UNIVERSIDAD DE ANTIOQUIA

Implementación de una solución de administración y supervisión de servidores como herramienta de contingencia para la Empresa EMTELCO S.A.S

Autor

Fabio de Jesús Gaviria Betancur

Universidad de Antioquia

Facultad de Ingeniería, Departamento de Ingeniería Electrónica y Telecomunicaciones

Medellín, Colombia

2019

Tabla de contenido

Índice de tablas

Tabla de ilustraciones

1 Resumen

En los tiempos de hoy es importante conocer el estado de los servidores que se manejan dentro de una organización para garantizar el correcto funcionamiento de los mismos y así no perder tiempo, ni dinero, ya que generalmente estos estos servidores son trascendentales porque manejan información crítica. Es necesario por lo tanto que se mantengan prestando el servicio el mayor tiempo posible, y debido a esto, en el escenario donde se presente un evento de falla o anomalía se tendría que reportar oportunamente a los administradores de la plataforma para que se tomen las medidas necesarias para evitar una denegación del servicio o pérdida de información, previniendo un problema mayor a la empresa.

Es importante que estos reportes sean confiables, ya que si son falsas alarmas el sistema perdería credibilidad, lo cual se traduce en gastos innecesarios y demoras en los tiempos de respuesta, devaluando el trabajo realizado por el operador de la plataforma.

Este proyecto realiza una comparación entre diferentes herramientas de monitoreo, de las cuales finalmente se escogió la más viable para la empresa según los requerimientos que se tienen con el fin de iniciar la implementación del piloto. Seguidamente se procede a investigar sobre la herramienta seleccionada para saber cuál es la forma en que se debe instalar y configurar.

Definida la herramienta a implementar, se procedió a realizar la implementación de la misma, llevando en un registro todo el proceso y de esta manera en un futuro pueda ser de utilidad para otros profesionales que decidan implementar o realizar modificaciones de configuración a esta herramienta.

Con la herramienta instalada se procedió a realizar la configuración de la misma, anexando los dispositivos que se iban a monitorear durante la prueba del piloto. Luego se generaron los informes de monitoreo para saber cuál es el estado de los agentes en el sistema.

Finalmente se evaluó el funcionamiento de la herramienta y el estado de los dispositivos, así como también, se realizó la instalación en producción de la herramienta y a la entrega del manual en el cual quedan estipulados todos los pasos para instalar y configurar la herramienta de monitoreo seleccionada.

2 Introducción

EMTELCO es una empresa prestadora de servicios de telecomunicaciones, enfatizada en servicios de contact center y soluciones Business Process Outsourcing (BPO) [1]. Para el desarrollo de sus actividades diarias, dispone de plataformas de Tecnologías de la Información (TI), que incluyen más de 400 servidores, diferentes tipos de redes, canales de telefonía entre otros. Estas plataformas son administradas mediante diferentes herramientas de gestión que les permite a los encargados detectar y solucionar posibles inconvenientes en poco tiempo.

Entre las herramientas de gestión actualmente utilizadas por EMTELCO están: Spacewalk para la administración de los servidores bajo sistemas operativos (OS) Linux, PRTG para el monitoreo de redes y el OP Manager para el monitoreo de servidores y aplicaciones. Estas herramientas son operadas por personal capacitado que se encarga de emitir las alertas de posibles fallos al personal de operación de plataforma, para brindar soluciones que se ajusten a las políticas de la empresa.

El grupo de trabajo de Operación de Plataforma tiene a cargo la administración de los servidores y sus servicios. Desde principios del año en curso (2019), el personal de monitoreo ha detectado la necesidad de implementar una herramienta alterna a la herramienta actual OP Manager, que sirva como plan de contingencia para mejorar las actividades de administración, monitoreo y configuración; en búsqueda de anticipar los inconvenientes para garantizar un buen rendimiento en sus servicios. Esto debido a que se han evidenciado algunas fallas en el software utilizado, como alarmas enviadas por debajo del umbral señalado por la empresa, fallos en la conectividad con algunos servidores; fallas que se han evidenciado al realizar algunas actividades de despliegue de aplicaciones, o de control de cambios que requieren el reinicio del servidor y el OP Manager no registra los tiempos de apagado.

3 Objetivos

3.1 Objetivo general.

Implementar una solución tecnológica de contingencia que permita suplir las necesidades de monitoreo de servicios, control centralizado de equipos, administración de actualizaciones y reportes en tiempo real del estado de los servidores en una sola herramienta de gestión.

3.2 Objetivos específicos.

1. Analizar las diferentes herramientas que cumplen los requerimientos establecidos en el objetivo general y compararlas con la herramienta utilizada actualmente, para seleccionar la que se considere mejor opción.
2. Estudiar la herramienta seleccionada determinando el mejor método de instalación y la implementación de las funcionalidades, documentando cada paso realizado.
3. Implementar la herramienta seleccionada en un servidor fuera de producción, configurarla y probarla en un entorno controlado generando un informe de cada una de las funcionalidades evaluadas.

4 Marco teórico

4.1 Sistemas de gestión y monitoreo.

Dentro del ámbito de la administración de redes, se conoce con el nombre de monitoreo de red a un sistema que realiza un control constante de una red de computadores, intentando detectar defectos y anomalías; en caso de encontrar algún desperfecto, envía un informe a los administradores.

Si bien EMTELCO cuenta con buenas herramientas de gestión y monitoreo para atender la red de equipos y servicios asociados, como lo son PRTG para el monitoreo de redes y OP Manager para el monitoreo de servidores, siempre hay oportunidad de buscar mejoras en la estructuración de la operación. En este caso se detectó la necesidad de disponer de una herramienta integrada que facilite las actividades de monitoreo y gestión en una sola consola, no solo para la atención de eventos en la red o en los servidores, sino también para la gestión de las configuraciones mismas de los equipos, lo que daría una mejor administración por parte del equipo de operación de plataforma de servidores. Además, permite una rápida corrección de problemas, dar espacio para detectar condiciones que evidencien la posible aparición de eventos y tomar medidas antes que se puedan convertir en una falla real.

4.2 Mecanismos de monitoreo

Los mecanismos de monitoreo son herramientas automatizadas que verifican constantemente el estado de los componentes de la infraestructura de Tecnologías de la Información [TI], permitiendo registrar y visualizar en mínimas fracciones de tiempo los cambios o anomalías detectadas.

4.2.1 Visor de eventos y Registro de Sucesos

Cuando se habla de un Event viewer o visor de eventos, se hace referencia a una herramienta que permite visualizar y administrar los registros de sucesos o Event Log, que indican los problemas de hardware, software y eventos de seguridad de los equipos que posean sistema operativo Windows 7 o superior [3]. Estos registros pueden ser de tres tipos:

- **Aplicaciones:** Guardan los sucesos relacionados a los programas y aplicaciones.
- **Seguridad:** Almacenan los intentos e inicio de sesión autorizados, no autorizados, uso de los archivos y otros elementos.
- **Sistema:** Guardan los eventos relacionados con los componentes del sistema, los tipos de mensajes.

Los tipos de mensajes que muestra el visor de sucesos: son de error (error), advertencia (warning), información (information), accesos de acertados (Success Audit) y accesos fallidos (Failure Audit) (Microsoft, 2010). La figura 1 es una imagen tomada de la interfaz del Visor de Eventos de una computadora.

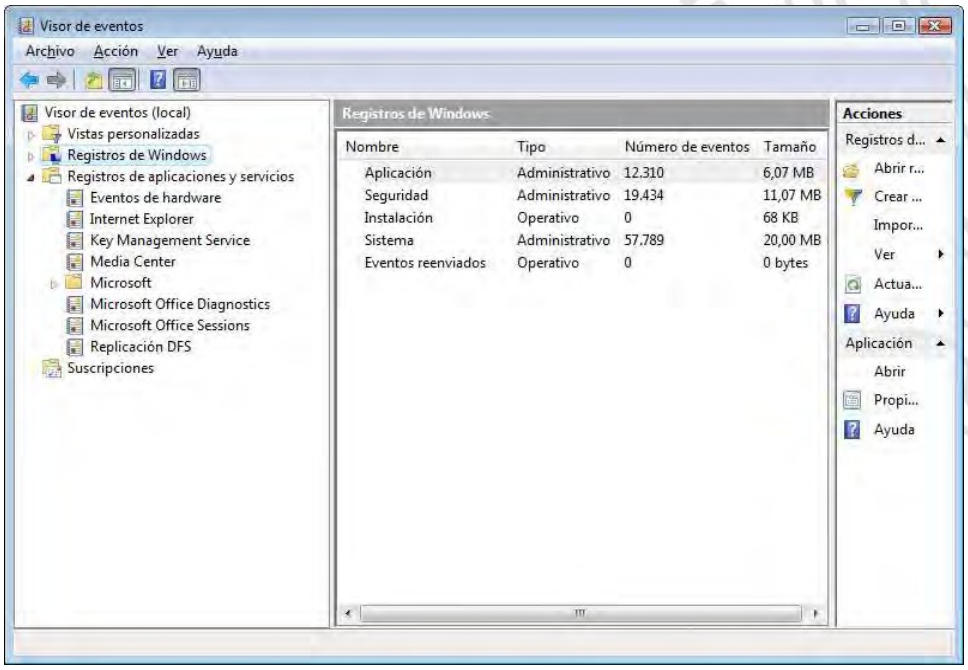


Figura 1. Visor de eventos.

4.2.2 Componentes de monitoreo remoto

Cuando hablamos de componentes de monitoreo remoto, hacemos referencia a las herramientas estandarizadas que ayudan a los administradores de la red o del sistema como tal, a determinar en donde se encuentra un problema, utilizando el acceso remoto para tal fin; esta identificación puede hacerse mediante comunicación remota directa, que ocurre cuando se utilizan los componentes locales de monitoreo del equipo, es decir, cuando se hace uso de protocolos estándar como ICMP o SNMP; la otra forma de realizarse es por medio de comunicación remota indirecta, que es cuando se requiere la instalación local de software adicional o agentes que se encargan de establecer la comunicación del equipo con el repositorio de monitoreo.

La elección del uso de comunicación remota directa o indirecta, depende en gran parte del administrador de la plataforma, considerar las ventajas y desventajas que tienen ambos métodos. Por ejemplo, el utilizar el protocolo SNMP tiene la desventaja que al ser un protocolo estándar lleva más información de la que realmente se requiere monitorear y eso implica que se debe ser más cuidadosos al momento de configurar la herramienta del monitoreo. Pero es mucho más sencillo de configurar en los equipos que requerimos monitorear, ya que solo es habilitar el protocolo y configurar la dirección IP del servidor donde tenemos la herramienta utilizada para monitorear; mientras que utilizar agentes implica tener que instalar el agente en cada equipo que se requiere monitorear, o desinstalarla en caso de querer cambiar la herramienta de gestión.

En el caso de la empresa Emtelco S.A.S se considera que el software a implementar va a tener una función de contingencia que sirva de apoyo a OP Manager que es la herramienta de gestión utilizada como principal, la cual recibe la información por medio del protocolo SNMP. Esto porque debido a la gran cantidad de servidores que se monitorean, se vuelve muy tedioso el ingresar a cada servidor e instalar el agente, además de las autorizaciones que se deben dar en el firewall y las herramientas utilizadas para la seguridad informática de la empresa; esto se vuelve de alta importancia al momento del desarrollo de este proyecto.

4.2.3 Parámetros críticos y comunes en los dispositivos TI

Los diferentes dispositivos de TI, se componen de varias partes de las cuales algunas son fundamentales para su funcionamiento, es decir, sin estas partes no van a poder funcionar; y se tienen otras partes que afectan en un porcentaje su funcionamiento pero sin dejarlo fuera de operación; por ejemplo, en una computadora si se daña el procesador, la memoria RAM o la fuente de poder, esa computadora no va a funcionar, por lo que decimos que estas partes son críticas para el dispositivo, pero si tenemos saturación en

la red, seguramente se va a poner lenta y va a ser incomodo, pero la herramienta puede seguir realizando su trabajo. Es por esto que independientemente de cuál sea el modelo o marca de los dispositivos de TI, se pueden encontrar parámetros críticos comunes. Para el desarrollo de este proyecto se resumen en la siguiente tabla 1 Monitoreo básico del estado de los dispositivos, los parámetros críticos considerados.

Tabla 1 Monitoreo básico del estado de los dispositivos.

Parámetros	Descripción
Sistema	1.Uso de procesador(es). 2.Uso del disco duro (aplica solo para servidores de aplicaciones). 3.Utilización de la memoria RAM.
Entorno.	1.Estado del ventilador (Fan). 2.Estado del sensor de temperatura. 3.Estado del sistema de suministro de energía
Red.	1.Interconectividad entre los dispositivos (disponibilidad de las interfaces). 2.Utilización de las interfaces de red. 3.Tiempo de respuesta.

5 Metodología

5.1 Búsqueda de la herramienta de monitoreo.

En el mercado actual se encuentran decenas de herramientas de gestión y monitoreo de servidores, algunas muy amigables, otras llamativas y otras muy completas; es por eso que para poder iniciar la búsqueda de la más adecuada para Emtelco S.A.S, partimos de las necesidades que presenta la empresa en el momento, dando suma importancia al objetivo general planteado en el presente proyecto.

Al considerar que la herramienta a implementar va a funcionar como contingencia, se considera como uno de sus ejes en inversión tecnológica el uso de herramientas open surce, ya que no se justifica realizar un doble gasto en dos herramientas que cumplan las mismas condiciones.

Dentro de la búsqueda inicial que se realizó en distintos foros de monitoreo se encontraron que las opciones de software open surce más mencionadas, y con una mayor frecuencia de aparición en las búsquedas, son las siguientes:

- Zabbix.
- Zenoss.
- Cacti.
- Nagios.

5.1.1 Necesidades:

- La herramienta debe presentar vistas de los sensores al usuario final en tiempo real.
- Debe tener la capacidad de detectar fallas antes de generar un impacto que afecte la infraestructura TI, ser proactiva.
- Generar alertas inmediatas sobre fallas e información detallada para identificar rápidamente las causas raíz y así mejorar los tiempos de respuesta y resolución.
- Visibilidad de redes e infraestructuras no controladas (No Agentes).
- Flexibilidad para implementar rápidamente nuevos elementos de monitoreo a medida que cambien las prioridades del negocio.
- Fácil implementación, sin una curva de aprendizaje empinada.
- Generar reportes amigables de tendencias de desempeño, estadísticas de fallas y cumplimiento de las ANS (Acuerdos de Nivel de Servicio).

Dado que ya se tienen claras cuáles son las falencias que tiene la empresa en cuanto a materia de monitoreo de infraestructura, se procede ahora a realizar una breve descripción de cada una de las herramientas mencionadas y se finalizara esta fase escogiendo la que mejores beneficios le brinde a la empresa teniendo en cuenta las necesidades.

5.1.2 ZABBIX

Herramienta de monitorización capaz de recopilar datos de servidores y aplicaciones, por medio de agentes instalados en las máquinas cliente [4].
Esta herramienta tiene un sistema proactivo de acciones donde puede solucionar automáticamente errores de servidores con pequeñas tareas de ejecución.

5.1.2.1 Ventajas:

- Su comunidad es bastante activa.
- Es potente a bajo nivel.
- Buena interfaz gráfica.
- Gráficos en tiempo real, recoge valores cada 30 segundos.
- Los datos se almacenan en una base de datos Mysql.

- Altamente configurable.
- Flexibles permisos de usuarios.
- 100% Libre

5.1.2.2 Desventajas:

- A partir de 1000 nodos puede disminuir su rendimiento.
- Difícil crear y definir plantillas de informes y alertas. Las configuraciones pueden requerir muchos clics y pasos para completarlas.
- Es difícil de depurar cuando hay errores.

5.1.3 ZENOSS

Herramienta que dispone de una interfaz muy intuitiva posibilidad de percibir de un vistazo toda la información de un servidor [5].
La configuración que tiene dicha herramienta es especialmente difícil de manipular, y dispone de multitud de Pluggins para poder monitorizar equipos en una red automáticamente utilizando SSH y SNMP. Este software no necesita usar agentes remotos, porque usando SSH puede solicitar cualquier comando a cualquier servidor para poder extraer toda la información necesaria.

5.1.3.1 Ventajas:

- Es capaz de monitorizar múltiples plataformas.
- Gran capacidad a la hora de gestionar eventos.
- Muy potente y flexible.
- Interfaz gráfica agradable, de buen diseño.

5.1.3.2 Desventajas:

- Puede ser difícil su adaptación.
- La capa de base de datos se puede hacer pesada en grandes entornos.
- El panel puede llegar a ser lento.
- Se requiere de grandes conocimientos para su optimización.
- Mapas de topologías no tan potentes y claros como los de otras aplicaciones.

5.1.4 CACTI.

Herramienta web que nos presenta en una interfaz gráfica todos los chequeos que queramos realizar en servidores y redes [6].
Principalmente, la aplicación está enfocado a la representación de los datos en gráficos para hacer que el usuario tenga mayor conocimiento de la gravedad de las diferentes alertas que aparezcan en la aplicación.

5.1.4.1 Ventajas:

- Fácil migración desde Nagios.
- Se puede configurar el envío automático de informes cada cierto tiempo.
- Fácil instalación.
- Buena interfaz gráfica.

5.1.4.2 Desventajas:

- Configuración y edición compleja, debido a que se deben hacer modificaciones de forma manual al configurar la herramienta.
- Falta usabilidad en la interfaz gráfica.
- Coste de aprendizaje elevado.
- Informes sencillos.
- Muy pobre su tratamiento de SNMP.

5.1.5 NAGIOS

Herramienta de sistema de monitoreo que permite a las organizaciones identificar y resolver problemas de infraestructura de Tecnología Informática (TI) antes de que afecten los procesos de negocios críticos.
Al día de hoy, son muchos los organismos que utilizan Nagios, usando la versión Core, que corresponde a la versión de Software Libre, es 100% personalizable, lo que tiene como ventaja que puedes generar tus propios scripts, monitorizando así lo que más interese a la organización donde esté instalado [7].

5.1.5.1 Ventajas:

- Se encuentran muchos perfiles con experiencia Nagios.
- La configuración manual puede darle mucha potencia a la hora de monitorizar casos aislados y particulares.

- Ofrece muchos pluggins para adaptar Nagios a las necesidades del usuario.
- Para la configuración básica es muy fácil.
- Permite definir políticas de notificación.

5.1.5.2 Desventajas:

- Configuración y edición compleja debido a la necesidad de hacer modificaciones de forma manual para dejar lista la herramienta.
- El interfaz gráfico carece de una buena usabilidad
- Coste de aprendizaje elevado
- Cada instalación al final resulta compleja en el que más que un producto estándar tenemos una implementación propia, con cientos de parches, código propio o de terceros y complicada de evolucionar o de mantener por terceros.
- Informes sencillos
- Muy pobre en su tratamiento de SNMP, tanto en las consultas constantes (polling) como en la gestión de alarmas (traps).

5.2 Implementación de la herramienta seleccionada para el monitoreo

La implementación de este sistema nace como una solución alterna para soportar el monitoreo de los dispositivos que hacen parte de la infraestructura de la operación, en caso de que OP Manager genere inconvenientes, esto para tener la contingencia en caso de que el sistema principal no esté cumpliendo con las operaciones para las cuales fue estipulado. Así que se realizó una investigación y se compartió la información con las áreas interesadas para así tomar una decisión sobre cuál era la mejor opción en las aplicaciones que monitorean la infraestructura de una red. Se evaluaron diferentes opciones en sistema de monitoreo y se escogió Zabbix, gracias a su ambiente amigable, fácil instalación y la ventaja de que cada uno de sus componentes son totalmente gratuitos y disponibles en la web.

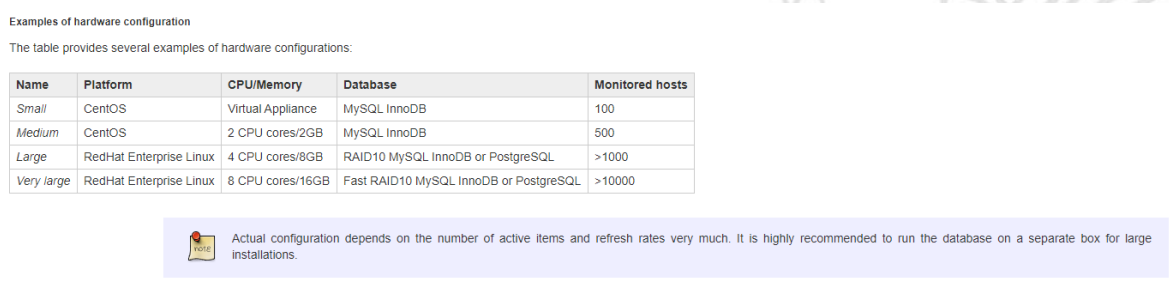
Después de haber realizado una instalación prueba de la herramienta, se procede a desinstalarla y se hace una investigación más a fondo, consultando manuales y guías de instalación directamente en la página oficial de Zabbix, se investigan bien los requerimientos mínimos y recomendados para una buena instalación y mejor aprovechamiento de la herramienta, con el fin de poder brindar una buena documentación a las personas encargadas de la administración a futuro.

5.2.1 Prerrequisitos.

Se ponen a consideración los diferentes requisitos para la implementación de la herramienta de monitoreo, tanto en hardware como en software.

5.2.1.1 Prerrequisitos de Hardware

Como podemos apreciar en la imagen y considerando el requerimiento de Emtelco S.A.S de monitorear 440 Servidores, se destina por parte de la empresa un servidor virtual con 2 CPU cores y 2 GB de memoria RAM, con el sistema Operativo centOS 7 para la implementación del proyecto.



Examples of hardware configuration

The table provides several examples of hardware configurations:

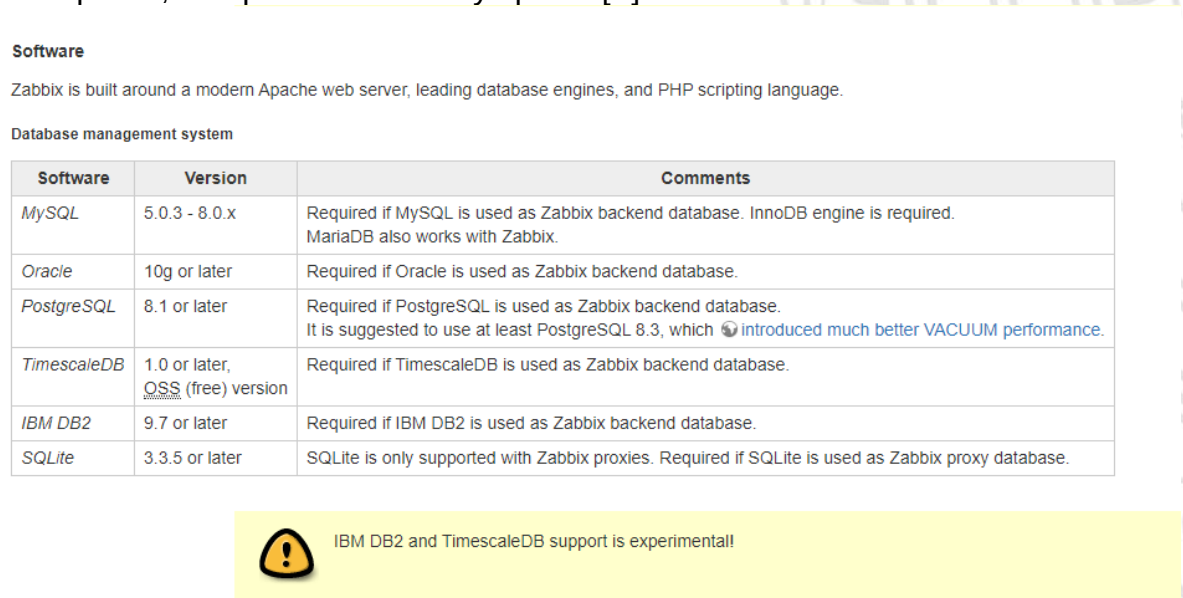
Name	Platform	CPU/Memory	Database	Monitored hosts
Small	CentOS	Virtual Appliance	MySQL InnoDB	100
Medium	CentOS	2 CPU cores/2GB	MySQL InnoDB	500
Large	RedHat Enterprise Linux	4 CPU cores/8GB	RAID10 MySQL InnoDB or PostgreSQL	>1000
Very large	RedHat Enterprise Linux	8 CPU cores/16GB	Fast RAID10 MySQL InnoDB or PostgreSQL	>10000

Actual configuration depends on the number of active items and refresh rates very much. It is highly recommended to run the database on a separate box for large installations.

Figura 2. Prerrequisitos de hardware.

5.2.1.2 Prerrequisitos de Software.

Para la base de datos de acuerdo a la siguiente imagen, por disposición de la empresa, nos piden utilizar Mysql 8.0. [9]



Software

Zabbix is built around a modern Apache web server, leading database engines, and PHP scripting language.

Database management system

Software	Version	Comments
MySQL	5.0.3 - 8.0.x	Required if MySQL is used as Zabbix backend database. InnoDB engine is required. MariaDB also works with Zabbix.
Oracle	10g or later	Required if Oracle is used as Zabbix backend database.
PostgreSQL	8.1 or later	Required if PostgreSQL is used as Zabbix backend database. It is suggested to use at least PostgreSQL 8.3, which introduced much better VACUUM performance.
TimescaleDB	1.0 or later, OSS (free) version	Required if TimescaleDB is used as Zabbix backend database.
IBM DB2	9.7 or later	Required if IBM DB2 is used as Zabbix backend database.
SQLite	3.3.5 or later	SQLite is only supported with Zabbix proxies. Required if SQLite is used as Zabbix proxy database.

IBM DB2 and TimescaleDB support is experimental!

Figura 3. Bases de datos admitidas por zabbix.

Otros requisitos exigidos por Zabbix son el Apache en la versión 1.3.12 o superior y el PHP en la versión 5.4 o superior, dado que el centOS 7 trae instaladas por defecto la versión 2.4.6 y de PHP la versión 5.6.24, se cumple con ambos requisitos por lo que no es necesario realizar actualizaciones.

Frontend

The following software is required to run Zabbix frontend:

Software	Version	Comments
Apache	1.3.12 or later	
PHP	5.4.0 or later	
		PHP extensions:
gd	2.0.28 or later	PHP GD extension must support PNG images (*--with-png-dir*), JPEG (*--with-jpeg-dir*) images and FreeType 2 (*--with-freetype-dir*).
bcmath		php-bcmath (*--enable-bcmath*)
ctype		php-ctype (*--enable-ctype*)
libXML	2.6.15 or later	php-xml or php5-dom, if provided as a separate package by the distributor.
xmlreader		php-xmlreader, if provided as a separate package by the distributor.
xmlwriter		php-xmlwriter, if provided as a separate package by the distributor.
session		php-session, if provided as a separate package by the distributor.
sockets		php-net-socket (*--enable-sockets*). Required for user script support.
mbstring		php-mbstring (*--enable-mbstring*)
gettext		php-gettext (*--with-gettext*). Required for translations to work.
ldap		php-ldap. Required only if LDAP authentication is used in the frontend.
ibm_db2		Required if IBM DB2 is used as Zabbix backend database.
mysqli		Required if MySQL is used as Zabbix backend database.
oci8		Required if Oracle is used as Zabbix backend database.
pgsql		Required if PostgreSQL is used as Zabbix backend database.

Figura 4. Software necesario para la Instalación de zabbix.

Y por último dado que el monitoreo va a ser realizado utilizando el protocolo SNMP, es necesario instalar el requerimiento opcional net-snmp.

Server

Mandatory requirements are needed always. Optional requirements are needed for the support of the specific function.

Requirement	Status	Description
libpcre	Mandatory	PCRE library is required for Perl Compatible Regular Expression (PCRE) support. The naming may differ depending on the GNU/Linux distribution, for example 'libpcre3' or 'libpcre1'. Note that you need exactly PCRE (v8.x); PCRE2 (v10.x) library is not used.
libevent		Required for bulk metric support and IPMI monitoring. Version 1.4 or higher. Note that for Zabbix proxy this requirement is optional; it is needed for IPMI monitoring support.
libpthread		Required for mutex and read-write lock support.
zlib		Required for compression support.
OpenIPMI	Optional	Required for IPMI support.
libssh2		Required for SSH support. Version 1.0 or higher.
fping		Required for ICMP ping items.
libcurl		Required for web monitoring, VMware monitoring, SMTP authentication, `web.page.*`, Zabbix agent items, HTTP agent items and Elasticsearch (if used). Version 7.28.0 or higher is recommended. Libcurl version requirements: - SMTP authentication: version 7.20.0 or higher - Elasticsearch: version 7.28.0 or higher
libiksemel		Required for Jabber support.
libxml2		Required for VMware monitoring and XML XPath preprocessing.
net-snmp		Required for SNMP support

Figura 5. Software adicional para usar SNMP Protocol.

5.2.2 Instalación de la base de datos.

Una vez validados los requisitos y verificado que el servidor entregado para el proyecto cumple con todos a cabalidad, procedemos a instalar la base de datos Mysql 8.0 como fue solicitado por el encargado del área de plataforma de la empresa, a continuación, se indican los pasos utilizados para este fin y en el anexo A podemos visualizar un paso a paso con las evidencias respectivas e la instalación. Se debe tener en cuenta que estas instalaciones deben realizarse como supe usuario o usuario Root.

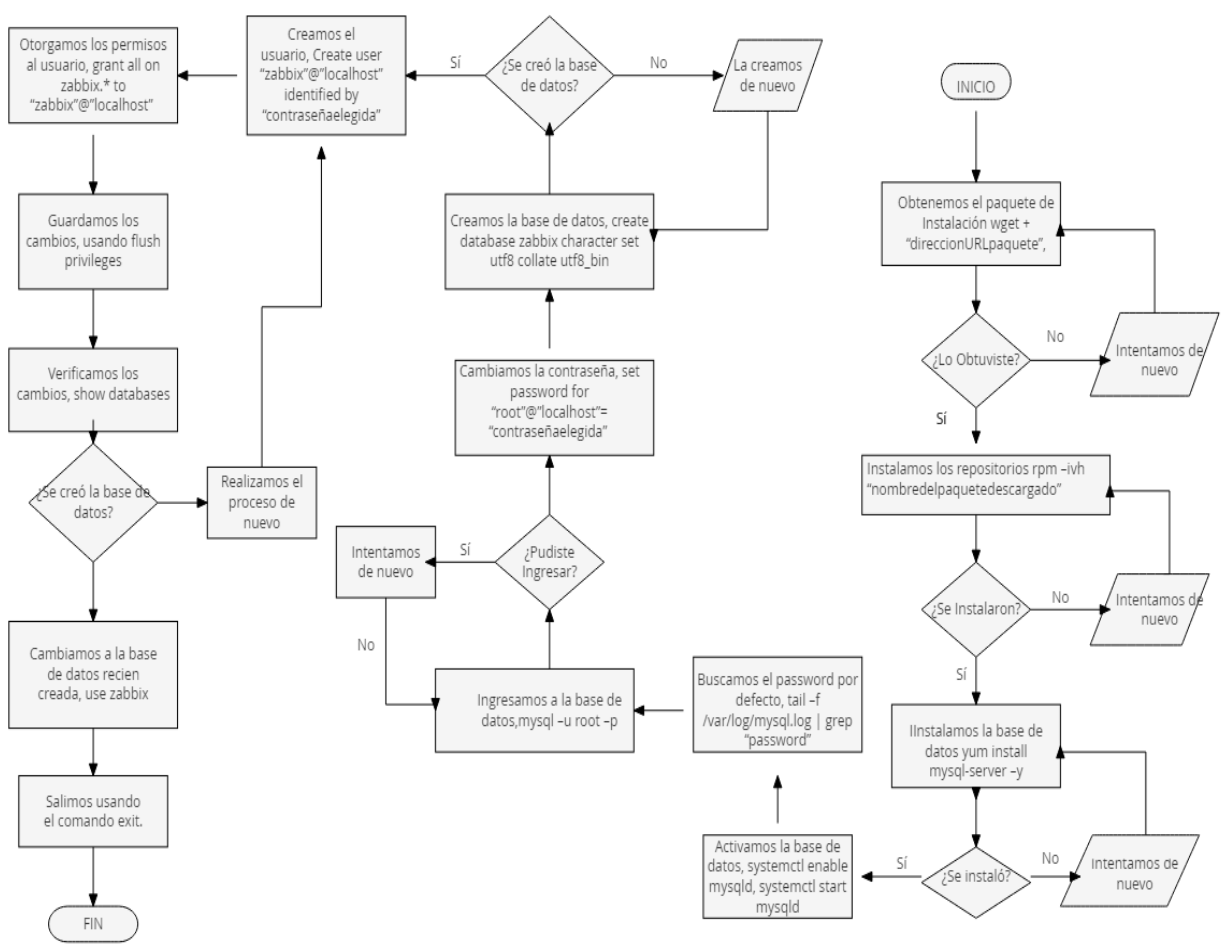


Figura 6. Diagrama de flujo, instalación base de datos

5.2.3 Instalación de la herramienta Zabbix.

Comenzamos por descargar e instalar los paquetes RPM necesarios para ejecutar la instalación, esta parte se realiza directamente desde la página oficial de zabbix, ya que es herramienta totalmente libre, en el anexo B podremos observar los pasos detallados para la implementación del software correspondiente.

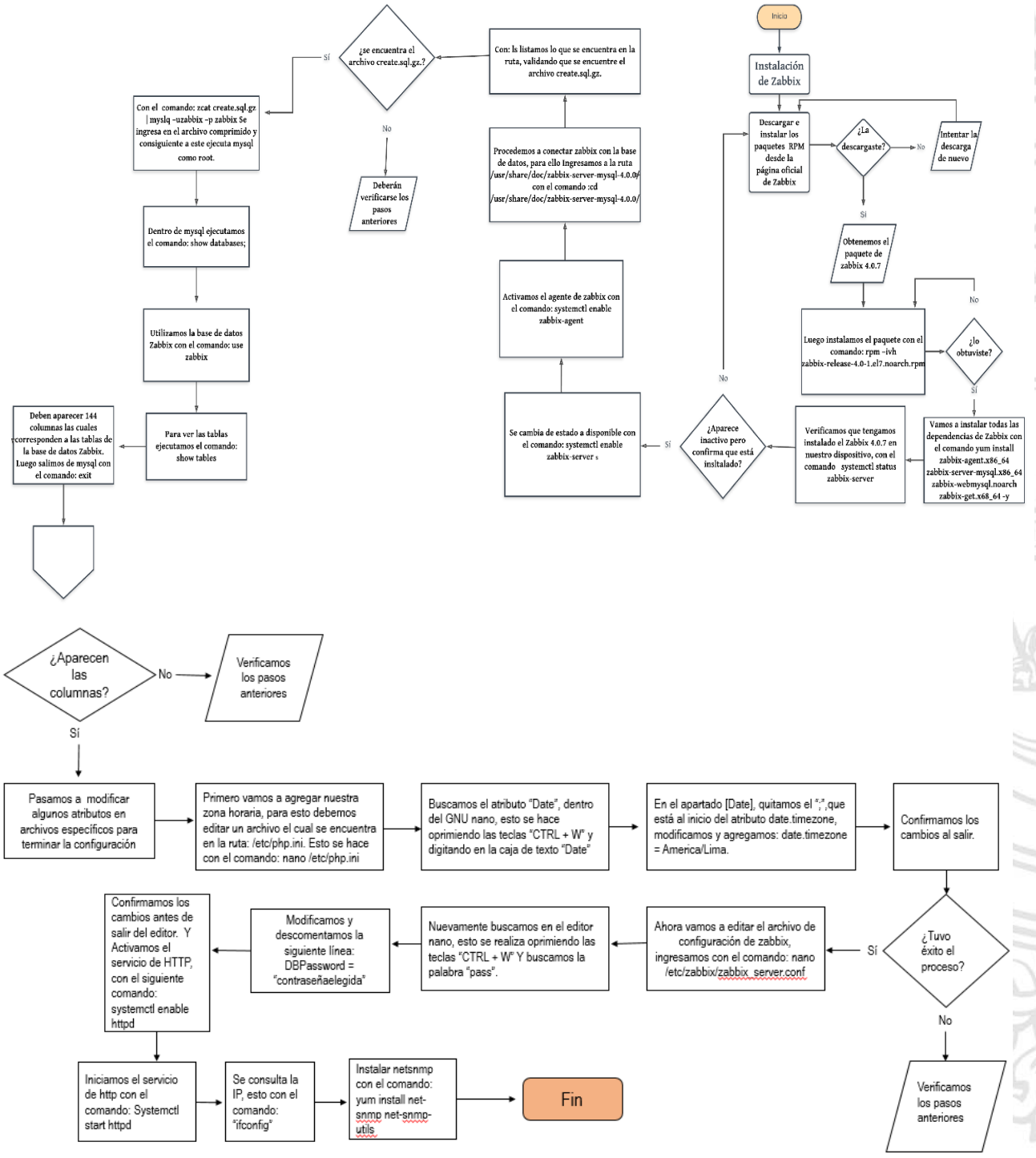


Figura 7. Diagrama de flujo, instalación de Zabbix

5.2.4 Configuración de los servidores a monitorear en Zabbix.

Ahora procedemos a explicar cómo agregar hosts al sistema de monitorización de redes Zabbix, en el sistema operativo Oracle Linux 7, considerando la necesidad de adquirir los conocimientos necesarios para un buen funcionamiento del software, que nos permita recibir alertas de acuerdo a las necesidades propias del área de tecnología y de la Empresa en general. Se detallan los pasos a seguir para agregar hosts al sistema de monitoreo tanto con el sistema operativo windows, como a equipos con el sistema operativo Linux; además se detalla la configuración a realizar para seleccionar los diferentes ítems a monitorear y los umbrales que se utilizaran para generar los diferentes tipos de alertas.

Dado que la empresa consideró realizar el monitoreo utilizando el protocolo SNMP, solo se explica esta parte, en caso de querer o necesitar instalar el agente de Zabbix, se debe consultar el cómo hacerlo en la página directa de Zabbix o en cualquier otro medio.

5.2.4.1 Configuración de SNMP en servidores.

Se procede a configurar el protocolo SNMP en los servidores Windows y Linux respectivamente, en el anexo C podremos observar los pasos detallados con las imágenes respectivas tomadas durante la implementación.

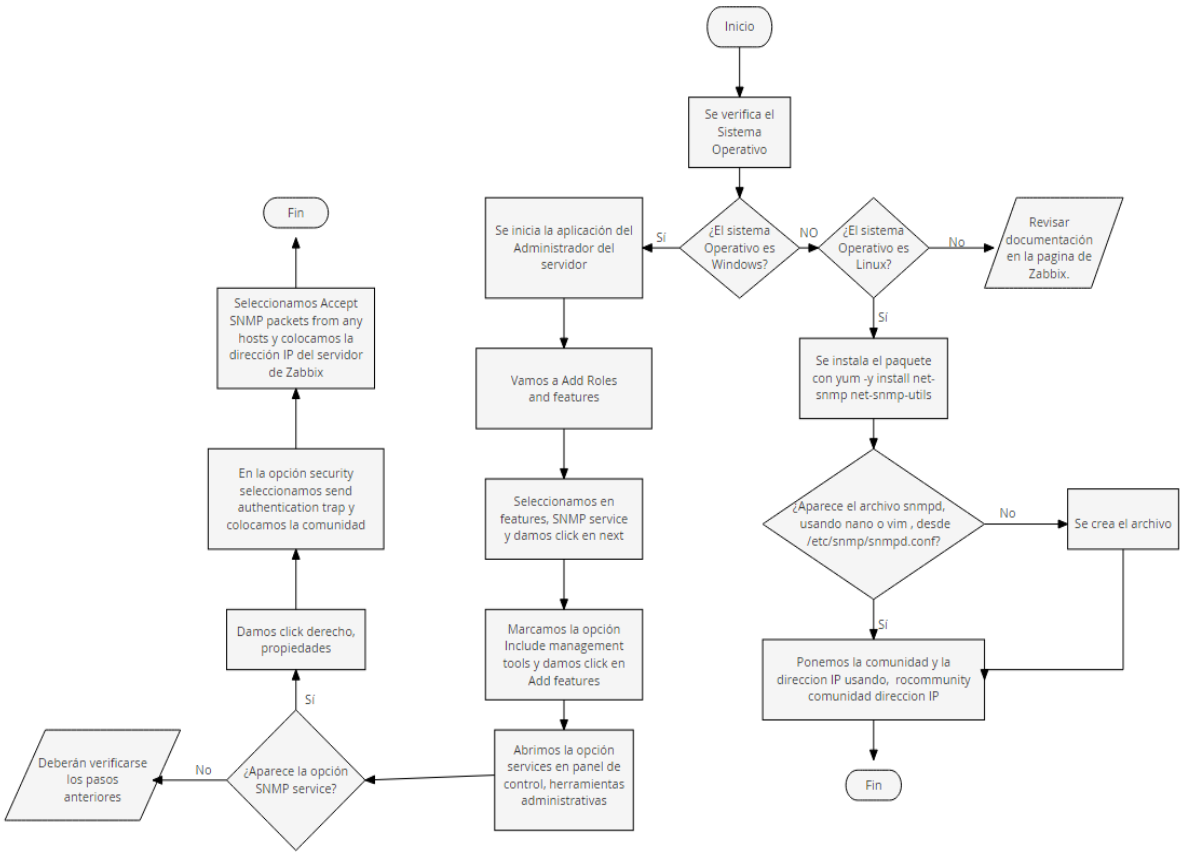


Figura 8. Diagrama de flujo, configuración SNMP

5.2.4.2 Agregar un host a la plataforma de gestión de Zabbix.

Se procede a agregar los servidores que se desean monitorear en Zabbix, de acuerdo al objetivo del proyecto, en la primera fase se realizan pruebas con 4 servidores, en la fase de pruebas se realizan pruebas con 20 servidores y en la fase final de implementación se agregan todos los servidores de la compañía, para garantizar el correcto funcionamiento de los mismos, en el apéndice D se detallan los pasos y se adjuntan las evidencias tomadas.

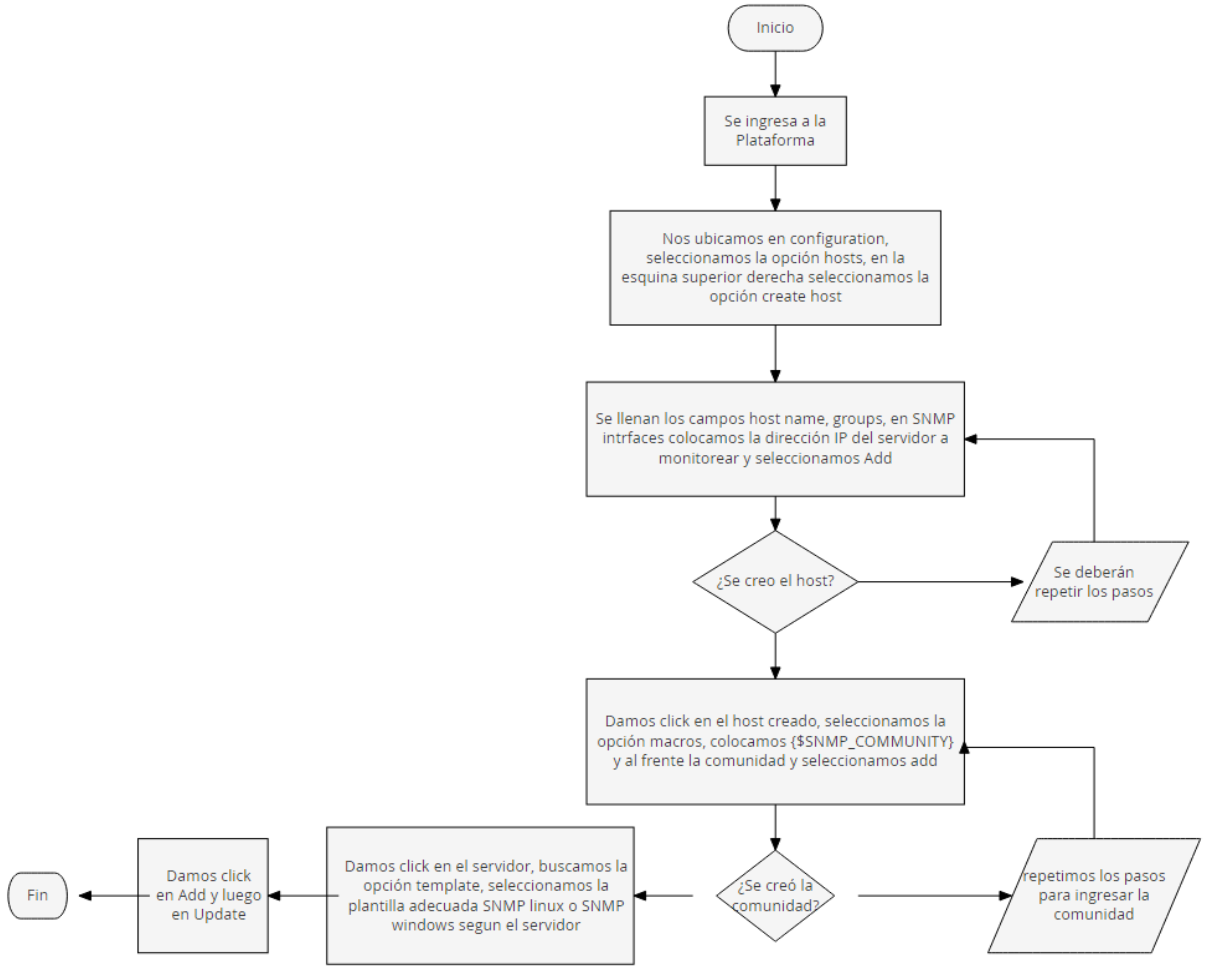


Figura 9. Diagrama de flujo, agregación de hosts

5.2.5 Configuración de notificaciones vía Email en Zabbix.

A continuación, se mostrará cómo realizar el proceso para la configuración de las notificaciones enviadas por Zabbix vía Email, si se llega a presentar contingencias o información sobre un servidor específico. Esto para tener una mejor administración de los recursos y evitar incidencias que se puedan presentar de cara al futuro y que puedan llegar a generar consecuencias muy difíciles de arreglar o irreversibles. Con estos sistemas lo que se busca es anticiparse a estos problemas observando el comportamiento del servidor en tiempo real y las 24 horas del día, los 7 días de la semana, más detalles en el anexo E.

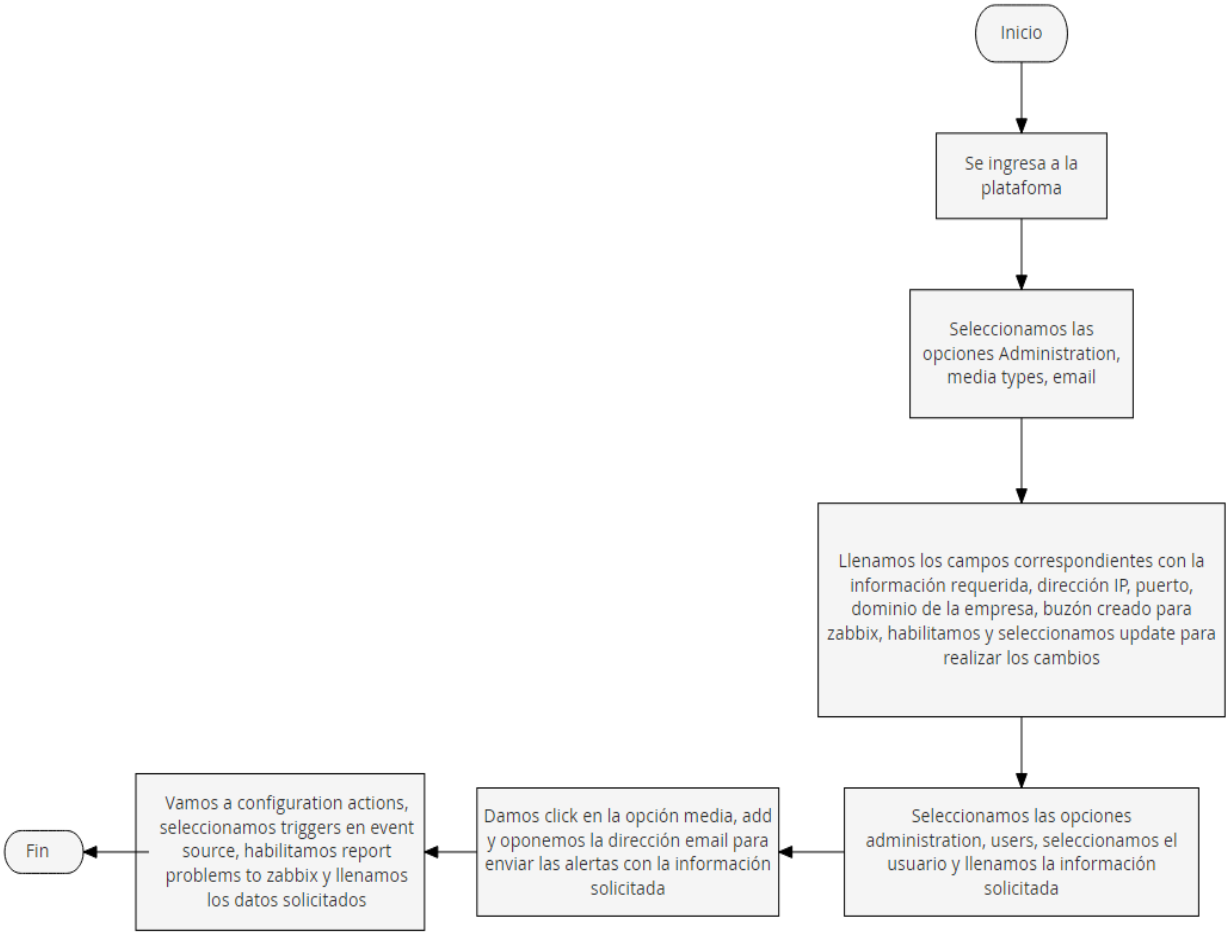


Figura 10. Diagrama de flujo, Notificaciones email

6 Resultados y análisis

6.1 Resumen de análisis de las diferentes herramientas de monitoreo

Una vez obtenidas y clasificadas las herramientas pre-seleccionadas se implementó un laboratorio virtual, utilizando VMware Workstation Pro en la versión 15, instalada en el puesto de trabajo del realizador del proyecto, donde se instalaron de una forma lógica y ordenada las dos herramientas que más se ajustaban a los requerimientos, de acuerdo a la tabla 2. Para este proceso se instalan de forma virtual dos equipos con sistema operativo Linux y dos equipos con sistema operativo Windows, apoyados en un blog de la web donde se realiza un montaje similar [8]. Los cuatro servidores virtuales instalados se configuran en una red aparte de la red principal de Emtelco S.A.S, para evitar inconvenientes, trabajando así en un sistema totalmente aislado.

Tabla 2 Comparación de funciones entre software Open Surce.

Característica	Zabbix	Zennos	Cacti	Nagios
Interfaz Web	X	X	X	X
Alarmas	X	X	X	X
Gráficas	X	X	X	X
Reportes	X	X		X
Open Surce	X	X	X	
Instalación en diferentes Sistemas Operativos	X			X
Fácil de Usar	X			X
Envío de Notificaciones, Email o SMS	X			X
Escalable y Robusto	X			X

6.1.1 Resultados del software Nagios.

En esta primera prueba se pudo descargar el software de nagios sin ningún inconveniente desde la página oficial de nagios, se siguieron las instrucciones respectivas de instalación, aunque fueron algo complicadas ya que la mayoría de instrucciones se realizan desde la ventana de comandos, se presentaron algunos inconvenientes al configurar el monitoreo de los servidores con el sistema operativo Windows usando el protocolo SNMP, solo fue posible configurarlos utilizando el agente, sin embargo con la agregación de los servidores con sistema operativo Linux no se presentaron inconvenientes. Debido a que no se tenían buenos conocimientos y no se realizó un estudio detallado de esta herramienta, solo fue posible realizar el monitoreo de conectividad realizando ping cada 3 minutos, en las consultas realizadas para la configuración de las demás necesidades de monitoreo de la empresa, se encontró que había información muy diversa, se mostraban diferentes métodos y no fue posible configurarlas todas.

Tabla 3 Conclusiones de Nagios.

VENTAJAS	DESVENTAJAS
Fácil de Instalar	Pobre Interfaz Web.
	Reportes Básicos.
	Creación de hosts y configuración por línea de comandos.

6.1.2 Resultados del software Zabbix.

En la primera fase de prueba de instalación de esta herramienta, se descargó el software desde la página oficial de Zabbix, se encontró material de la instalación respectiva usando el protocolo SNMP y utilizando agente para la configuración, por cuestiones de tiempo se realizó el monitoreo de los tres servidores mediante el agente de Zabbix y el cuarto servidor se realizó por medio del protocolo SNMP, encontrando que al utilizar el agente era mucho más práctico y fácil de configurar, sin embargo, se puedo notar que no era tan complicado tampoco utilizar el protocolo SNMP, con el cual fue posible configurar el monitoreo de uso de la CPU, de la memoria RAM, del disco duro y la conectividad del equipo. Dado que se pudo validar el monitoreo de las herramientas acordes con la necesidad de la empresa, se sugiere la implementación de esta herramienta como desarrollo del proyecto.

Tabla 4 Conclusiones de Zabbix.

VENTAJAS	DESVENTAJAS
Buena Interfaz gráfica.	No es sencilla la configuración básica.
Reportes variados.	
Toda la configuración se la realiza vía web.	
Envío de alertas por correo.	

Dentro de las pruebas que se desarrollaron se consideró que la herramienta de monitoreo pudiera emitir alarmas mediante el uso del protocolo SNMP, de la carga de la CPU, conectividad mediante ping, tiempo fuera de actividad, uso de la memoria RAM y uso del disco duro. Luego de estas pruebas y realizar una exposición a los ingenieros encargados de la administración de la plataforma de TI, se decide que la mejor opción es la implementación de la herramienta Zabbix, como complemento de OP Manager.

6.2 Informe de monitoreo de la herramienta Zabbix.

Una vez instalada y conectada con la base de datos la herramienta, de acuerdo a lo visto en la metodología, desde cualquier equipo conectado a la red Ingresamos a la dirección IP, que usamos para el servidor zabbix anteriormente, adicionándole la ruta zabbix: **“IP/zabbix/”**, debe aparecer algo como esto, le damos a next step:

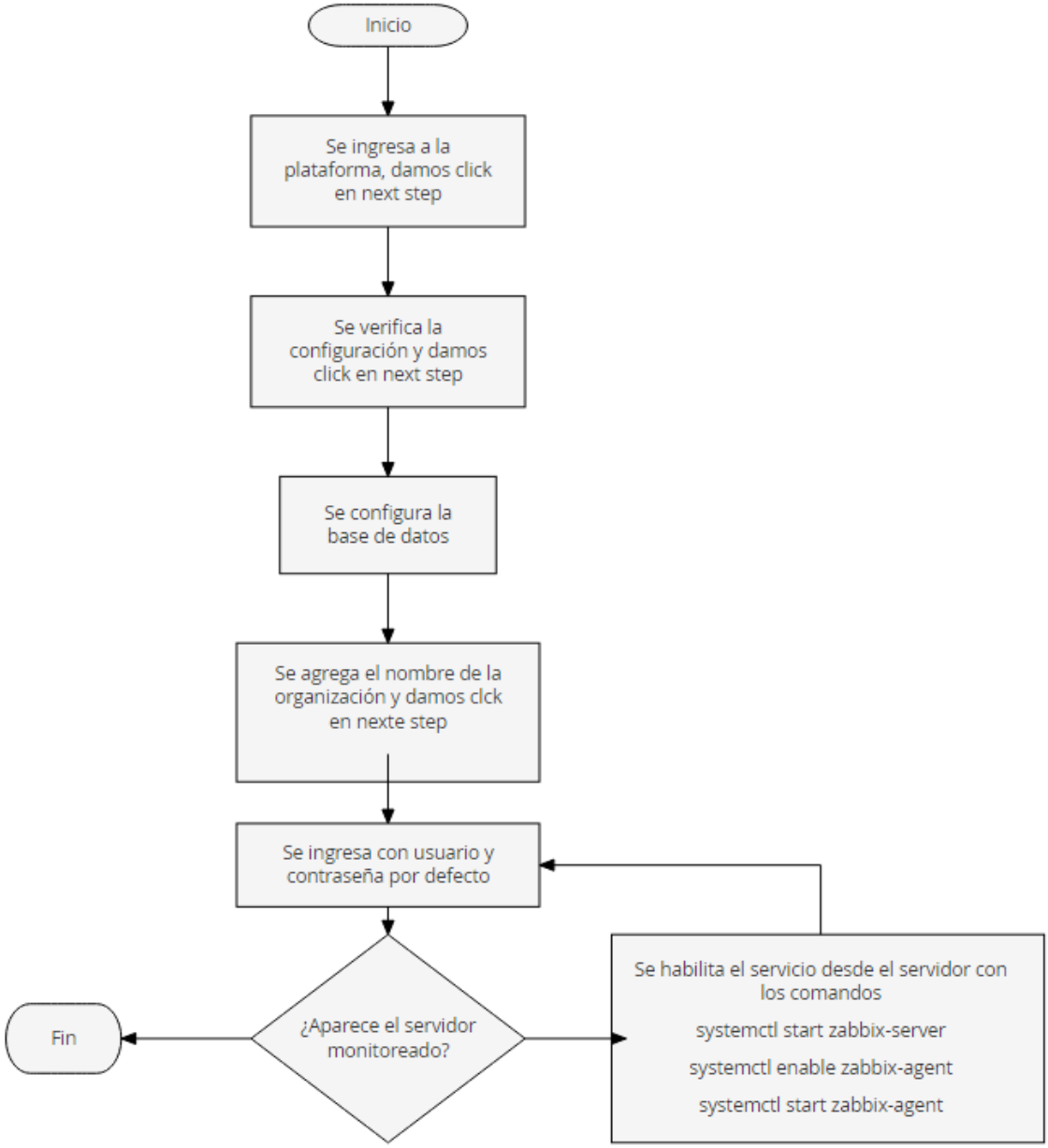


Figura 11. Diagrama de flujo, informes vía email

6.3 Verificación del monitoreo de servidores.

Uno de los factores más importante de nuestra herramienta es el de poder tener un control de las anomalías que se presenten en los servidores de la compañía, por lo que saber interpretar los gráficos con los registros arrojados por zabbix se vuelve de suma importancia. A continuación, se muestran los pasos para visualizar las gráficas entregadas por la herramienta y una imagen de ejemplo de su funcionamiento, es de aclarar que este tipo de vista puede ser modificado por el administrador de acuerdo a las necesidades y requerimientos.

1. Para verificar seleccionamos la opción Monitoring.
2. Seleccionamos la parte que dice Graphs
3. Seleccionamos all en la parte que dice groups.
4. Seleccionamos el host y una de las gráficas disponibles.

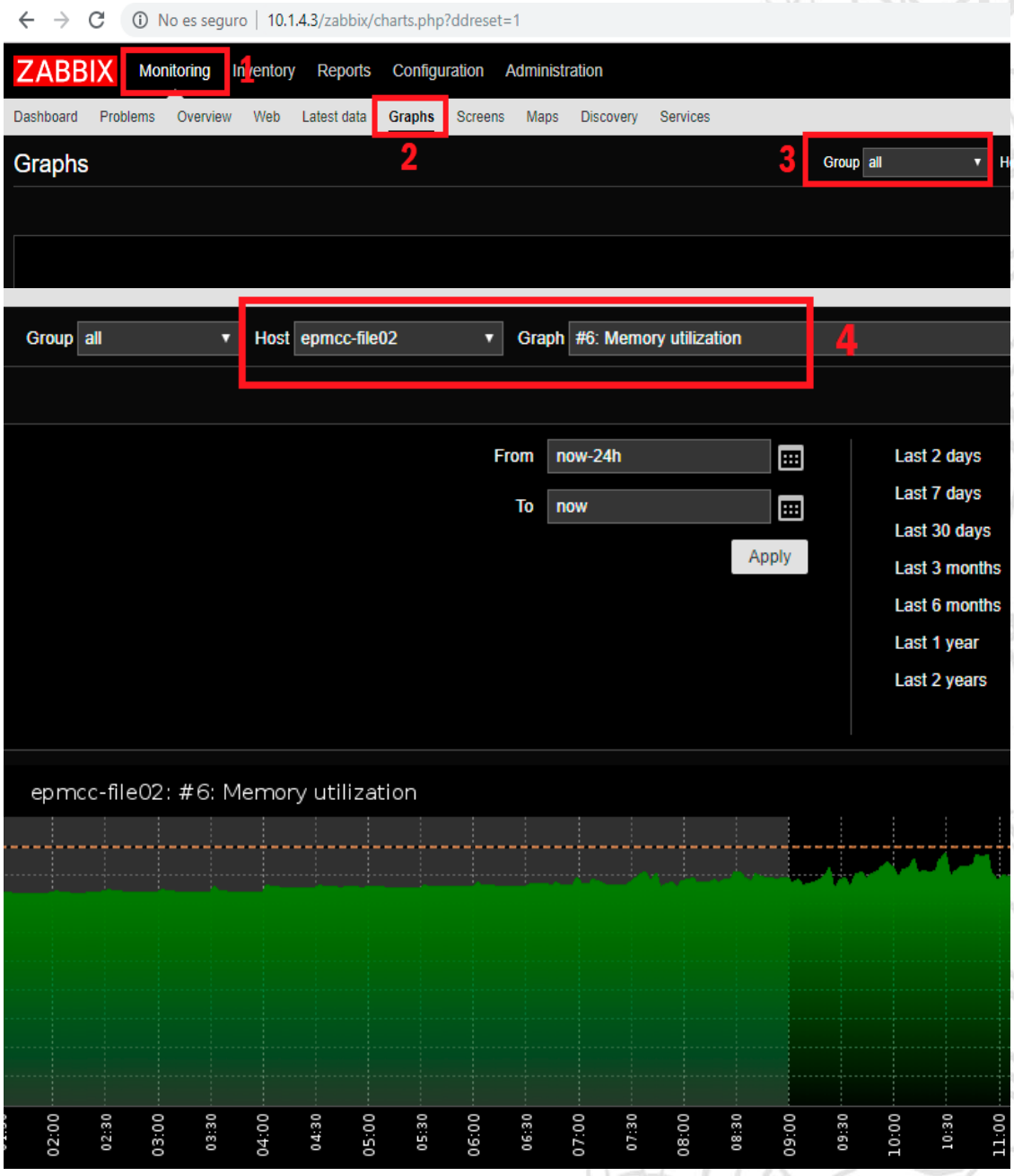


Figura 12. Verificación de monitoreo de un host.

6.4 Verificación del envío de correos.

Una vez configurado el correo como vimos en la metodología, cuando ocurra algún problema con un servidor o "device", agregada a Zabbix, este reportara directamente a el correo de la persona a la cual le configuramos la opción de envío. Además, se puede validar en "Reports" y en el apartado "Action Log" donde se muestran las notificaciones enviada por Zabbix, en este lugar debe aparecer "Sent" en color verde informando que la notificación se envió de manera correcta.

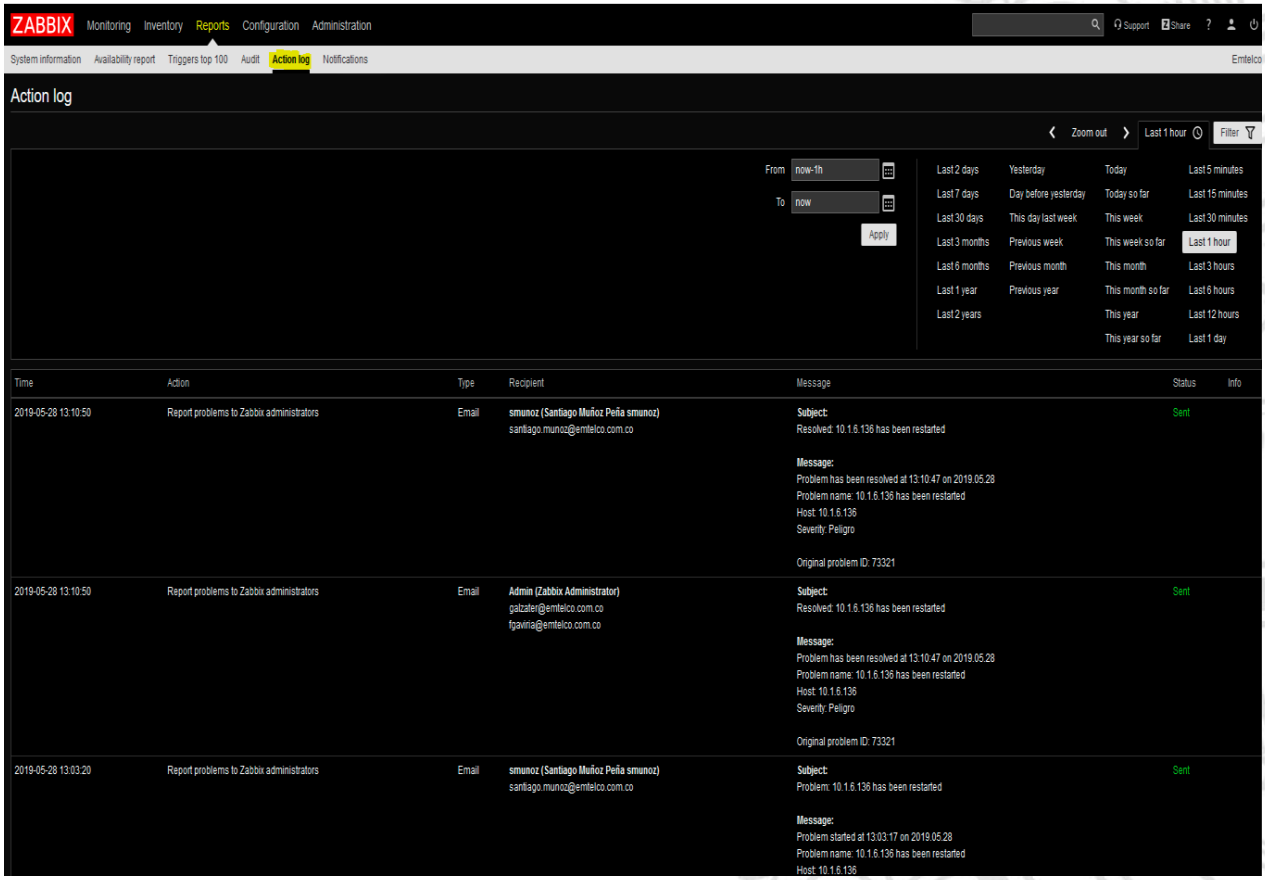


Figura 13. Vista correo enviado desde zabbix.

Ahora revisamos nuestro buzón y comprobamos funcionamiento.

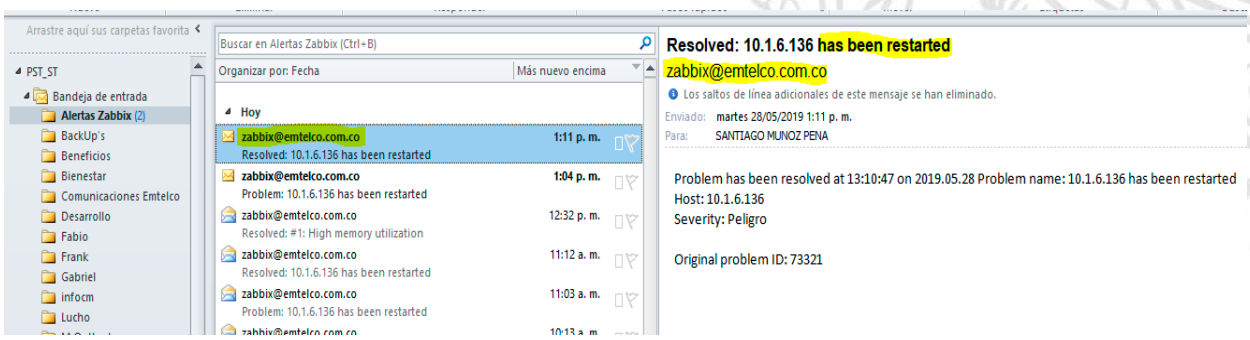


Figura 14. Verificación de correo enviado al buzón.

7 Conclusiones

- Mediante la ejecución de este proyecto se evidencia la gran funcionalidad que puede tener un sistema de monitoreo TI, el cual puede contar de diferentes herramientas que son de gran ayuda a la hora de mantener un control de los eventos que se presenten en la compañía donde se encuentre implementada la herramienta.

- De acuerdo a la instalación de la herramienta Zabbix, es importante tener en cuenta que se debe contar con los recursos suficientes a nivel de servidor y red para que esta herramienta pueda trabajar de manera óptima explotando sus diferentes funciones sin ningún inconveniente.

- Al momento de llevar a cabo la configuración del protocolo SNMP en los dispositivos a monitorear, es de gran importancia tener claro que versión del protocolo se va a utilizar y cuál será el nombre de la comunidad, pues si no se realiza esta configuración de la misma manera en el dispositivo y la herramienta de monitoreo, no será posible obtener los traps de dados para detallar el estado del dispositivo monitoreado.

- Los informes que entrega la herramienta de monitoreo Zabbix de los dispositivos monitoreados pueden ser de diferentes formas gráficas, por lo cual es importante tener en cuenta cual es el grafico más apto para los datos que se deseen representar y así lograr que sean de mejor entendimiento.

- En general la herramienta de monitoreo Zabbix es muy amigable con el usuario pues su configuración no se torna complicada, cuenta con muchas funciones, su interfaz gráfica es muy llamativa y la versión libre permite monitorear gran cantidad de nodos, por lo cual es una buena opción para las empresas que deseen empezar a llevar un control de sus sistemas mediante una herramienta de buen rendimiento que los mantenga al tanto de las eventualidades.

8 Referencias

[1]. Emtelco S.A.S, (2019). “Quienes somos”. [online] Available at http://www.emtelco.com.co/nosotros

[2] Monitoreo, “Definición de monitoreo”. [En línea]. Disponible en: https://definicion.de/monitoreo/

[3] Microsoft (2004). Event Viewer. Microsoft Corporation. [En línea]. Disponible en: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-xp/bb457163(v=technet.10)?redirectedfrom=MSDN

[4]. Zabbix. Plataforma de monitoreo [online] Available at https://www.ecured.cu/ZABBIX

[5]. Zenoss. Plataforma de monitoreo. [online] Available at https://pandorafms.com/blog/es/herramientas-de-monitoreo-de-redes/

[6]. Cacti. Plataforma de monitoreo. [online] Available at https://www.ecured.cu/Cacti

[7]. Nagios. Plataforma de monitoreo. [online] Available at https://www.ecured.cu/Nagios

[8]. Windows Server 2012 – Introducción a los cluster – Como preparar un laboratorio virtual. [online] Available at https://blog.soporteti.net/windows-server-2012-introduccion-a-los-cluster-como-preparar-un-laboratorio-virtual/

[9]. Documentación de Zabbix 4.2. [online] Available at https://www.zabbix.com/documentation/4.2/manual/installation/requirements

Apéndice A

Instalación de la base de datos.

Obtenemos el paquete de Instalación de la base de datos.
Con el comando: **wget + "direccionURLpaquete"**, se obtiene el paquete.

```
[root@localhost tmp]# wget http://repo.mysql.com/mysql80-community-release-el7-1.noarch.rpm
```

Instalamos los repositorios necesarios.
con el comando: **rpm –ivh "nombredelpaquetedescargado"** se instalan los paquetes obtenidos.

```
[root@localhost tmp]# rpm -ivh mysql80-community-release-el7-1.noarch.rpm
```

Instalamos la base de datos Mysql.
Instalamos Mysql server con el comando: **yum install mysql-server –y**

```
[root@localhost tmp]# yum install mysql-server -y
```

Activamos la base de datos.
El comando **systemctl enable mysqld**, permite activar el daemon o servicio de mysql y con el comando **systemctl start mysqld**, ejecutamos el servicio.

```
[root@localhost tmp]# systemctl enable mysqld
[root@localhost tmp]# systemctl enable mysqld
```

Configuramos Mysql 8.0.

Después de la instalación e iniciación de Mysql, se deben configurar algunos archivos para el correcto funcionamiento del servicio.

Con el comando: **tail –f /var/log/mysql.log | grep "password"**, buscamos la contraseña de Root de mysql, directamente en el archivo mysql.log

```
[root@localhost tmp]# tail -f /var/log/mysqld.log | grep "password"
2018-10-03T02:07:21.783216Z 5 [Note] [MY-010454] [Server] A temporary password is generated for root@localhost: F0slRB#ebe81
```

Ingresamos a mysql como Root, ingresando la contraseña anteriormente obtenida. Se ingresa con el comando: **mysql –u root –p**

```
[root@localhost tmp]# mysql -u root -p
Enter password:
```

Para efectos de seguridad y comodidad, vamos a cambiar la contraseña de mysql, esto se realiza con el comando: **set password for “root”@”localhost”= “contraseñaelegida”; en este caso usamos 1234@Mudar**

```
mysql> set password for "root"@"localhost"= "1234@Mudar";
Query OK, 0 rows affected (0.12 sec)
```

Creamos la base de datos, tablas y usuarios necesarias en mysql 8.0 para Zabbix, ya que este utiliza su propia base de datos y usuario en mysql 8.0.

Primero se crea la base de datos, esto se realiza con el comando:
create database zabbix character set utf8 collate utf8_bin;

```
mysql> create database zabbix character set utf8 collate utf8_bin;
Query OK, 1 row affected, 1 warning (0.06 sec)
```

Creamos el usuario de zabbix en mysql, con el comando:
Create user “zabbix”@”localhost” identified by “contraseñaelegida”

```
mysql> create user "zabbix"@"localhost" identified by "1234@Mudar";
Query OK, 0 rows affected (0.02 sec)
```

Le otorgamos permisos de súper usuario en mysql a el usuario zabbix con el comando:
grant all on zabbix.* to “zabbix”@”localhost”;

```
mysql> grant all on zabbix.* to "zabbix"@"localhost";
Query OK, 0 rows affected (0.08 sec)
```

Para que los cambios surtan efecto, se deben refrescar los privilegios de mysql, con el comando: **flush privileges;**

```
mysql> flush privileges;
Query OK, 0 rows affected (0.00 sec)
```

Con el comando: **show databases;** observamos y validamos la creación de la base de datos.

```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| sys                |
| zabbix             |
+--------------------+
5 rows in set (0.01 sec)
```

Con el comando: **use zabbix;** cambiamos la base de datos por defecto a la que acabamos de crear.

```
mysql> use zabbix;
Database changed
```

Luego salimos de mysql escribiendo: **exit**

```
mysql> exit
Bye
```

Apéndice B

Instalación de la herramienta Zabbix.

Obtenemos el paquete de zabbix 4.0.7 con el comando:
wget http://repo.zabbix.com/zabbix/4.0/rhel/zabbix-release-4.0-1.el7.noarch.rpm

```
[root@localhost tmp]# wget http://repo.zabbix.com/zabbix/4.0/rhel/7/x86_64/zabbix-release-4.0-1.el7.noarch.rpm
```

Luego instalamos el paquete con el comando:
rpm –ivh zabbix-release-4.0-1.el7.noarch.rpm

```
[root@localhost tmp]# rpm -ivh zabbix-release-4.0-1.el7.noarch.rpm
```

Vamos a instalar todas las dependencias de Zabbix lo primero que se instala es el agente (este se puede o no utilizar, pero para efecto de prueba se instala), después zabbix server para mysql, el frontend de zabbix web y por último se obtiene la aplicación zabbix. Todo esto se realiza con el comando:

yum install zabbix-agent.x86_64 zabbix-server-mysql.x86_64 zabbix-web-mysql.noarch zabbix-get.x68_64 -y

```
[root@localhost tmp]# yum install zabbix-agent.x86_64 zabbix-server-mysql.x86_64 zabbix-web-mysql.noarch zabbix-get.x86_64 -y
```

Hasta este punto ya tenemos instalado el Zabbix 4.0.7 en nuestro dispositivo.
Vamos a validar que esto sea así:
Ejecutamos el comando: **systemctl status zabbix-server.** Aparece inactivo, pero confirma que esta instalado.

```
[root@localhost tmp]# systemctl status zabbix-server
● zabbix-server.service - Zabbix Server
   Loaded: loaded (/usr/lib/systemd/system/zabbix-server.service; disabled; vendor preset: disabled)
   Active: inactive (dead)
```

Observando que esta desactivado, se cambió de estado a disponible con el comando:
systemctl enable zabbix-server

```
[root@localhost tmp]# systemctl enable zabbix-server
Created symlink from /etc/systemd/system/multi-user.target.wants/zabbix-server.service to /usr/lib/systemd/system/zabbix-server.service.
```

Hacemos lo mismo y activamos el agente de zabbix con el comando:
systemctl enable zabbix-agent

```
[root@localhost tmp]# systemctl enable zabbix-agent
Created symlink from /etc/systemd/system/multi-user.target.wants/zabbix-agent.service to /usr/lib/systemd/system/zabbix-agent.servic
```

Ahora procedemos a conectar zabbix con la base de datos, para ello Ingresamos a la ruta /usr/share/doc/zabbix-server-mysql-4.0.0/ con el comando:
cd /usr/share/doc/zabbix-server-mysql-4.0.0/

y con: **ls** listamos lo que se encuentra en la ruta, validando que se encuentre el archivo **create.sql.gz**.

```
[root@localhost tmp]# cd /usr/share/doc/zabbix-server-mysql-4.0.0/
[root@localhost zabbix-server-mysql-4.0.0]# ls
AUTHORS  COPYING  ChangeLog  NEWS  README  create.sql.gz
```

Con el siguiente comando: **zcat create.sql.gz | myslq –uzabbix –p zabbix**
Se ingresa en el archivo comprimido y consiguiente a este ejecuta mysql como root.

```
[root@localhost zabbix-server-mysql-4.0.0]# zcat create.sql.gz | mysql -uzabbix -p zabbix
Enter password:
```

Dentro de mysql ejecutamos el comando: **show databases;**

```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| zabbix             |
+--------------------+
2 rows in set (0.00 sec)
```

Utilizamos la base de datos Zabbix con el comando: **use zabbix;**

```
mysql> use zabbix;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
```

Para ver las tablas ejecutamos el comando: **show tables;**

```
mysql> show tables;
```

Deben aparecer 144 columnas las cuales corresponden a las tablas de la base de datos Zabbix. Luego salimos de mysql con el comando: **exit**

```
144 rows in set (0.01 sec)
```

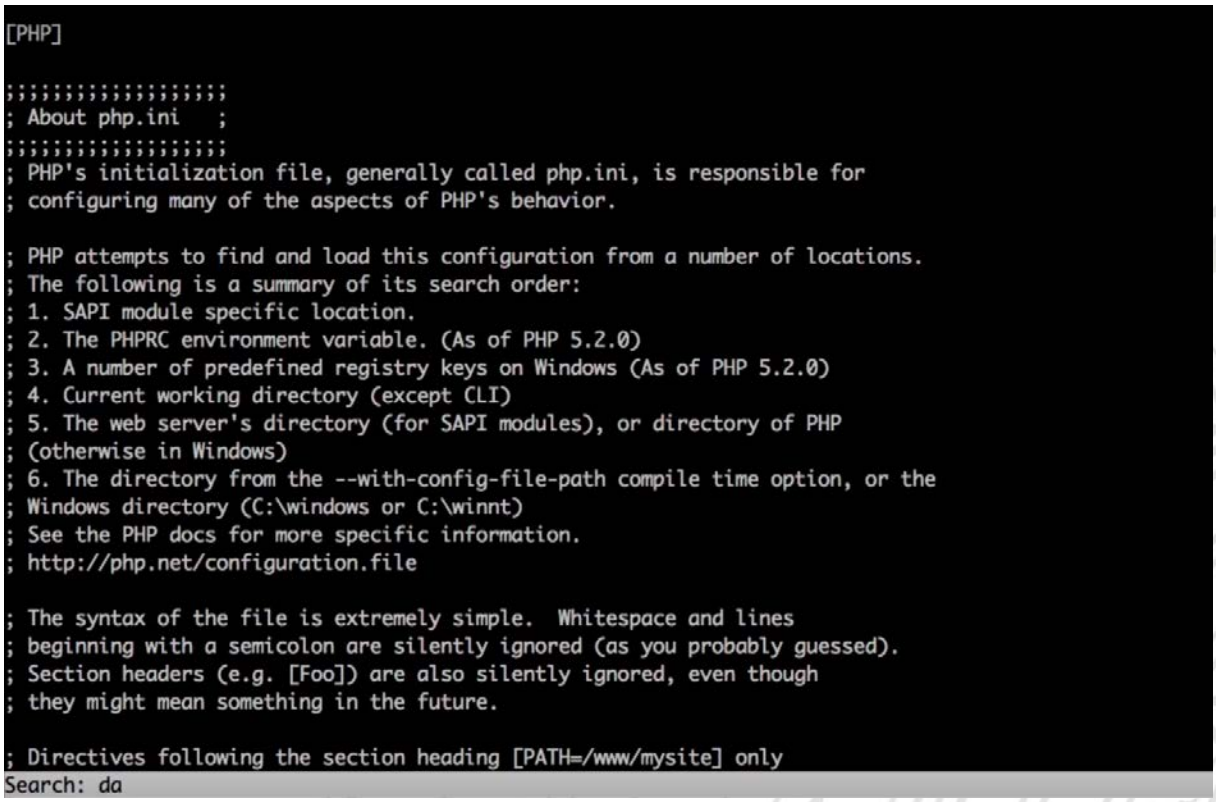
Ahora vamos modificar algunos atributos en archivos específicos para terminar la configuración:

Primero vamos a agregar nuestra zona horaria, para esto debemos editar un archivo el cual se encuentra en la ruta: /etc/php.ini.

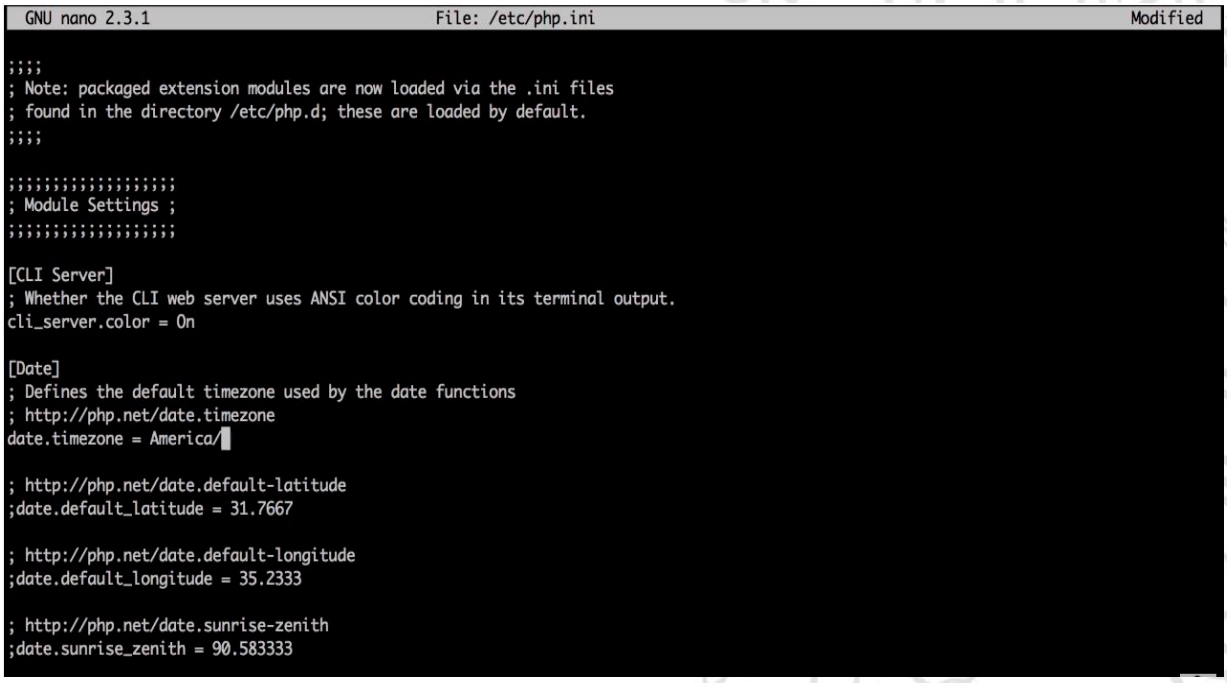
Esto se hace con el comando: **nano /etc/php.ini**

```
[root@localhost zabbix-server-mysql-4.0.0]# nano /etc/php.ini
```

Buscamos el atributo **“Date”**, dentro del GNU nano, esto se hace oprimiendo las teclas **“CTRL + W”** y digitando en la caja de texto **“Date”**



En el apartado **[Date]**, quitamos el **";"**, que está al inicio del atributo date.timezone, modificamos y agregamos:
date.timezone = America/Lima.



Confirmamos los cambios al salir.

```
Save modified buffer (ANSWERING "No" WILL DESTROY CHANGES) ?
 Y Yes
```

Ahora vamos a editar el archivo de configuración de zabbix, ingresamos con el comando:
nano /etc/zabbix/zabbix_server.conf

```
[root@localhost zabbix-server-mysql-4.0.0]# nano /etc/zabbix/zabbix_server.conf
```

Nuevamente buscamos en el editor nano, esto se realiza oprimiendo las teclas **“CTRL + W”**
Y buscamos la palabra **“pass”.**

```
############ GENERAL PARAMETERS #################

### Option: ListenPort
#       Listen port for trapper.
#
# Mandatory: no
# Range: 1024-32767
# Default:
# ListenPort=10051

### Option: SourceIP
#       Source IP address for outgoing connections.
#
# Mandatory: no
# Default:
# SourceIP=

### Option: LogType
#       Specifies where log messages are written to:
#               system  - syslog
#               file    - file specified with LogFile parameter
#               console - standard output
#
# Mandatory: no
Search: pass
```

Modificamos y descomentamos la siguiente línea:
DBPassword = **“contraseñaelegida”**

```
  GNU nano 2.3.1                          File: /etc/zabbix/zabbix_server.conf

# Mandatory: no
# Default:
# DBSchema=

### Option: DBUser
#       Database user. Ignored for SQLite.
#
# Mandatory: no
# Default:
# DBUser=

DBUser=zabbix

### Option: DBPassword
#       Database password. Ignored for SQLite.
#       Comment this line if no password is used.
#
# Mandatory: no
# Default:
DBPassword=1234@Mudar
```

Confirmamos los cambios antes de salir del editor.

```
Save modified buffer (ANSWERING "No" WILL DESTROY CHANGES) ?
 Y Yes
```

Activamos el servicio de HTTP, con el siguiente comando:
systemctl enable httpd

```
[root@localhost zabbix-server-mysql-4.0.0]# systemctl enable httpd
Created symlink from /etc/systemd/system/multi-user.target.wants/httpd.service to /usr/lib/systemd/system/httpd.service.
```

Iniciamos el servicio de http con el comando:
Systemctl start httpd

```
[root@localhost zabbix-server-mysql-4.0.0]# systemctl start httpd
```

Se consulta la IP, esto con el comando: **“ifconfig”**

```
[root@localhost ~]# ifconfig
ens192: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.1.4.3  netmask 255.255.255.0  broadcast 10.1.4.255
```

Instalar netsnmp con el comando: **yum install net-snmp net-snmp-utils**

```
yum install net-snmp net-snmp-utils
```

Apéndice C

Configuración de SNMP en servidores con S.O Windows.

En los servidores con sistema operativo Windows el rol de SNMP viene desinstalado por defecto, por lo que debemos instalarlo, de la siguiente manera:

1. Se inicia la aplicación del Administrador del servidor y se accede al menú agregar roles y funciones.
2. Damos click en siguiente varias veces hasta llegar a la parte Features.
3. Seleccionamos SNMP Service y damos click en siguiente.

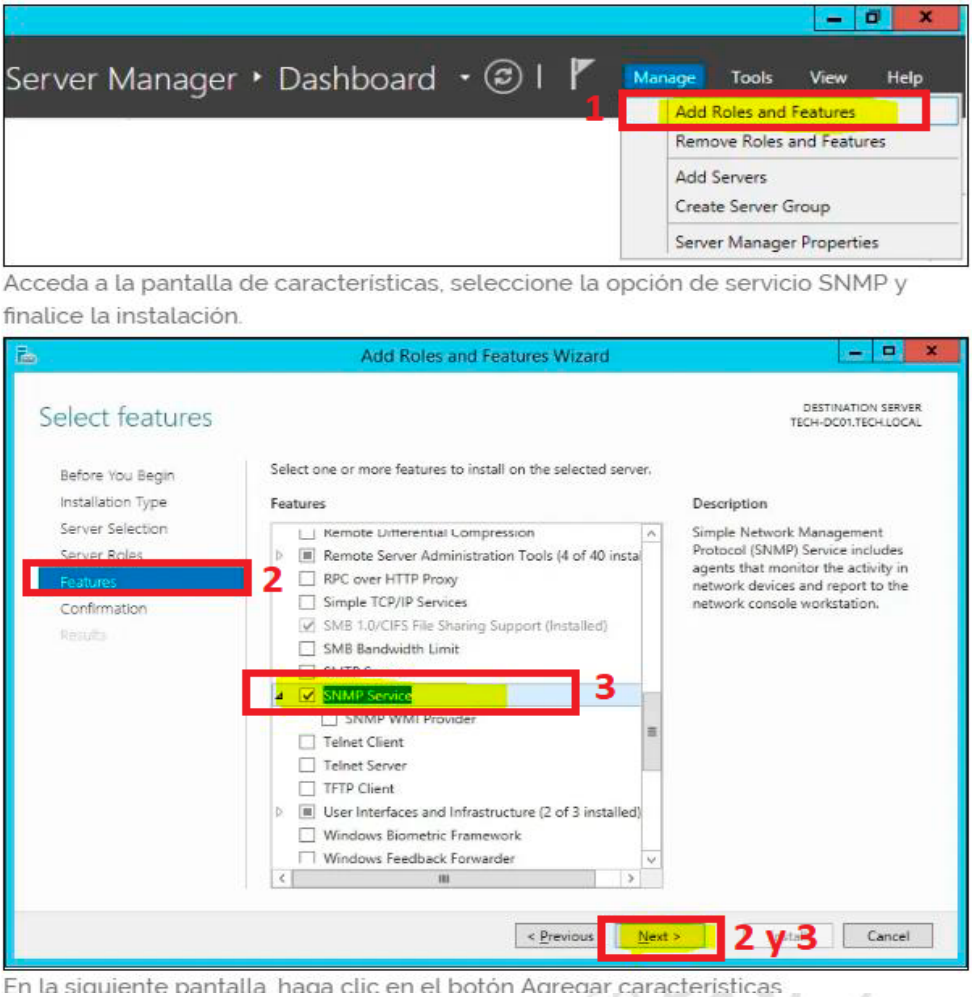
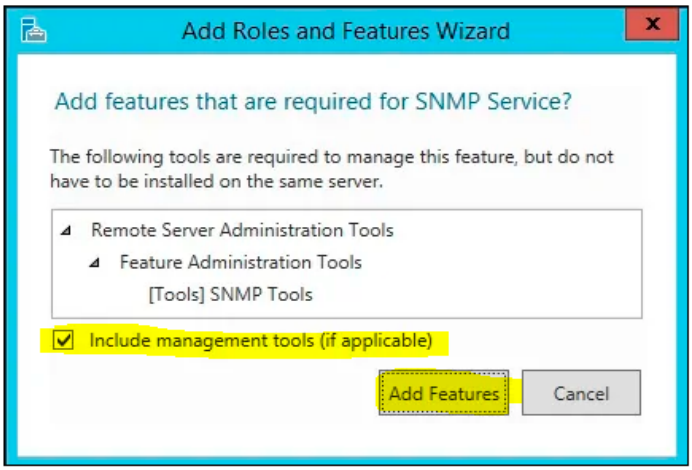


Figura 15. Adición de SNMP en Windows Server.

Una vez instalado procedemos a configurar el protocolo, para ello damos click en agregar características (Add Features).

En la siguiente pantalla, haga clic en el botón Agregar características.



La función SNMP se instaló en su computadora, pero aún necesitamos configurar el servicio SNMP.

Figura 16. Configuración del rol SNMP Protocol en Windows Server.

Abrimos la pantalla de administración de servicios de Windows, esto se hace desde el panel de control, herramientas administrativas o desde la ventana ejecutar escribiendo services.msc; seleccionamos SNMP service, damos click derecho y abrimos donde dice propiedades.

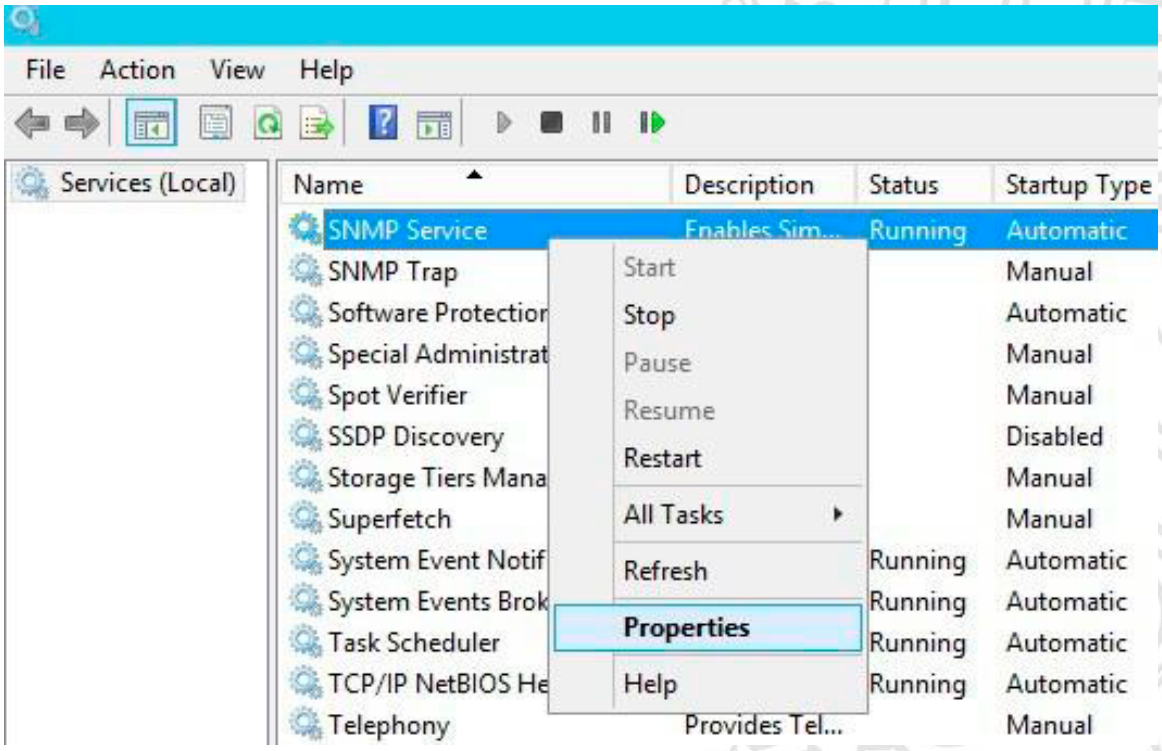


Figura 17. Se busca el servicio SNMP en Windows Server.

Finalmente procedemos de la siguiente manera:

1. Seleccionamos la pestaña Security.
2. Agregamos la comunidad, en este caso 3mt3lc0
3. Agregamos la ip o el nombre del servidor donde tenemos Zabbix, en este caso 10.1.4.3

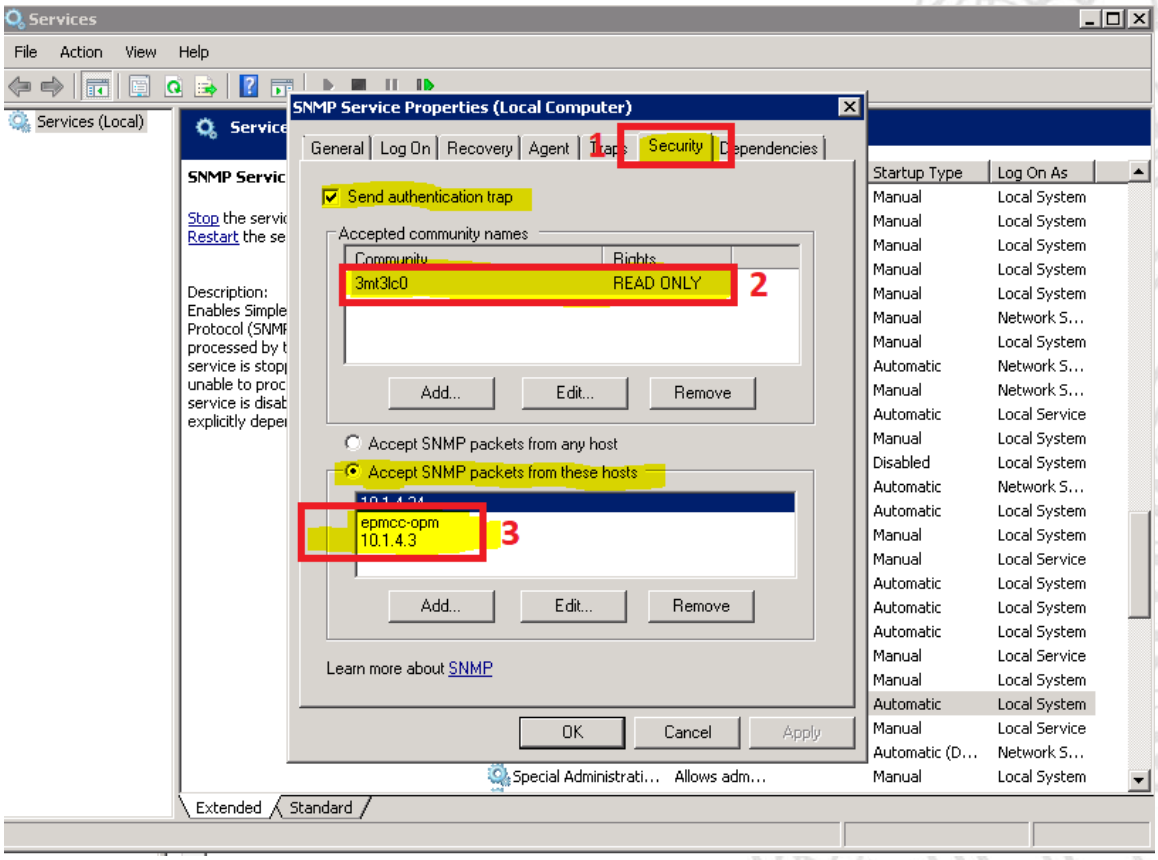


Figura 18. Configuración del Protocolo SNMP en Windows Server.

Configuración de SNMP en servidores con S.O Linux.

Por defecto SNMP se instala con el sistema operativo, sin embargo, en caso de no hacerse o de haber desinstalado antes el servicio, lo podemos instalar de nuevo de la siguiente manera, vamos al servidor que deseamos monitorear, entramos como usuario con permisos de instalacion a la terminal y ponemos:

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

Para configurar la comunidad y agregar la dirección IP del servidor de Zabbix, en este caso la comunidad es 3mt3lc0 y la IP del servidor es 10.1.4.3; debemos abrir y editar el archivo snmpd.conf en la ruta

/etc/snmp/snmpd.conf; si no existe se crea el archivo. Para editar se puede usar un editor como vim o nano.

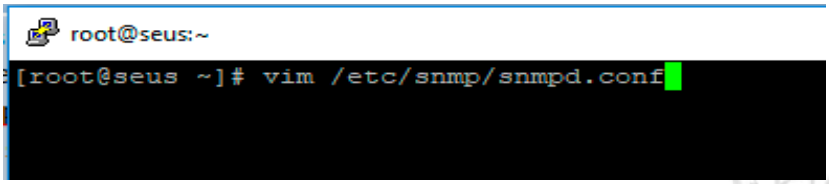


Figura 19. Configuración del protocolo SNMP en Linux paso 1.

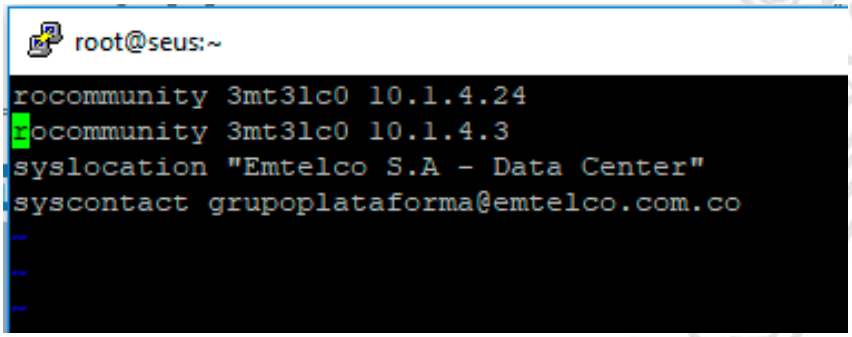


Figura 20. Configuración del protocolo SNMP en Linux paso 2.

Apéndice D

Agregar un host a la plataforma de gestión de Zabbix.

Lo primero que debemos hacer es ingresar a la plataforma de gestión de Zabbix.

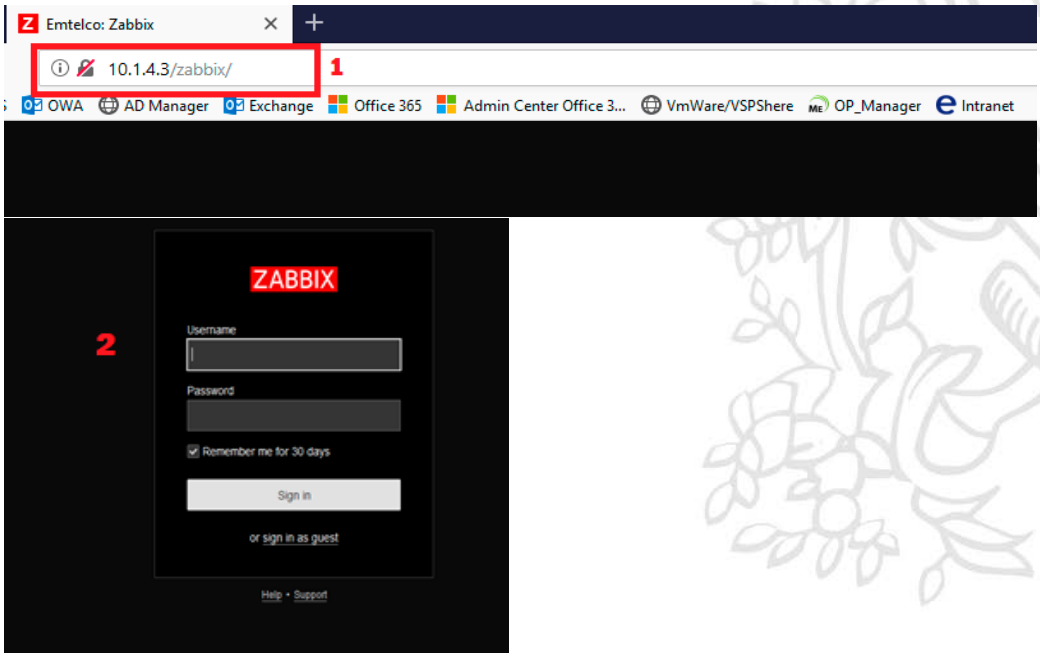


Figura 21. Pantalla de ingreso a la plataforma de zabbix.

8.1.1.1.1 Creación del host.

Procedemos a crear el host en la plataforma, como se enuncia en los siguientes pasos:

1. Nos ubicamos en la pestaña Configuration.
2. Seleccionamos la opción Hosts.
3. En la esquina superior derecha damos click en la opción créate Host.

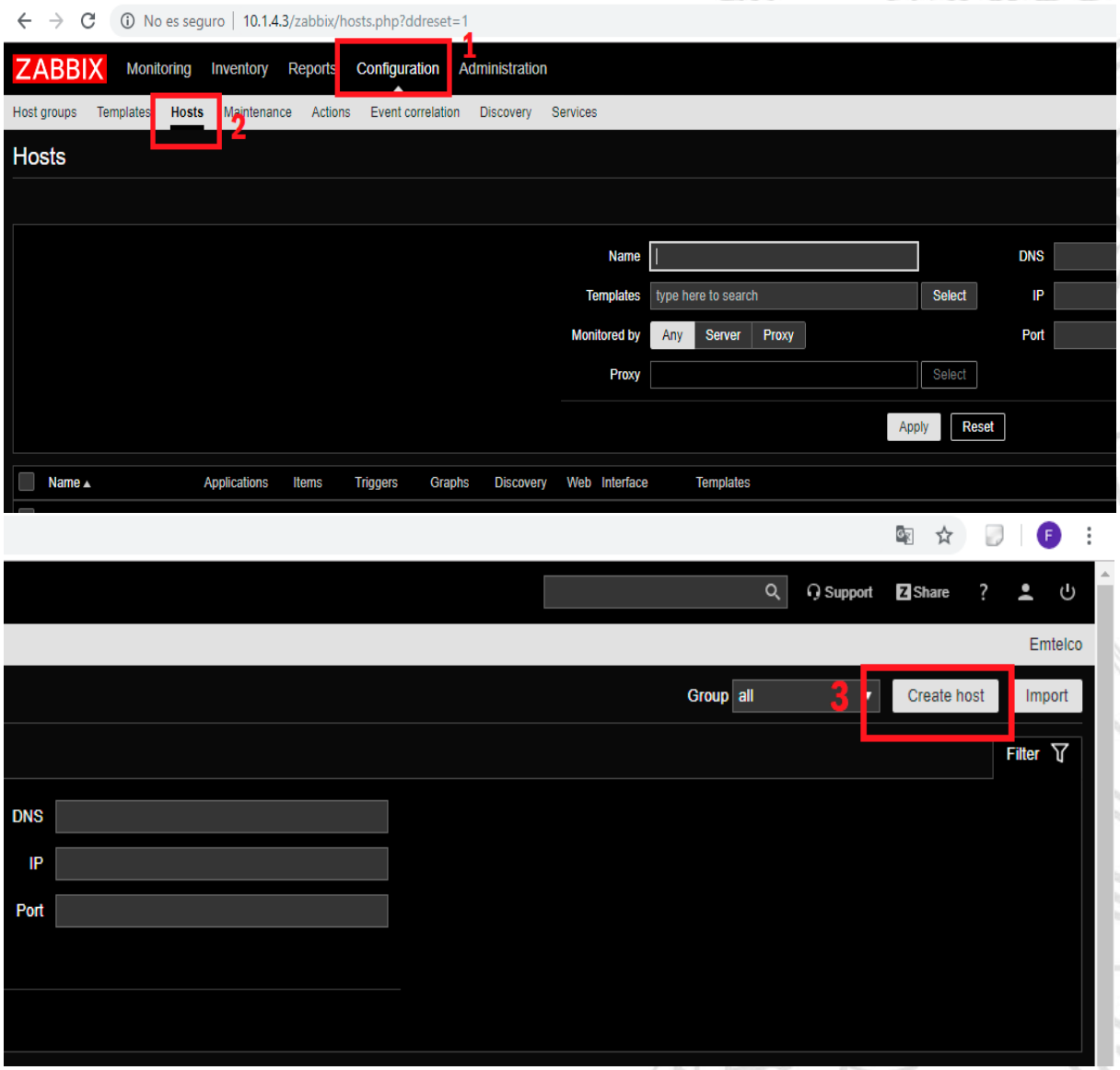


Figura 22. Creación de un host en zabbix (1).

Como segundo procedemos a colocar la información básica del host

1. Llenamos los campos que nos aparecen. En host name colocamos un nombre a nuestro host.
2. En groups seleccionamos un grupo de acuerdo al equipo que se va a monitorear, en nuestro caso seleccionamos Linux Server o Windows Server, según el sistema operativo del host. (También podemos crear nuestros propios grupos en la pestaña host groups)
3. En agent interfaces seleccionamos la opción remove.
4. En la opción SNMP Interfaces seleccionamos Add.
5. Colocamos la IP del servidor a monitorear.
6. Finalmente damos click en la opción Add en la parte de abajo.

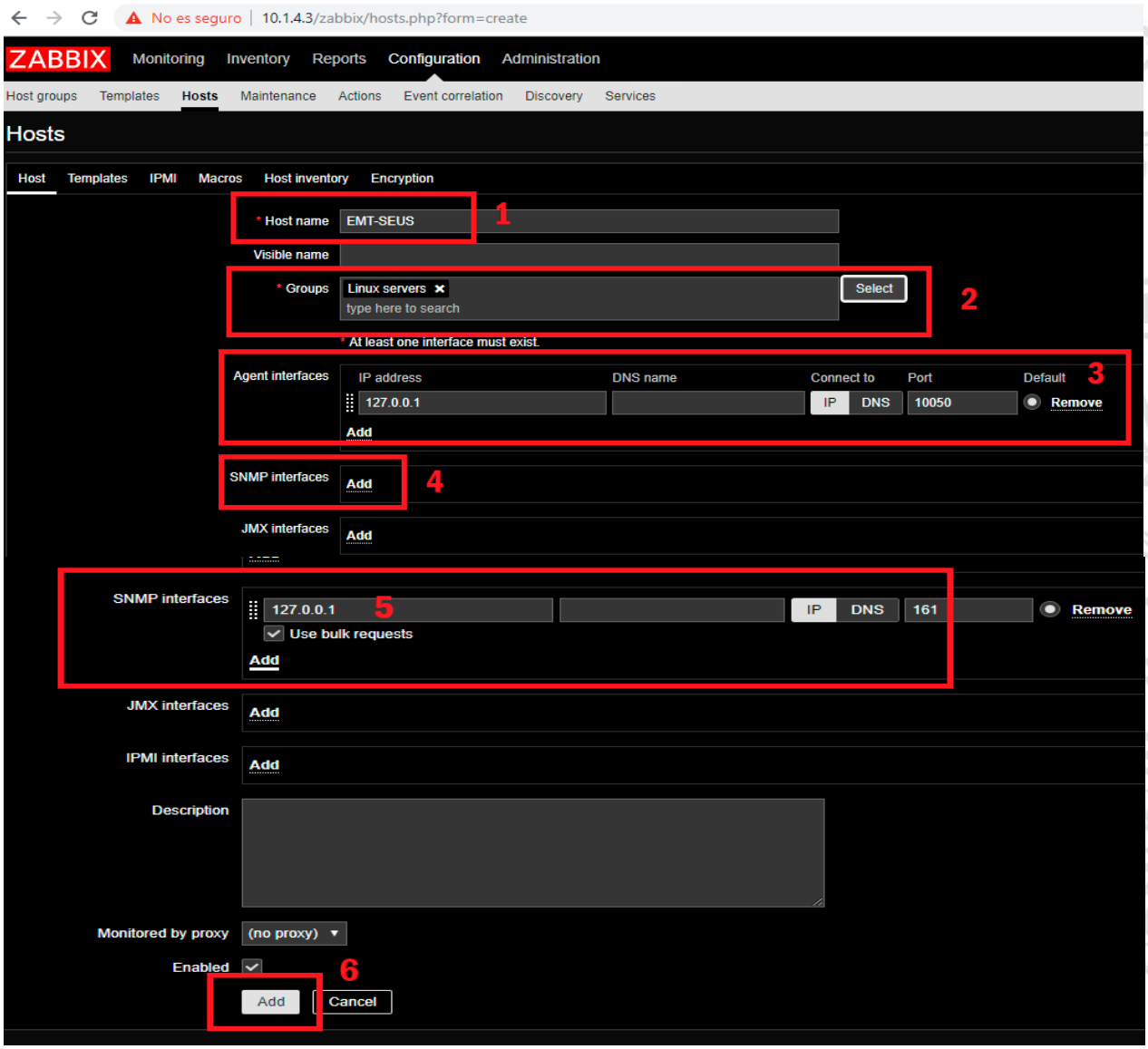


Figura 23. Creación de un host en zabbix (2).

8.1.1.1.2 Agregación de la comunidad.

1. Damos click en el host creado.
2. Seleccionamos la opcion Macros.
3. Colocamos las lineas {$SNMP_COMMUNITY} y al frente la comunidad 3mt3lc0 en este caso.
4. Seleccionamos la opcion Add y luego Update.

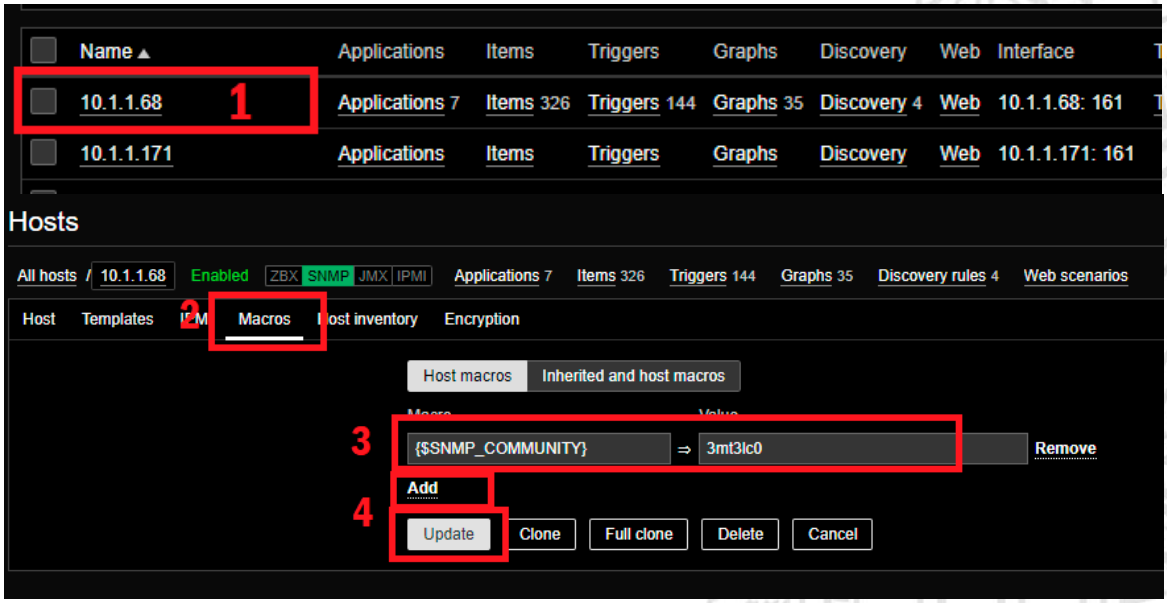


Figura 24. Adicionando la comunidad en un host.

8.1.1.1.3 Agregación de una plantilla de monitoreo.

1. Para agregar una plantilla, damos click en el servidor, luego en template.
2. Seleccionamos una de las plantillas en uestro caso seleccionamos una de Sistema Operativo para SNMP, Template OS Linux SNMP v2.
3. Damos click en Add y luego en Update.

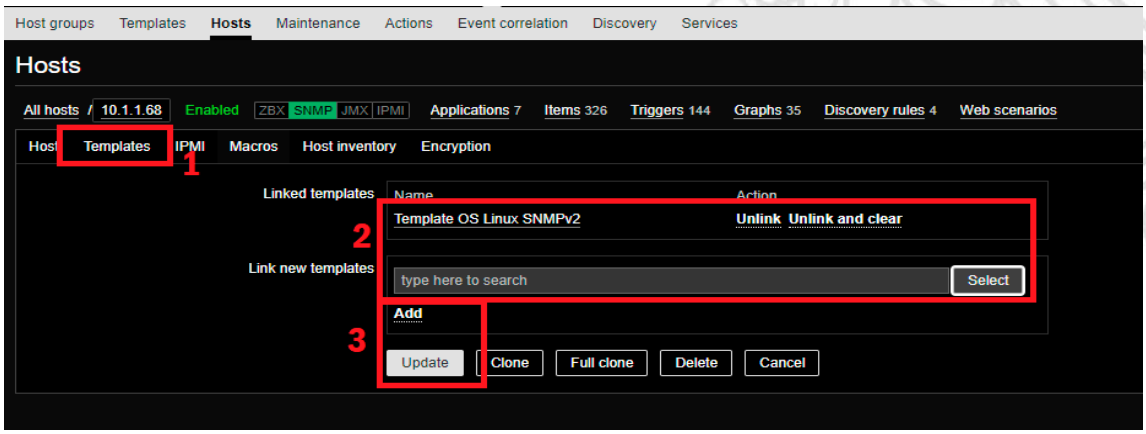


Figura 25. Creación de una plantilla de monitoreo.

Apéndice E

Configuración de notificaciones vía Email en Zabbix.

Lo primero que debemos hacer es ingresar a la plataforma como usuario administrador, como se mostró antes; luego en el panel de navegación ingresamos a l parte "*Administración*" y luego a "*Media Types*".

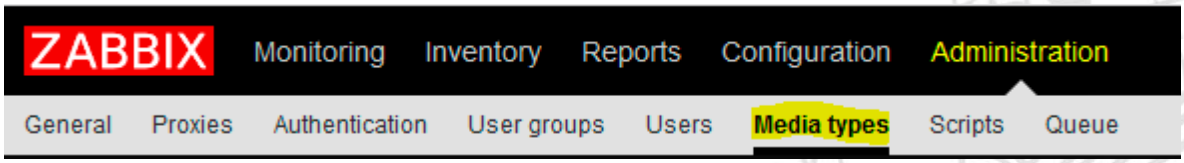


Figura 26. Configuración notificaciones vía email (1).

Una vez ahí seleccionamos la casilla "*Email*" en la lista de despliegue en la parte de debajo de zabbix.

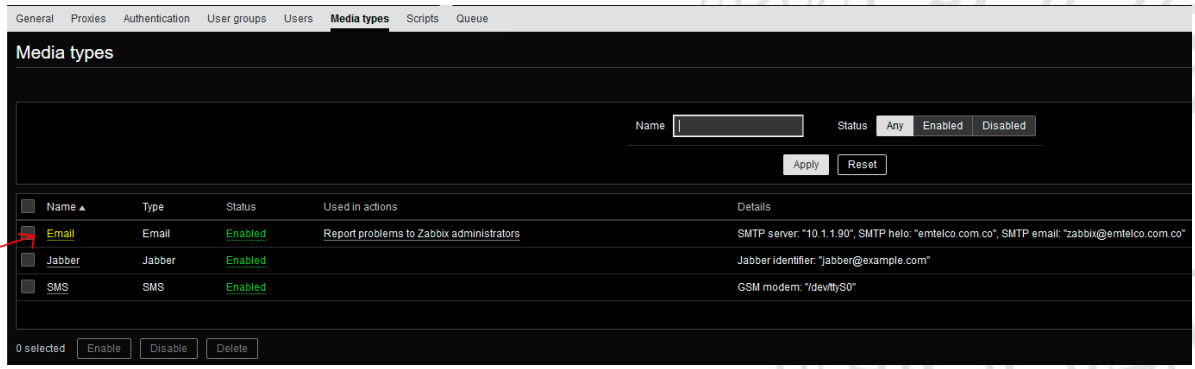


Figura 27. Configuración notificaciones vía email (2).

En el apartado de "Media Types" configuramos "Media Type", de la siguiente manera:
Name: Email
Type: Email
SMTP server: 10.1.4.3 (La Dirección IP que estemos usando en el servidor)
SMTP server port: 25
SMTP helo: Emtelco.com.co
SMTP email: Zabbix@emtelco.com.co (Se debe crear el buzón zabbix)
Los demás en "NONE", y la última casilla ENABLE, deben estar activada y seleccionamos UPDATE.

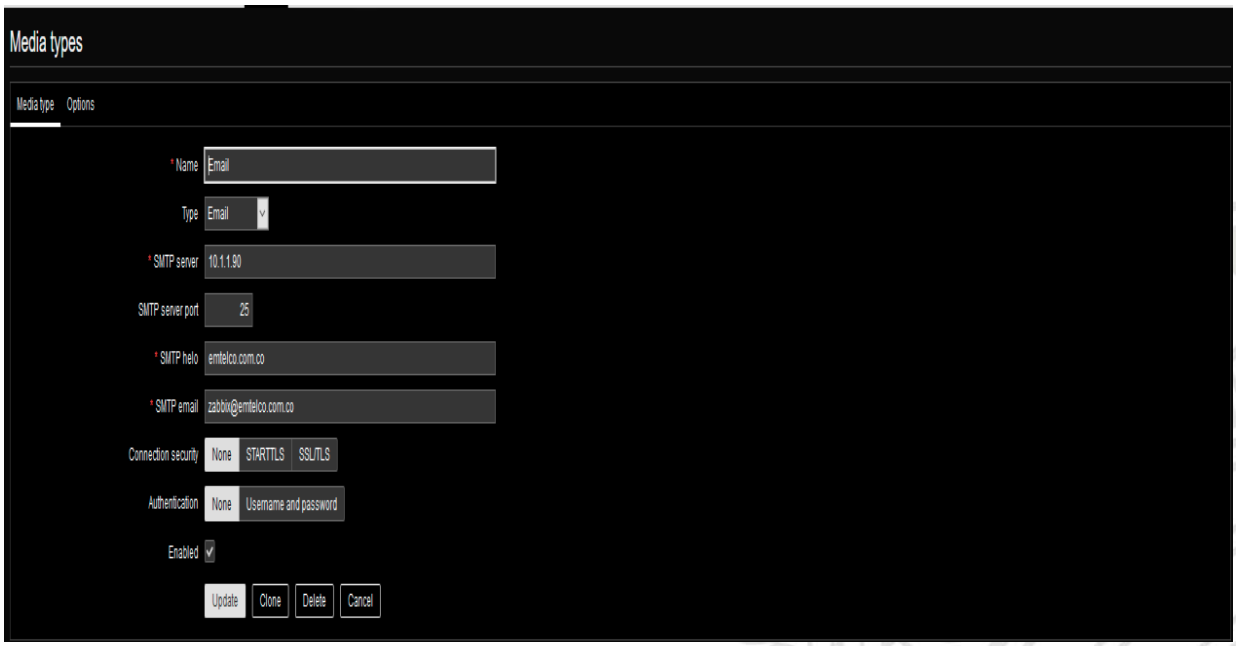


Figura 28. Configuración notificaciones vía email (3).

Luego vamos nuevamente al panel e ingresamos otra vez a “Administration” pero esta vez vamos a ir al apartado “Users”.

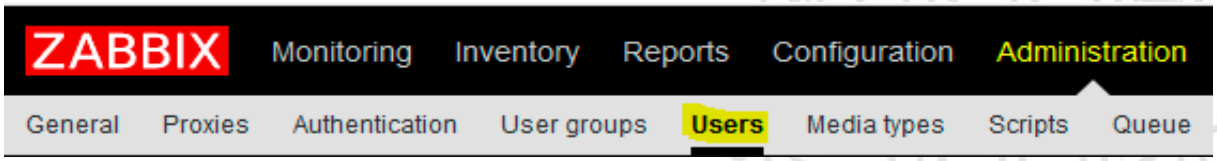


Figura 29. Configuración notificaciones vía email (4).

Se abrirá la siguiente ventana, aquí seleccionar al usuario (en este caso “Admin”), e ingresar a él, dando click sobre él.

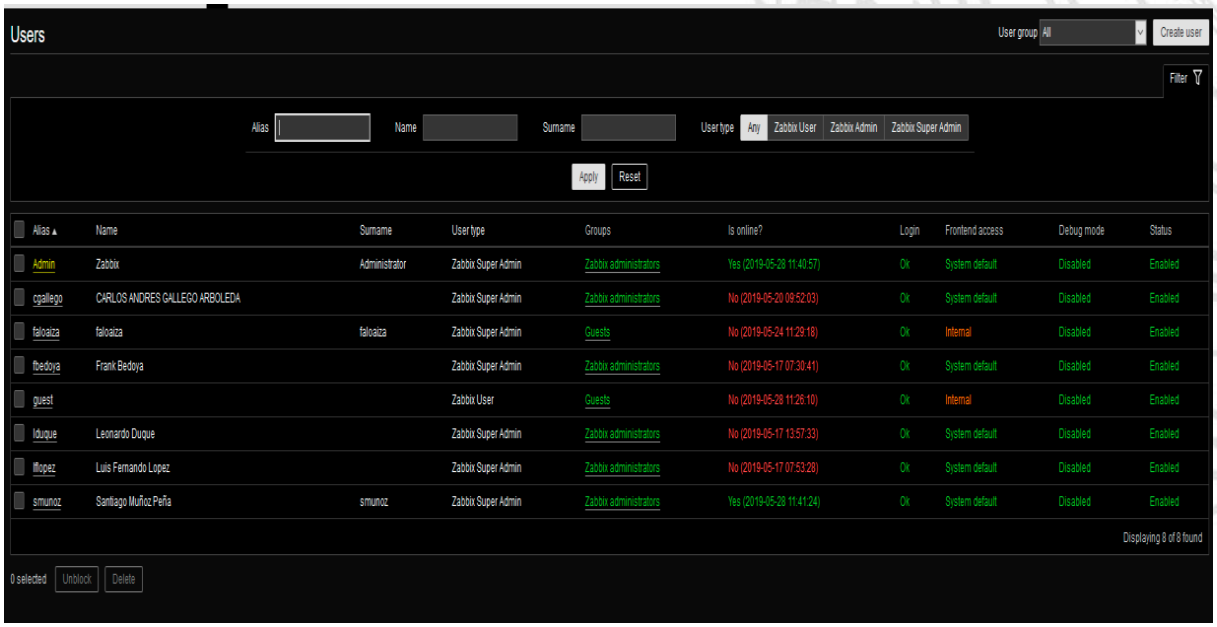


Figura 30. Configuración notificaciones vía email (5).

Al realizar este paso nos abrirá la siguiente ventana, aquí debemos ingresar al apartado “Media”, el cual se encuentra como segunda opción en el lado superior izquierdo.

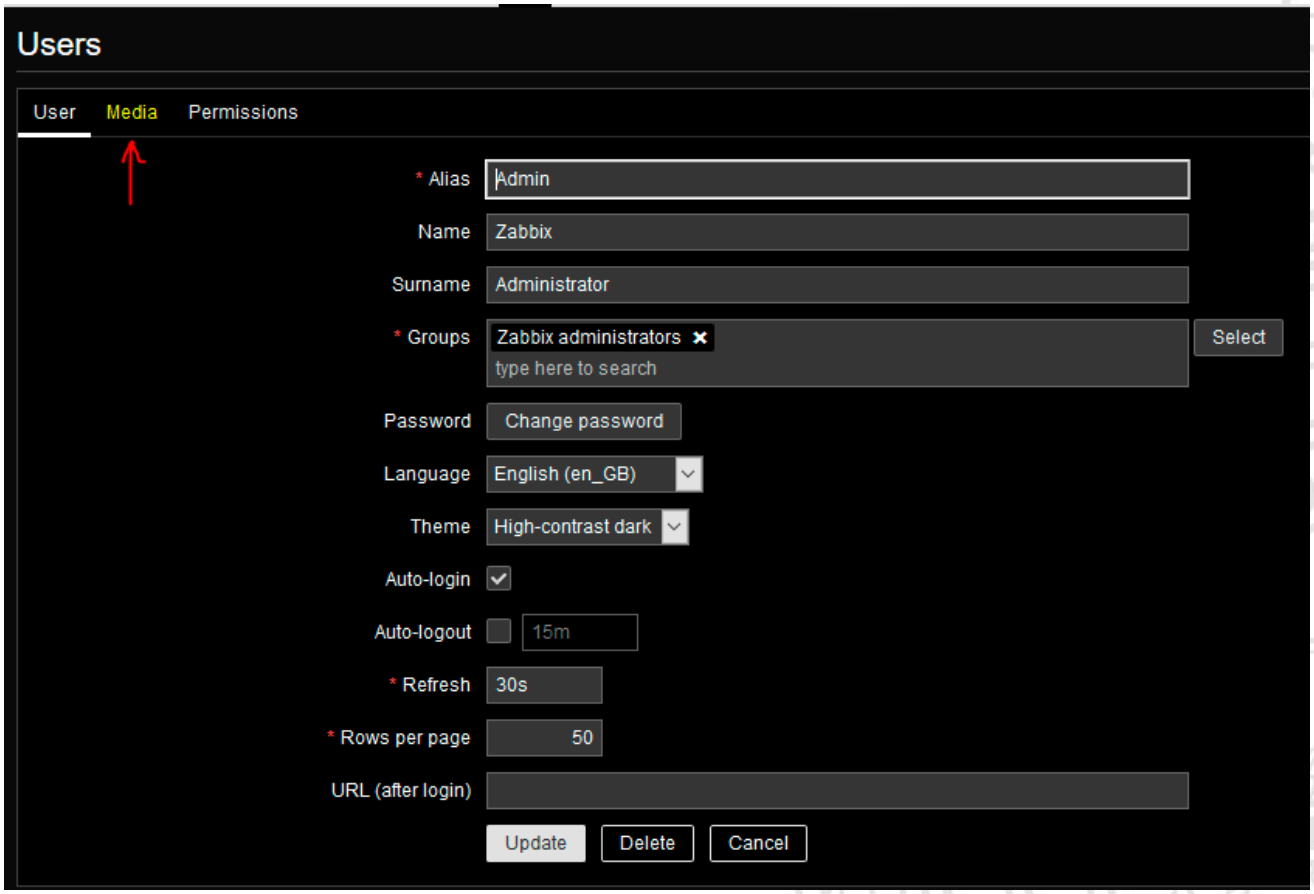


Figura 31. Configuración notificaciones vía email (6).

Después de estar en “Media”, damos click sobre “ADD” o agregar, para añadirle a nuestro usuario una dirección de correo en la cual notificar.
En Type” debe seleccionarse “Email”, en “Send to” agregamos lo usuarios a quien se enviara la notificación, en este caso ponemos los emails de Fabio Gaviria practicante realizador del proyecto y de Gabriel Álzate Asesor externo del proyecto; y en “Use if severity” se marcan todas excepto “Not classified”. “ENABLED” debe estar activada y luego en “Add”.

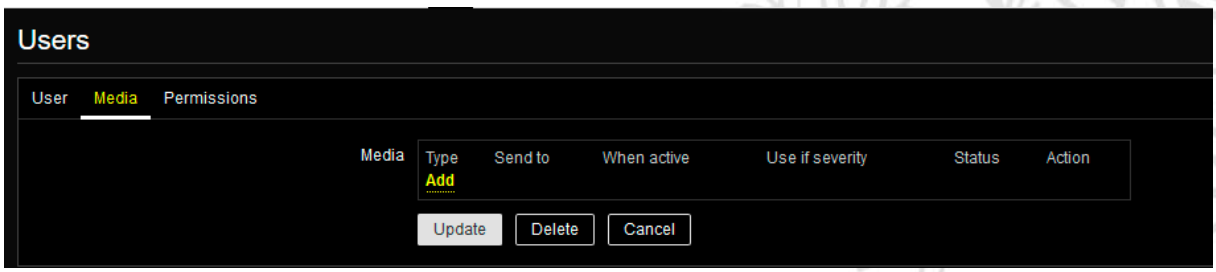


Figura 32. Configuración notificaciones vía email (7).

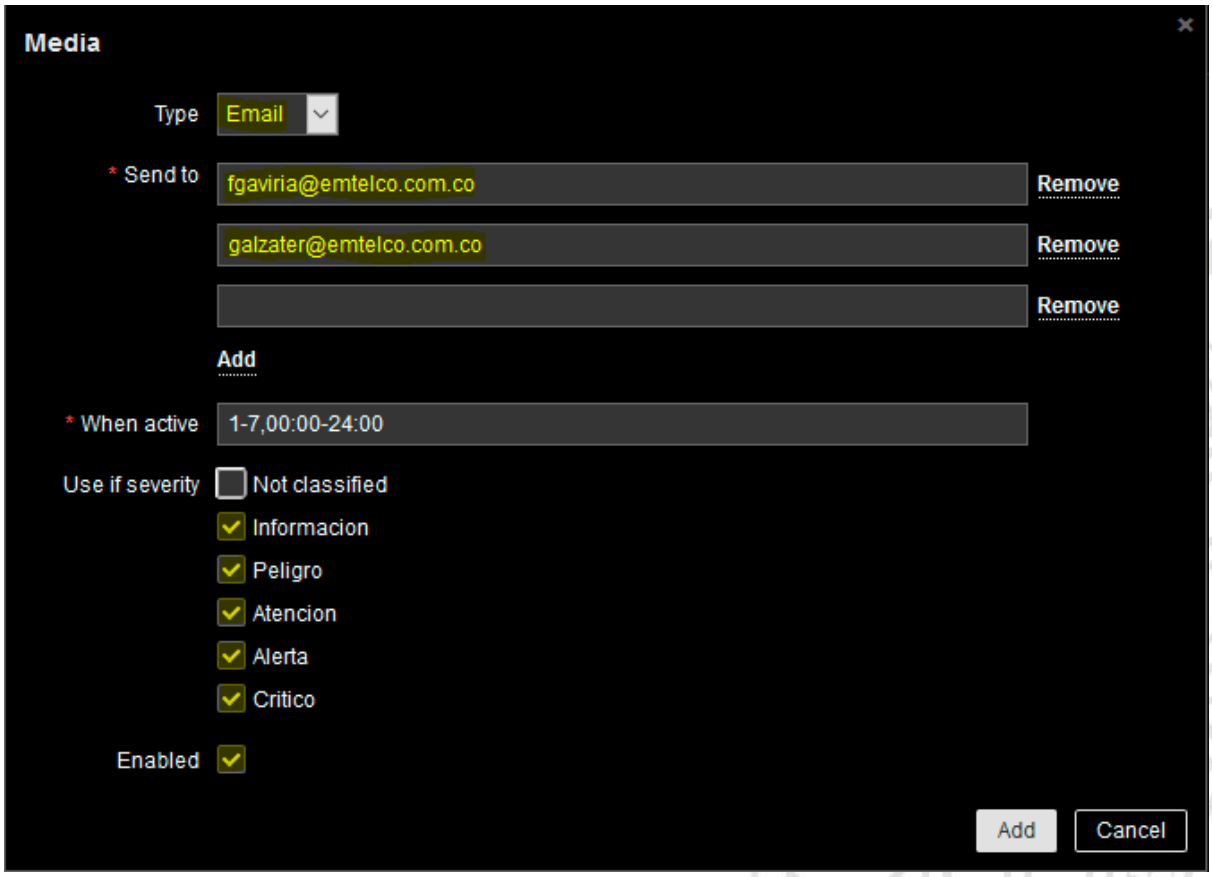


Figura 33. Configuración notificaciones vía email (8).

Ahora procedemos a actualizar dando click en “Update”.

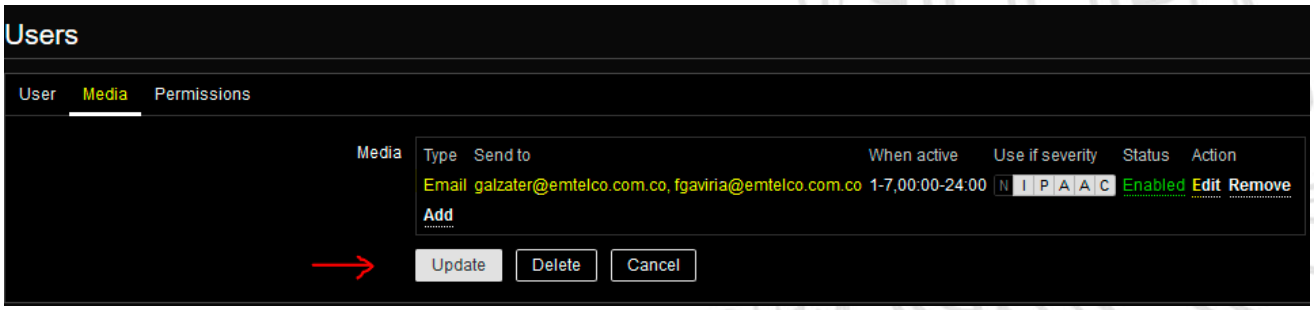


Figura 34. Configuración notificaciones vía email (9).

Volvemos al panel e ingresamos a “Configuration” y luego a “Actions”.

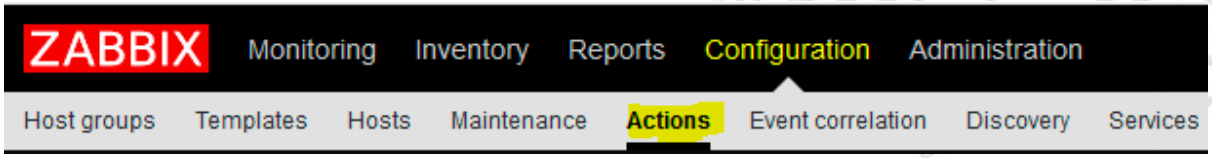


Figura 35. Configuración notificaciones vía email (10).

Acá realizamos lo siguiente, en el lado superior derecho, hay un apartado que se llama “Event Source”, se debe buscar la opción “Triggers”. Debe aparecer la columna: “Report problems to Zabbix administrators”. En esta misma columna el “Status” debe estar “Enabled”. Ingresamos ahora a “Report problems to Zabbix administrators”

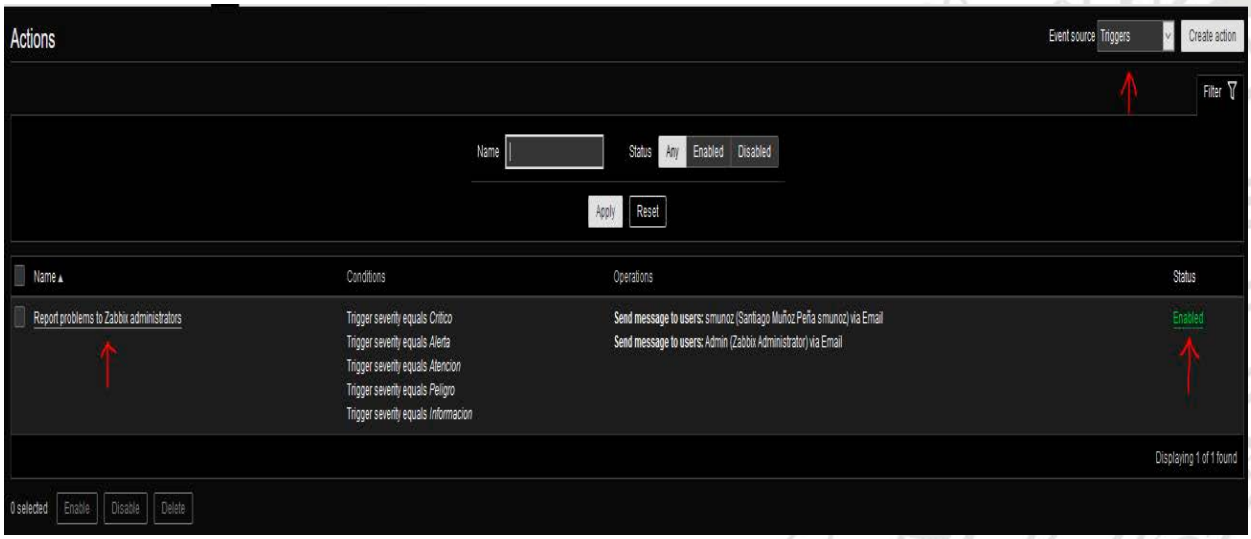


Figura 36. Configuración notificaciones vía email (11).

Después de ingresar a “Report problems to Zabbix administrators” en la primera opción de la parte superior izquierda “Action”, vamos a el apartado “New Condition” y seleccionamos, “Trigger Severity”

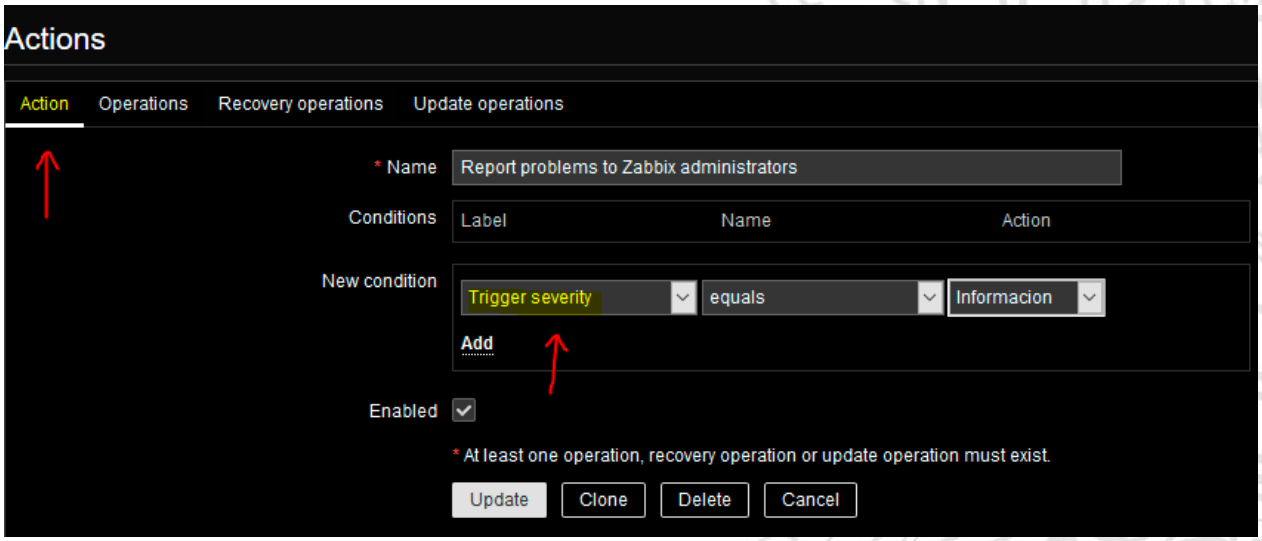


Figura 37. Configuración notificaciones vía email (12).

Ahora, vamos a agregar las condiciones en las cuales el programa va a notificar los problemas relacionados con las Devices, en este caso, agregamos todas, menos la que indica “Not Classified”. Esto se debe hacer agregando una a una y seleccionándolas en “Add”, para que se guarden en “Conditions”, cuando terminemos de agregar todas hacemos click, en el apartado “Operations” en la parte superior izquierda es la segunda opción.

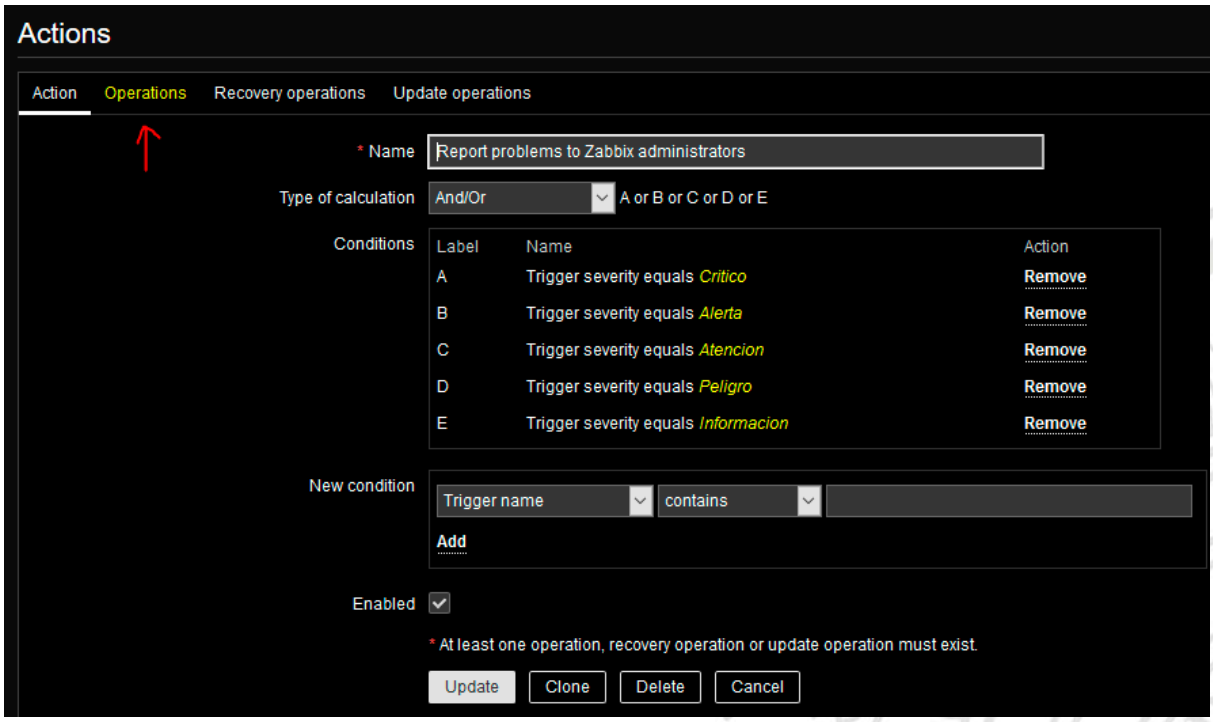


Figura 38. Configuración notificaciones vía email (13).

Una vez dentro de "Operations", vamos a el apartado "Operations" y clickeamos en "New"

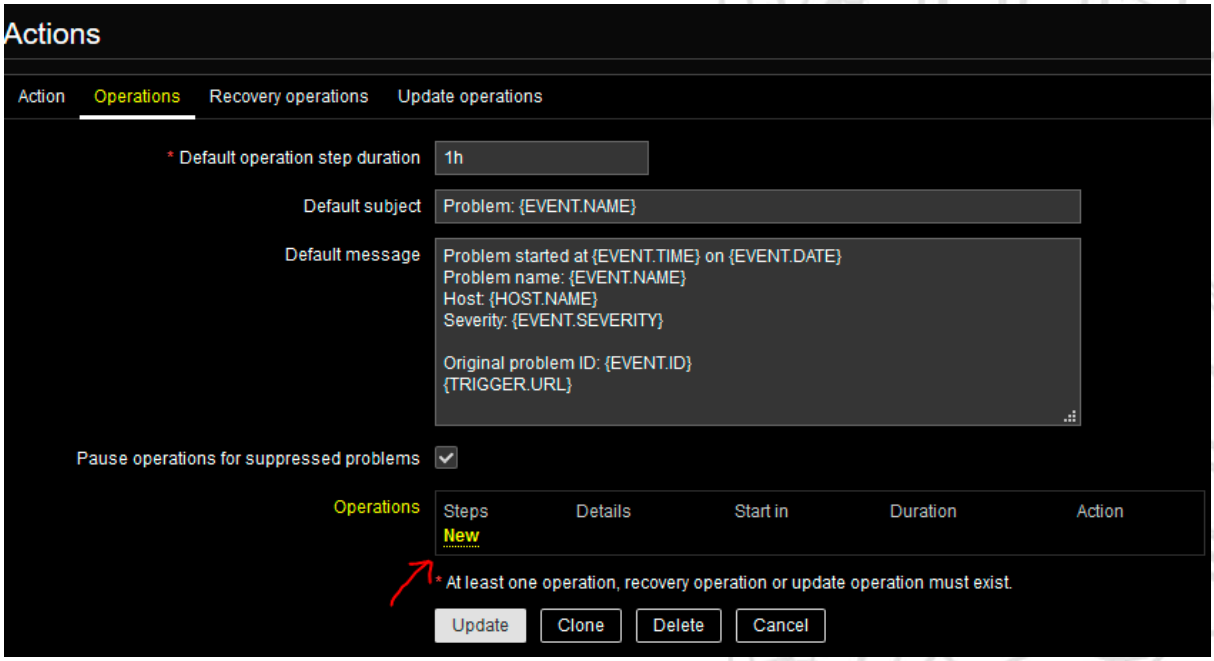


Figura 39. Configuración notificaciones vía email (14).

En la ventana que se nos abre en "New", seleccionamos "Operation Type", elegimos "Send Message"; en "Operation details" debe elegir si se envía las notificaciones a un Usuario o un grupo, en este caso se agrega un usuario; Seleccionamos "Add" para agregarlos y clickeamos en "Recovery Operations"

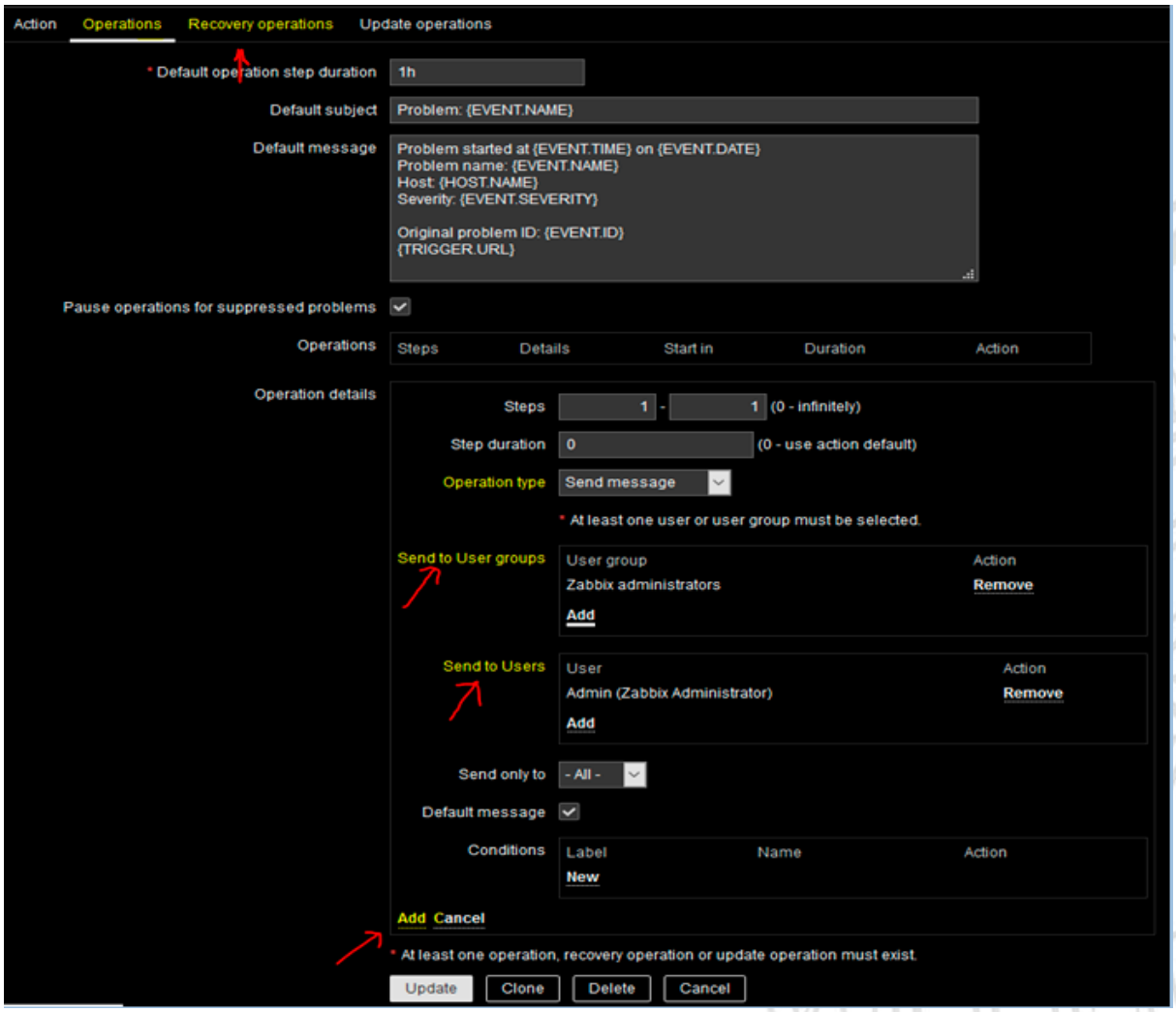


Figura 40. Configuración notificaciones vía email (15).

Ahora, al clickear “Update” nos enviara directamente a el apartado Actions” Que debe aparecer con la configuración de la siguiente manera.

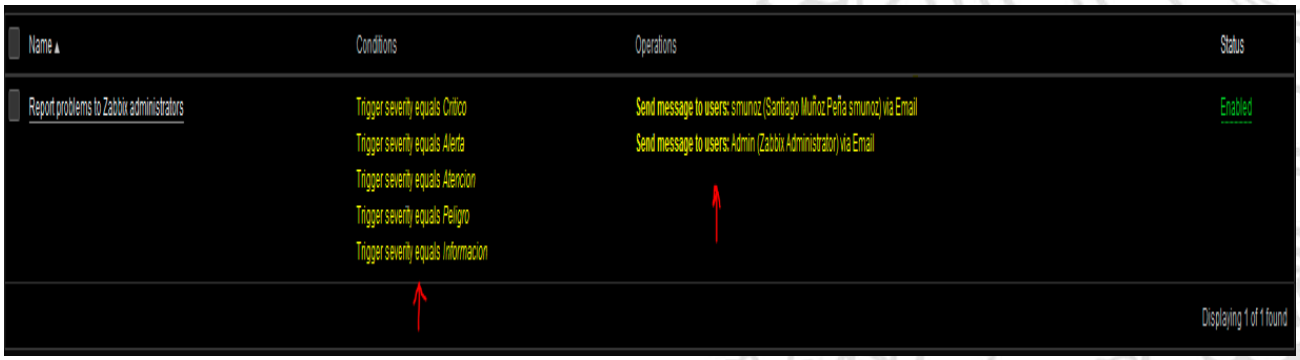


Figura 41. Configuración notificaciones vía email (16).

Apéndice F

Informe de monitoreo de la herramienta Zabbix.

Figura 42. Pantalla de primer inicio.

Como es el primer inicio del sistema debemos tener en cuenta que todo el siguiente apartado debe estar Ok, y en color verde.

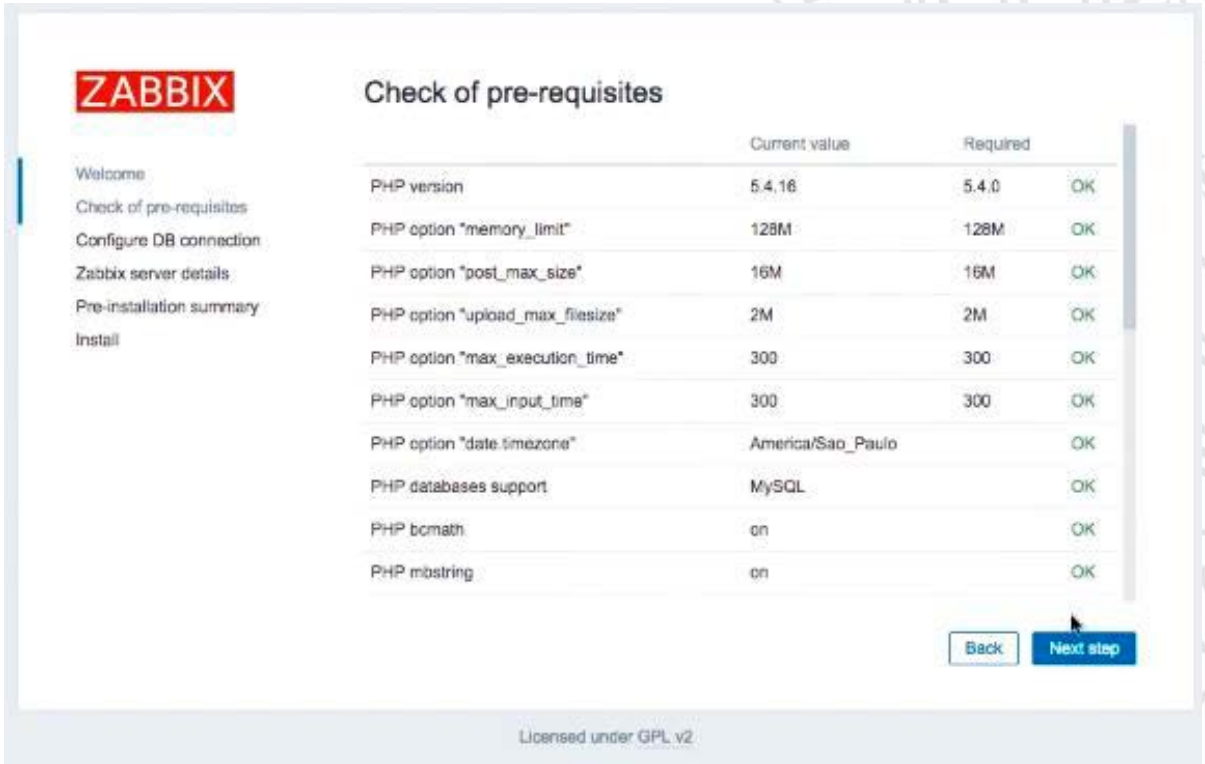


Figura 43. Pantalla de validación de Instalación de zabbix.

Iniciamos con el usuario y contraseña que colocamos en los pasos anteriores.

Figura 44. Pantalla de conexión con la base de datos Mysql.

Ahora agregamos el nombre de la organización y damos click en next step.

Figura 45. Pantalla de configuración de nombre y puerto.

Ahora realizamos la comprobación final de zabbix y nuevamente damos click en siguiente paso.

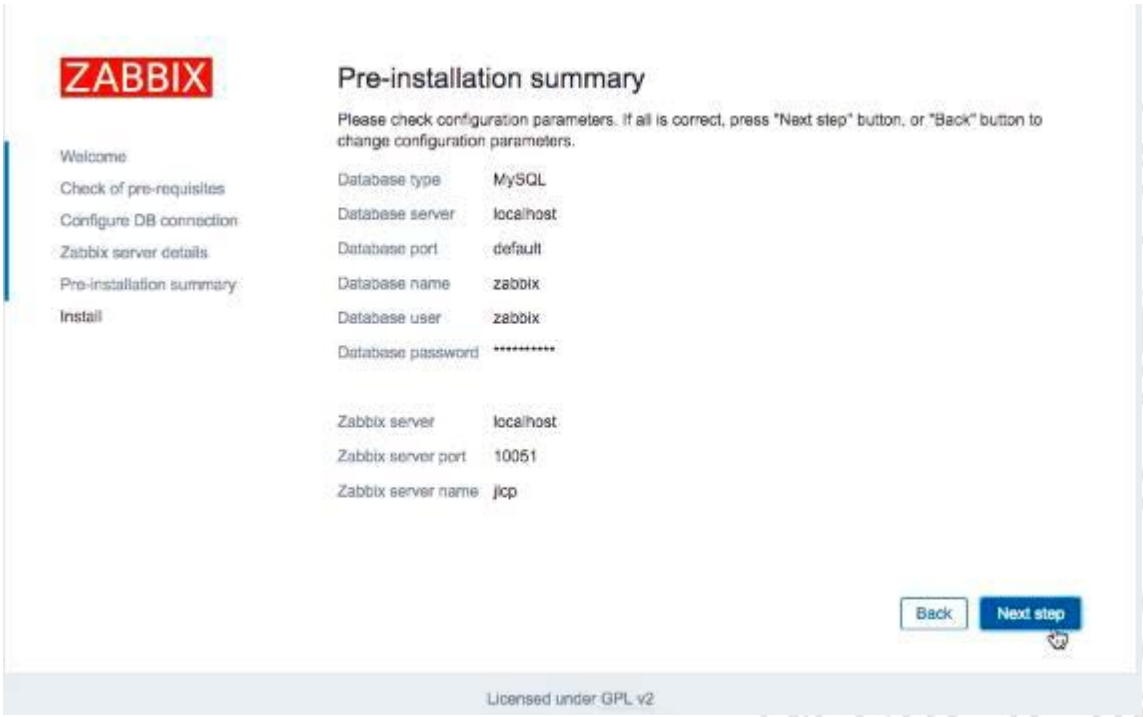


Figura 46. Pantalla de comprobación de la pre-Instalación.

Luego de este paso nos debe mostrar la interfaz de ingreso, donde el ingreso por defecto es:

User: Admin.
Password: zabbix.

Figura 47. Pantalla de Inicio de zabbix.

En este punto debe verse la dashboard de Zabbix, pero aún no está monitoreando nada, ya que el servicio y el agente están apagados.

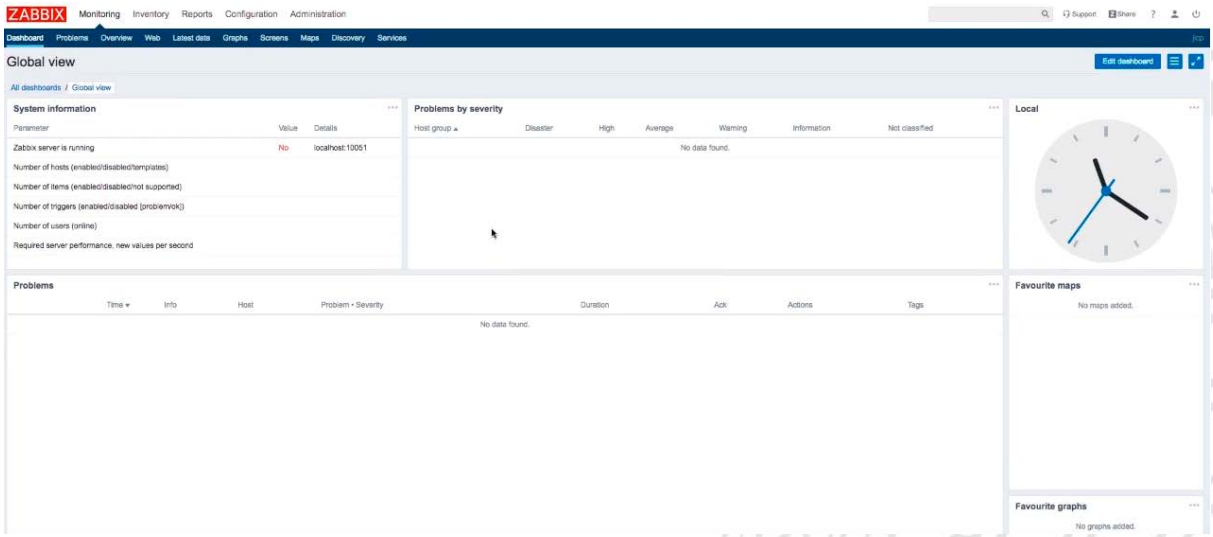


Figura 48. Pantalla de la dashboard de zabbix.

Ahora procedemos con la activación de Zabbix, para esta parte debemos ingresar al servidor de Zabbix, y teclear los comandos que se indican a continuación, se anexa imagen de la pantalla al momento de realizar el procedimiento.

Con el comando: systemctl start zabbix-server, iniciamos el servidor.

```
[root@localhost zabbix-server-mysql-4.0.0]# systemctl start zabbix-server
```

Con el comando: systemctl enable zabbix-agent, dejamos disponible el agente del servidor, el cual solo se instala en este servidor, para monitorear los demás servidores usaremos el protocolo SNMP.

```
[root@localhost zabbix-server-mysql-4.0.0]# systemctl enable zabbix-agent
```

Con el comando: systemctl start zabbix-agent, activamos el agente.

```
[root@localhost zabbix-server-mysql-4.0.0]# systemctl start zabbix-agent
```

Usamos el comando systemctl status zabbix-agent, para validar lo realizado.

```
[root@localhost zabbix-server-mysql-4.0.0]# systemctl status zabbix-agent
● zabbix-agent.service - Zabbix Agent
   Loaded: loaded (/usr/lib/systemd/system/zabbix-agent.service; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2018-10-02 23:21:17 -03; 4s ago
  Process: 1848 ExecStart=/usr/sbin/zabbix_agentd -c $CONFFILE (code=exited, status=0/SUCCESS)
 Main PID: 1850 (zabbix_agentd)
```

Y con esto deberíamos ingresar a zabbix mostandonos el monitoreo funcional.

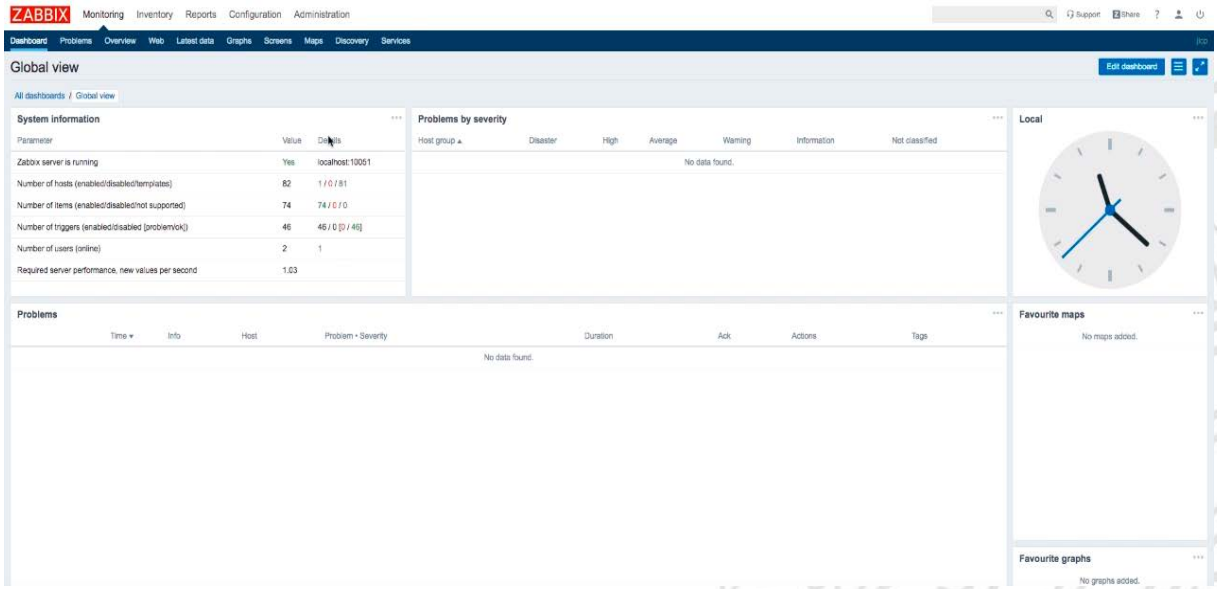


Figura 49. Pantalla de monitoreo del servidor principal de zabbix.