tiene el entorno grafico para Ubuntu 9.1 server con el navegador Firefox, como podemos observar en la figura 10.

El comando apt-get, es una potente herramienta de línea de órdenes diseñada para trabajar con el *Advanced Packaging Tool* (APT) de Ubuntu realizando funciones de instalación de nuevos paquetes de software, actualización de paquetes de software, actualización del índice de paquetes, e incluso actualización de todo el sistema Ubuntu, para lo cual se requiere estar conectado a internet.

Figura 10. Navegador Firefox en Ubuntu 9.1 server



Fuente: Autora.

6.2 INSTALACION DE ZABBIX.

La versión de zabbix que se implementará en el presente trabajo es la actualmente estable1.8.4:

zabbix-1.8.4.tar.gz

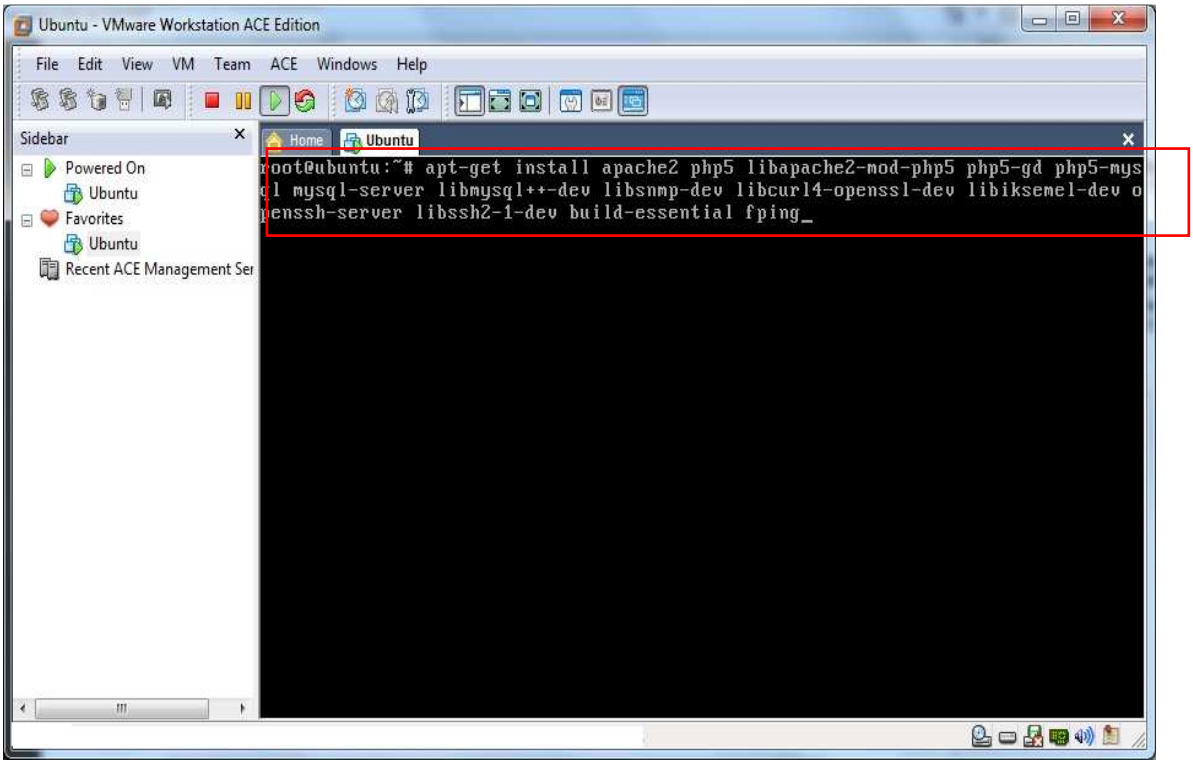
6.2.1 Instalación de requisitos previos.

Zabbix necesita un servidor Web con soporte PHP y un contenedor para sus datos como MySQL. Además es necesarioque PHP tenga soporte GD y el sistema las

librerías para SNMP, CURL y JABBER, tambiénse necesita las herramientasde compilación necesarias. Para todo esto,se debe ejecutar desde consola como root:

apt-get install apache2 php5 libapache2-mod-php5 php5-gd php5-mysql mysql-server libmysql++-dev libsnmp-dev libcurl4-openssl-dev libiksemel-dev openssh-server libssh2-1-dev build-essential fping

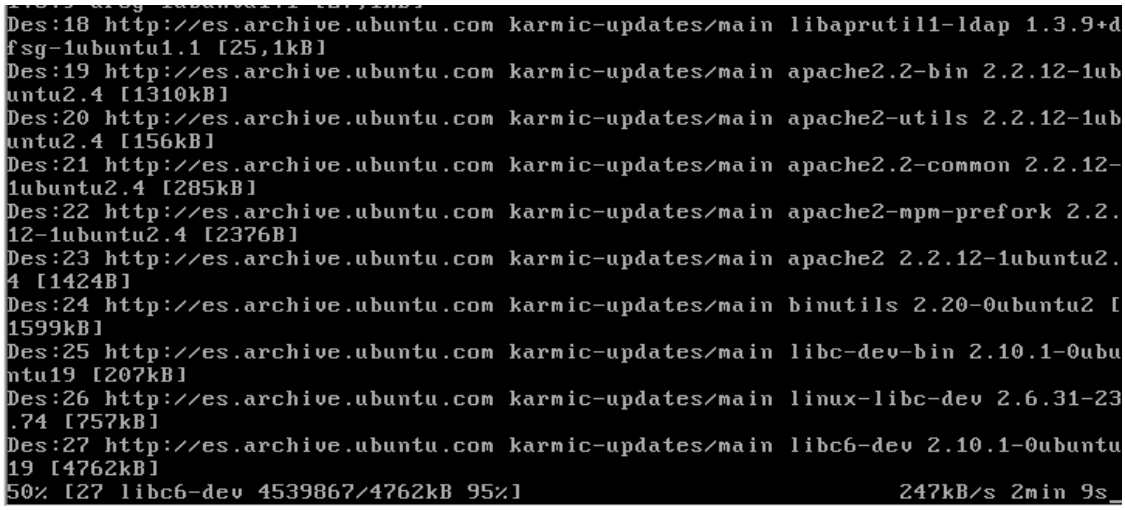
Figura 11. Instalación de requisitos previos



Fuente: Autora.

El instalador indica el espacio en disco que se va a utilizar y solicita la confirmación de la continuación como se observa:

Figura 12. Confirmación de instalación de requisitos previos

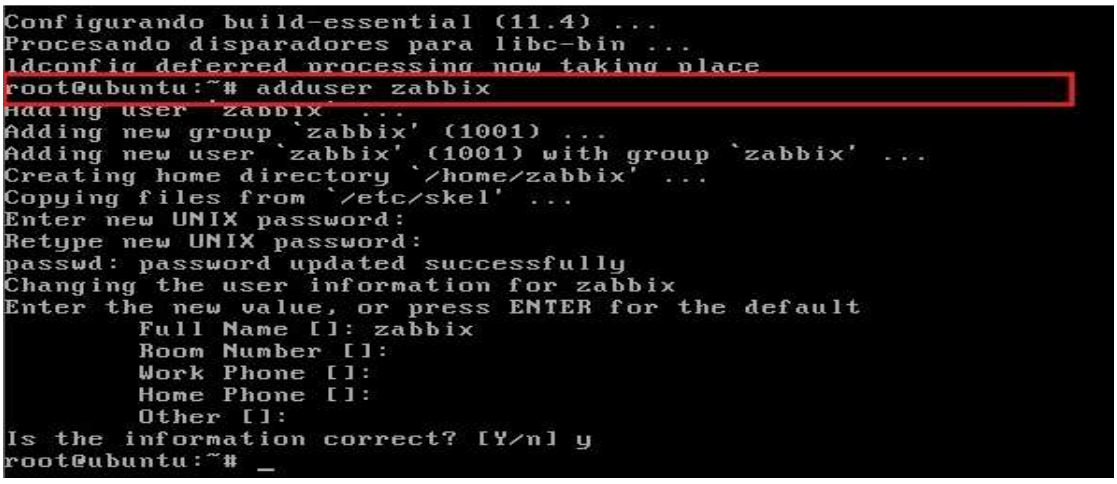


Fuente: Autora.

6.2.2 Creación de usuario zabbix.

Se debe crear un usuario llamado zabbix para que el funcionamiento sea seguro, para ello ejecutamos el siguiente comando como root.

Figura 13. Creación de usuario zabbix



Fuente: Autora.

6.2.3 Descargar fuentes.

Se descarga los archivos de compilación de zabbix, Las ultimas fuentes las podemos descargar visitando la páqina:http://sourceforge.net, para ello, se usa el comando wget,el cual permite la descargade contenidos desde servidores HTTP, HTTPS y FTP.Se ejecuta los siguientes comandos como root y zabbix para descargarlas y descomprimirlas, con esto se generará un directorio donde se encuentra todo el código fuente.

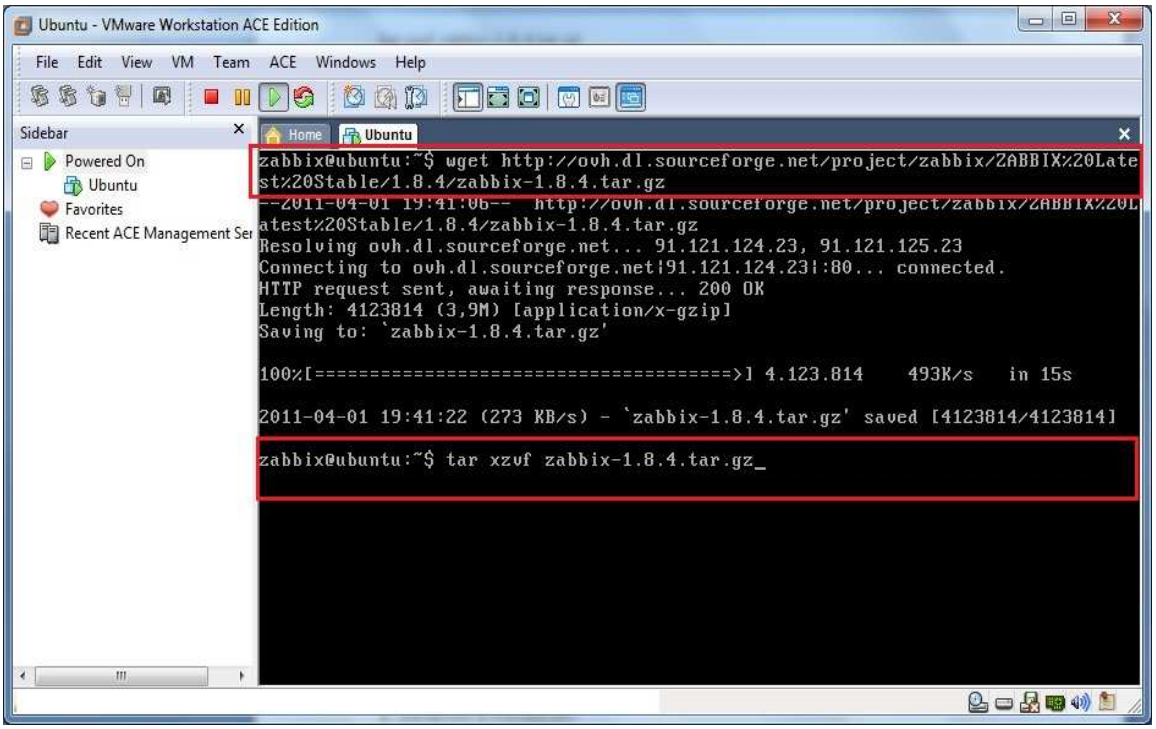
su - zabbix

wget

http://ovh.dl.sourceforge.net/project/zabbix/ZABBIX%20Latest%20Stable/1.8.4/zabbix-1.8.4.tar.gz

tar xzvf zabbix-1.8.4.tar.gz

Figura 14. Descargando y desempaquetando Fuentes zabbix



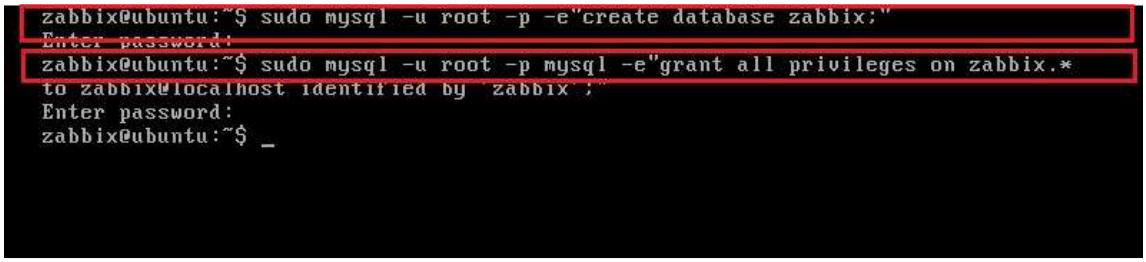
Fuente. Autora.

6.2.4 Creación del esquema.

El servidor de bases de datos (MySql, PostgreSQL u Oracle) debe estarse ejecutando y se debe tener acceso root o a una cuenta validad con permisos para crear bases de datos en el servidor, se ha optado por utilizar Mysql.

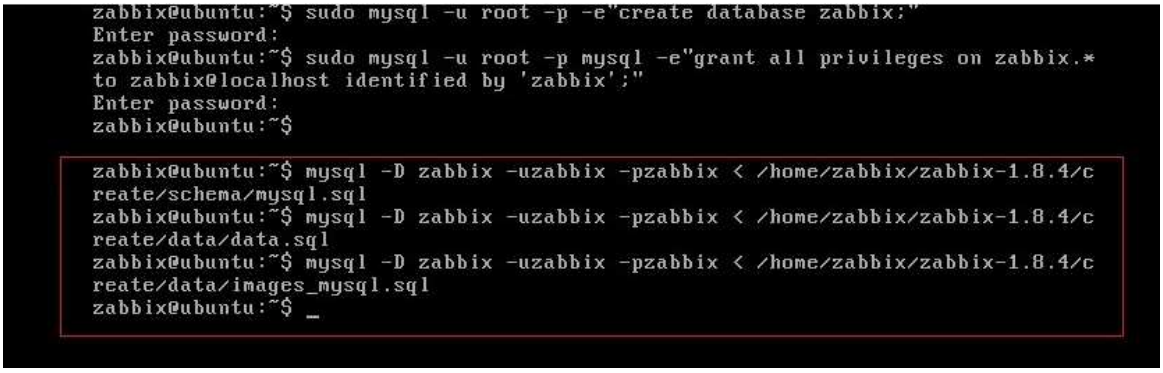
Dentro de las fuentes descargadas se incluyen unas plantillas para la creación del esquema y otras opciones, para lo cual se ejecuta los comandos como usuario zabbix para dejar funcionando el almacén de datos, como se observa en la figura 16.

Figura 15. Creación de base de datos y configuración de acceso para zabbix



Fuente: Autora.

Figura 16. Configuración de la base de datos Mysql

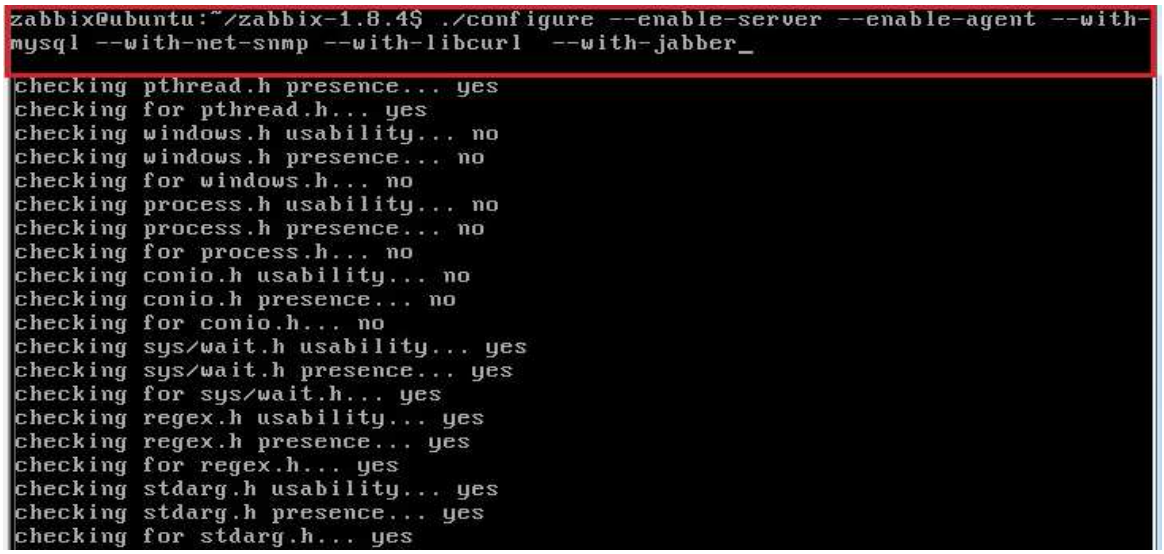


Fuente: Autora.

6.2.5 Configurar e instalación desde las fuentes.

Como está desarrollado en C++ antes de instalar se debe compilar, para lo cual se configura las opciones de compilación con el programa “configure”. Se configuran las fuentes para dar soporte como servidor, instalar el agente en el servidor zabbix, usar Mysql como contenedor de datos, soporte para net-snmp, curl y jabber. Para ello se ejecuta como usuario zabbix, el comando de la siguiente figura:

Figura 17. Configuración de las fuentes de instalación

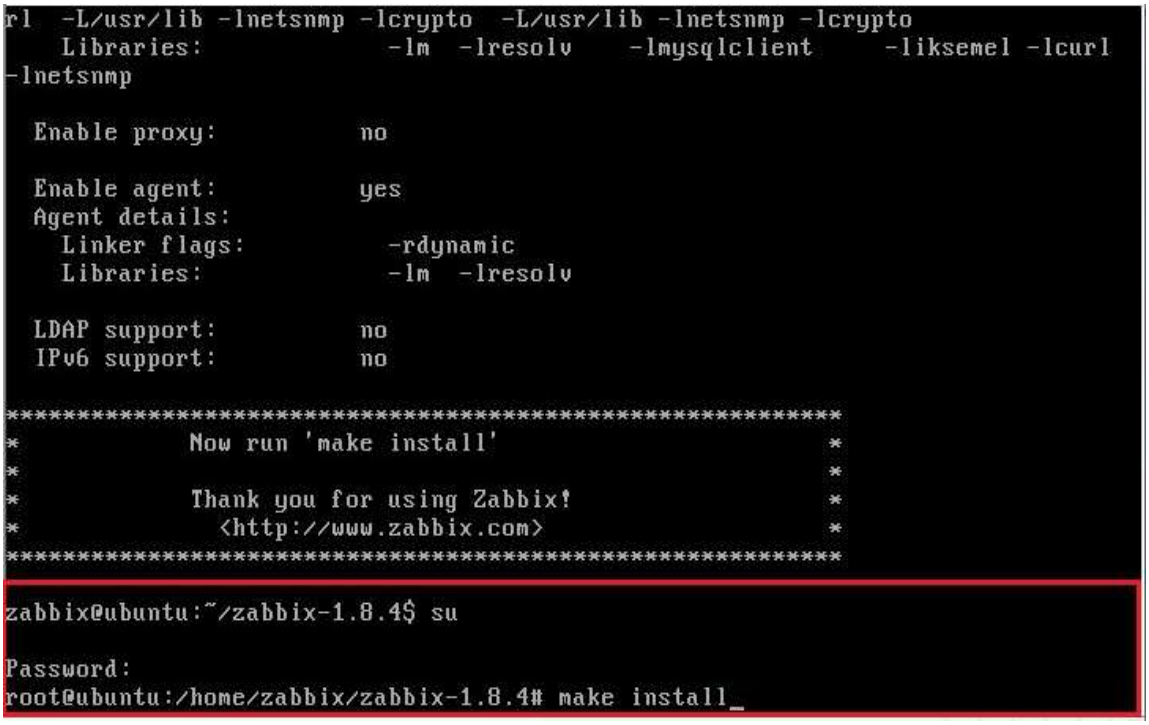


Fuente: Autora.

La figura 18, permite observar el resultado de la configuración de las fuentes y confirma que se ha predeterminado los siguientes parámetros: Activación de servidor, Motor de base de datos Mysql, librería cURL, soporte de jabber, protocolo net-snmp y activación del agente zabbix para Linux. Luego, se compila e instala las fuentes, para ello se ejecuta como zabbix.

su
make install

Figura 18. Comando de compilación e instalación de fuentes zabbix



Fuente: Autora.

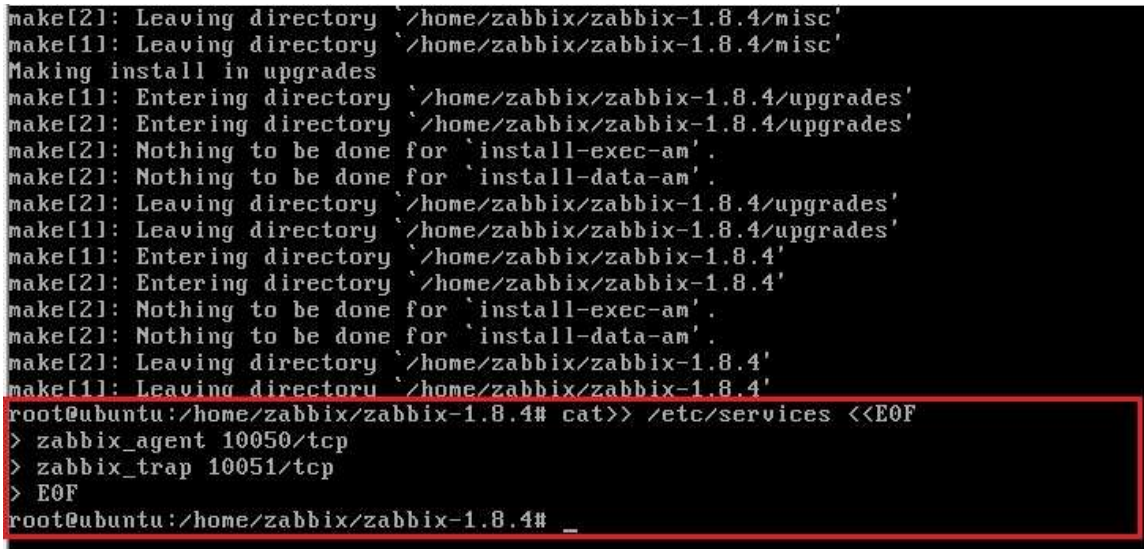
6.2.6 Configuración del sistema.

Se edita el archivo /etc/services, se agrega las siguientes 2 líneas para registrar el tipo de servicio, que se usará en esos puertos:

zabbix_agent 10050/tcp
zabbix_trap 10051/tcp

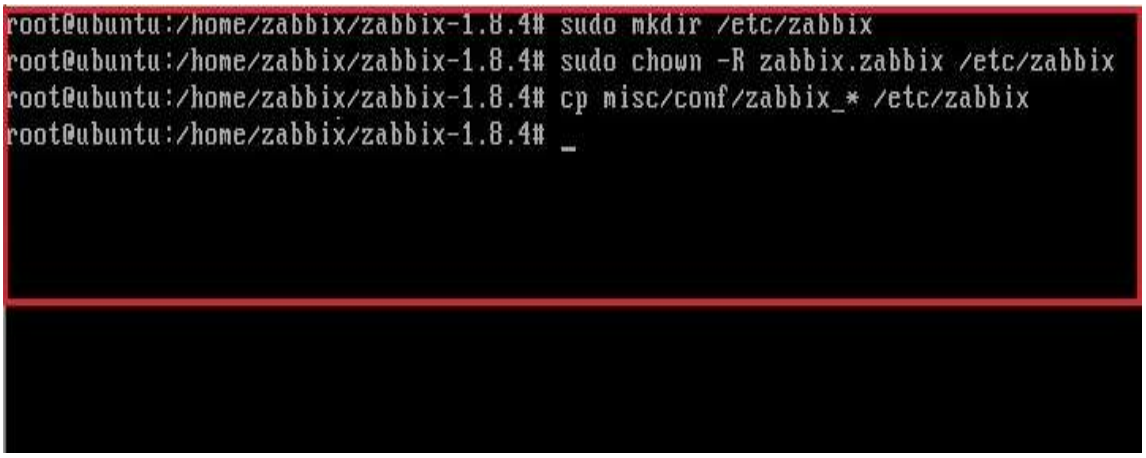
Luego, se crea el directorio donde se almacenarán los ficheros de configuración y se le asigna el propietario. Se ejecuta los comandos como se observa en la figura 20.

Figura 19. Configuración de puertos



Fuente: Autora.

Figura 20. Creación de directorio para almacenamiento de ficheros de configuración



Fuente: Autora.

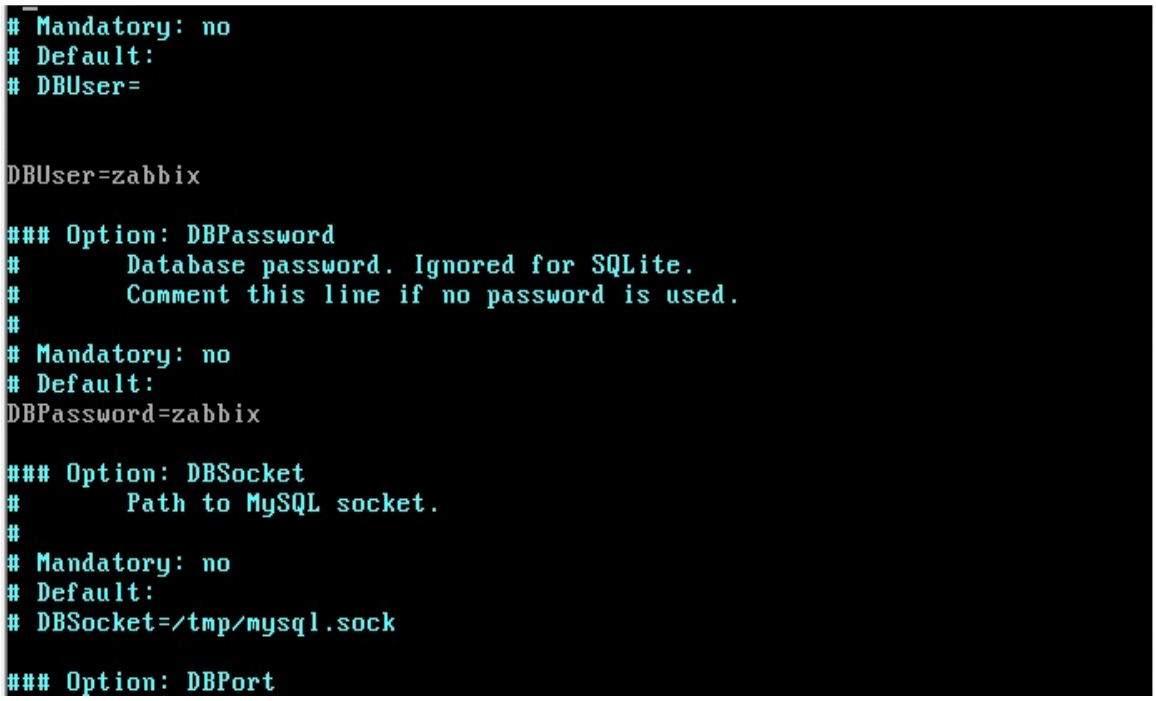
Finalmente, se edita el fichero de configuración del servidor zabbix para declarar los parámetros de conexión, para ello se utilizo nano, el cual es un sencillo editor de textos para el terminal, que viene instalado por defecto en Ubuntu:

Sudo nano /etc/zabbix/zabbix_server.conf

DBUser=zabbix

DBPassword=zabbix

Figura 21. Configuración de parámetros de conexión a BD de Mysql

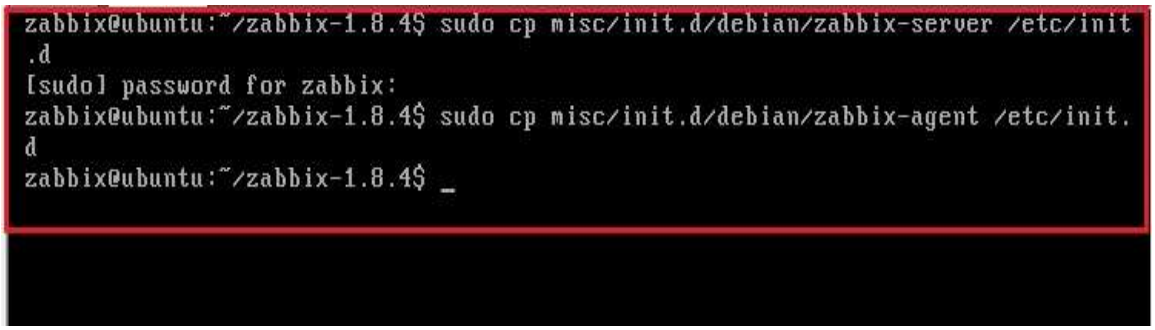


Fuente: Autora.

6.2.7 Configuración scrips de inicio.

Para que el servidor Zabbix y el agente arranquen de forma predeterminada durante el inicio del sistema, se ejecuta:

Figura 22. Configuración de Script de Arranque



Fuente: Autora.

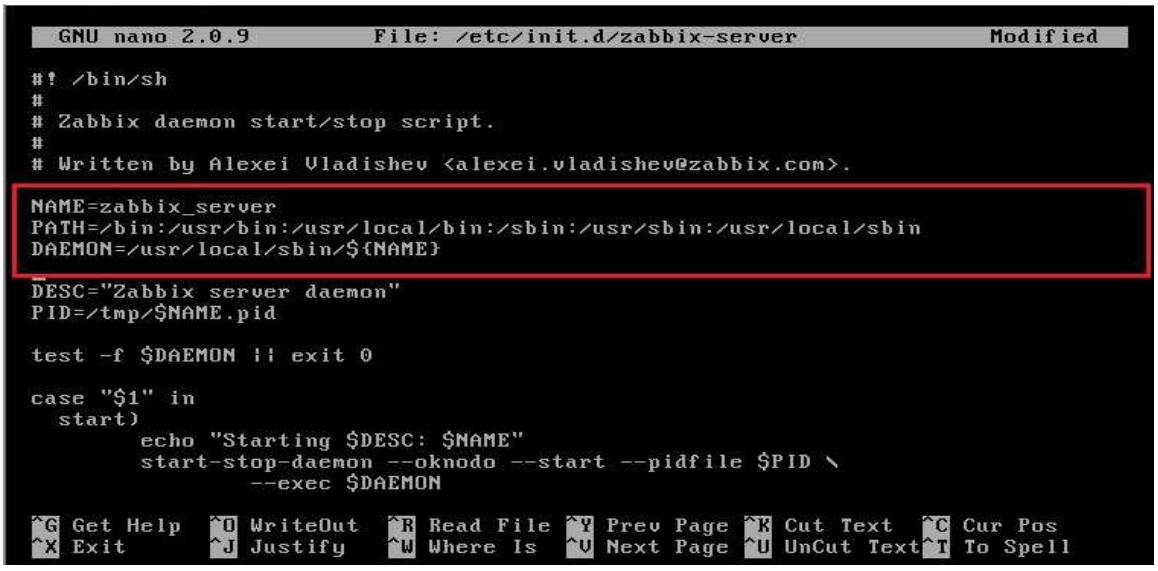
Luego se edita los ficheros tanto para el servidor como para el agente:

sudo nano /etc/init.d/zabbix-server

sudo nano /etc/init.d/zabbix-agent ,

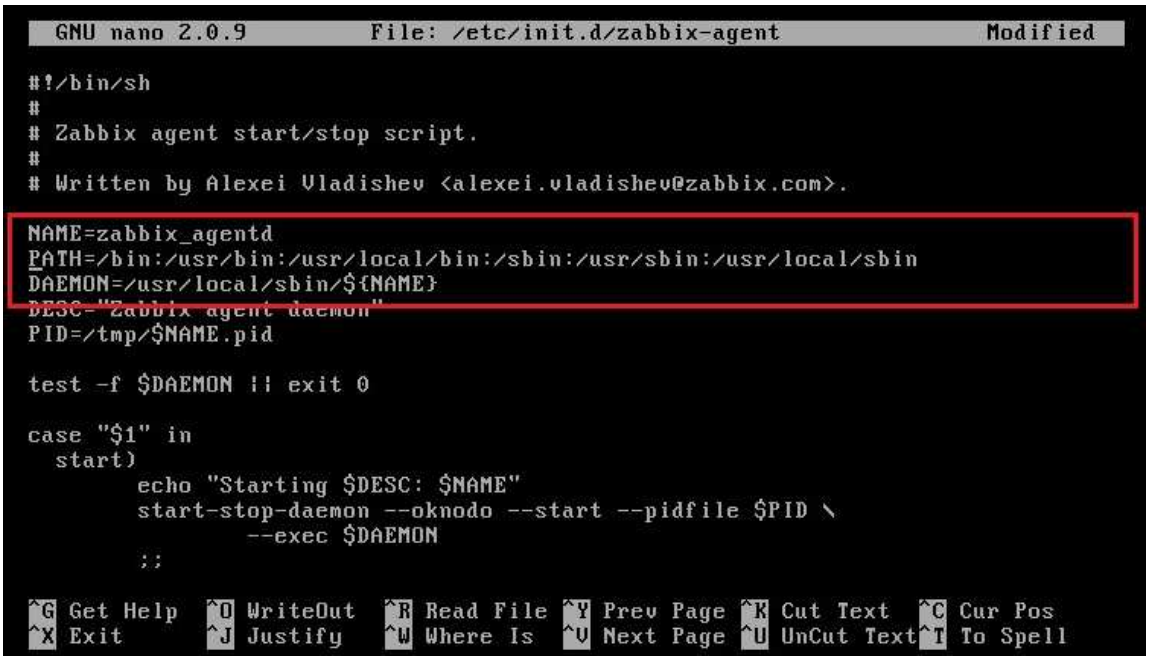
Como se observa en las figuras 23 y 24, se agrega dos líneas correspondientes al camino o ruta del servicio.

Figura 23. Edición de script de inicio para servidor



Fuente:Autora.

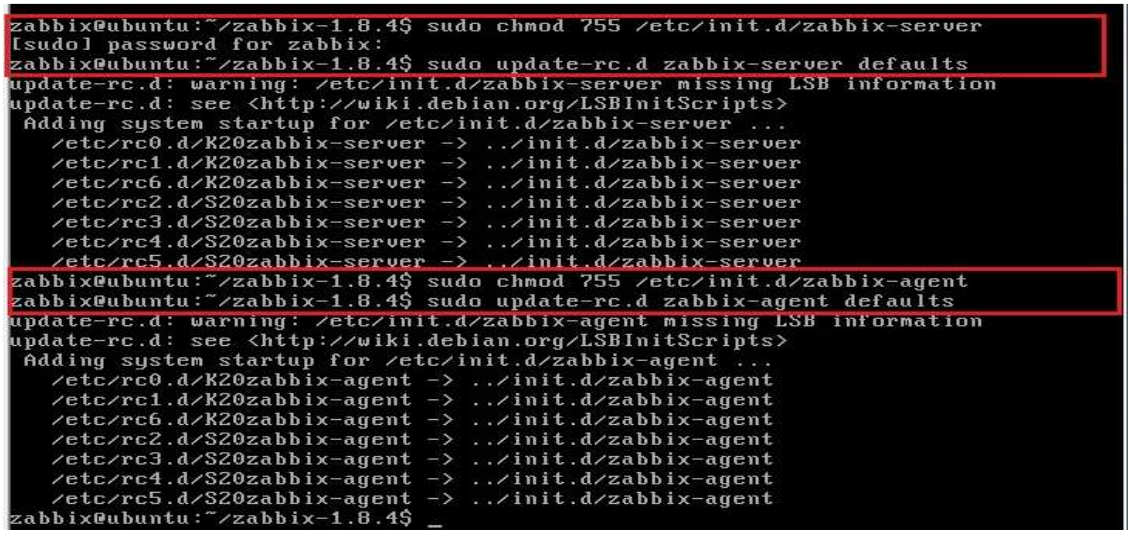
Figura 24. Edición script de inicio para agente



Fuente: Autora.

Por último se asignan permisos y se configura el nivel de arranque en el que van a iniciar.

Figura 25. Asignación de permisos a script

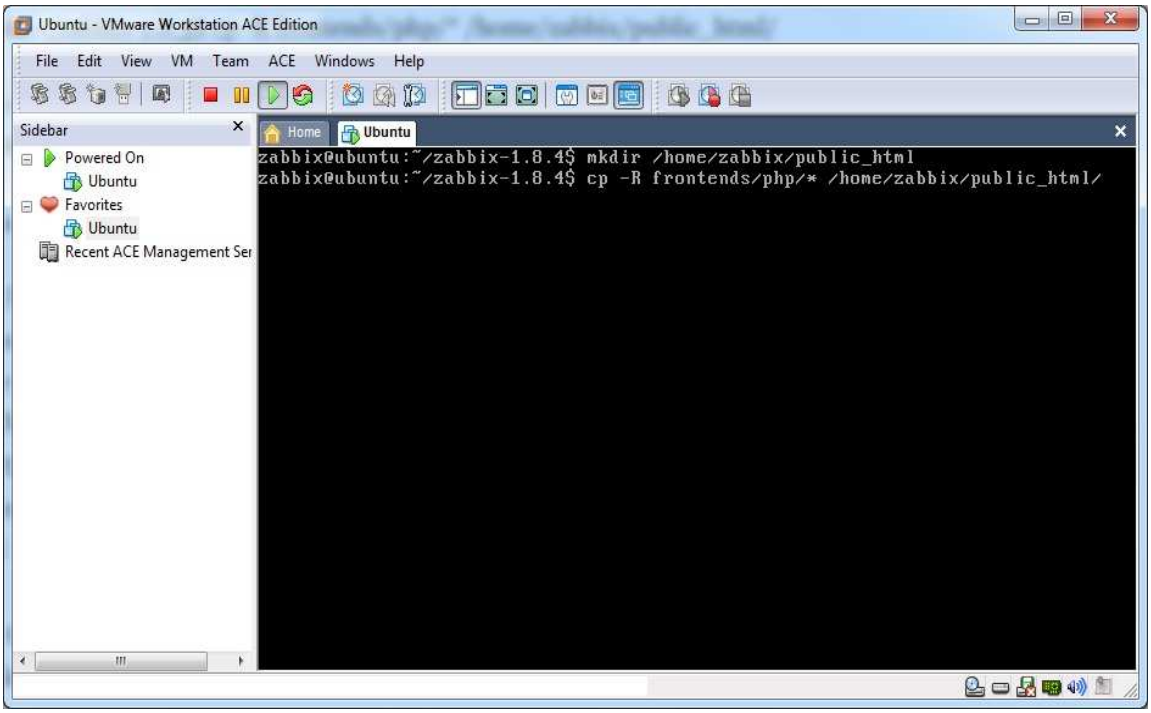


Fuente: Autora.

6.2.8Instalacionfront - end

Los archivos que componen la interfaz web, se encuentran dentro de la carpeta que se crea cuando se descompacta el código, dentro del directorio frontends/php. Entonces se ingresa los siguientes comandos:

Figura 26. Configuración de Interfaz web

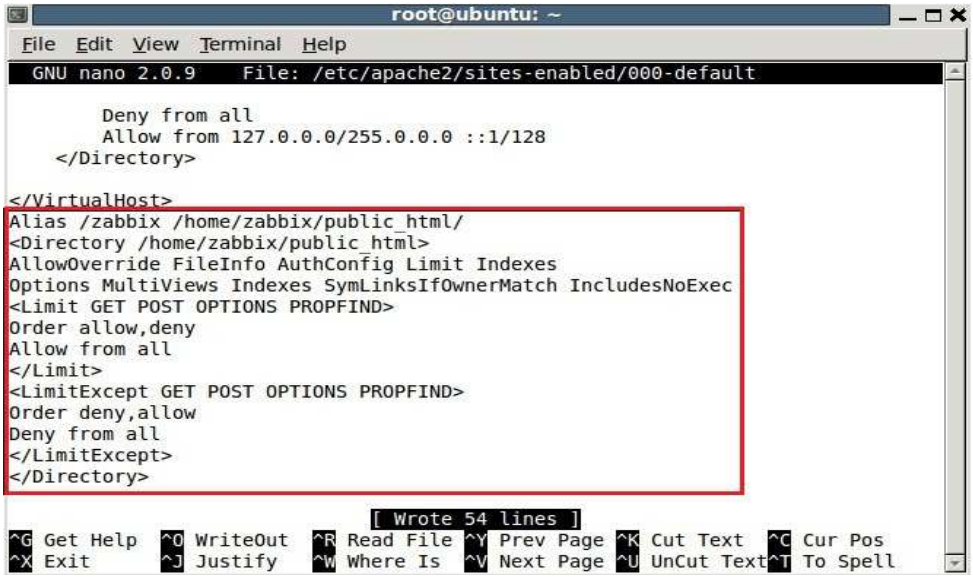


Fuente: Autora

Se modifica el apache con el comando descrito, agregando las líneas que muestra la figura 27.

Sudo nano /etc/apache2/sites-enabled/000-default

Figura 27. Configuración del apache



6.2.9 Parámetros PHP

Zabbix requiere que algunos parámetros de php sean modificados, para lo cual se edita el fichero php.ini.

Sudo nano /etc/php5/apache2/php.ini

Memory limit=128M

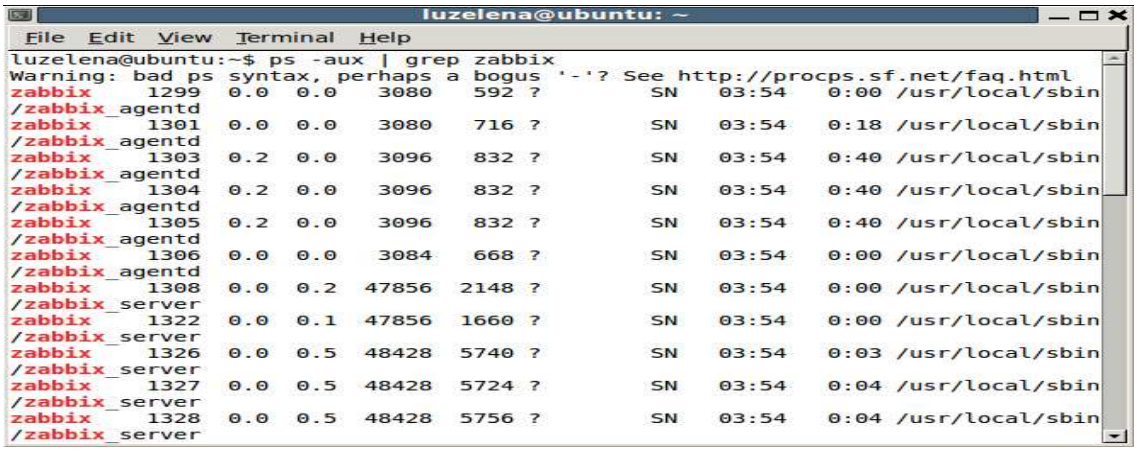
Post max size=16M

Max execution time=300

Date.timezone=America/Bogotá #se consulta :http://php.net/date.timezone

Finalmente, antes de iniciar la configuración de la interfaz web desde el navegador firefox , se hace la comprobación utilizando la terminal de comandos de Ubuntu, sobre el correcto funcionamiento del agente y servidor previamente instalados:

Figura 28. Funcionamiento de servidor y agente zabbix



Fuente. Autora.

6.2.10 Instalación de snmp para Ubuntu

Para realizar la monitorización a través del protocolo snmp, es necesario realizar la respectiva instalación, lo cual se hace desde la terminal de comandos de Ubuntu:

Figura 29. Instalación snmp para ubuntu

```
zabbix@ubuntu:~$ sudo apt-get install snmp
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes NUEVOS:
  snmp
0 actualizados, 1 se instalarán, 0 para eliminar y 18 no actualizados.
Se necesita descargar 0B/157kB de archivos.
Se utilizarán 610kB de espacio de disco adicional después de esta operación.
Seleccionando el paquete snmp previamente no seleccionado.
(Leyendo la base de datos ...  00%
75811 ficheros y directorios instalados actualmente.)
Desempaquetando snmp (de .../snmp_5.4.1~dfsg-12ubuntu7_i386.deb) ...
Procesando disparadores para man-db ...
Configurando snmp (5.4.1~dfsg-12ubuntu7) ...
zabbix@ubuntu:~$
```

Fuente. Autora.

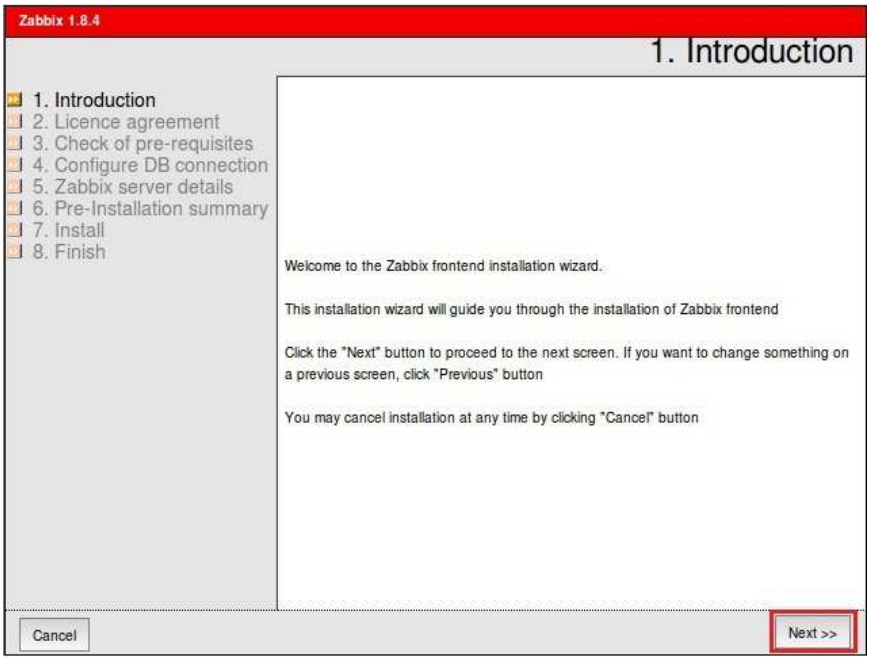
6.3 CONFIGURACION DE INTERFAZ WEB

Se debe configurar la interfaz web, para lo cual se ingresa a través de un explorador, para este caso, firefox de Ubuntu, e ingresamos de la forma:

http://localhost/zabbix

Se avanza con la opción Next>>.

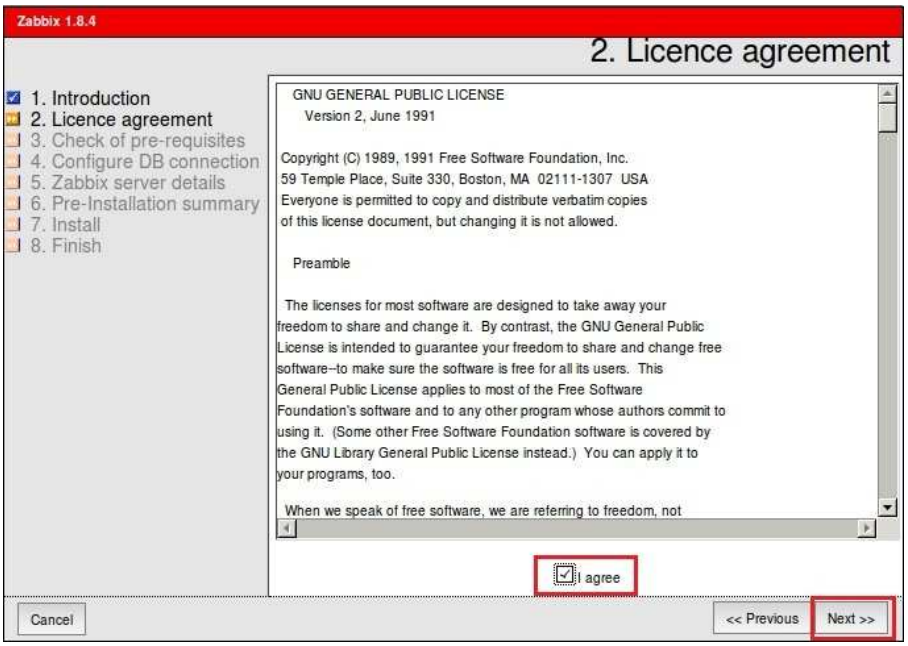
Figura 30. Ingreso a configuración en servidor local



Fuente: Autora.

Se aceptan los términos de licencia, como se muestra en la figura 30.

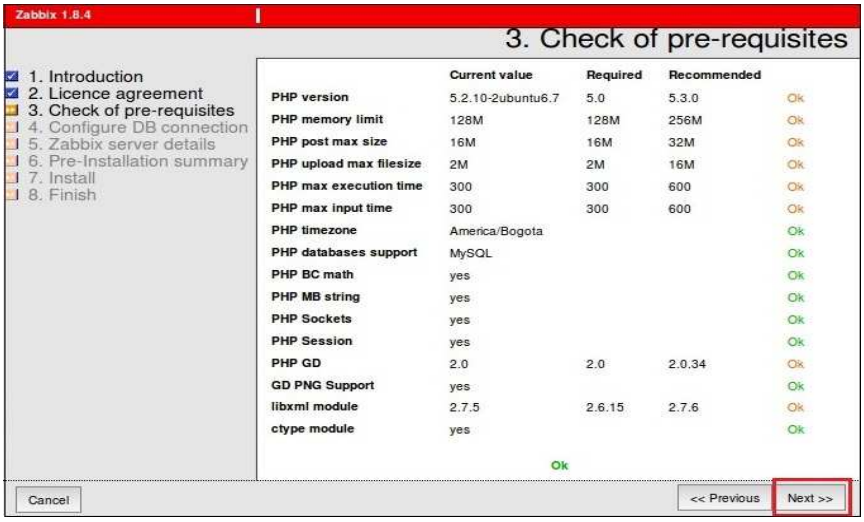
Figura 31. Aceptación de Licencia



Fuente: Autora.

Se cheque la instalación correcta de prerrequisitos y configuración de parámetros php.

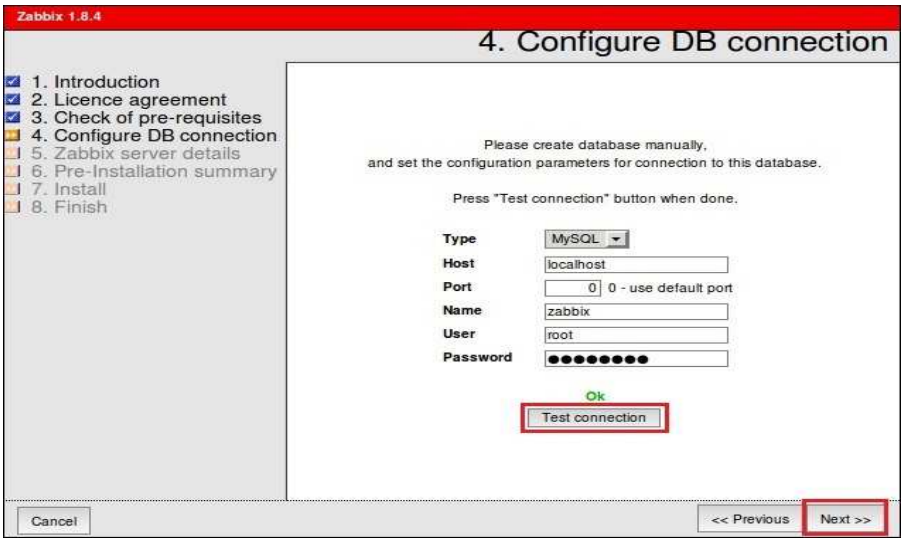
Figura 32. Lista de chequeo de pre-requisitos



Fuente: Autora.

Luego, se configura la conexión a la base de datos, introduciendo el nombre, usuario y contraseña. Se hace un test de la conexión y si todo es correcto, se puede pulsar Next.

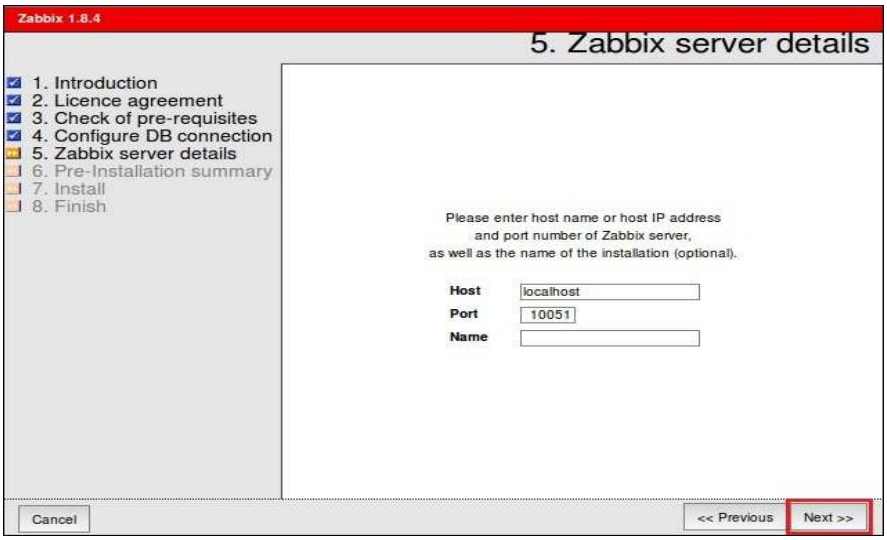
Figura 33. Configuración de la conexión con la base de datos



Fuente:Autora.

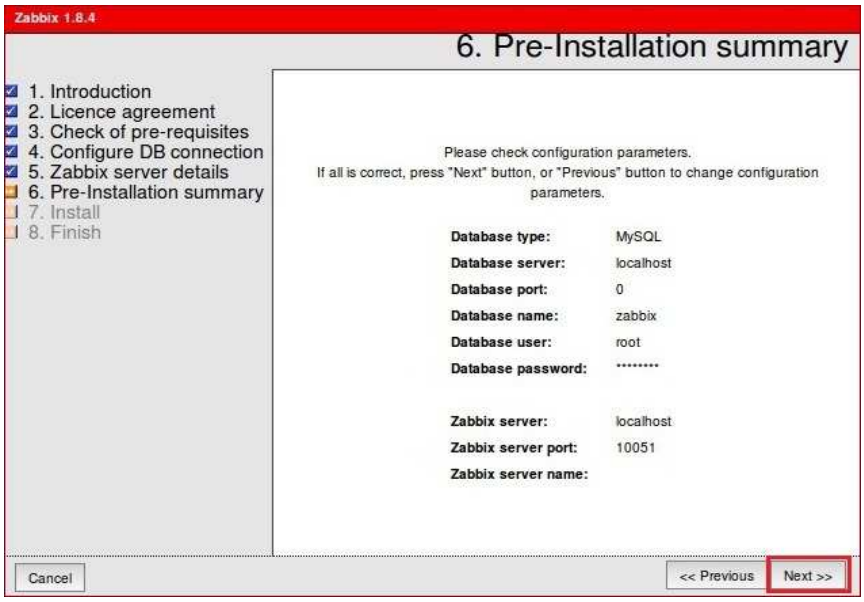
Se confirma el puerto previamente configurado.

Figura 34. Confirmación de puerto servidor



Fuente: Autora.

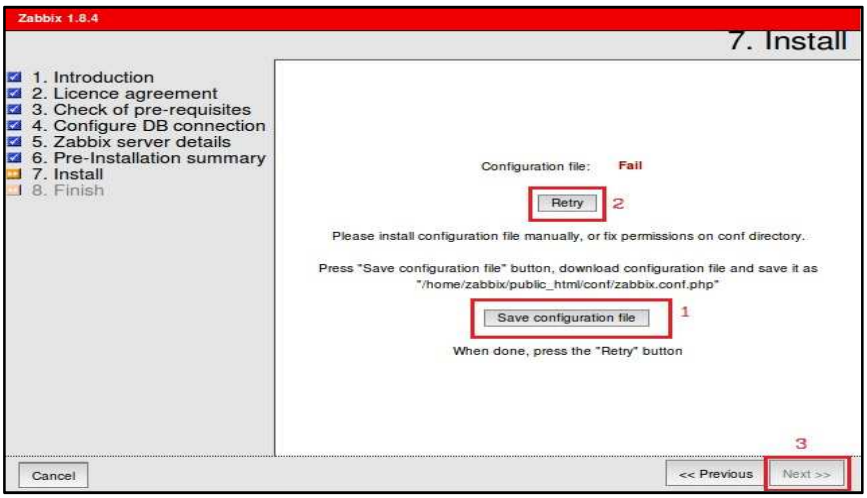
Figura 35. Resumen de la instalación



Fuente: Autora.

En la siguiente figura, se solicita el fichero de configuración, para lo cual se activa la opción1: Save configuration file, luego seguardaen eldirectorio /homer/zabbix/public_html/zabbix.conf.php. Una vez subido se pulsa la opción Retry, para poder avanzar con en el botón Next.

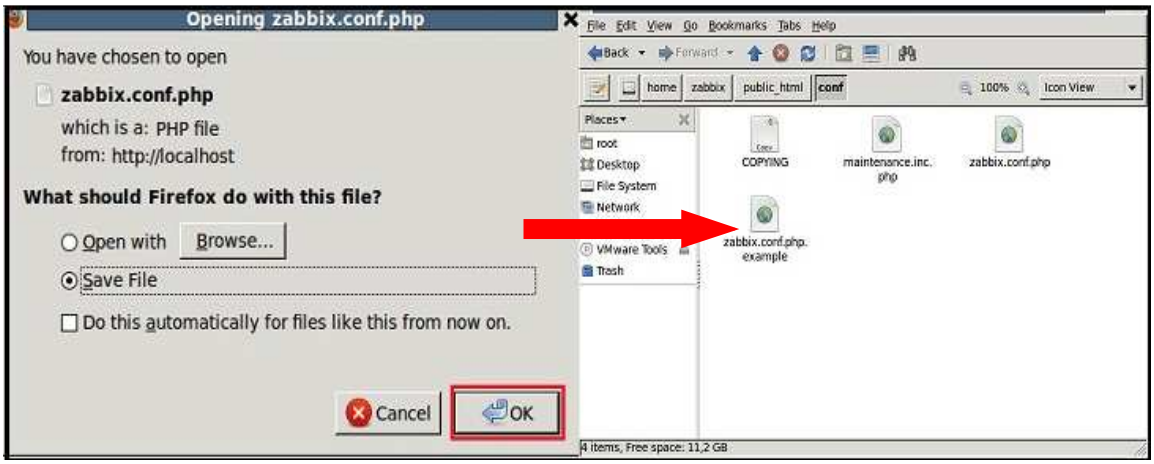
Figura 36. Solicitud de permisos para modificación en fichero de configuración



Fuente: Autora.

El procedimiento anteriormente descrito se muestra en la siguiente figura:

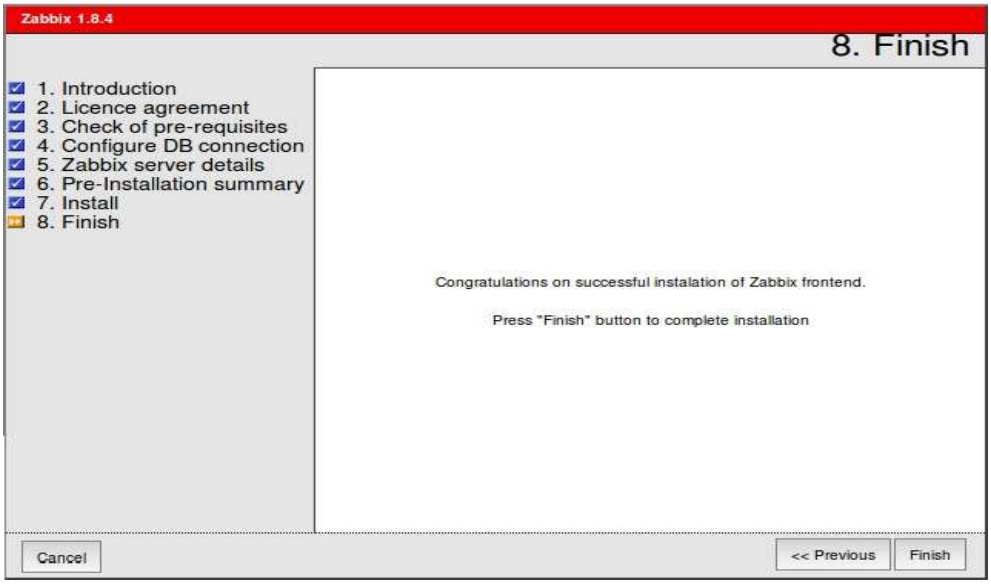
Figura 37. Guardando fichero zabbix.conf.php, opción 2



Fuente: Autora.

Finalmente, se logra que el proceso de configuración de la interfaz web, termine en forma exitosa.

Figura 38. Finalización proceso de configuración



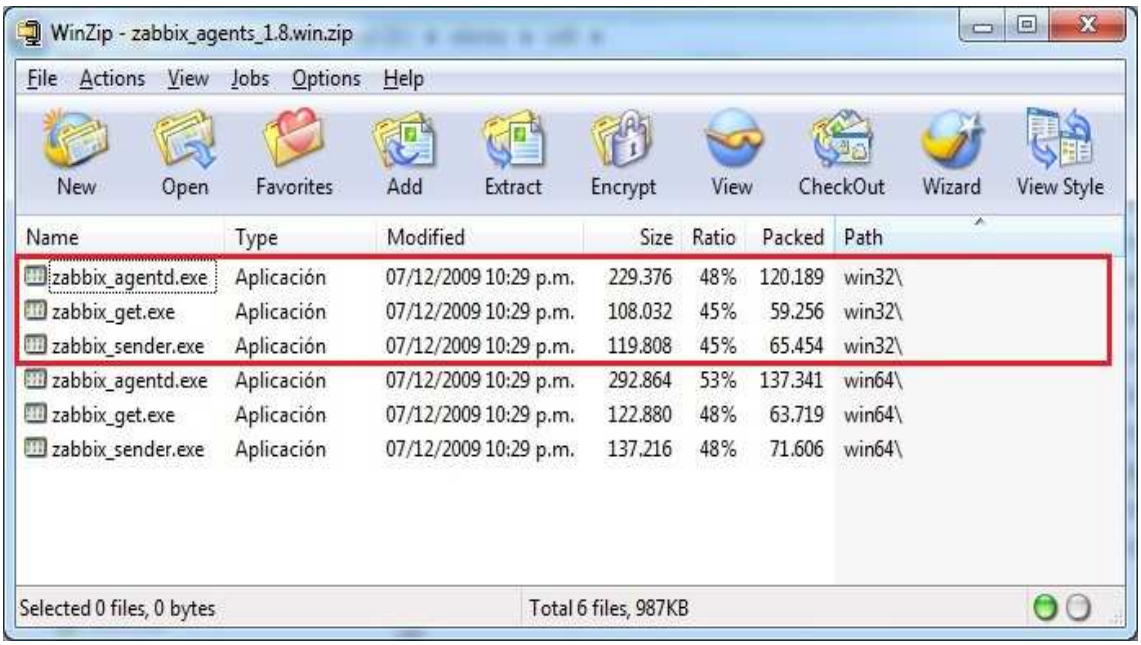
Fuente: Autora.

6.4 INSTALACION DE AGENTE ZABBIX EN MAQUINAS WINDOWS

La herramienta zabbix tiene disponible agentes para monitorización de diferentes sistemas operativos como Solaris, AIX, Linux, Windows. En el presente trabajo, se hará el procedimiento de instalación del agente zabbix en una máquina Windows.

La página web de zabbix, tiene disponible un archivo comprimido con los agentes para este sistema.

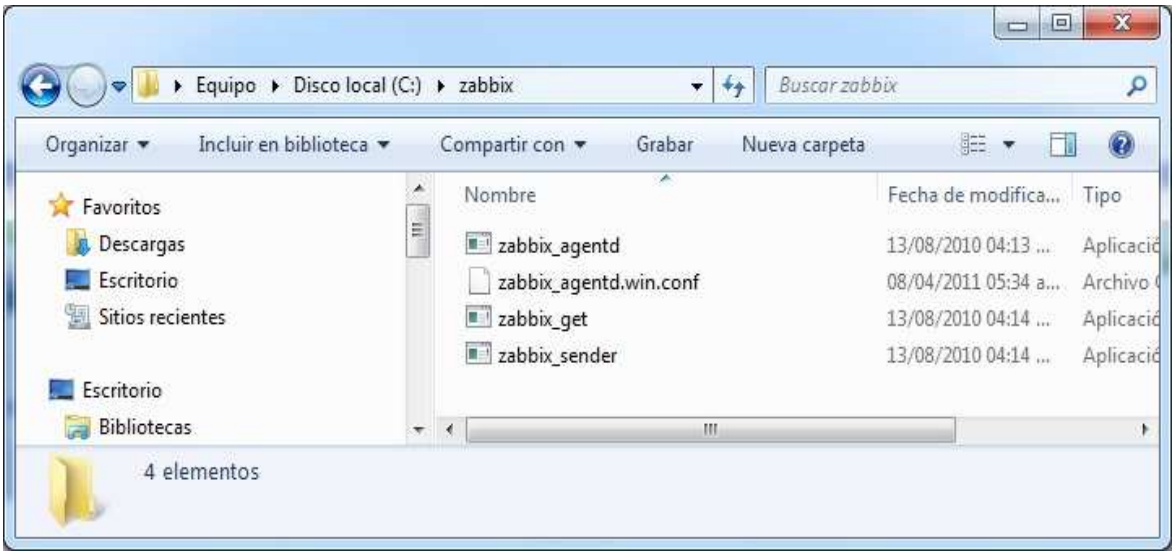
Figura 39. Agentes zabbix para maquina windows



Fuente. Autora.

Se copia los tres archivos indicados para maquinas windows de 32 bits y se lleva a una carpeta que se debe crear con nombre zabbix dentro de la unidad C:\\.

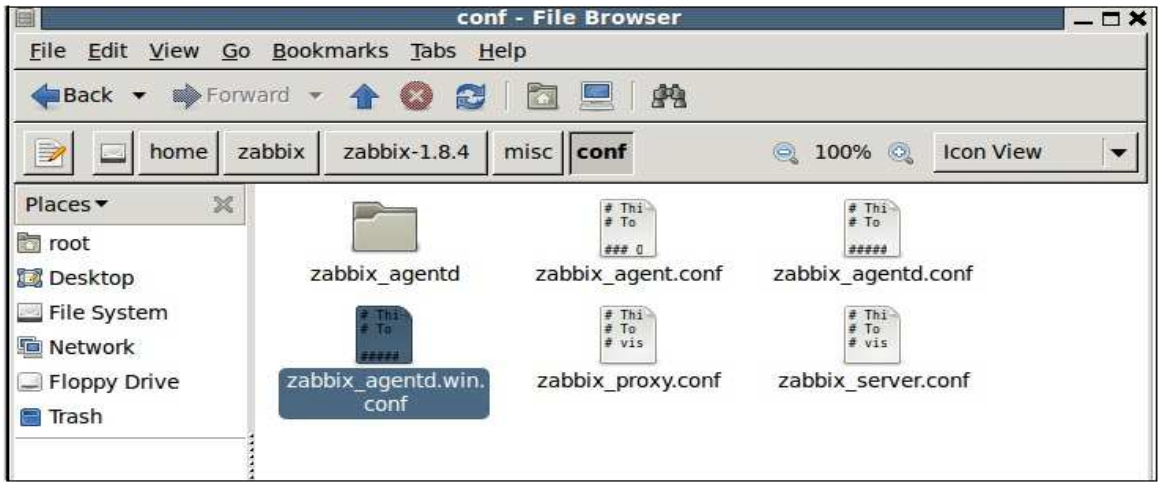
Figura 40. Carpeta zabbix con archivos requeridos



Fuente: Autora.

Como se observa en la figura anterior, se copió un nuevo archivo el cual fue extraído de los archivos generados en la configuración realizada en el servidor zabbix bajo Linux Ubuntu server, tal como se observa en la ruta siguiente:

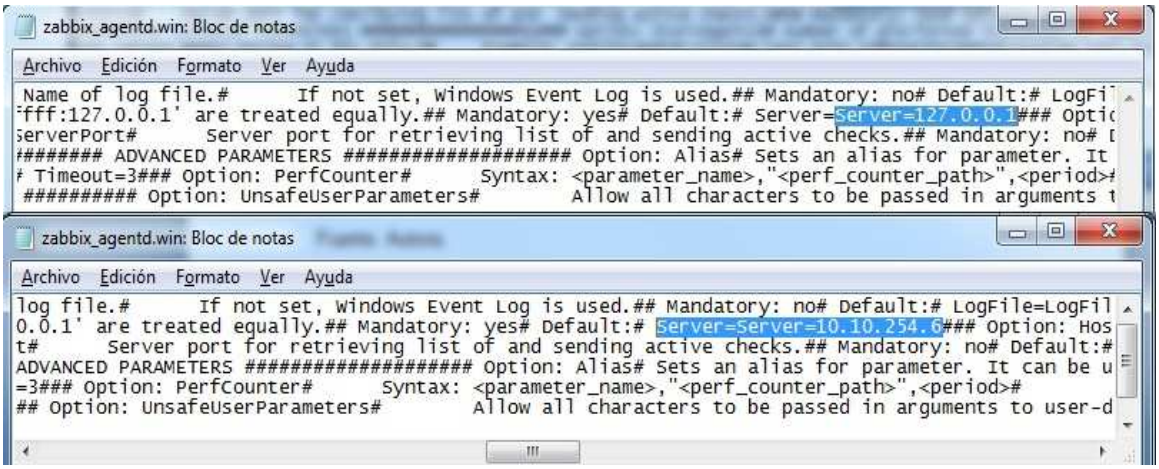
Figura 41. Ruta de archivo de configuración en Linux



Fuente. Autora.

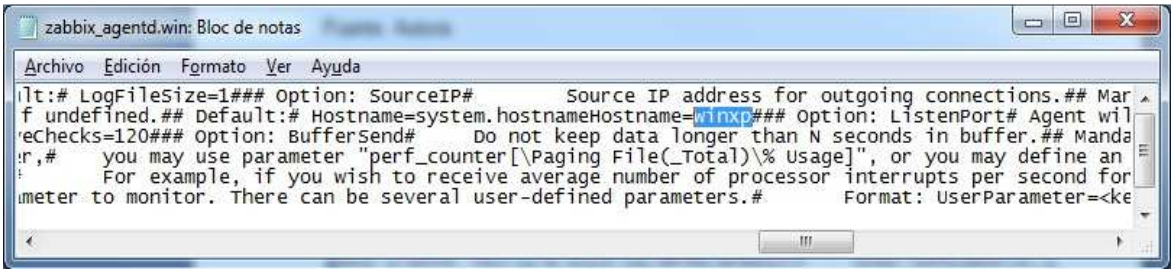
Lo siguiente, es editar el nuevo archivo: zabbix-agentd.win, se abre con el block de notas y se define la dirección del servidor y el nombre que se le va a colocar a la máquina windows que actuará como agente.

Figura 42. Edición archivo de configuración agente Windows



Fuente. Autora.

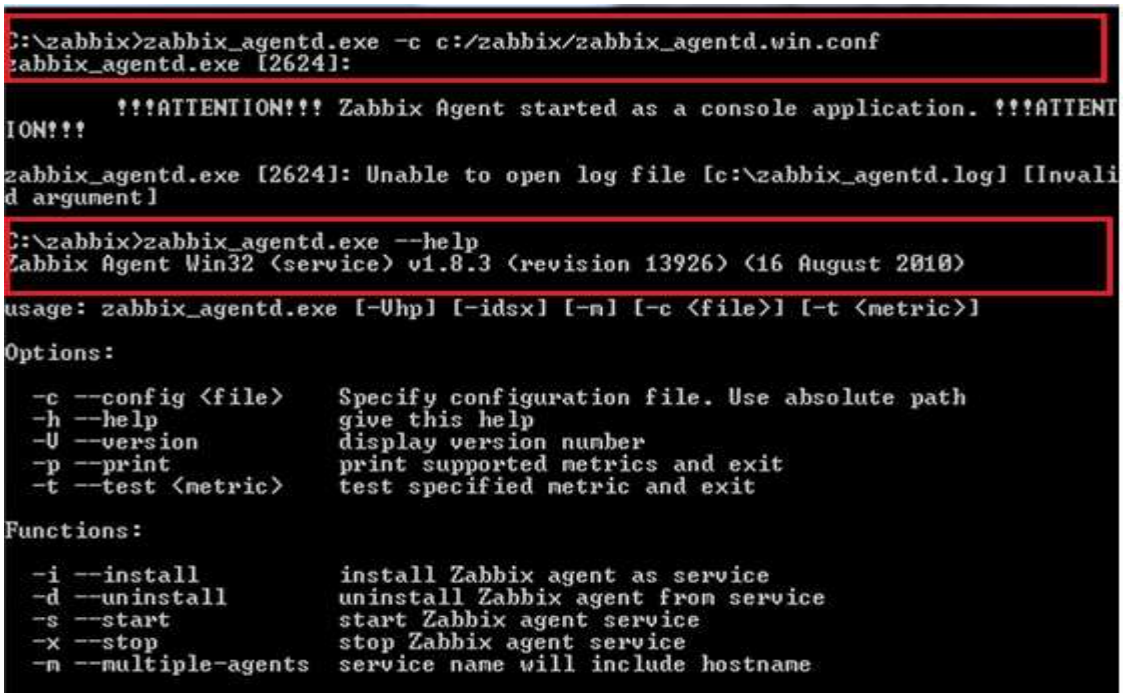
Figura 43. Configuración de campo hostname



Fuente. Autora

Luego, se ejecuta el archivo C:\zabbix>zabbix_agentd.exe –c c:/zabbix/zabbix-agentd.win.conf, se instalará el agente usando la configuración del archivo editado. Como se observa, aparece un error 2624, entonces se procede a llamar la ayuda del agente zabbix, la cual nos muestra un listado de opciones como se ve en la figura 44.

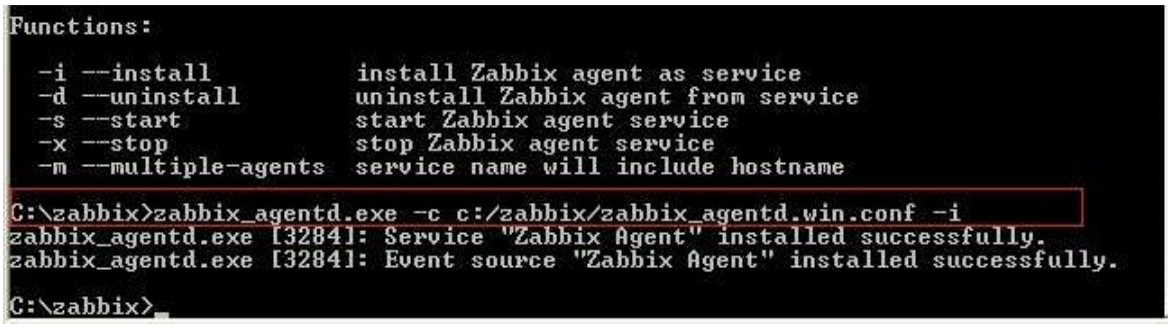
Figura 44. Comando de instalación agente en máquina windows



Fuente: Autora.

Por último, se ejecuta nuevamente el archivo con la opción i (install).

Figura 45. Instalación agente en maquina windwos xp



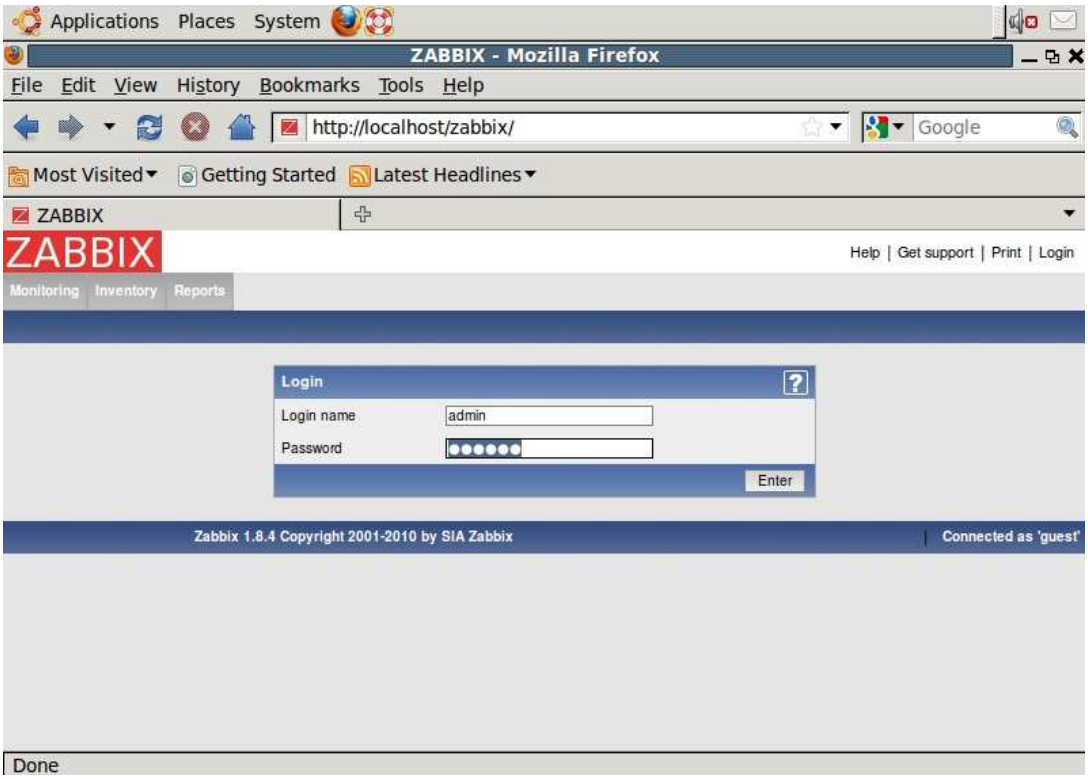
Fuente. Autora.

6.5 IMPLEMENTACION ZABBIX

Para el ingreso a la herramienta zabbix, es necesario la autenticación con el usuario admin y password zabbix.

Todas las tareas de monitorización se realiza desde la interfaz web, se puede agregar dispositivos, configurar todas las opciones del zabbix como crear plantillas, definir alarmas, generar gráficas y otras muchas características avanzadas de monitorización que ofrece la herramienta zabbix.

Figura 46. Autenticación para ingreso a zabbix

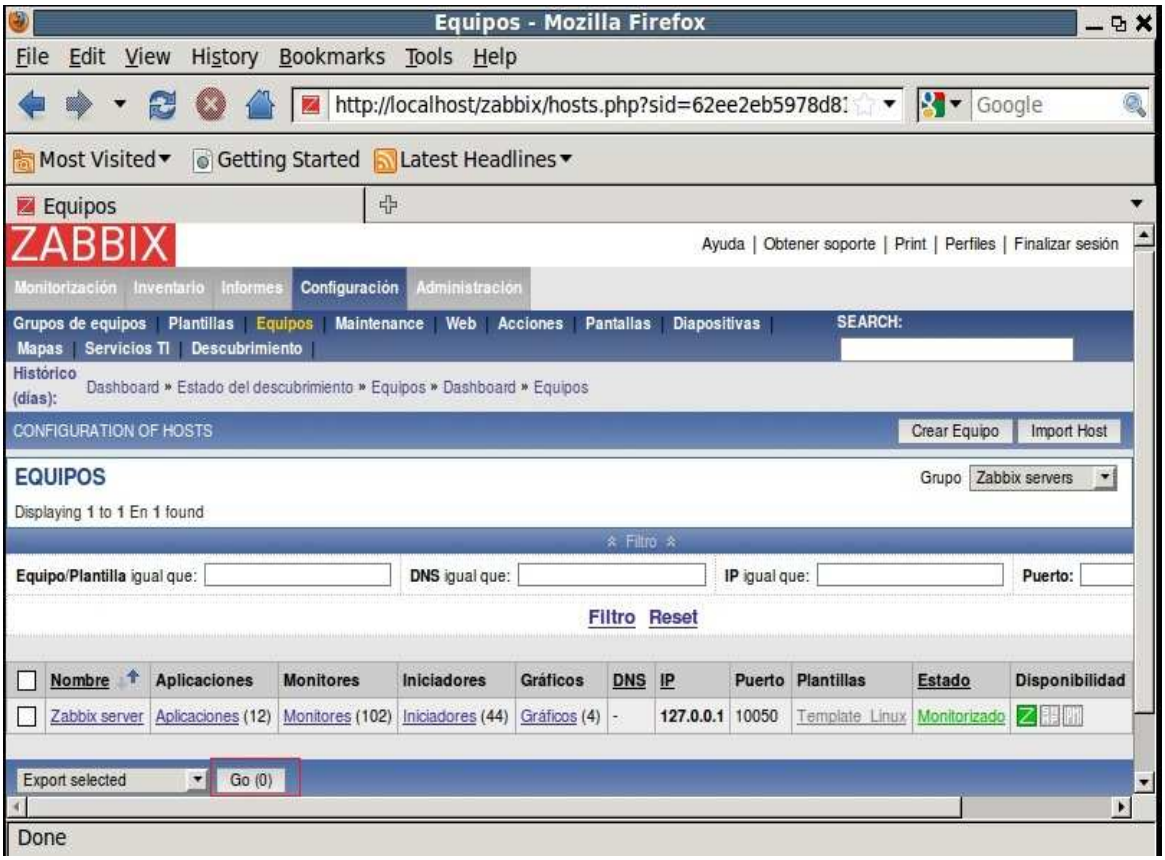


Fuente: Autora.

6.5.1 Creación de un Equipo.

Lo primero que se debe hacer, es agregar los dispositivos que se encuentran conectados a la red IP. En la figura 47, se tiene el frontend de zabbix, en el menú se elige Configuración, desde aquí se definen los parámetros de datos, reportes, gráficas. Se ingresa por la opción Hosts, para iniciar la primera tarea de agregación.

Figura 47. Creación de equipo



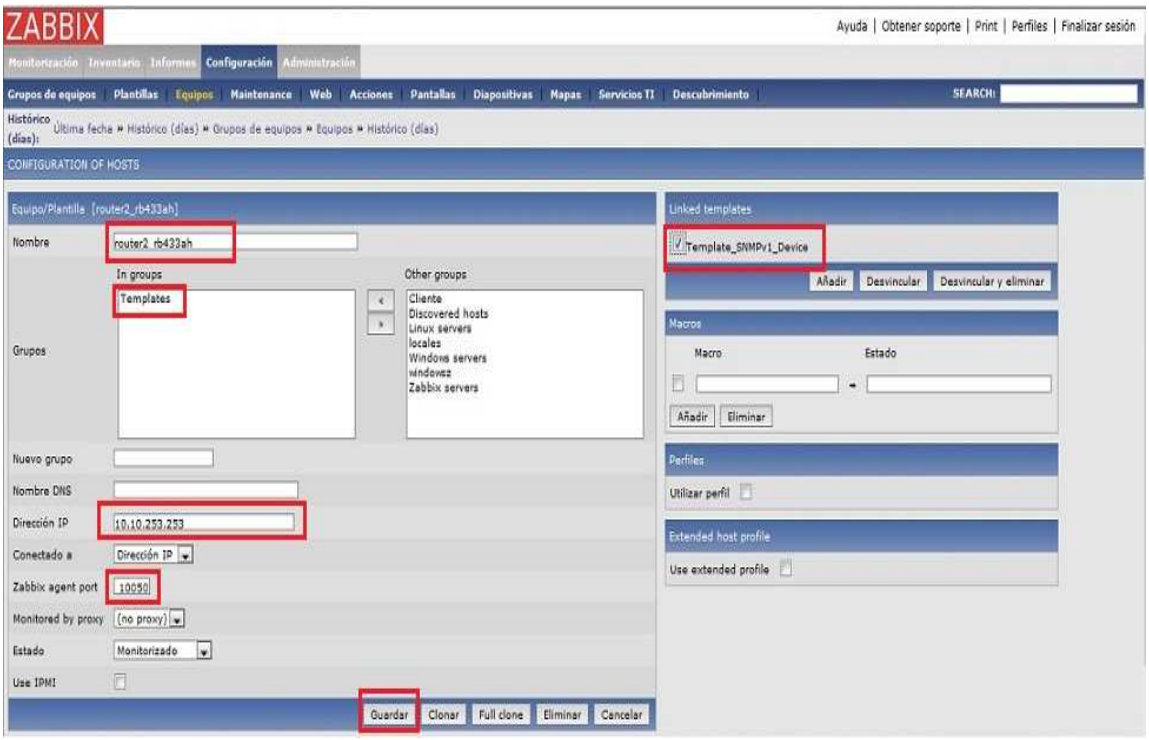
Fuente: Autora.

Se muestra el primer elemento ya creado por defecto, corresponde al mismo sistema, en donde se configuro el agente y el servidor, en la columna

de“disponibilidad” se puede observar el color verde,señala que el agente zabbix estáinstalado y activado, en la columna “estado” indica que está siendo monitorizado. Esta última opción se activa desde el botón inferior Go.

Para la creación de hosts, se llenan los campos que solicitan como la dirección ip, un grupo al que debe pertenecer siempre, debido a que los permisos se dan sobre grupos y no sobre un elemento en particular; se debe adicionar una plantilla la cual corresponde al sistema operativo que tiene instalado el equipo a agregar.

Figura 48. Configuración de un equipo



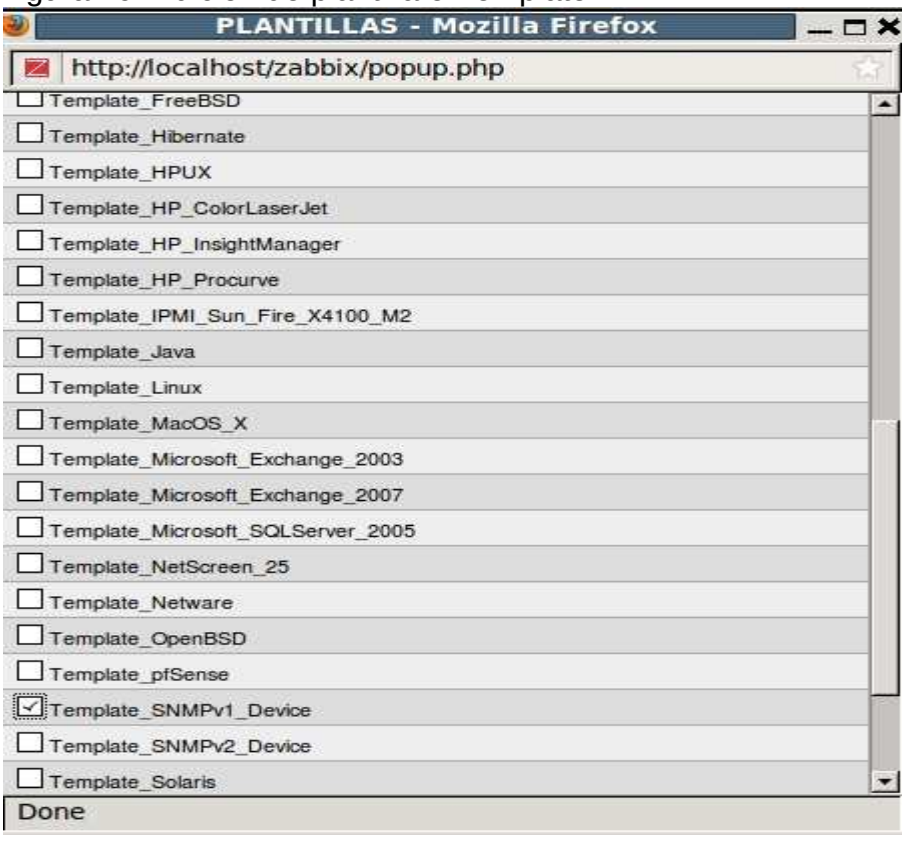
Fuente: Autora.

Una plantilla o Template, es una entidad lógica prediseñada con diferentes Items (monitores), Trigger (Iniciadores) y aplicaciones con el fin de ser aplicadas en dispositivos que comparten los mismos parámetros de medición, por ejemplo el uso de memoria, la carga del procesador. Es viable, tener plantillas que ya tenga

configurados los ítems a monitorizar en un elemento, en el caso que no se cuente con la plantilla para el equipo creado entonces se debe crear el ítem o descargar las plantillas (si está disponible) desde la página: www.zabbix.com.

En la figura 47, se observa la creación de un dispositivo el cual se nombra router2_rb433ah y corresponde a un router mikrotic, en el campo Linked Templates se le adiciona una planilla o template, para lo cual se elige la opción “Template-SNMPv1_Device”, en el campo grupo se elige Templates, se escribe la IP del equipo en el campo correspondiente y en “Conectado a” se selecciona **Dirección IP**del router.

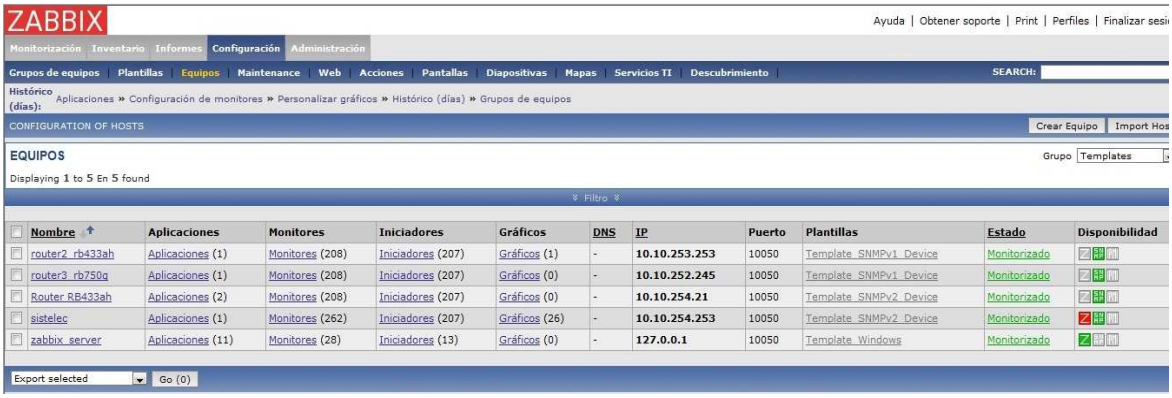
Figura 49. Adición de plantilla o Template



Fuente. Autora.

Continuando con la adición de equipos o hosts, en la figura 50, se puede observar un listado previamente con la opción de monitorización activada, al igual que el snmp, lo cual indica que para monitorizar los dispositivos se utilizará dicho protocolo y no con el agente zabbix.

Figura 50. Listado de dispositivos monitorizados



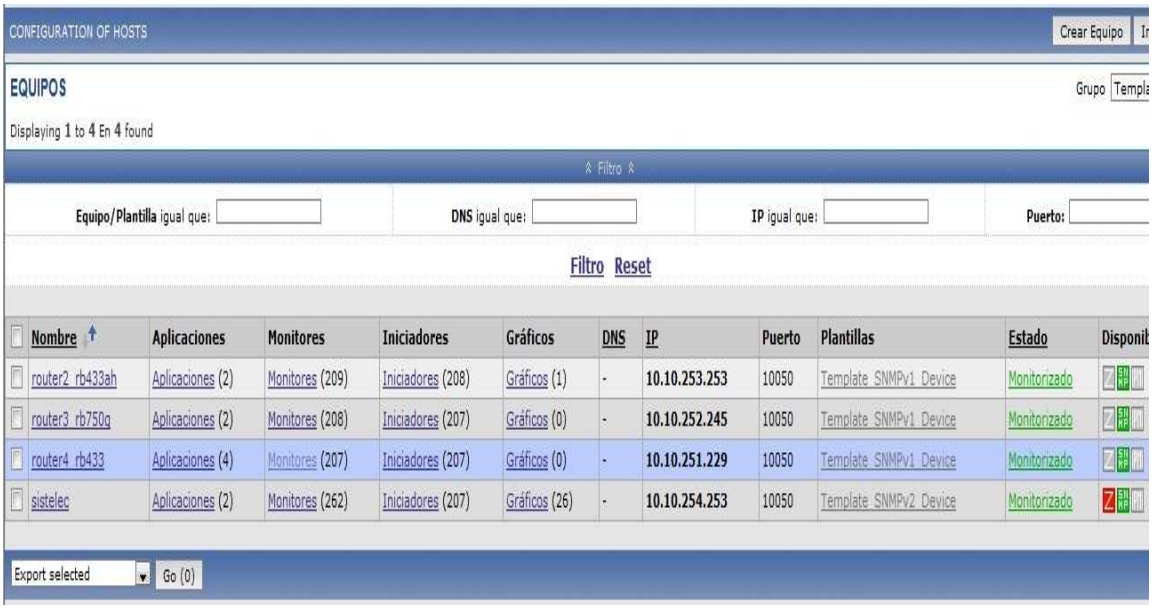
Fuente. Autora.

6.5.2 Creación de un monitor

Para la creación de un monitor o ítem se debe llevar a cabo con éxito la creación de dispositivos, en donde se pueda observar el estado de disponibilidad resaltado en color verde (Figura 50), lo que implica que debe tener comunicación con el servidor zabbix, ya sea a través del agente, del protocolo snmp o IMPI.

El proceso inicia desde la opción equipos del menú de configuración, para el paso uno, se selecciona la opción monitores y luego crear monitor. Para el ejemplo se va a crear un monitor para el dispositivo router4_rb433, llamado uptime (tiempo activo del dispositivo desde la última vez que se reinicializó).

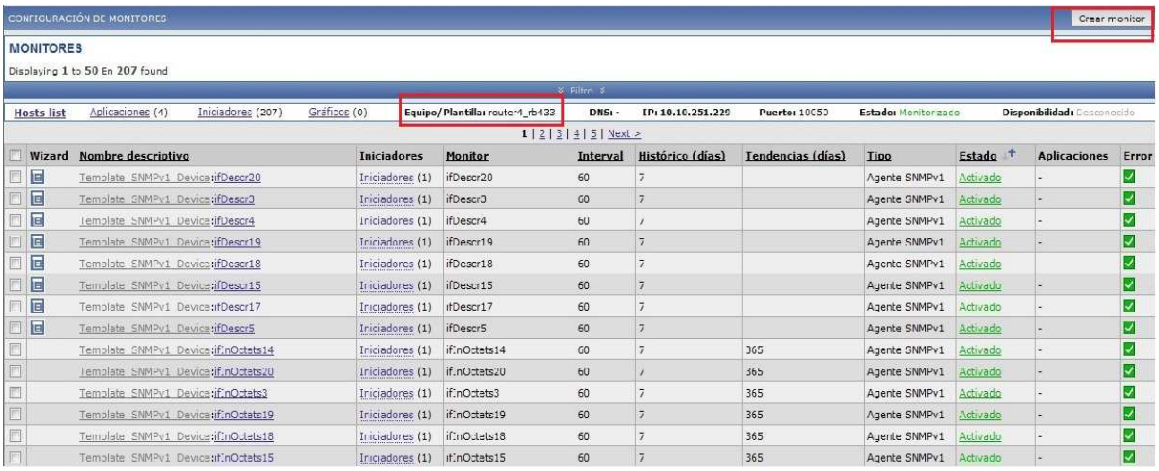
Figura 51. Paso uno para creación de monitores



Fuente. Autora.

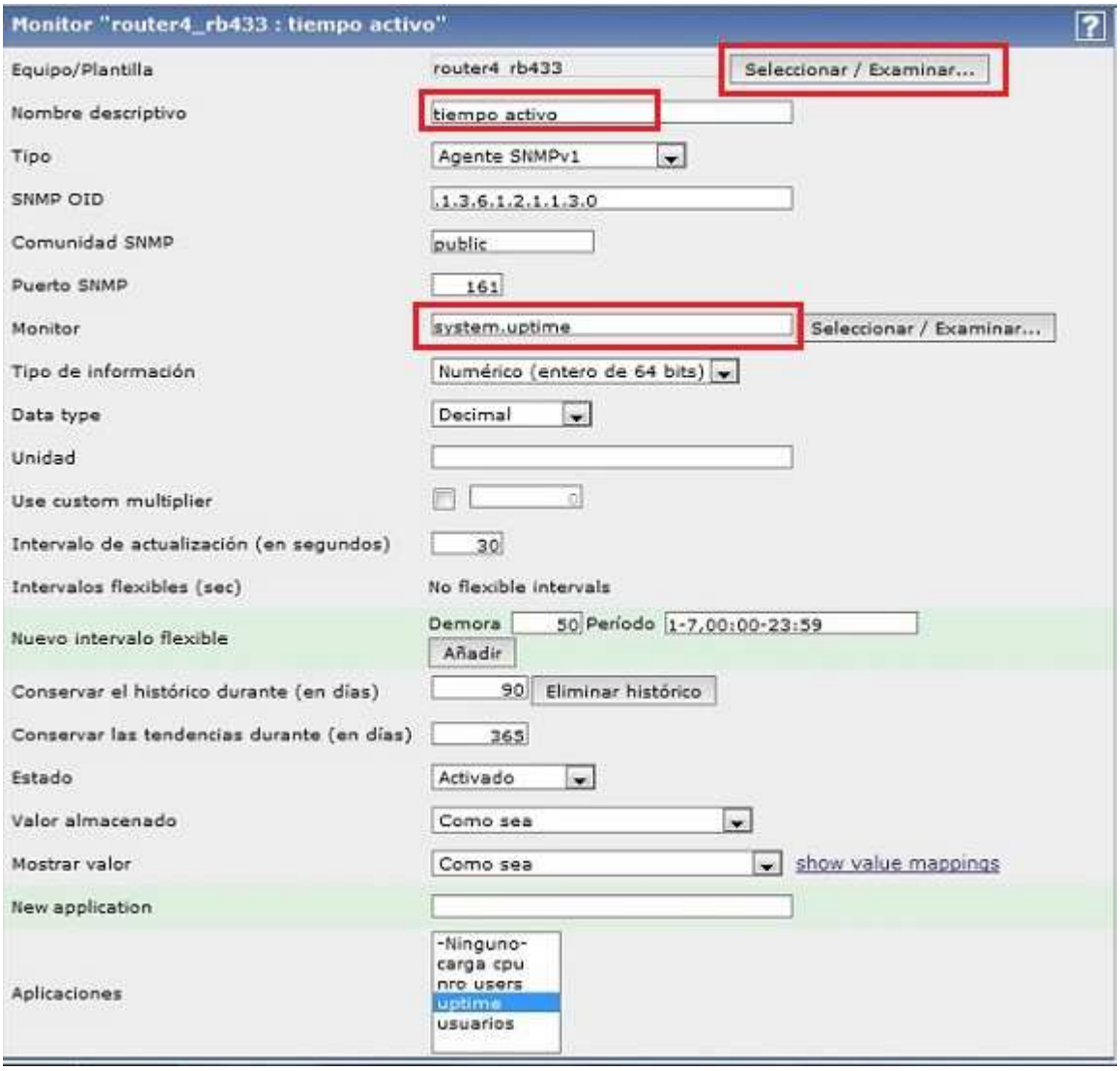
En el paso dos, se observa un listado de monitores predeterminados para el router4_rb433, definidos según la plantilla que fue vinculada para este dispositivo, procedemos a seleccionar la opción crear monitor del botón superior.

Figura 52. Paso dos para creación de monitores



Fuente: Autora.

Figura 53. Paso tres para creación de ítem

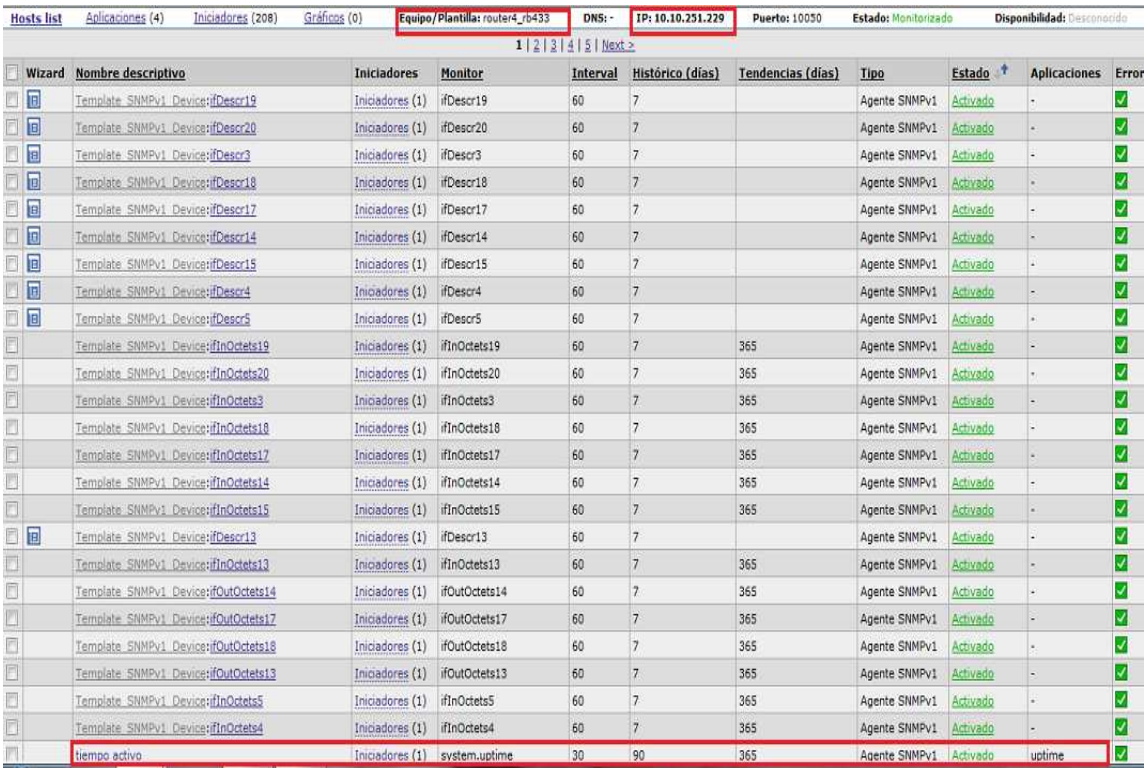


Fuente. Autora.

Como se observa en la figura 53, se debe seleccionar el equipo al que le va agregar el ítem o monitor uptime (tiempo activo del dispositivo), luego llena el campo para describir el parámetro que se va a medir (ítem), después se debe seleccionar desde un listado el monitor que hace referencia al nombre técnico que recibe el ítem. Los demás datos aparecen por defecto. Por último se guarda.

Se debe activar el ítem creado para el router4_rb433, como se muestra en la figura siguiente:

Figura 54. Activación de monitor



Hosts list | Aplicaciones (4) | Iniciadores (208) | Gráficos (0) | Equipo/Plantilla: router4_rb433 | DNS: - | IP: 10.10.251.229 | Puerto: 10050 | Estado: Monitorizado | Disponibilidad: Desconocido

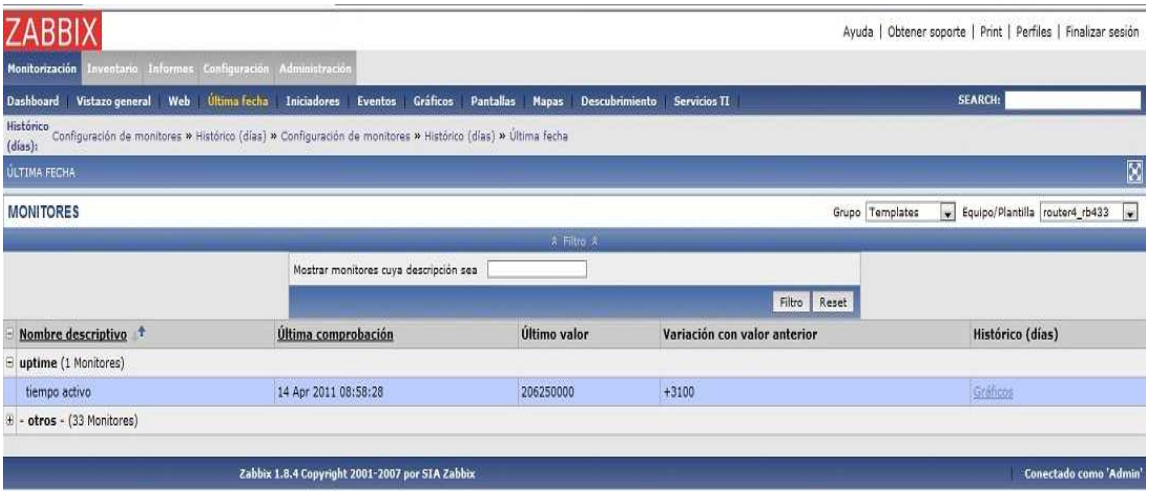
1 | 2 | 3 | 4 | 5 | Next >

Wizard	Nombre descriptivo	Iniciadores	Monitor	Interval	Histórico (días)	Tendencias (días)	Tipo	Estado	Aplicaciones	Error
	Template_SNMPv1_Device:ifDescr19	Iniciadores (1)	ifDescr19	60	7		Agente SNMPv1	Activado	-	
	Template_SNMPv1_Device:ifDescr20	Iniciadores (1)	ifDescr20	60	7		Agente SNMPv1	Activado	-	
	Template_SNMPv1_Device:ifDescr3	Iniciadores (1)	ifDescr3	60	7		Agente SNMPv1	Activado	-	
	Template_SNMPv1_Device:ifDescr18	Iniciadores (1)	ifDescr18	60	7		Agente SNMPv1	Activado	-	
	Template_SNMPv1_Device:ifDescr17	Iniciadores (1)	ifDescr17	60	7		Agente SNMPv1	Activado	-	
	Template_SNMPv1_Device:ifDescr14	Iniciadores (1)	ifDescr14	60	7		Agente SNMPv1	Activado	-	
	Template_SNMPv1_Device:ifDescr15	Iniciadores (1)	ifDescr15	60	7		Agente SNMPv1	Activado	-	
	Template_SNMPv1_Device:ifDescr4	Iniciadores (1)	ifDescr4	60	7		Agente SNMPv1	Activado	-	
	Template_SNMPv1_Device:ifDescr5	Iniciadores (1)	ifDescr5	60	7		Agente SNMPv1	Activado	-	
	Template_SNMPv1_Device:ifInOctets19	Iniciadores (1)	ifInOctets19	60	7	365	Agente SNMPv1	Activado	-	
	Template_SNMPv1_Device:ifInOctets20	Iniciadores (1)	ifInOctets20	60	7	365	Agente SNMPv1	Activado	-	
	Template_SNMPv1_Device:ifInOctets3	Iniciadores (1)	ifInOctets3	60	7	365	Agente SNMPv1	Activado	-	
	Template_SNMPv1_Device:ifInOctets18	Iniciadores (1)	ifInOctets18	60	7	365	Agente SNMPv1	Activado	-	
	Template_SNMPv1_Device:ifInOctets17	Iniciadores (1)	ifInOctets17	60	7	365	Agente SNMPv1	Activado	-	
	Template_SNMPv1_Device:ifInOctets14	Iniciadores (1)	ifInOctets14	60	7	365	Agente SNMPv1	Activado	-	
	Template_SNMPv1_Device:ifInOctets15	Iniciadores (1)	ifInOctets15	60	7	365	Agente SNMPv1	Activado	-	
	Template_SNMPv1_Device:ifDescr13	Iniciadores (1)	ifDescr13	60	7		Agente SNMPv1	Activado	-	
	Template_SNMPv1_Device:ifInOctets13	Iniciadores (1)	ifInOctets13	60	7	365	Agente SNMPv1	Activado	-	
	Template_SNMPv1_Device:ifOutOctets14	Iniciadores (1)	ifOutOctets14	60	7	365	Agente SNMPv1	Activado	-	
	Template_SNMPv1_Device:ifOutOctets17	Iniciadores (1)	ifOutOctets17	60	7	365	Agente SNMPv1	Activado	-	
	Template_SNMPv1_Device:ifOutOctets18	Iniciadores (1)	ifOutOctets18	60	7	365	Agente SNMPv1	Activado	-	
	Template_SNMPv1_Device:ifOutOctets13	Iniciadores (1)	ifOutOctets13	60	7	365	Agente SNMPv1	Activado	-	
	Template_SNMPv1_Device:ifInOctets5	Iniciadores (1)	ifInOctets5	60	7	365	Agente SNMPv1	Activado	-	
	Template_SNMPv1_Device:ifInOctets4	Iniciadores (1)	ifInOctets4	60	7	365	Agente SNMPv1	Activado	-	
	tiempo activo	Iniciadores (1)	system.uptime	30	90	365	Agente SNMPv1	Activado	uptime	

Fuente: Autora.

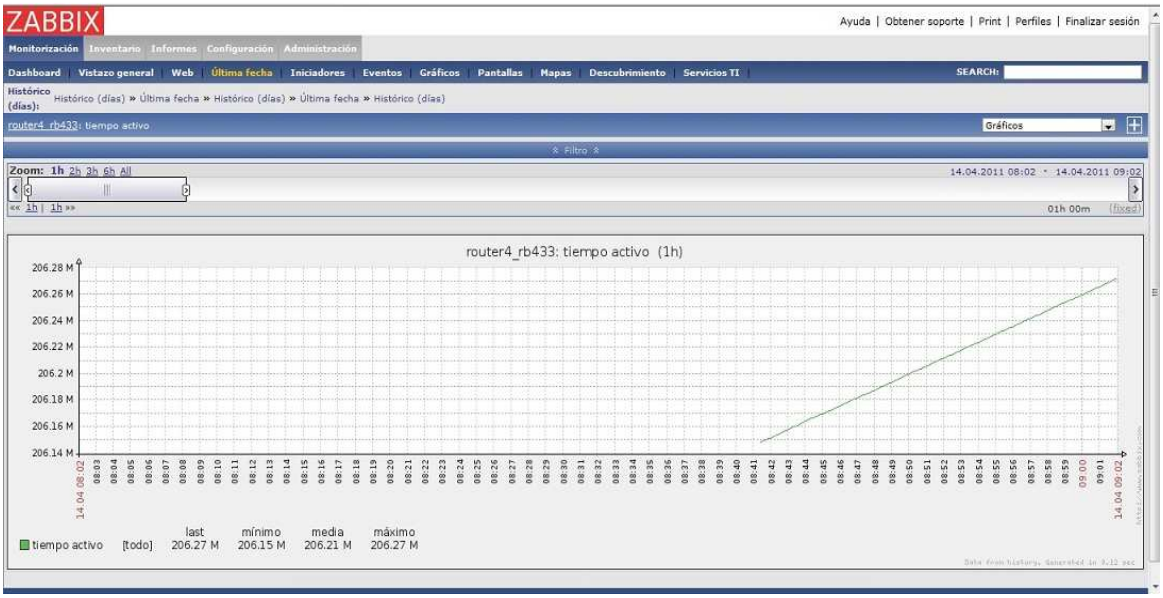
Para verificar que el ítem inició la recolección de datos, entonces se escoge la opción ultima fecha del menú monitorización.

Figura 55. Verificación de monitor recolectando datos



Fuente. Autora.

Figura 56. Gráfica de recolección datos



Fuente. Autora.

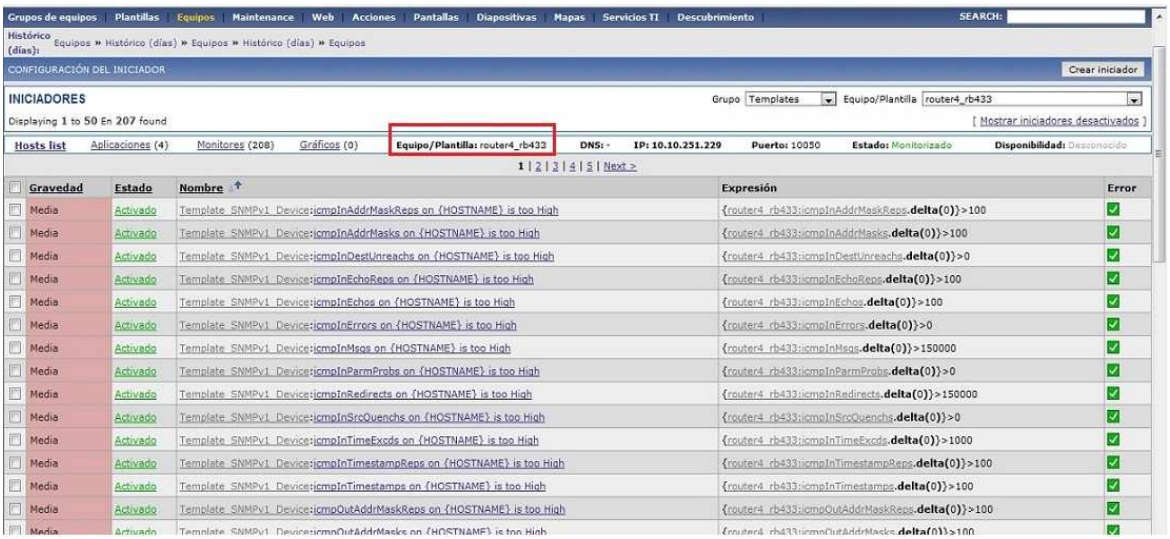
6.5.3 Creación de iniciadores

La información recolectada por los monitores (ítems), es administrada y clasificada por los iniciadores o trigger. Un trigger en zabbix, es una entidad que define umbrales para la clasificación de los ítems.

Para crear un iniciador, se selecciona la opción crear iniciador desde equipos del menú configuración.

Para este caso, se escoge, la opción iniciador del router4-rb433.

Figura 57. Paso uno para creación de iniciadores



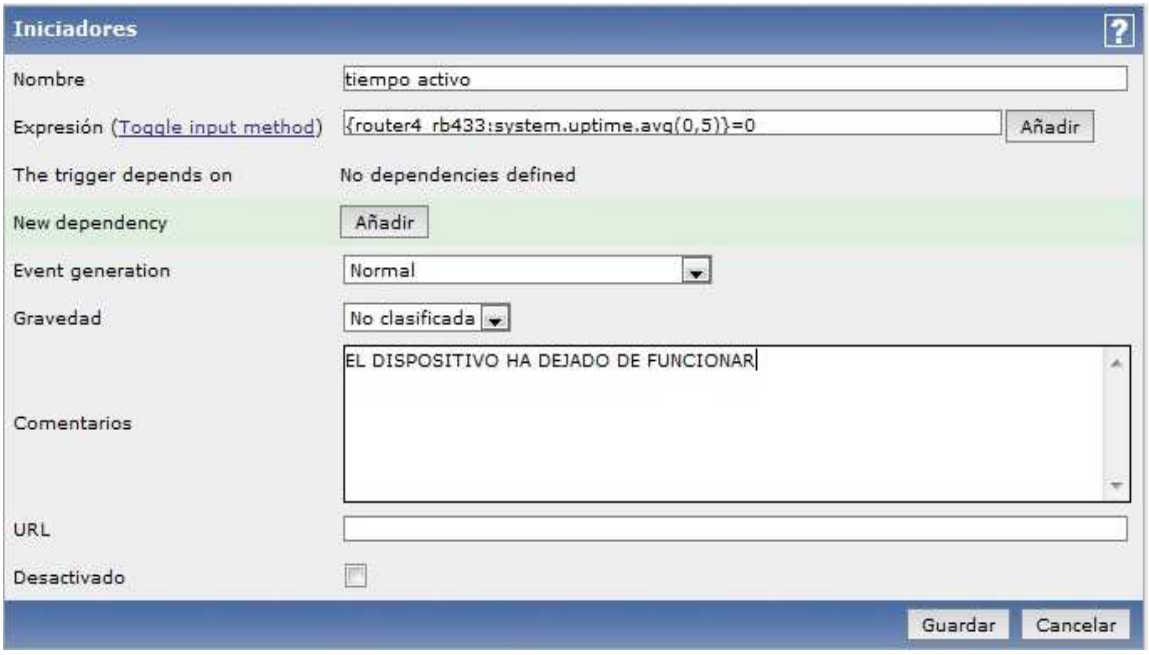
Fuente. Autora.

Luego, se selecciona el ítem y se definen los parámetros bajos los cuales el iniciador se activará o indicará que existe una alerta. Para este caso se creará un trigger para el ítem “tiempo activo”.

Figura 58. Paso dos para creación de trigger

Fuente. Autora.

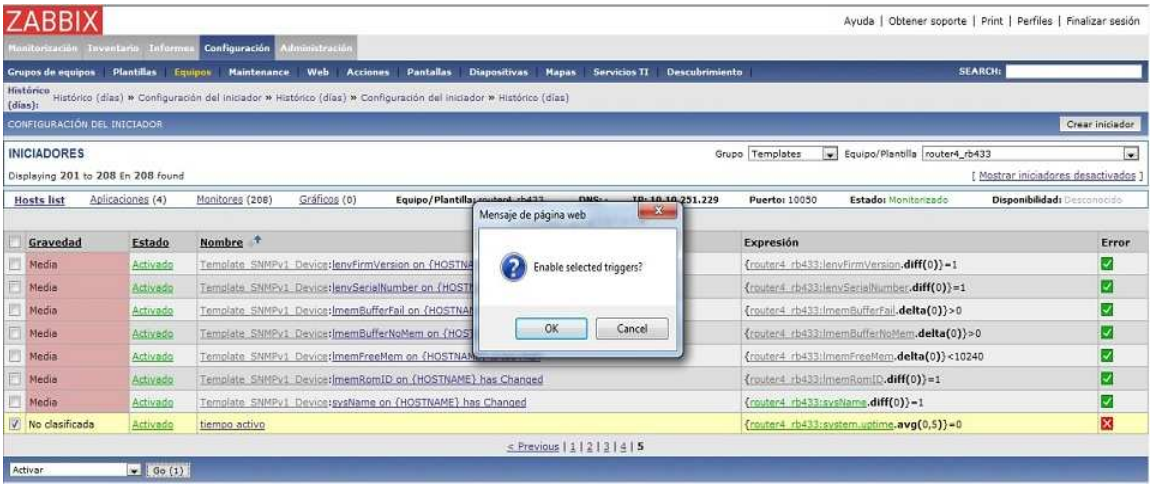
Figura 59. Paso tres para la creación de iniciadores



Fuente. Autora.

Finalmente, se coloca un comentario referente a que se ha cumplido la condición del ítem, en este caso el tiempo activo del equipo. En la figura, se puede ver en el listado, el triggeractivado que se acaba de crear.

Figura 60. Activación de iniciador tiempo activo



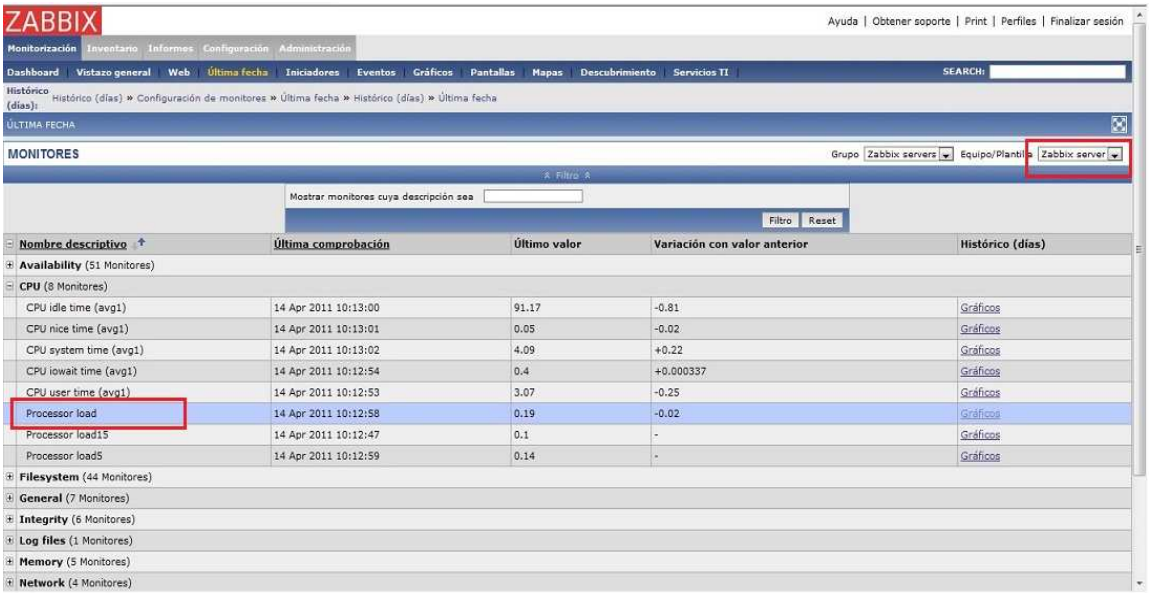
Fuente. Autor.

6.5.4 Gráficas

Para observar la monitorización de ítems sobre dispositivos mediante gráficas, se ingresa por la opción “ultima fecha”, del menú monitorización.

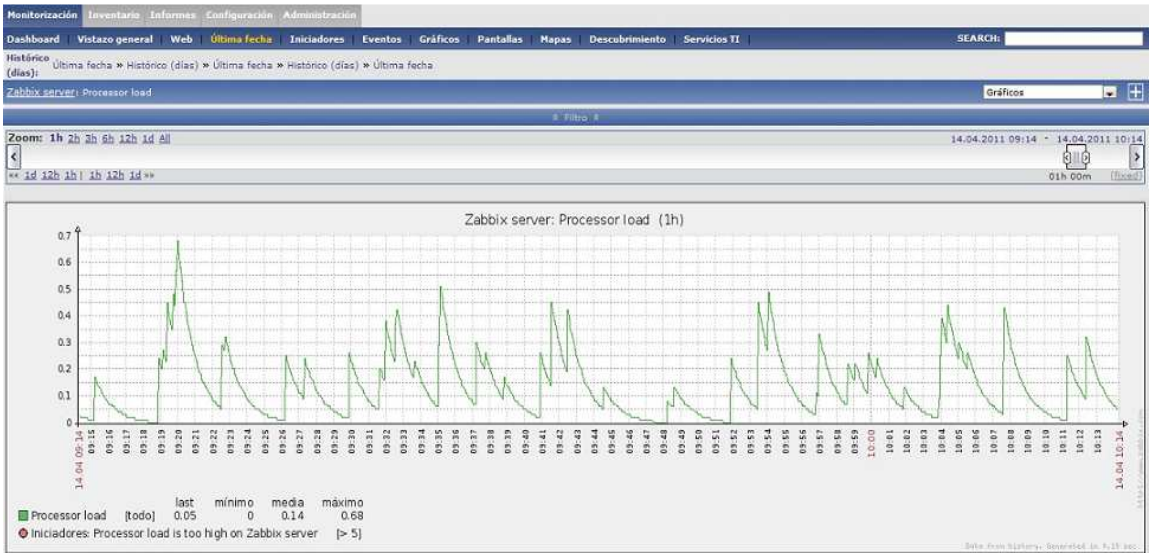
Para analizar la carga del procesador del servidor zabbix, se debe escoger el dispositivo desde la opción superior derecha, luego se escoge el ítem Processor Load y la opción Graficar.

Figura 61. Selección gráfica para servidor zabbix



Fuente. Autora

Figura 62. Gráfica carga del procesador en el servidor zabbix



Fuente. Autora.

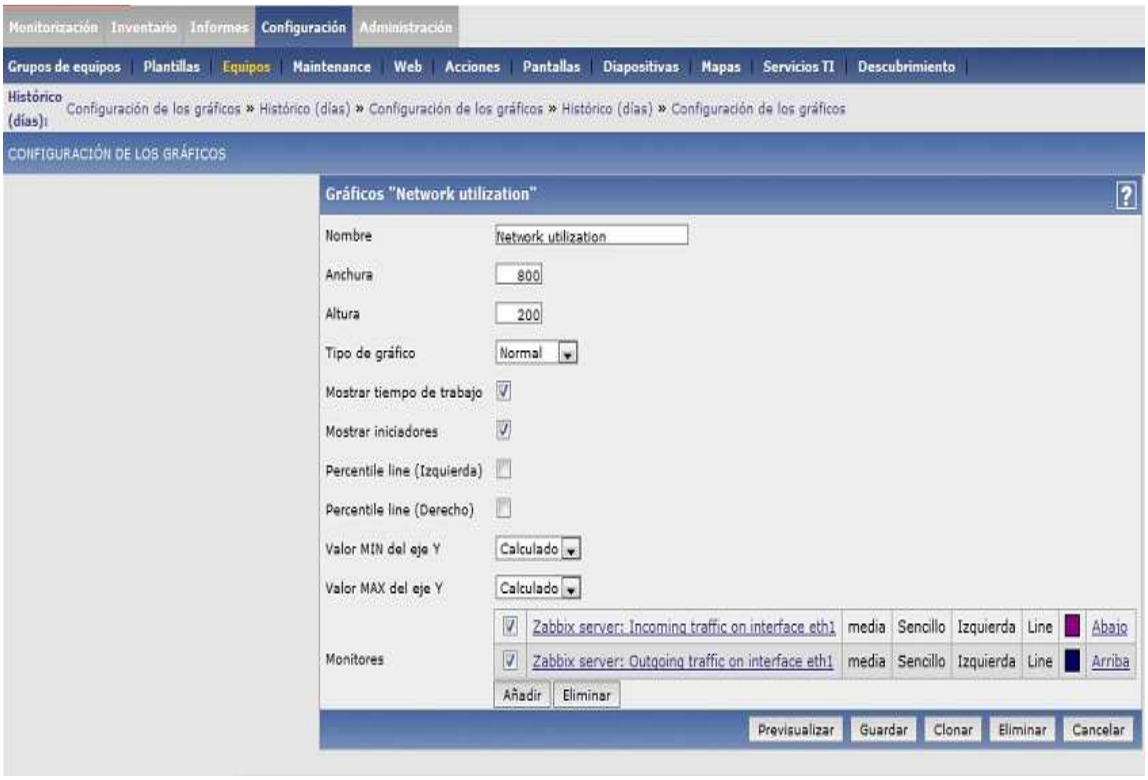
Se puede observar que para la carga de procesador que durante una hora desde las 9:14am hasta las 10:14 el pico más alto se registro a las 9:20 am.

6.5.5 Comparación de parámetros mediante uso de gráficas

Para realizar la comparación de parámetros definidos sobre dispositivos, se ingresa por la opción hosts del menú configuración.

Para este caso, se va a realizar el grafico del tráfico de entrada y salida que registra la interfaz eth1 del servidor zabbix.

Figura 63. Paso uno para creación de gráficas

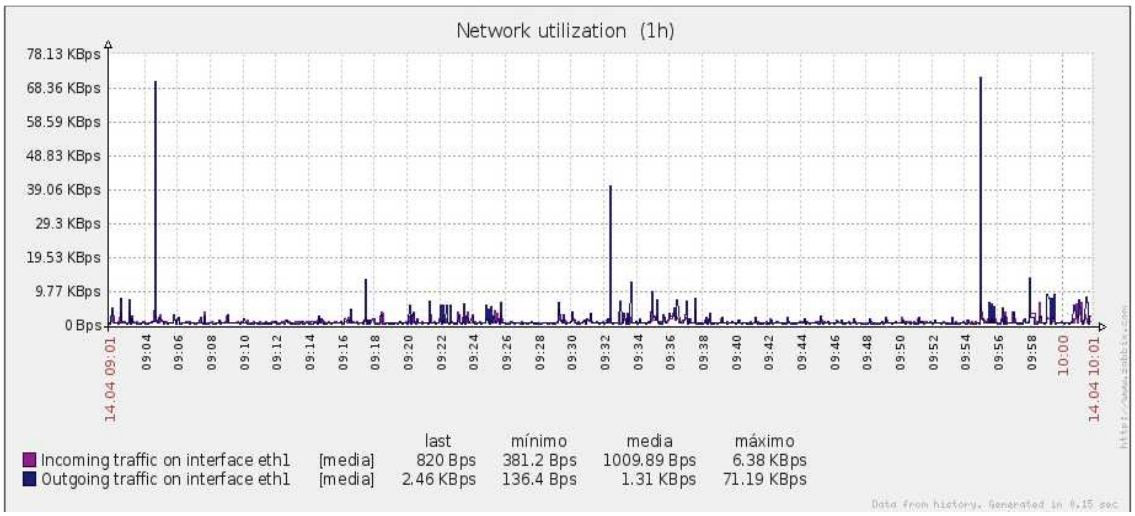


Fuente. Autora.

En la figura 63, por la opción añadir, se selecciona los dos parámetros para la interfaz cada uno se le define diferente color para el graficado. Luego se selección pre visualizar y la herramienta genera la siguiente figura.

En donde el color azul represente el tráfico de salida, el cual registra un mayor índice, con el color violeta se observa el tráfico de entrada en la interfaz eth1.

Figura 64. Grafico de utilización de red en el servidor zabbix



Fuente: Autora.

Por último, se hizo una comparación del tráfico registrado en la grafica 64 mediante la utilización de una página en internet: www.speedtest.net, como se muestra en la figura 65.

Figura 65. Prueba realizada a zabbix server

Se puede observar que los datos, arroja de una forma proporcional la misma información, que el servidor zabbix registra en la gráfica 64.

7. CONCLUSIONES

La tecnología Web, considerada como una forma de acceso fácil, económica e integrada, a la información de gestión de red, constituye sin duda alguna, una de las tendencias de futuro más prometedoras en el mercado de plataformas paraadministración de redes. Por medio de un navegador frontal, es posible realizar todas tareas de monitorización de dispositivos de una red empresarial en forma local o remota.

La popularidad del protocolo SNMP es debido a su sencillez y potenciapara monitorizar los recursos y servicios, sin sobrecargar mucho la red, esto, ha sido una de las razones por las cuales se ha mantenido como estándar y que sea la base de monitorización de muchas herramientas como zabbix que también ofrece otras posibilidades de vigilancia como a través de su agentes instalados y de las tecnologías que soporta como IPMI.

Implementar una solución de monitoreo que sea eficiente y efectiva, es una labor que implica bastante dedicación, la herramienta escogida zabbix, se puede considerar de alta calidad y desempeño, a la vez muy atractiva por su facilidad en el manejo, además la implementación de un proyecto de monitorización bajo esta herramienta de software libre resulta factible económicamente debido a la omisión de costos de licenciamiento, lo queconstituye una gran oportunidad para el desarrollo tecnológico de las pequeñas y mediana empresas PYMES, las cuales conforman un importante lugar en el mercado nacional.

El aumento sostenido de tamaño y complejidad de las redes de computadores, conllevana que cada vez, sea mayor la necesidad de una correctaadministración por parte de personalcualificado y del apoyo para esta tarea, de las herramientas de monitorización, que permiten realizar un estudio detallado sobre la red supervisada conociendo sufuncionamiento, proporcionando la posibilidad de solucionarcualquiertipo de falla presentada, identificando en tiempo real: su origen, sumagnitud y su influencia en el resto de la red.

8. REFERENCIAS BIBLIOGRAFICAS

ARQUITECTURA SNMP. Grupo de ingeniería telemática UdC. Disponible en: http://www.tlmat.unican.es/siteadmin/submaterials/95.pdf.

FRATERNEO GNU LINUX, Promoviendo el software libre y la educación. Disponible en: http://fraterneo.blogspot.com/2010/12/5-aplicaciones-libres-para-monitoreo-de.html

GOMEZ FERRER José Luis, SOLUCIONES TIC AVANZADAS. Disponible en: http://blog.e2h.net/2010/05/07/instalando-zabbix-la-ultima-solucion-de-monitorizacion-de-codigo-abierto/

GUZMAN CASTILLO Paola Fernanda. “Gestión en redes de computadoras”. Libro para la Especialización en Telecomunicaciones Universidad Industrial del Santander, Mayo de 2010.

INTRODUCCION A LA GESTION DE REDES. Disponible en: http://lacnic.net/documentos/lacnicx/Intro_Gestion_Redes.pdf.

JIMENEZ ALFARO Abraham Jorge, Herramientas de redes virtuales, México 2005 Disponible en: http://newton.azc.uam.mx/mcc/01_esp/

MANUAL ZABBIX 1.8. Disponible en: http://www.zabbix.com/documentation/1.8/manual/installation/installation_from_source.

MILLAN TEJEDOR Ramón Jesús. CONSULTORIA ESTRATEGICA EN TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACIÓN. Disponible en: http://www.ramonmillan.com/tutoriales/gestionred.php

MONITORIZACION Y GESTION DE RED. Infolan, tecnología aplicada a la gestión. Disponible en: http://www.infolan.es/web/pdf/dipt_SNMPc.pdf

PERPINAN Antonio. ADMINISTRACION DE REDES GNU/LINUX. Fundación Código Libre Dominicano. Disponible en: http//www .codigolibre .org

RED DE AREA LOCAL ADMINISTRACION Y GESTION. Editorial MacGraw-Hill, curso mailxmail. Disponible en: http://www.mailxmail.com/curso-red-informatica-bases.

STALLINGS William. SNMP, SNMPV2, SNMPV3, and RMON 1 and 2. Third Edition, Addison-wesley. 1999.

SUMMAN, MANEJO DOCUMENTAL E INFRAESTRUCTURA TECNOLOGICA Disponible en: http://www.summan.com/index.php/software/zenoss-.html

T-QoSMoS,QUALITY OF SERVICES MONITORING SOLUTIONS. Disponible en:http://www.tecsidel.es/tecsidel/fileadmin/downloads/Tic/productos-propios/Triptico_tQoSMOS-es_v1.0.pdf

ZENOSS. Monitorización de tecnología en la empresa. Disponible en: http://www.aplicacionesempresariales.com/zenoss-monitorizacion-de-tecnologia-en-la-empresa.html