ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Maestría En Sistemas De Información Gerencial

ñMONITOREO, ANÁLISIS DE LOGS Y GESTIÓN DE ALARMAS SOBRE LOS DISPOSITIVOS DEL CENTRO DE TECNOLOGÍAS DE INFORMACIÓN DE LA ESCUELA SUPERIOR NAVAL DE LA ARMADA DEL ECUADOR.ò

EXAMEN DE GRADO (COMPLEXIVO)

Previo a la obtención del grado de:

MAGÍSTER EN SISTEMAS DE INFORMACIÓN GERENCIAL

EDWIN ALEXANDER GUAMAN ALDAZ

GUAYAQUIL ï ECUADOR

AÑO 2015

AGRADECIMIENTO

Agradezco al Creador, Jehová mi Dios, quien me ha dado, en entendimiento, paciencia, para seguir este ideal tan ansiado y muy representativo en mi vida profesional. A mí querida madre que ha sido desde siempre el azimut a seguir dándome ejemplo de fortaleza, perseverancia, a mi esposa e hijos que he sacrificado tiempo valioso por cumplir esta meta.

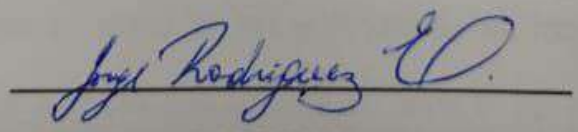
DEDICATORIA

El presente trabajo lo dedico a mi familia, hermanos, amigos y compañeros y en especial a mis hijos Edwin Guaman Jaen, Bianca Guaman Villamar que siempre han estado conmigo en las buenas y en las malas dándome su total apoyo incondicional

TRIBUNAL DE SUSTENTACIÓN

MGS. LENÍN FREIRE COBO
DIRECTOR MSIG

MGS. CARLOS SALAZAR LOPEZ
PROFESOR DELEGADO
POR LA UNIDAD ACADÉMICA



MGS JORGE RODRIGUEZ ECHEVERRIA
PROFESOR DELEGADO
POR LA UNIDAD ACADÉMICA

RESUMEN

Tomando en consideración la gestión que realiza los técnicos de redes del centro de datos de la Escuela Superior Naval, como es el de monitorear los diferentes eventos que se produce a diario, el conocer el estado de los distintos dispositivos que conforman el centro de datos, prevenir, incidentes, fallos, de sus componentes, como son a nivel de Infraestructura, enlaces y servicios.

Por tal razón se optó en la implementación, configuración de un sistema de monitoreo integral basado en software de libre distribución open source como son las herramientas Zabbix.

Dichas herramientas de monitoreo son de libre distribución compatibles con sistemas operativos como son Unix y las distribuciones de GNU/Linux, las mismas que cuentan con una gama de bondades que la convierten en una gran solución que nos ayudara en las actividades de monitoreo en el centro de datos donde nos alertara de cualquier alertar de eventos, incidentes, fallos, sobre los distintos dispositivos de sus componentes a nivel de

infraestructura, enlaces, servicios, esto contribuye al buen funcionamiento o estado de la red.

Para realizar dicha implementación se realizó un levantamiento de toda la infraestructura a nivel de servidores, servicios, enlaces, dispositivos activos (swtich, routers), a base de investigación vía web, a las comunidades de ayuda que cuenta el software libre y los diferentes logs y manuales, se realizó la implementación en la distribución de GNU/Linux Ubuntu Server 14.02 LTS.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

APACHE	Servicio de código abierto
BROWSER	Navegador
CETEIN	Centro de la Tecnología de la Información
DVD	Disco digital de mayor almacenamiento que el CD
ESSUNA	Escuela Superior Naval
FRONTEND	Capa frontal
GNOME	Entorno de escritorio gráfico
GNU	GNU no es Unix
GPL	Licencia pública general de GNU
IA-64	Arquitectura de los microprocesadores Itanium DE 64 bit
ICMP	Protocolo de Control de Mensajes de Internet
IP	Protocolo de Internet
LTS	Soporte de Tiempo Largo
MIB	Base de Información Gestionada
MIB-II	Base de Información Gestionada versión para SNMP2
SNMP	Protocolo Simple de Administración de Red
SSL	Seguridad de la capa de transporte
ULTRASPARC	Arquitectura con un conjunto de instrucciones reducidas.
USB	Dispositivo de almacenamiento de datos.

ÍNDICE DE FIGURAS

INTRODUCCIÓN

La implementación de un sistema de monitoreo, análisis de logs para los distintos tipos de componentes que forman parte del centro de datos de la Escuela Superior Naval, es para mantener a los técnicos informados de por medio de notificaciones y alarmas que provee esta aplicación Zabbix, en caso de generarse algún evento sobre algunos de los dispositivos o servicios que se encuentran trabajando; de tal manera que se pueda disponer de información del estado de cada componente del centro de datos en tiempo real y de información histórica.

Esta nos ayudara a de optimizar al máximo los tiempos de reacción y atención del personal técnico ante un incidente o problema**.**

Tomando en consideración el trabajo que desempeña la Escuela Superior Naval es de suma importancia proveer un soporte técnico tanto de su infraestructura como de sus servicios en el menor tiempo posible vista que no solamente en una institución educativa sino que es una institución militar.

Donde fluye información de entidades internas a nivel FF.AA. y externas (Gubernamentales, empresa pública) nacional e internacional la misma que por diferentes eventos que no pueden ser corregidos a tiempo producen un retardo en las comunicaciones.

Mantener habilitados todos sus servicios es de vital importancia para el buen desempeño de la institución, ya que por medio de los sistemas y equipos activos se mantiene la comunicación.

CAPÍTULO 1

GENERALIDADES

1.1 Descripción del Problema.

Actualmente la Escuela Superior Naval no cuenta con un sistema o herramienta de monitoreo que permitan conocer el estado de los distintos dispositivos que conforman el centro de datos, ni alertar de eventos, incidentes, fallos, sobre los distintos dispositivos de sus componentes, los cuales se detallan a continuación:

- INFRAESTRUCTURA (Componentes y subcomponentes)
    - Servidores con sistema operativo Windows
    - Servidores con sistema operativos Linux
    - Switches Cisco

- Switches HP
- Routers (Cisco, linsys, ubiquiti, dlink)
- Firewalls Cisco
- Central telefónica hibrida
- Dispositivos para interconexión radial (inalámbrica)

- ENLACES
  - Radioenlaces locales
  - Ultimas millas con los proveedores de internet
- SERVICIOS
  - Servicios corporativos gestionados (internet, correo, web, etc.)
  - Sistemas y aplicativos internos.
  - Base de datos (MySQL, PostgreSQL, MS SQL, Oracle).

No se cuenta con una herramienta de recolección y análisis de logs, que ayuden la generación de alertas y notificaciones o al análisis del personal técnico, al momento de realizar las tareas de resolución de problemas o evaluación del comportamiento de los sistemas y/o de la infraestructura TI.

Esto se traduce en tiempo de respuestas elevadas que impactan a la operación del área y a las actividades de la organización ya que no existe forma de que el área técnica detecte las fallas de un componente hasta que el usuario final reporte las afectaciones de un servicio, producto de algún fallo en los sistemas o la infraestructura.

1.2 Solución Propuesta.

Un sistema configurable y administrarle vía interface web como lo es la herramienta Zabbix, que soporte:

- Monitoreo mediante: ICMP, SNMP (versión 2 y 3), Agentes y Scripts.
- Recolección centralizada de logs, mediante protocolo SYLOGS.
- Evaluación y análisis de los logs recolectados y generación de las respectivas notificaciones y alertas según las reglas definidas.
- Evaluación del estado de los componentes mediante los métodos previamente definidos y generación de las notificaciones de las alertas, según los parámetros configurados para cada componente.
- Métodos de notificación y alertas:

- Notificaciones y alertas visuales desde la interface web.
- Notificaciones sonoras generadas desde la interface web.
- Notificaciones vía mail.
- Notificaciones vía SMS.
- Notificaciones vía SMNP Traps
- Registro de información histórica.

Diseño/arquitectura.

- Un web aplication server que proporcionara el acceso a la interface gráfica para el usuario.
- Servidor de base de datos que contendrá la información de:
    - Inventario de dispositivos.
    - Perfiles y roles de usuarios.
    - Configuración de alarmas.
    - Estados de los dispositivos.
    - Logs
    - Información histórica, etc.
- Monitor server
    - El cual implementa las rutinas de monitoreo según los protocolos soportados y el análisis de logs y la generación de notificaciones y/o alertas.

- Componentes de la solución:
    - Servidor Zabbix
        - Web server
        - Data base server
        - SNMP server
        - SNMP traps server.
        - Sylogs server.
        - SMTP server.
        - SMS Gateway server.
        - Agent server.

    - Cliente (dispositivo a monitorear).
        - Pila TCP/IP activa y direccionamiento IP configurado.
        - Soporte SNMP activado y configurado.
        - Envío de Traps SNMP activado y configurado.
        - SYSLOG activado y configurado.
        - Agentes de monitoreo.

CAPÍTULO 2

METODOLOGÍA DE DESARROLLO DE LA SOLUCIÓN.

2.1 Protocolos ICMP, SNMP, MIB.

Protocolo ICPM.

(Internet Control Message Protocol - Protocolo de Control de Mensajes de Internet), la función de este protocolo es de verificar y controlar si un paquete no alcanza su destino, o si su vida ha expirado, si el encabezado lleva un valor no permitido, si es un paquete eco o respuesta, de esta manera se verifica los errores detectados durante la conexión de la red. ICMP proporciona así una comunicación entre el software IP de una máquina y el mismo software en otra.

Protocolo SNMP.

(Simple Network Management Protocol ï Protocolo Simple de Administración de Red), protocolo de gestión de red, facilita el

intercambio de información de administración entre dispositivos que soporten dicho protocolo de red, permite a los administradores supervisar el funcionamiento de la red, buscar y resolver sus problemas, y planear soluciones inmediatas, este protocolo se compone de una capa de aplicación del protocolo, una base de datos de esquema , y un conjunto de objetos de datos . Las versiones de SNMP más utilizadas son SNMP versión 1 (SNMPv1) y SNMP versión 2 (SNMPv2). Comúnmente son usan en routers, switches, servidores, estaciones de trabajo, impresoras, bastidores de módem, etc.

- **Operaciones y Mensajes SNMP**: el trabajo que realiza el protocolo SNMP por medio de una serie simple de operaciones da a los administradores de red la capacidad de monitorear y analizar los nodos activos administrados e interactuar con estos como se determina en la figura 2.1.

get-request	Solicita el valor de una variable específica, mediante su OID.
get-next-request	Solicita el valor de una variable sin conocer su nombre exacto. Útil para búsquedas secuenciales dentro de una rama MIB.
get-bulk-request	Solicita grandes bloques de datos, como por ejemplo varias filas de un subárbol MIB.
get-response	Respuesta por parte del Agente a las operaciones de *get-request*, *get-next-request* o *set-request*
set-request	Almacena, altera un valor en una variable específica
inform-request	Comunicación entre gestores SNMP, NMS
trap	Mensaje no solicitado enviado por un Agente a un NMS cuando ocurre algún evento

Figura 2. 1 Operación del protocolo SNMP
Fuente: (Wikipedia ORG) **[3]**

MIB.

(Management Information Base - Base de Información Gestionada), se considera como una base de datos con información jerárquica almacenada en forma de árbol, El formato de la MIB se define como parte de la SNMP. (El resto de los MIB son extensiones de esta base de información de gestión básica.), como es el MIB-I, MIB-II.

El árbol MIB detalla las jerarquías fijadas por las diferentes organizaciones como se lo determina en la figura 2.2.

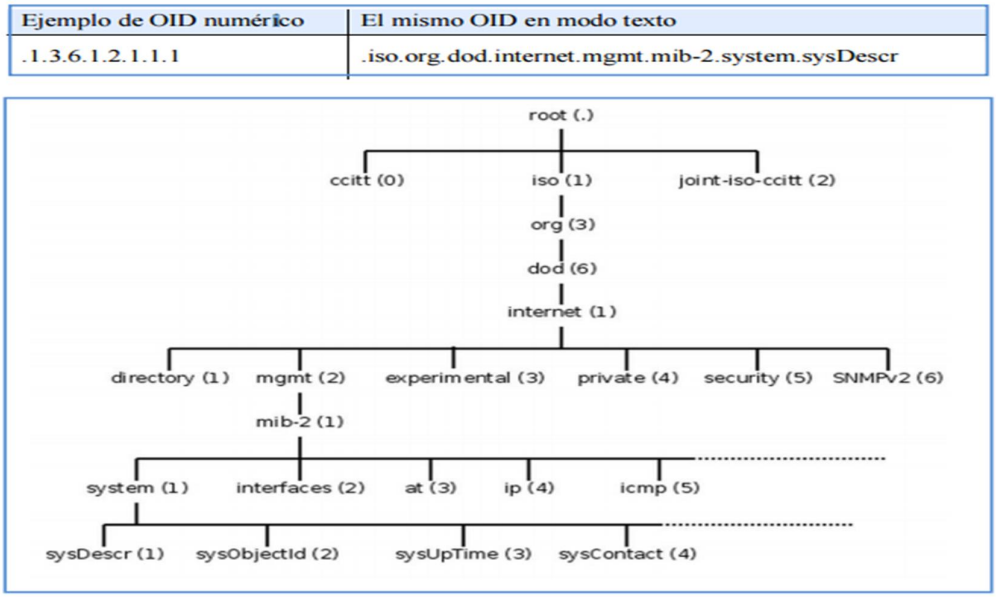


Figura 2. 2El árbol MIB
Fuente: (Wikipedia ORG) **[3]**

2.2 Software Libre

Software Libre se refiere a la libertad del usuario para, distribuir, copiar, ejecutar, estudiar, cambiar y mejorar el software. De modo más preciso, se refiere a cuatro libertades de los usuarios del software:

- La libertad (0), es la de usar el programa, con cualquier propósito.
- La libertad (1), es la de adaptar y estudiar las funcionalidades del programa para acoplarlo a tus necesidades. El acceso al código fuente es una condición previa para esto.
- La libertad (2), es la de distribuir copias.
- La libertad (3), es la de mejorar el programa y hacer públicas las mejoras a los demás; requisito previo el acceso al código fuente.

2.3 Proyecto GNU

El Proyecto GNU es la creación de un sistema operativo completo con software libre compatible con arquitectura Unix, GNU acrónimo (GNU´s Not Unix ï No es Unix).

En septiembre de 1983 Richard M. Stallman funda el proyecto GNU, para crear un sistema operativo completo de Software Libre, hoy tenemos varios sistemas operativos basados exclusivamente en Software Libre dando a todos el derecho de usar, compartir, estudiar y mejorar el software para cualquier finalidad.

Las principales licencias del proyecto GNU son la Licencia Pública General de GNU (GPL), y la Licencia Pública General Reducida de GNU (LGPL), aunque el nombre original de esta última era «Licencia Pública General de Bibliotecas de GNU». Con los años, se han establecido como las licencias de Software Libre más utilizadas.

El nombre reconoce que GNU aprendió del diseño técnico de Unix, pero también indica claramente que no están relacionados. A diferencia de Unix, GNU es Software Libre.

El diseño de GNU es modular igualando las cualidades de Unix. Esto significa que se le pueden añadir a GNU componentes de terceras partes; en 1991 Linus Torvarlds crea un núcleo idéntico a Unix, Linux, y

lo libera como software libre en 1992. La unión de Linux experimentadamente completo un sistema GNU y formo un sistema operativo completo.

2.4 Licencia GPL GNU:

Se considera que es una licencia libre y gratuita con derecho de copia para software, La Licencia Pública General de GNU (GNU GPL, por sus siglas en inglés).

La Licencia Pública General de GNU garantiza la libre distribución y modificación de todas las versiones de un programa, a fin de asegurarle dicha libertad a todos los usuarios. Las licencias para la mayoría del software y otras obras de índole práctica están diseñadas para privarle de la libertad para distribuir y modificar.

Las Licencias Públicas Generales están diseñadas para garantizarle a usted la libertad de distribuir copias de software libre (y cobrar por ellas, si así lo desea), obtener el código fuente, o tener la posibilidad de

obtenerlo, modificar el software o utilizar partes del mismo en nuevos programas libres, y saber que puede hacer estas cosas.

A fin de proteger a los desarrolladores y autores, la GPL explica claramente que no se ofrecen garantías por este software libre. Por el bien de los usuarios y de los autores, la GPL exige que las versiones modificadas se identifiquen como tales, de modo que los problemas que puedan contener estas versiones no se atribuyan erróneamente a los autores de versiones anteriores.

Por último, la buena acogida de estas distribuciones o modificaciones ha sido muy atractivo para las grandes empresas por lo que estas amenazan con patentar el uso de estos software. Los gobiernos de los diferentes países no deberían permitirles a las patentes restringir el desarrollo y el uso de software en computadoras para fines generales, pero, en el caso de que esto suceda, deseamos evitar el riesgo especial de que las patentes que se apliquen a un programa libre efectivamente otorguen tal exclusividad. Para lograrlo, la GPL garantiza la imposibilidad del uso de las patentes para apropiarse de un programa y restringir dicha libertad.

2.5 Ubuntu.

Ubuntu es una distribución Linux que ofrece un sistema operativo orientado principalmente a computadoras personales, servidores. Es una de las más importantes distribuciones de Linux a nivel mundial.

Se basa en Debian GNU/Linux y concentra su objetivo en la facilidad y libertad de uso, la fluida instalación y los lanzamientos regulares de las actualizaciones ayuda a mantener un sistema operativo robusto y estable para trabajados en el área de sistemas, su desarrollo es una muestra del concepto GNU/Linux, ya que todo su código fuente puede ser utilizado, modificado y redistribuido libremente bajo los términos GPL.

Canonical Ltd. es una empresa privada fundada y financiada por el empresario sudafricano Mark Shuttleworth, para la promoción de proyectos relacionados con software libre y uno de los proyectos más importante financiado hasta la fecha es la distribución de GNU/Linux ñUbuntuò, basada en Debian GNU/Linux. Que es una distribución Linux de software basado en el núcleo Linux, que incluye varios paquetes de

software satisfaciendo las necesidades de los usuarios, dando así el inicio de versiones más amigables como son (ediciones domésticas, empresariales y las más robustas que son para servidores), en algunos casos añaden aplicaciones, controladores propietarios.

Para nuestra propuesta se utilizó Ubuntu 12.04 LTS, como sistema operativo o plataforma y la instalación de la Herramienta ZABBIX, debido a la cantidad de información que se obtiene en la instalación tanto de la plataforma como de las herramientas de monitoreo, el uso de esta versión es porque en el CETEIN-ESSUNA (centro de datos), se encuentra instalado en el mismo está trabajando un squid proxy.

Características de Ubuntu:

- Soporta las plataformas i386, AMD64, UltraSPARC, PowerPC (no más a partir de la v7.04), IA-64.
- Su interfaz de usuario por defecto es GNOME, y se sincroniza con sus liberaciones.
- Ubuntu se basa en gran medida en los trabajos de las comunidades de Debian y GNOME.

- Las versiones estables son liberadas cada 6 meses.
- Su navegador web oficial es Mozilla Firefox.

2.6 Zabbix:

Es una herramienta robusta de monitoreo, es decir que es una aplicación que nos permite conocer el estado actual del funcionamiento de infraestructura en hardware y software.

Fue creado por el señor Alexei Vladishey y actualmente se desarrolla y se soporta por la compañía Zabbix SIA. Este sistema además nos permite monitorear la capacidad, el rendimiento y la disponibilidad de los servidores, equipos, aplicaciones y bases de datos de los diferentes dispositivos (routers, UPS, etc.). En un escenario real y complejo, nos permite saber qué está pasando con la plataforma en tiempo real e históricamente, sino ser capaz de anticipar eventos futuros que puedan afectar su desempeño, su característica primordial con sus alertas, visualizaciones, Monitoreo centralizado a través del administrador web, disponible para diferentes sistemas operativos Linux, Windows, Mac os, entre otros, envío de alertas vía correo electrónico, envío de alertas SMS.

Zabbix posee varias características que la hacen una eficaz y poderosa alternativa de monitoreo, entre otras:

- Es full Open Source. No hay costo de licencias involucradas.
- Tiene una arquitectura de 3 capas (base de datos, servidor, presentación)
- Basado en Linux con BD mysql o postgres.
- Full web.
- El monitoreo se realiza mediante agentes. Hay agentes Zabbix para Windows y Unix (Linux).
- Es capaz de monitorear cualquier dispositivo que soporte la interfaz SNMP (por ejemplo routers).

2.7 Implementación de la solución.

Para realizar la instalación primero se debe de instalar el sistema operativo.

2.7.1 Instalación de Ubuntu 12.04

Una vez que se obtiene el sistema operativo se lo puede instalar ya sea desde un USB, CD o un DVD, en nuestro caso insertaremos el CD unidad lectora de vuestro ordenador y reiniciamos, después de cargarse algunas cosas en memoria, la primera pantalla que veremos será la siguiente:

Arranque desde el CD y nos presenta una pantalla como se puede observar en la figura 2.3

Figura 2. 3 Primera Pantalla
Fuente: (Canonical Ltd, 2015) [1]

Se escoge el idioma de instalación y se presiona el botón instalar Ubuntu como se detalla en las figuras 2.4 y figura 2.5.

Figura 2. 4 Pantalla de inicio de instalación.
Fuente: (Canonical Ltd, 2015)

Figura 2. 5 Pantalla de opciones de instalación
Fuente: (Canonical Ltd, 2015) [1]

Inicia la preparación de la instalación de una manera descriptiva, donde se analiza 3 recursos básicos para una instalación exitosa, como se describe en las figuras 2.6 y figura 2.7.

- **Espacio en disco.**
- **Conectado a la corriente**.
- **Conexión a Internet**.

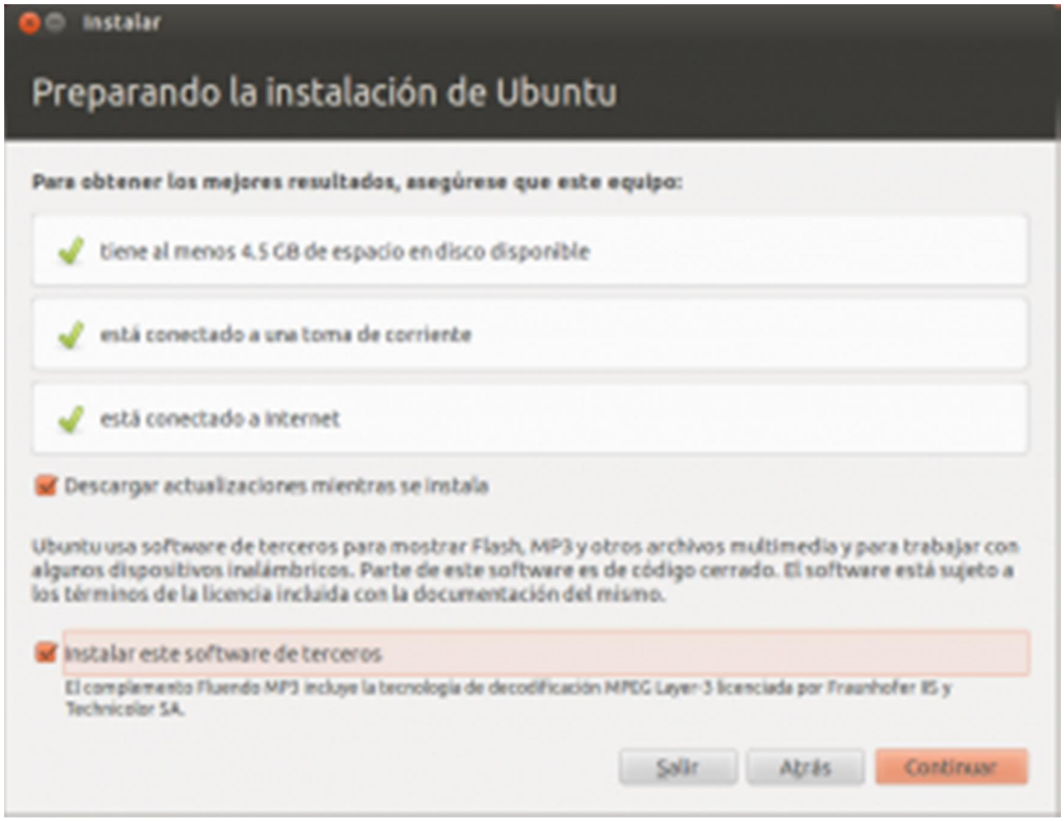


Figura 2. 6. Preparando la Instalación de Ubuntu
Fuente: (Canonical Ltd, 2015) [1]

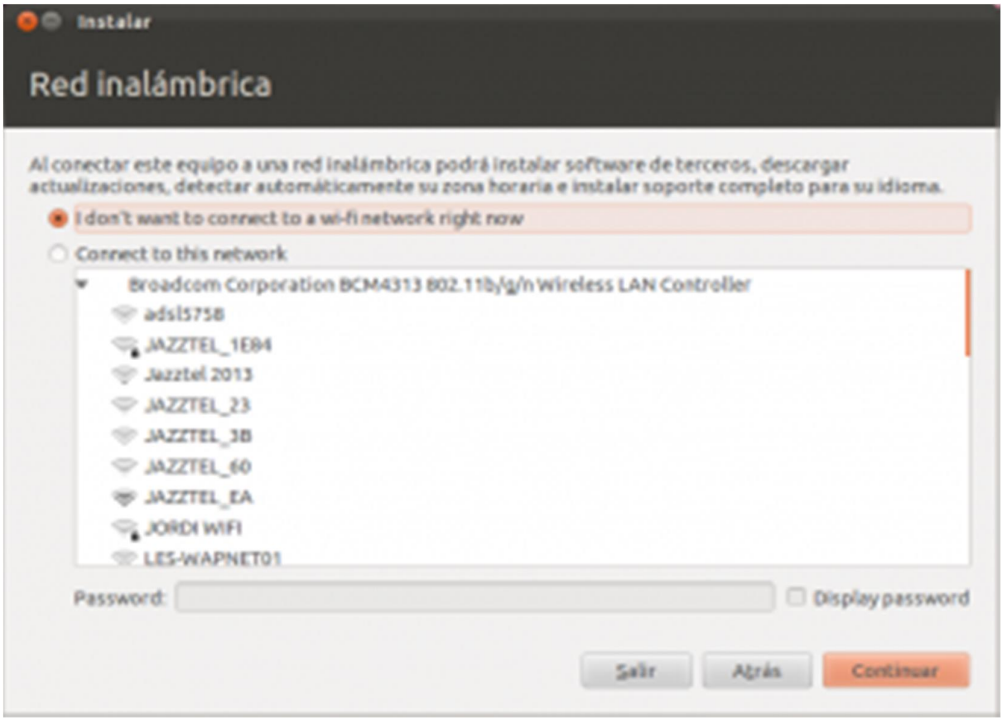


Figura 2. 7 Pantalla de configuración de las interfaces de red
Fuente: (Canonical Ltd, 2015) [1]

En la siguiente figura nos presenta los tipos de instalación, se escoge depende del escenario que se encuentra el Administrador.

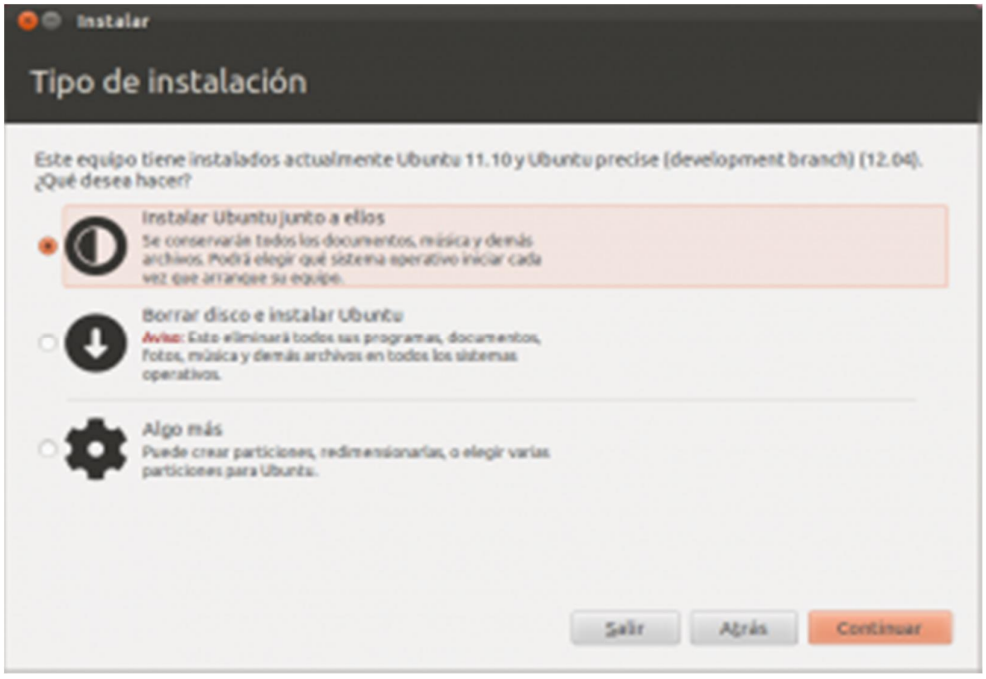


Figura 2. 8 Tipos de instalación
Fuente: (Canonical Ltd, 2015) [1]

Una vez que se realiza el particionamiento de los discos se escoge en la ventana borrar disco e instalar Ubuntu como se puede observar en la figura 2.9. Siguiente paso nos pide que escoja la zona horaria, idioma del teclado figuras 2.10 y figura 2.11

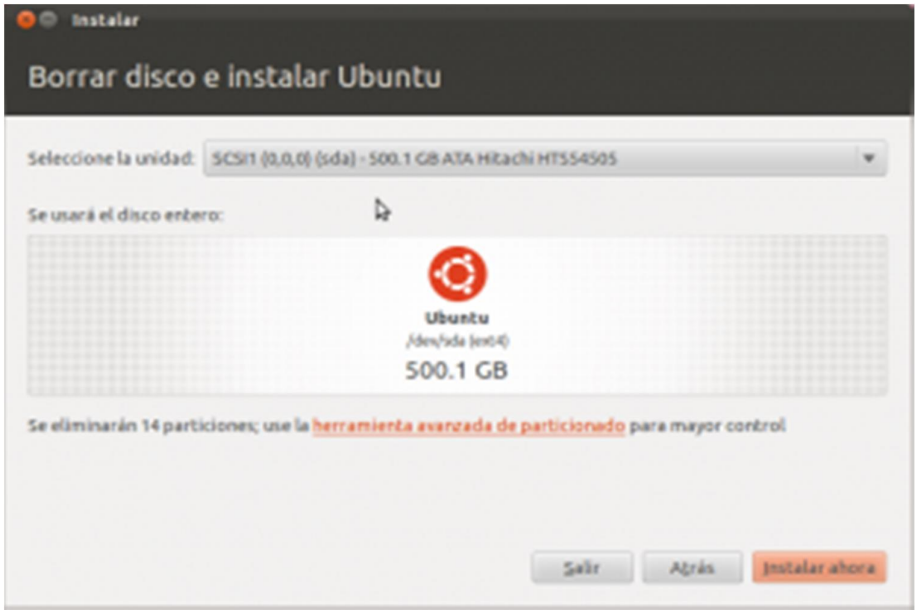


Figura 2. 9 Realiza partición del disco duro
Fuente: (Canonical Ltd, 2015) [1]

Figura 2. 10 Zona Horaria
Fuente: (Canonical Ltd, 2015) [1]

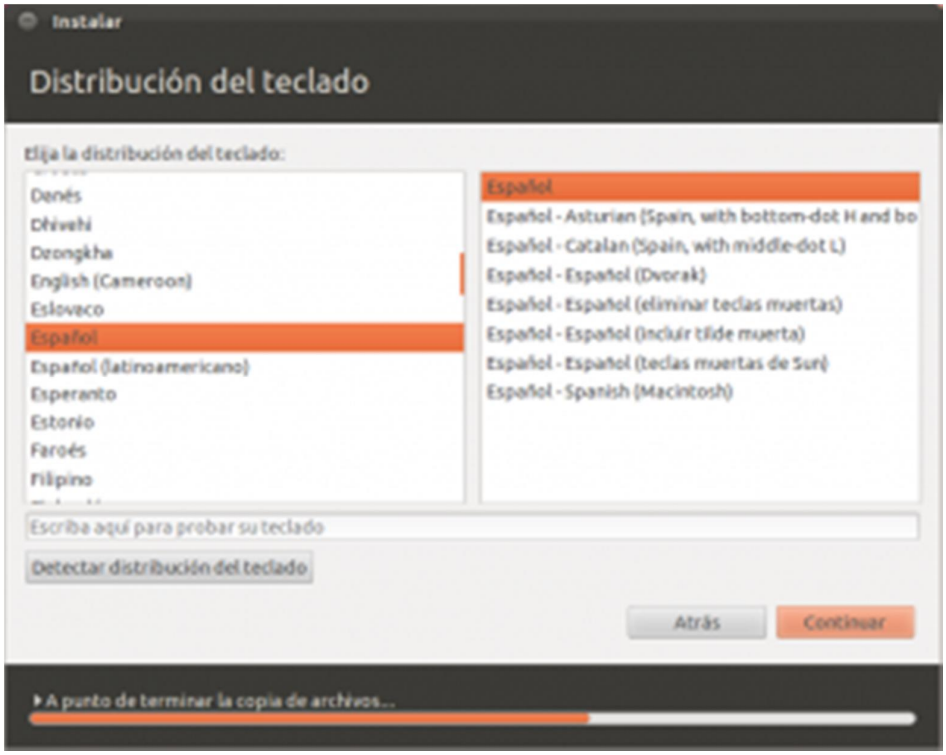


Figura 2. 11 Idioma del teclado
Fuente: (Canonical Ltd, 2015) [1]

Luego nos da la opción de un registro y creación de un usuario el mismo que nos servirá para acceder al root, luego finaliza la instalación figura 1.12 y figura 1.13

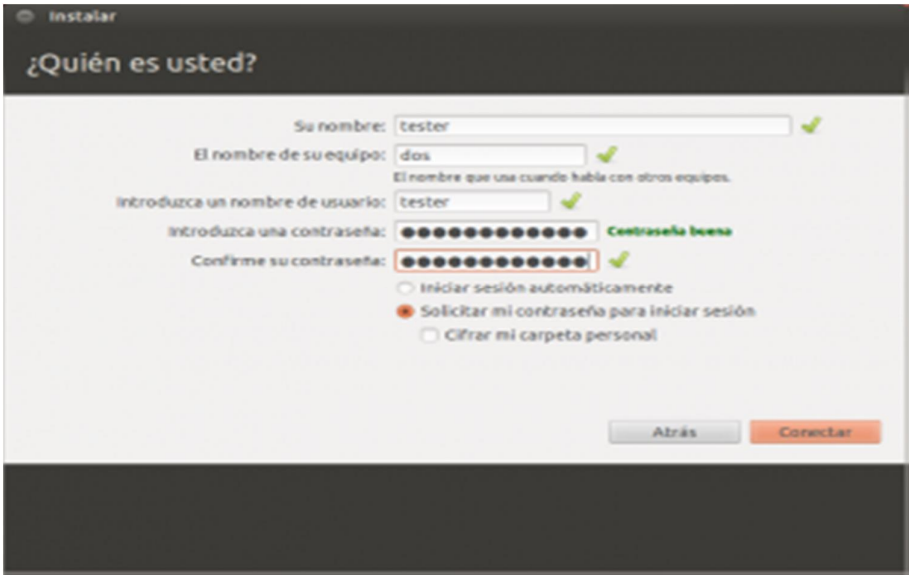


Figura 2. 12 Creación de clave root
Fuente: (Canonical Ltd, 2015) [1]

Figura 2. 13 Pantalla de finalización
Fuente: (Canonical Ltd, 2015) [1]

2.7.2 Instalación de ZABBIX.

En la siguiente figura 2.14, describimos las aplicaciones necesarias para la instalación previa de ZABBIX.

Software	Version	Comments
Apache	1.3.12 or later	
PHP	5.0 or later	
PHP modules: php-gd	GD 2.0 or later	PHP GD module must support PNG images.
PHP TrueType support		--with-ttf
PHP bc support		php-bcmath, --enable-bcmath
PHP XML support		php-xml or php5-dom, if provided as a separate package by the distributor
PHP session support		php-session, if provided as a separate package by the distributor
PHP socket support		php-net-socket, --enable-sockets. Required for user script support.
PHP multibyte support		php-mbstring, --enable-mbstring
MySQL php-mysql	3.22 or later	Required if MySQL is used as Zabbix back end database.

Figura 2. 14 Paquetes de instalación previos para Zabbix
Fuente: (Zabbix SIA, 2015) [6]

Se inicia con la premisa que la tarjeta de red se encuentra configura con la IP 10.128.x.x el mismo que se lo realiza en el archivo interfaces, el mismo que se lo voy a detallar a continúan el archivo editado:

ESSUNA-CTI-SRV-001@zabbix:~$sudo nano /etc/network/interfaces

- auto eth0
- iface eth0 inet static
- iface eth0 inet static
- address 10.128.x.x
- netmask 255.255.255.x

- network 10.128.x.x
- broadcast 10.128.x.x
- gateway 10.128.x.x
- dns-nameservers 200.93.x.x
- dns-nameservers 200.93.x.x

Una vez verificado el archivo de la interface de red, se puede reiniciar el servicio con el siguiente comando el mismo que es escrito en una misma línea.

ESSUNA-CTI-SRV-001@zabbix:~$sudo service networking restart

Por medio de los comandos wget, dpkg y apt-get se inicia la descarga del paquete que nos acoplara los repositorios, los mismos que nos ayudaran a instalar la versión 2.2 de Zabbix, compatible para Ubuntu, en el transcurso de la descarga El instalador indica el espacio en disco que se va a utilizar y solicita la confirmación de la instalación como se observa en la figura 2.15, el uso de los comandos lo describo a continuación esto desde el prontuario ESSUNA-CTI-SRV-001@zabbix:~$:

- wget http://repo.zabbix.com/zabbix/2.2/ubuntu/pool/main/z/zabbix-release/zabbix-release_2.2-1+trusty_all.deb.
- sudo dpkg -i zabbix-release_2.2-1+trusty_all.deb. .

- sudo apt-get update. .

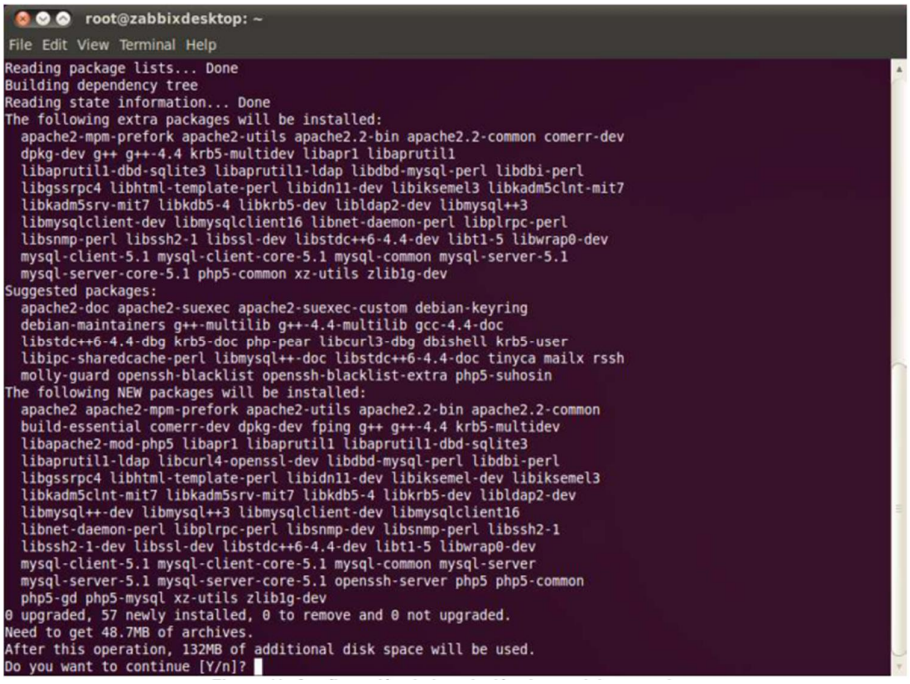


Figura 2. 15 Descarga repositorios
Fuente: (Zabbix SIA, 2015) [6]

Una vez finalizado la descarga de los repositorios se inicia la instalación del servidor Zabbix y el frontend, para ello se usa el siguiente comando partiendo desde el prontuario ESSUNA-CTI-SRV-001@zabbix:~$:

sudo apt-get install zabbix-server-mysql zabbix-frontend-php.

Inicia el proceso de descarga de paquetes para los servicios LAMP, en este proceso nos pedirá la creación de un usuario root para el MySql. Esta contraseña son pedirá nuevamente en la instalación Zabbix para poder conectarse y crear la base de datos, tablas solicitadas por Zabbix. Además,

nos pedirá una nueva contraseña para el usuario Zabbix de MySql que usará el server y el frontend para conectarse a la base de datos como se detalla en la figura 1.16.

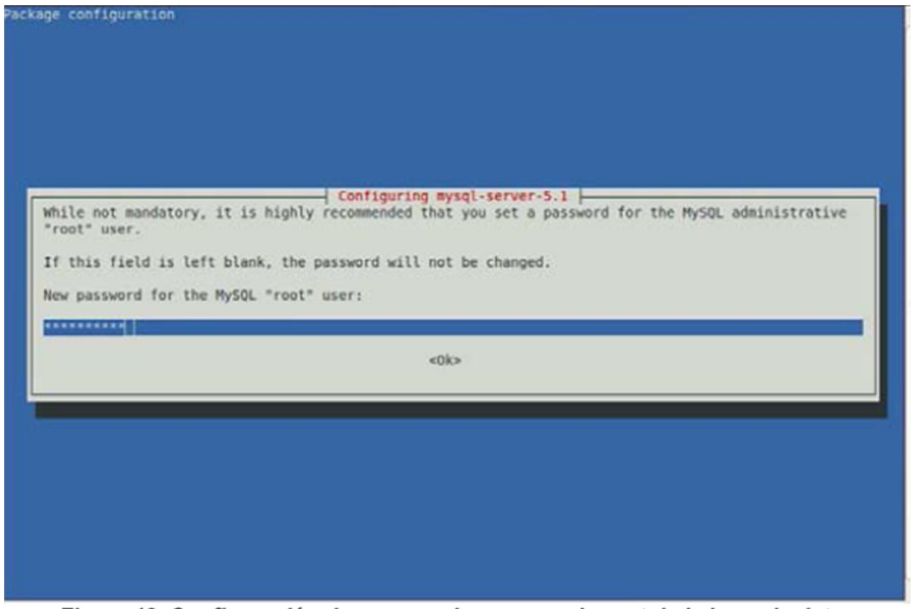


Figura 2. 16 Ingreso de la clave de la clave root de la base de datos
Fuente: (Zabbix ORG) [5]

Se editar los ficheros de configuración del servicio Apache con el siguiente comando:

ESSUNA-CTI-SRV-001@zabbix:~$sudo nano /etc/zabbix/apache.conf.

Se abrirá el fichero y se procede a cambiar la zona horaria del servicio apache, luego se procede a verificar, que sea similar a la zona horaria del servidor que estamos trabajando como se detalla en la figura 2.17 y figura 2.18.

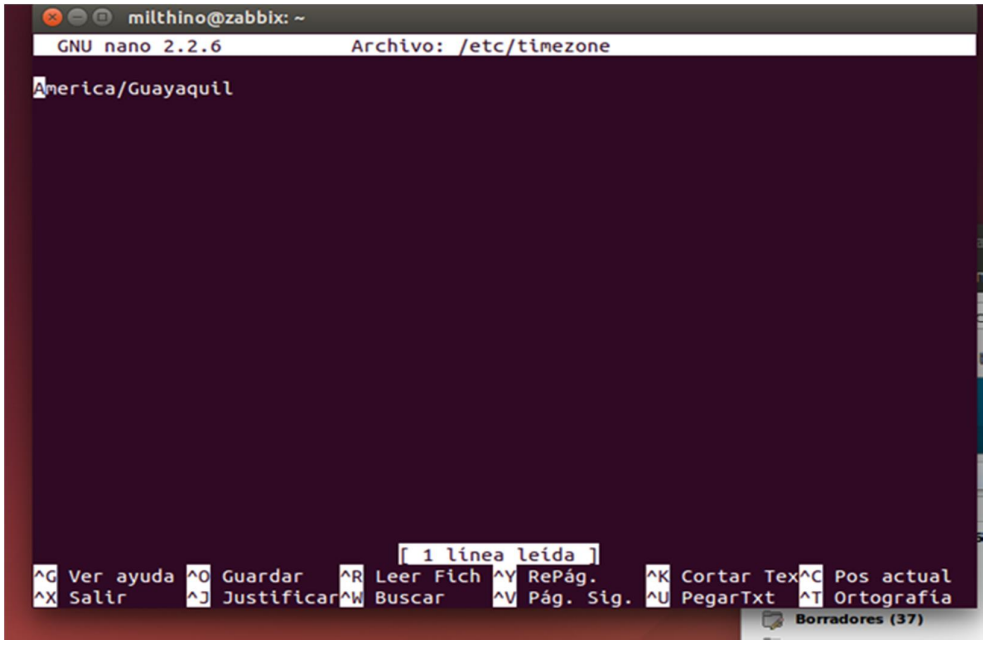


Figura 2. 17 Verificación de zona horaria en el servidor

Fuente: (Zabbix ORG) [5]

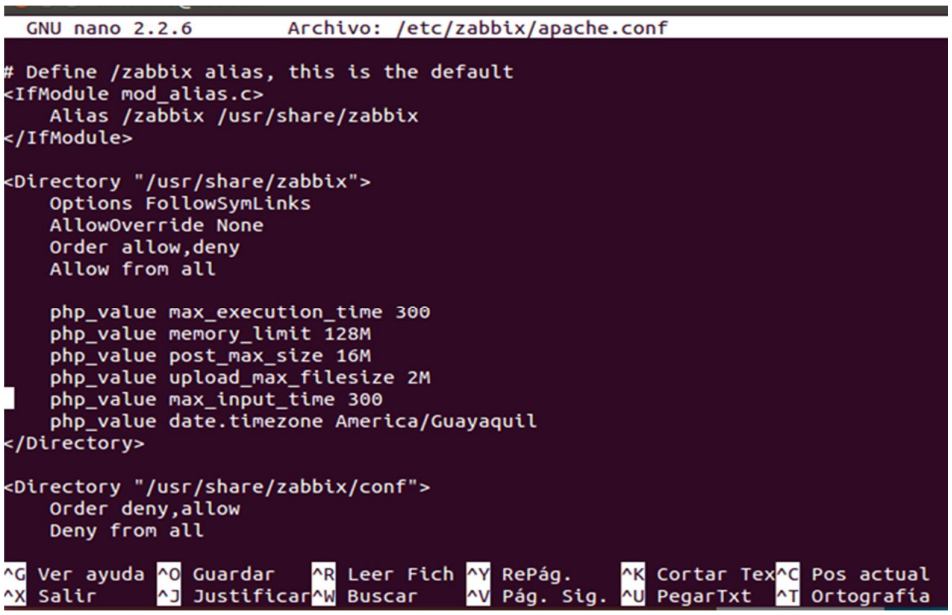


Figura 2. 18 Cambio de zona horaria en Apache
Fuente: (Zabbix SIA, 2015) [5]

Una vez cerrados los ficheros de la zona horaria, desde una terminal procedemos a realizar la configuración del enlace simbólico en apache y habilitarlo:

- sudo ln -s /etc/zabbix/apache.conf /etc/apache2/sites-available/001-zabbix.conf.
- sudo a2ensite 001-zabbix.
- sudo service apache2 reload.

Con los siguientes comandos ejecutados desde una terminal, configuramos la encriptación de las comunicaciones del frontend habilitando SSL en Apache y deshabilitamos el servidor web de la raíz como se describe a continuación desde el prontuario ESSUNA-CTI-SRV-001@zabbix:~$:

- sudo a2enmod ssl.
- sudo a2ensite default-ssl.
- sudo a2dissite 000-default.

Buscamos el archivo /etc/apache2/ports.conf para realizar el cambio en la línea donde se encuentra Listen 80 comentándola con el signo # para deshabilitar el puerto 80 que se encuentra en escucha, de esta manera el servidor solo atenderá peticiones en el al puerto 443-https. Como se describe en la figura 2.19

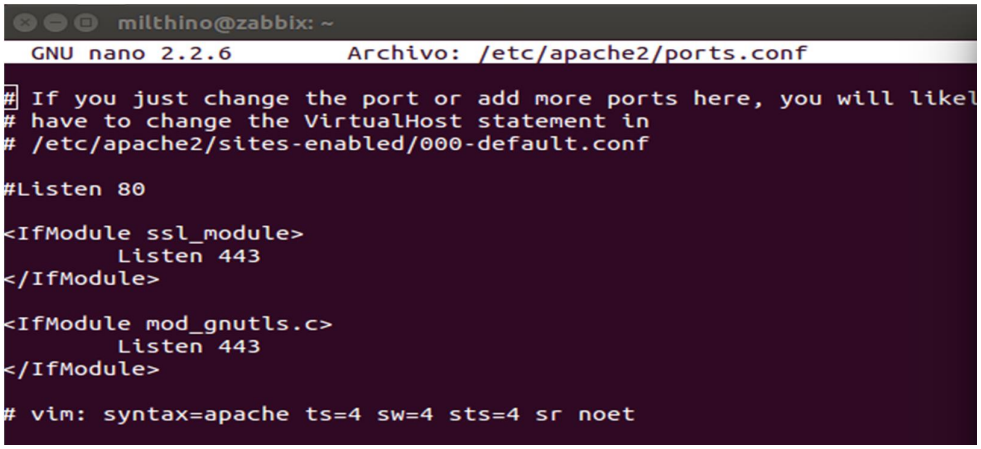


Figura 2. 19 Cambio de puerto de escucha
Fuente: (Zabbix SIA, 2015) [6]

Reiniciamos el servicio apache como se detalla en la figura 2.20

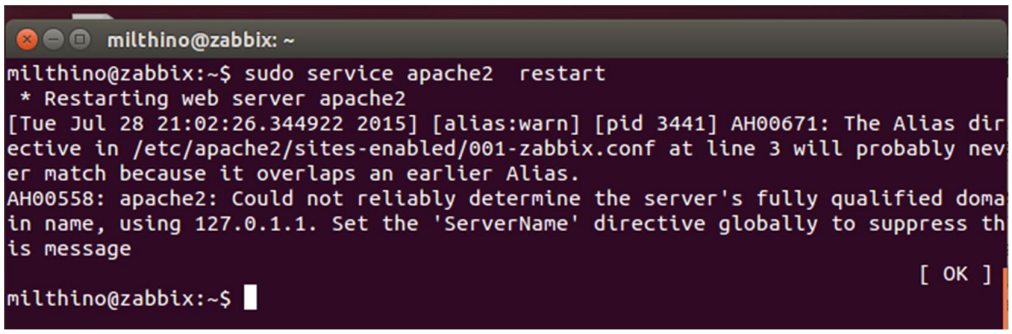


Figura 2. 20 Reinicio del servidor apache
Fuente: (Zabbix SIA, 2015) [6]

Después del reinicio del servicio antes mencionado finalizo la instalación de servidor Zabbix y el frontend, base de base de datos. Iniciamos con la configuración del frontend, desde el navegador, para ello en el browser escribimos https://192.168.0.100/zabbix como se detalla en la figura 2.21.

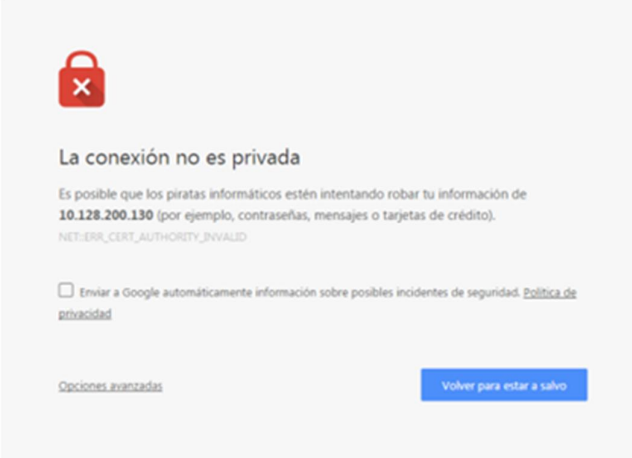


Figura 2. 21 Ingreso a la configuración de frontend
Fuente: (Zabbix SIA, 2015) [6]

Nota: por primera vez nos saldrá la conexión no es permitida, pero damos click en opciones avanzadas y presionamos en la opción Acceder a 10.128.200.130 (sitio no seguro). La configuración es intuitiva por eso se manejar más gráficos y descripción de los mismos:

Figura 2. 22 La página de bienvenida. Presionamos en "Next".
Fuente: (Zabbix SIA, 2015) [6]

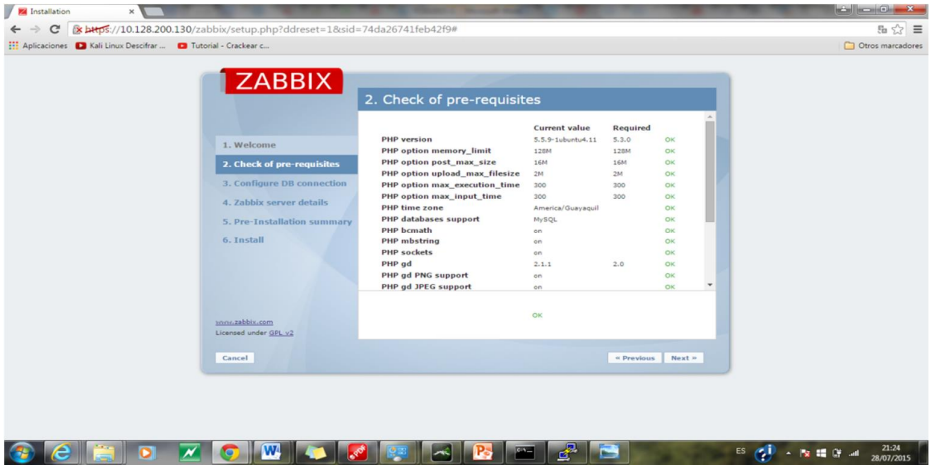


Figura 2. 23 Validación de la instalación de todas las dependencias.
Fuente: (Zabbix SIA, 2015) [6]

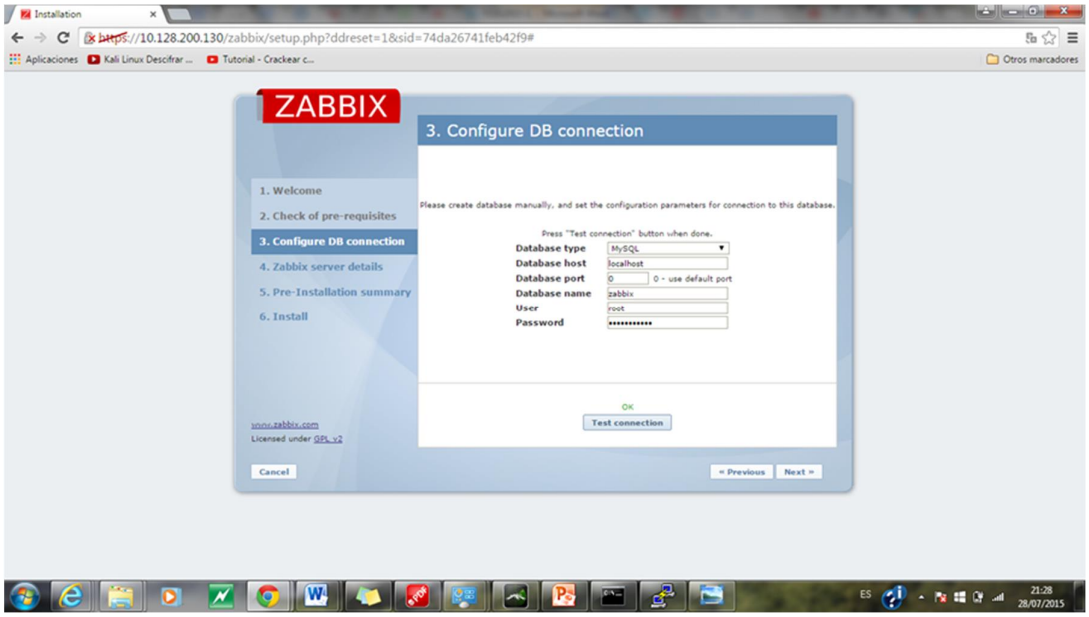


Figura 2. 24 Prueba de la conexión con la base de datos.
Fuente: (Zabbix SIA, 2015) [6]

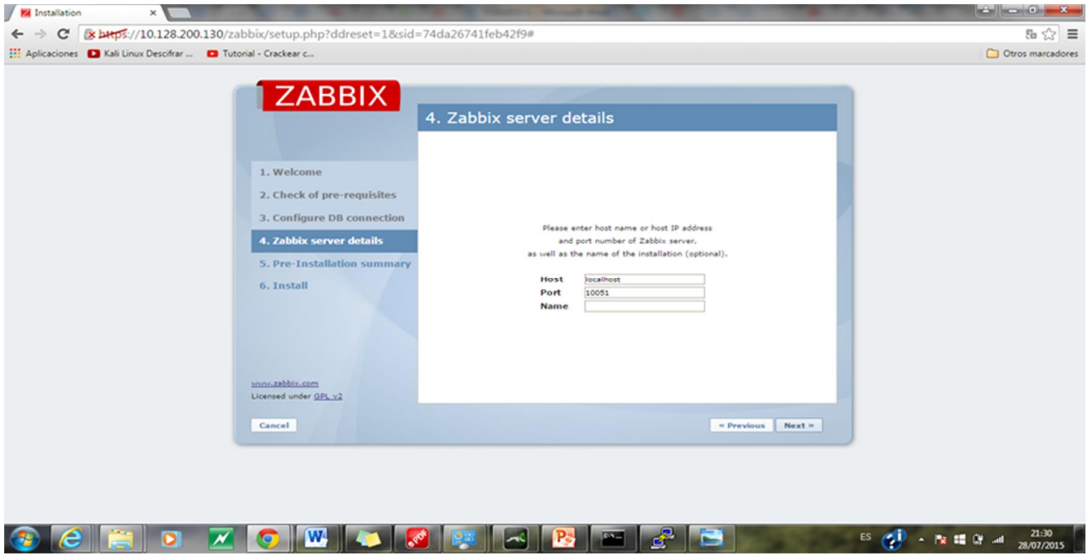


Figura 2. 25 Configuración de frontend con conexión Zabbix.
Fuente: (Zabbix SIA, 2015) [6]

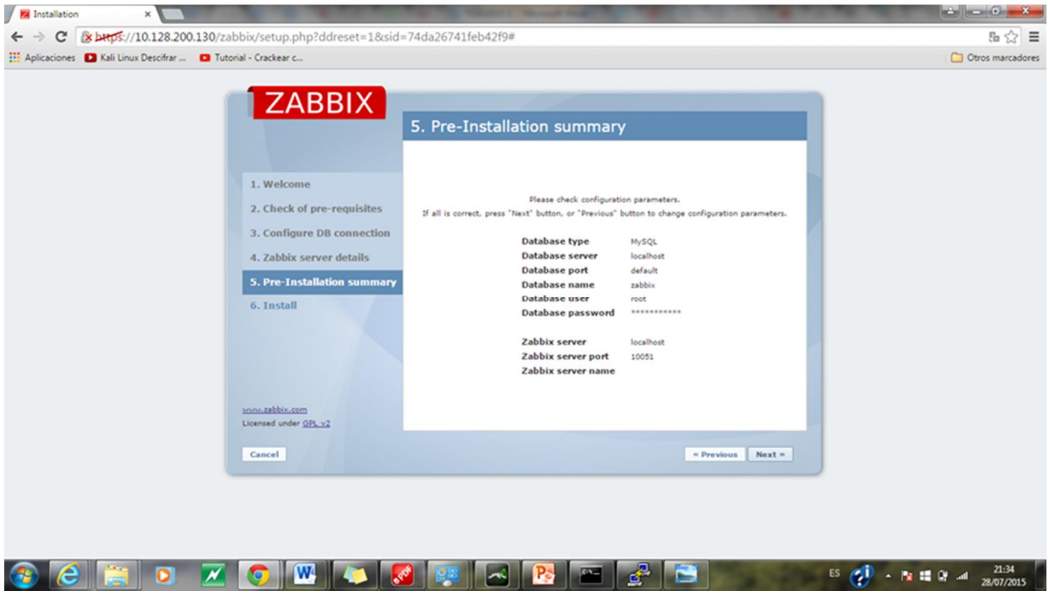


Figura 2. 26 Resumen de la configuración
Fuente: (Zabbix SIA, 2015) [6]

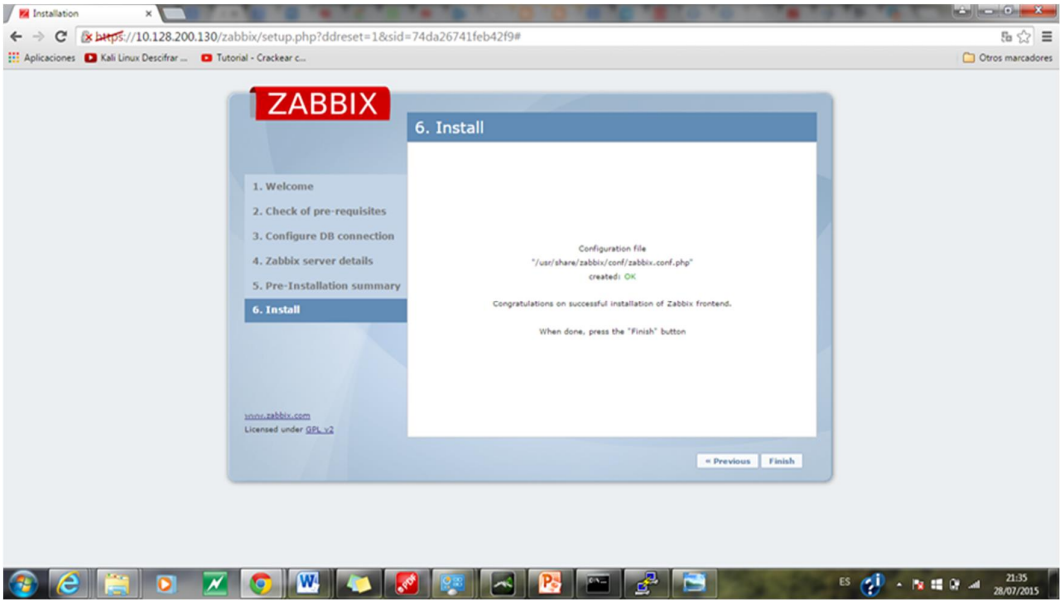


Figura 2. 27 Resumen de la configuración
Fuente: (Zabbix SIA, 2015) [6]

2.7.3 Instalación de Agente en Windows

Ir al sitio oficial para descargar el agente para Windows en mismo que se descarga zipiado o comprimido.

http://www.zabbix.com/downloads/2.2.0/zabbix_agents_2.2.0.win.zip

Una vez bajado el paquete comprimido, se lo extrae en esta ruta:

c:\zabbix_agents_2.2.0.win\.

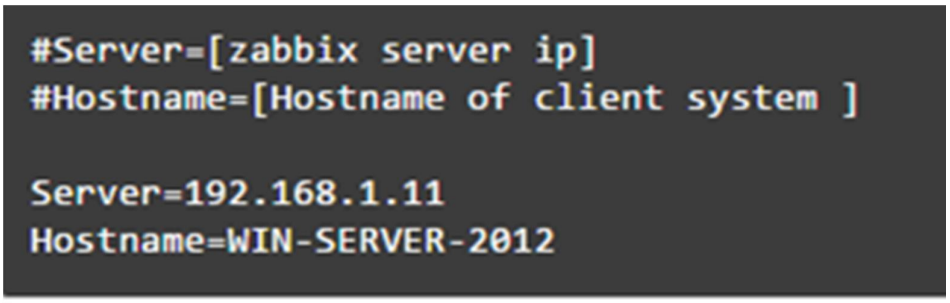
Se crea un archivo de configuración del agente de nombre:

c:\zabbix_agentd.conf.

Usando como ejemplo el archivo que se encuentra en:

c:\zabbix_agents_2.2.0.win\conf\ zabbix_agentd.win.conf.

Se cambia los siguientes parámetros como se detalla en la figura 1.27 y figura 1.28, donde se puede observar el archivo original y los parámetros a cambiar.



.

Figura 2. 28 Parámetros que se debe cambiar.
Fuente: (Zabbix SIA, 2015) [6]

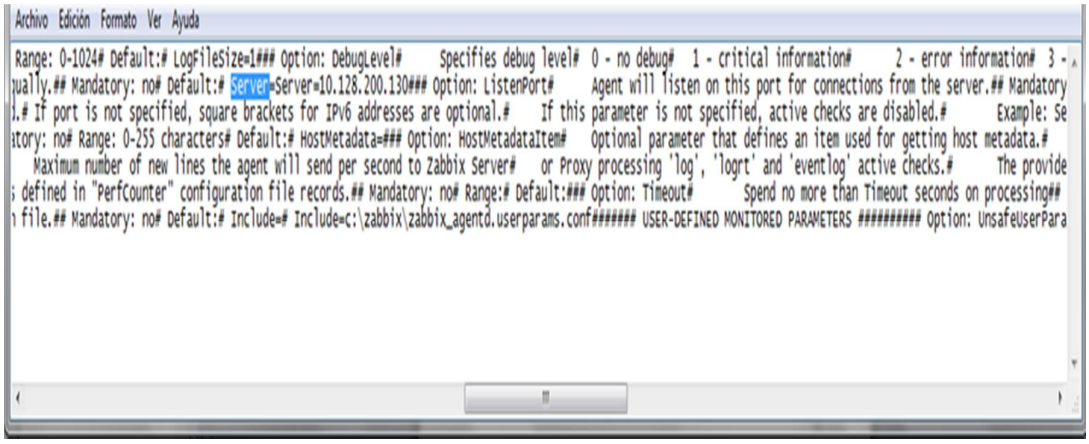


Figura 2. 29 Archivo original .conf
Fuente: (Zabbix SIA, 2015) [6]

browser = Es la IP del servidor Zabbix.

Hostname=Es el nombre del host que se instaló el agente.

Una vez realizados los cambios se procede a instalar el agente desde la línea de comandos de DOS CMD. Como se puede observar en la figura 2.30

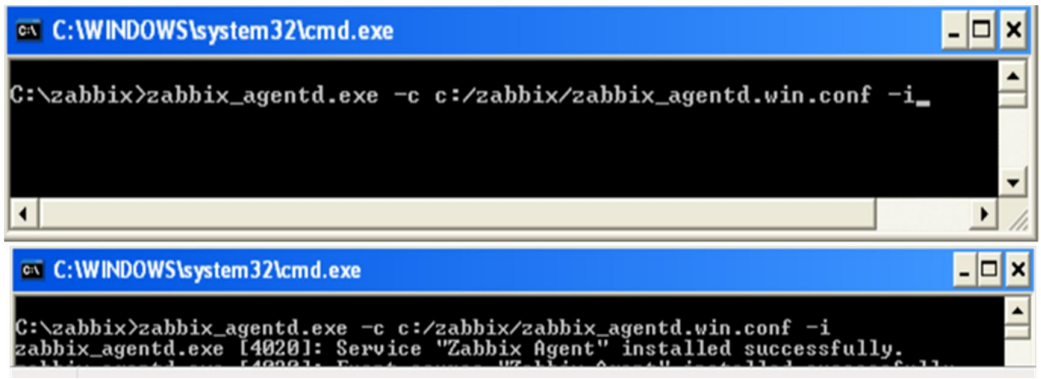


Figura 2. 30 Comandos para instalación del agente para Windows
Fuente: (Zabbix SIA, 2015)[6]

2.7.4 Agregación del servidor Zabbix al Forntend

Por defecto se agrega el servidor pero la opción monitoreo se encuentra desactivada en la figura 2.31 se puede observar el servidor con el nombre de Zabbix_server.

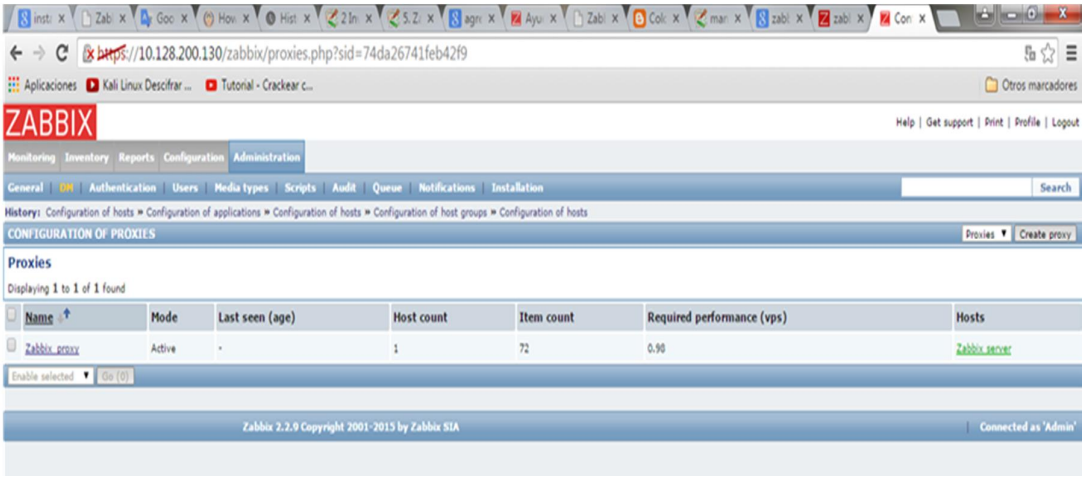


Figura 2. 31 Pantalla donde se observa el servidor agregado.
Fuente: (Zabbix SIA, 2015) [6]

2.8 Agregar de una máquina en Zabbix.

Nos dirigimos a la opción configurar, hosts, créate host, se abre una ventana donde se llena los campos, hacemos click en los Template para escogemos el Template OS Windows, como lo describo en la figura 2.32, figura 2.33 figura 2.34.

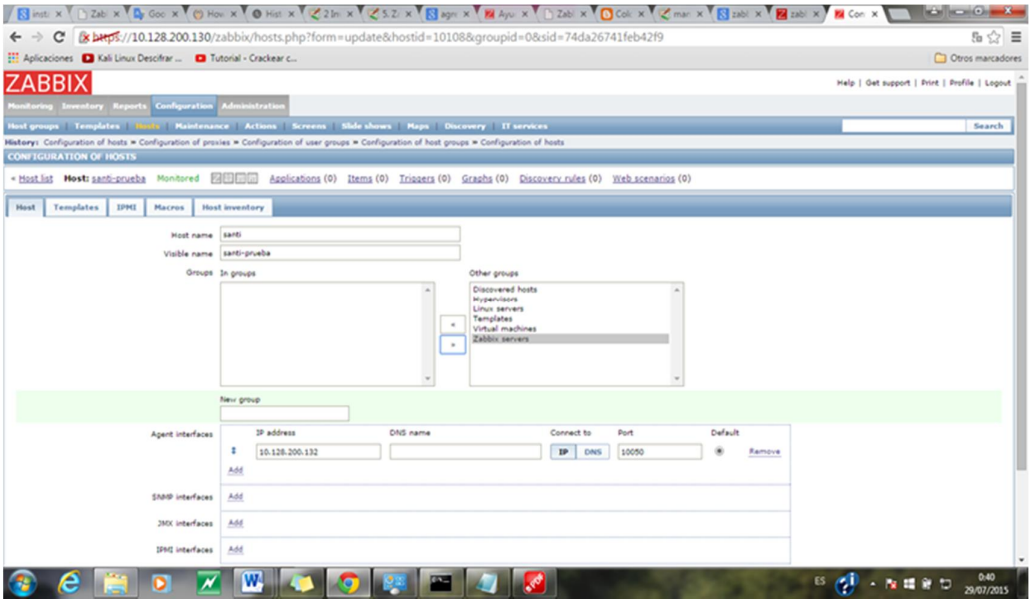


Figura 2. 32 Paso uno para agregar un host.
Fuente: (Coldbeer, 2014) [2]

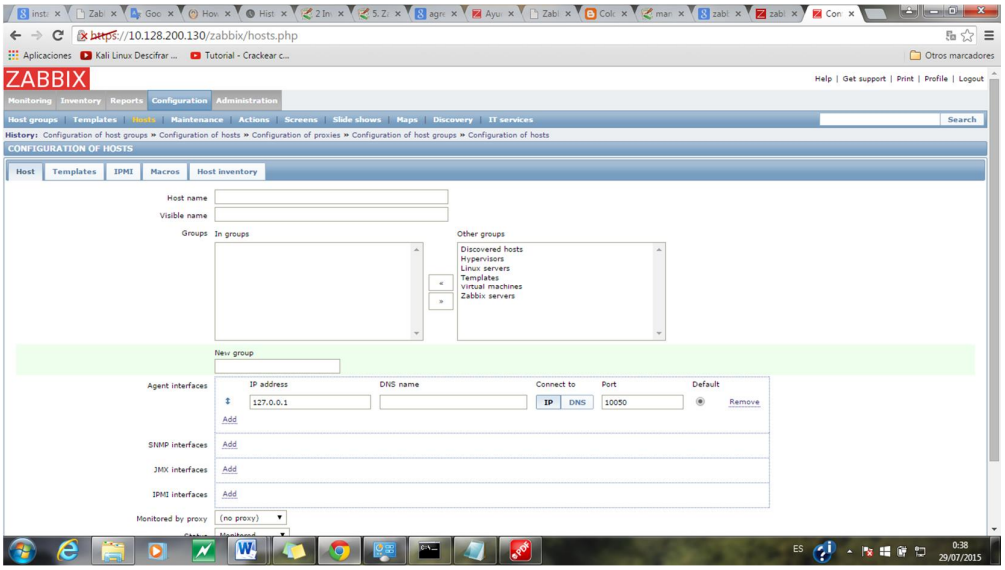


Figura 2. 33 Paso dos para agregar un host
Fuente: (Coldbeer, 2014) [2]

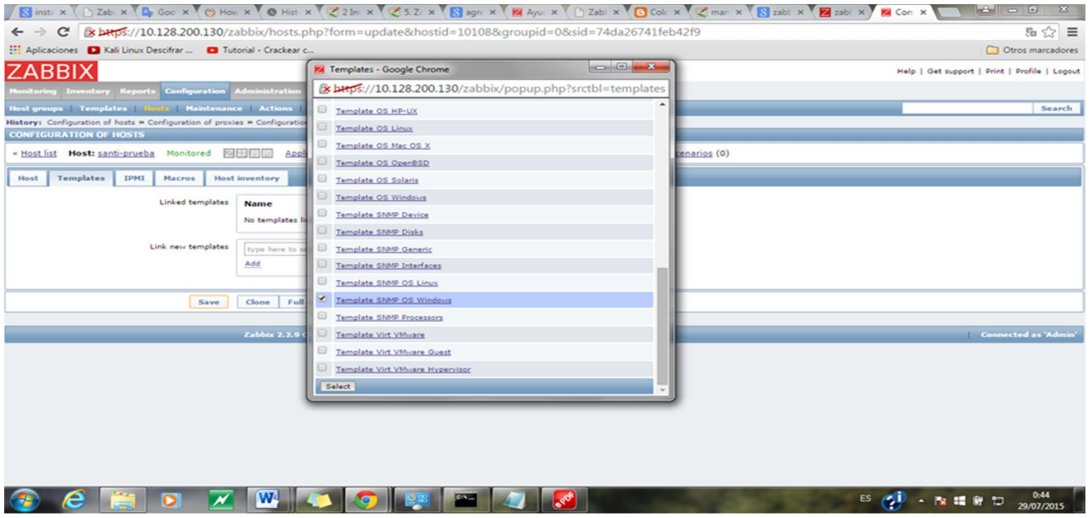


Figura 2. 34 Paso dos para agregar un host
Fuente: (Coldbeer, 2014) [2]

Una vez que se escoge o se agrega el Templates se grava y se activa como se observa en la figura 2.35

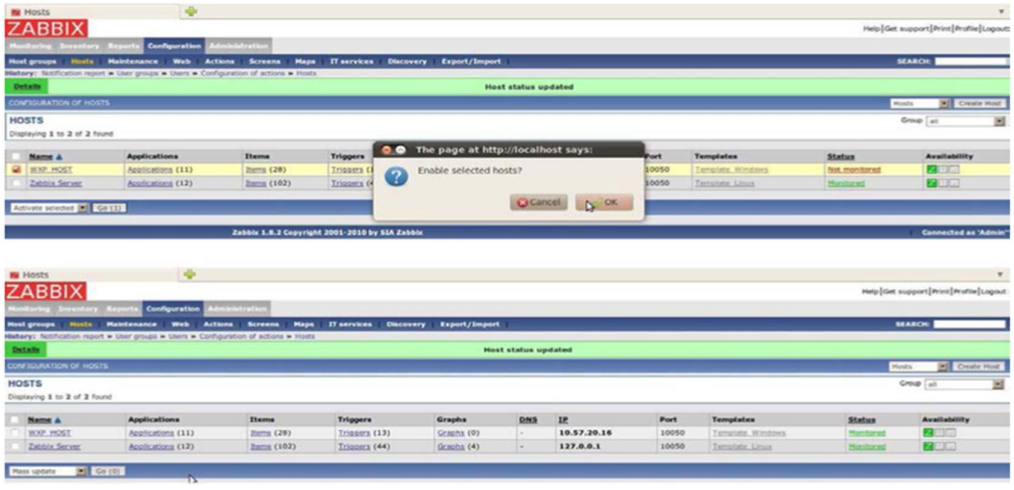


Figura 2. 35 Paso tres para agregar un host.
Fuente: (Coldbeer, 2014) [2]

2.9 Agregando un servidor de windows 2003 server.

Este servidor es un HP, Proliant ML370 G7, cuenta con la isntalacion de un active directory, provee el servicio DHCP donde se encuentra instalada una impresora HP P2055 dn. El procedimiento es similar a la agregacion del equipo anterior (Figura 2.36, figura 2.37).

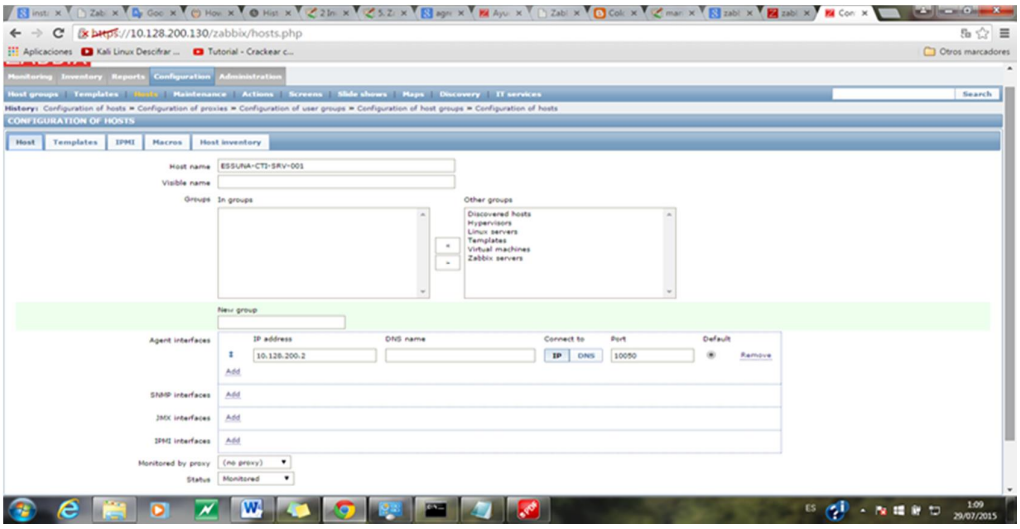


Figura 2. 36 Paso uno para agregar de un servidor Windows
Fuente: (Coldbeer, 2014) [2]

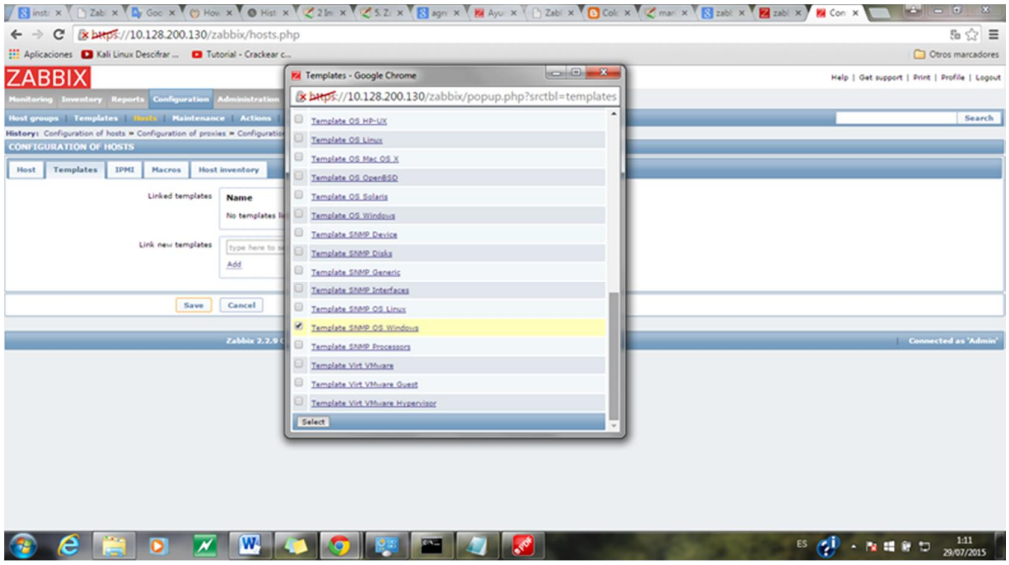


Figura 2. 37 Paso dos para agregar de un servidor Windows
Fuente: (Coldbeer, 2014) [2]

2.10 Agregando impresora en red mediante protocolo SNMP

Primero instalo el servicio para para las lecturas de los paquetes SNMP como se detalla en el figura 2.38.

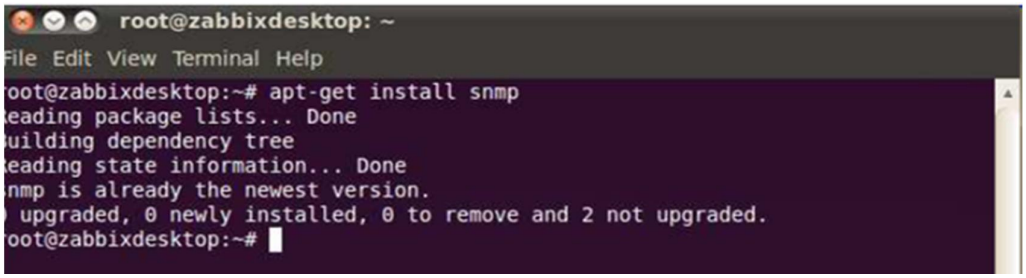


Figura 2. 38 Instalación SNMP
Fuente: (Coldbeer, 2014) [2]

Como es una impresora con protocolo TCP/IP, se puede agregarla a Zabbix , activando del protocolo SNMP, que cuenta dicha impresora en este caso es la impresora del CTI-ESSUNA. Por medio de una terminal en Ubuntu, se digita los siguientes comandos para verificar el buen funcionamiento del protocolo:

snmpstatus -v 2c -c public 10.128.x.x.

Se realiza los mismos procedimientos anteriores con el cambio en los Templates que en este caso se escoge Template SNMP Device como se describe en la figura 2.39

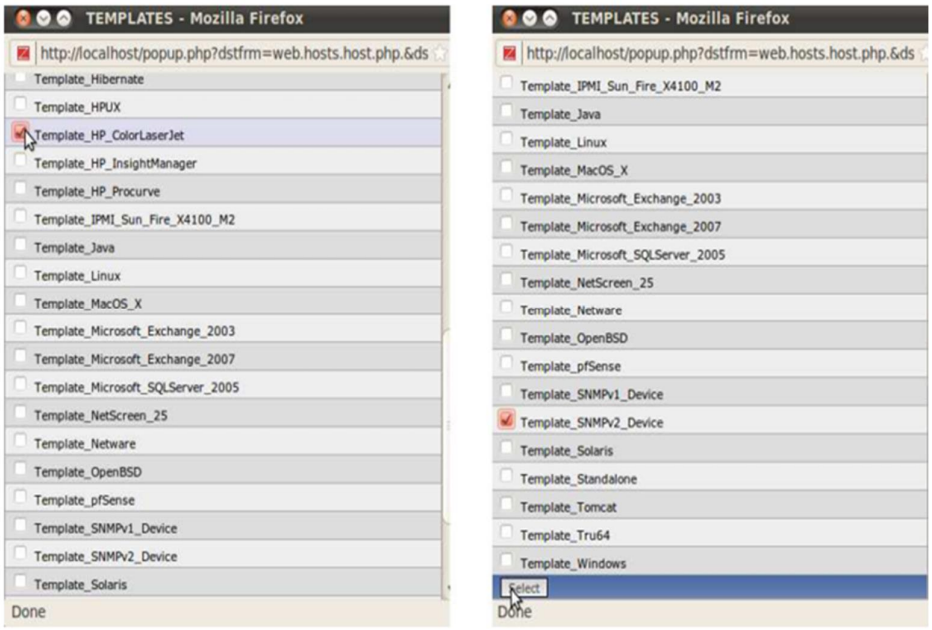


Figura 2. 39 Instalación del Template SNMP
Fuente: (Coldbeer, 2014)[2]

2.11 Agregación de un Switch Cisco Catalyst 2960.

Desde una terminal de Ubuntu se ejecuta el siguiente comando desde el prontuario ESSUNA-CTI-SRV-001@zabbix:~$:

snmpstatus -v 2c -c switc8c1894 10.128.X.X:161

snmpwalk -v 2c -c switc8c1894 10.128.X.X:161 | head -n 10

snmpget -v 2c -c switc8c1894 10.128.X.X:161 SNMPv2-MIB::sysName.0

Se inicia la agregación siguiendo los pasos anteriores como se observa en la figura 2.40

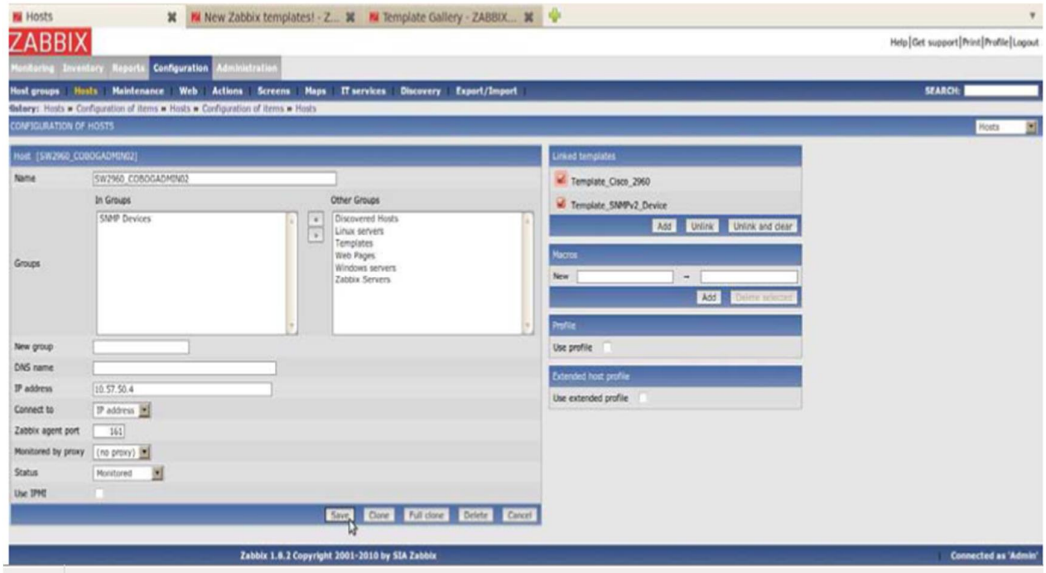


Figura 2. 40 Instalación Protocolo SNMP
Fuente: (Coldbeer, 2014) [2]

CAPÍTULO 3

ANÁLISIS DE RESULTADOS

3.1 Verificación de los servicios

Los resultados se basan por medio de alarmas que se producen al suceso de algún evento, posterior envía notificaciones al correo electrónico.

El uso bien estructurado de los Templates de Zabbix es el arma más poderosa, hace robusta la aplicación, permite realizar análisis de los diferentes dispositivos como en este caso el de un switch 3560 donde vamos a observar los gráficos de tráfico por puerto, monitoreo de cada

puerto, alerta de temperatura, alertas por puerto, gráficos consolidados como se puede observar en el figura 3.1, figura 3.2.

Figura 3.1 Monitoreo por puerto Switch CISCO 3560

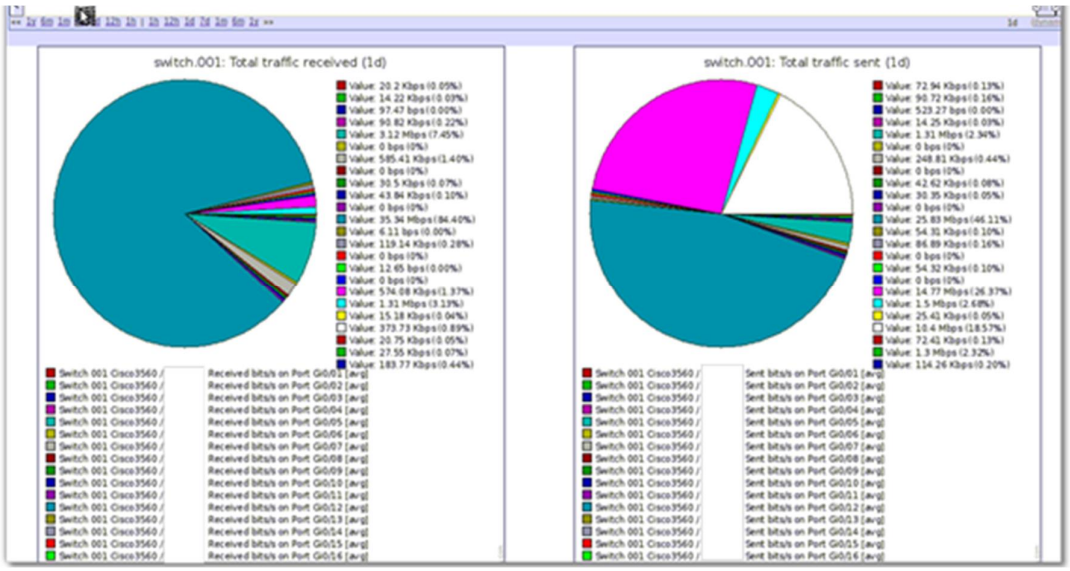


Figura 3.2 Estadística de uso de puerto Switch CISCO 3560

Presentamos en las figuras 3.3 y figura 3.4 las pantallas para el análisis del uso adecuado de los recursos en este caso el de un switch CISCO 2960.

Donde vamos a observar nos da gráficos de tráfico por puerto, monitorización de cada puerto, alerta de temperatura, alertas por puerto, gráficos consolidados, los templates para los Switches CISCO, nos proporcionan información de tráfico de cada puerto, su disponibilidad, colisiones, incluso hasta la temperatura del dispositivo.

Figura 3.3 Monitoreo de puerto SW CISCO 2960

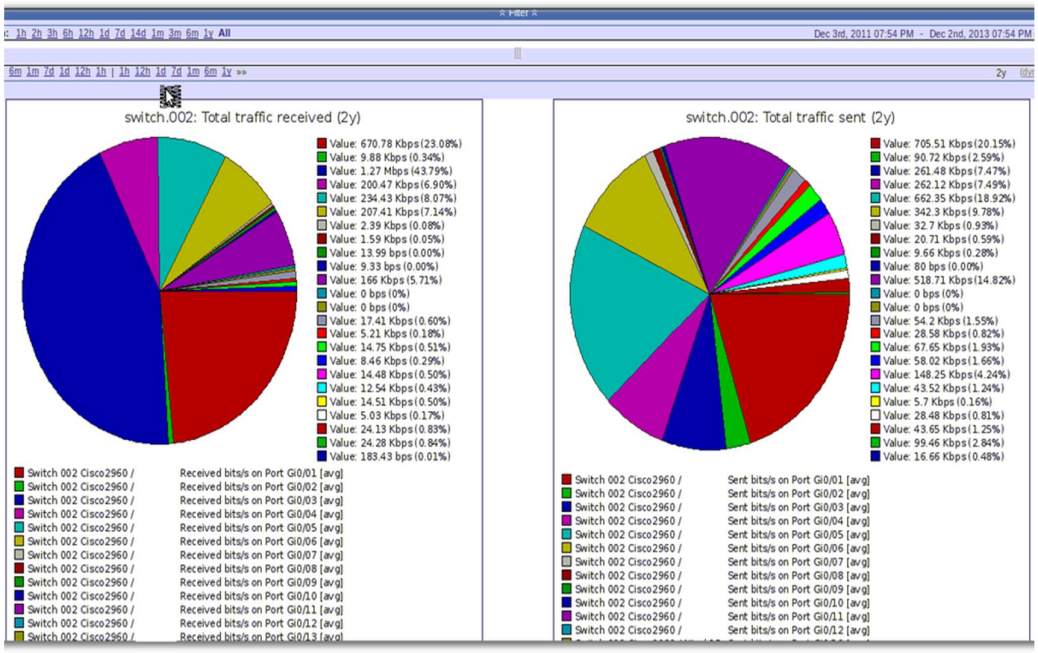


Figura 3.4 Estadística de puerto SW 2960

Se puede visualizar para un mayor análisis de resultados muchos gráficos como se requiere en una pantalla, se actualizan automáticamente como se puede observar en al grafico 3.5.

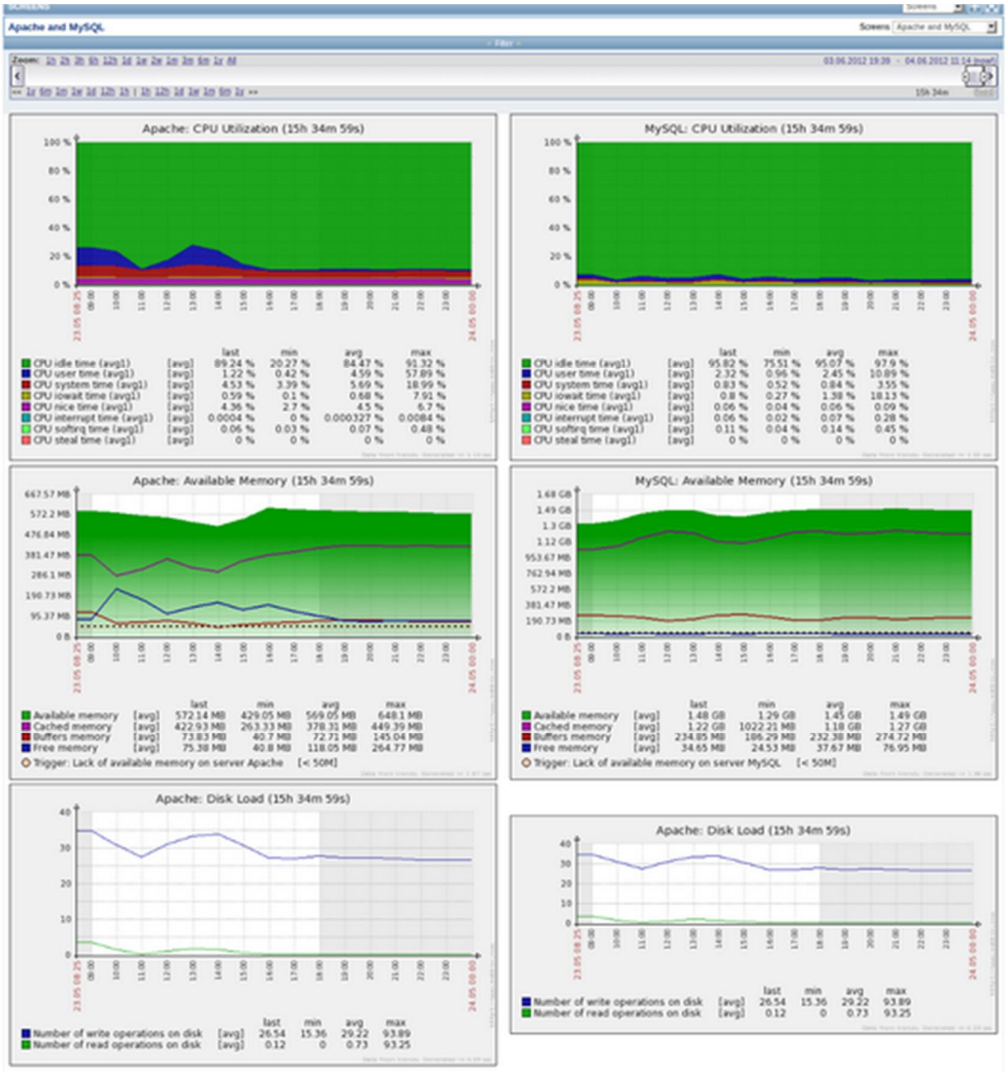


Figura 3.5 Uso de vario gráficos actualizados en línea

CONCLUSIONES Y RECOMENDACIONES

Conclusiones.

1. La necesidad de reducir los tiempo elevados a eventos producidos por mal funcionamiento de la infraestructura o de los servicios distribuidos por estos equipos, ha producido un impacto a las actividades cotidianas de le Escuela Superior Naval, motivo por el cual se ha visto la necesidad de implementar alguna solución informática para poder tener aviso inmediato de dichas eventualidades.
2. Estos eventos inesperados producían daños mayores en los equipos cuando no se tenía aviso de alguna falla eléctrica donde los daños económicos eran muy altos.
3. Actualmente por falta de ayuda técnica, no se ha podido implementar todos los mecanismos de monitoreo que brinda Zabbix

4. Tomando en consideración que el costo económico no es alto ya que se debe de considerar el tiempo invertido en la investigación el personal militar del centro de datos de la Escuela Superior Naval cuanta con otras funciones lo que ha mermado el interés por seguir aumentando más bondades de la herramienta.

Recomendaciones.

1. Se recomiendo profundizar en el aprendizaje de las funciones de Zabbix para poder implementar más funcionalidades
2. Se recomienda que los técnicos del área informática dedicados a la investigación o la implementación de nuevos proyectos no realicen funciones colaterales para poder realizar un buen monitoreo de los equipos
3. Por medio de la instalación de esta aplicación y la configuración de algunas bondades se a logrado observar los diferentes eventos producidos hasta la fecha en la Escuela Superior Naval
4. Se recomienda buscar asesoría particular para mejorar en el uso de la aplicación Zabbix.

BIBLIOGRAFÍA

[1] Canonical Ltd. (2015). *Ubuntu Community*. Recuperado el 15 de Julio de 2015, de http://www.ubuntu.com/download

[2] Coldbeer. (01 de Junio de 2014). *Instalar Zabbix 2.2.x en Ubuntu 14.04*. Recuperado el 19 de Julio de 2015, de coldbeer.blogspot.com/2014/06/instalar-zabbix-22x-en-ubuntu-1404.html

[3] Wikipedia ORG. (s.f.). *Simple Network Management Protocol*. Recuperado el 18 de Julio de 2015, de https://es.wikipedia.org/wiki/Simple_Network_Management_Protocol

[4] Winlinuxnet. (s.f.). *Monitoring router or other devices*. Recuperado el 20 de Julio de 2015, de http://winlinuxnet.blogspot.com/2011/06/monitoring-router-or-other-devices.html

[5] Zabbix ORG. (s.f.). *Instalación de los Templates*. Obtenido de www.zabbix.org/wiki/Zabbix_Templates/Official_Templastes

[6] Zabbix SIA. (27 de 01 de 2015). *Información detallada de las características de Zabbix*. Recuperado el 17 de 07 de 2015, de https://www.zabbix.com/documentation/2.2/start