Universidad Autónoma Metropolitana-Azcapotzalco
División de Ciencias Básicas e Ingeniería
Licenciatura en Ingeniería en Computación

Sistema de monitoreo de una Red Corporativa para dispositivos compatibles con SNMP

Estancia Profesional

Trimestre 2018 Invierno
30 de marzo de 2018

Uriel Joshua Estrada Padilla
2143033294

M. en C. José Alfredo Estrada Soto

Ing. Mario Ernesto Gómez Romero

Yo, José Alfredo Estrada Soto, declaro que aprobé el contenido del presente Reporte de Proyecto de Integración y doy mi autorización para su publicación en la Biblioteca Digital, así como en el Repositorio Institucional de UAM Azcapotzalco.

M. en C. José Alfredo Estrada Soto

Yo, Mario Ernesto Gómez Romero, declaro que aprobé el contenido del presente Reporte de Proyecto de Integración y doy mi autorización para su publicación en la Biblioteca Digital, así como en el Repositorio Institucional de UAM Azcapotzalco.

Ing. Mario Ernesto Gómez Romero

Yo, Uriel Joshua Estrada Padilla, doy mi autorización a la Coordinación de Servicios de Información de la Universidad Autónoma Metropolitana, Unidad Azcapotzalco, para publicar el presente documento en la Biblioteca Digital, así como en el Repositorio Institucional de UAM Azcapotzalco.

Uriel Joshua Estrada Padilla

Índice.

Índice de Figuras.

Índice de Tablas.

Formato del CD.

Este documento únicamente incluye el Reporte de Proyecto Terminal, anexo al CD, también se encontrarán 3 archivos que corresponden a los anexos, que, sirven como material entregable como se había comprometido en la Propuesta de Proyecto Terminal.

Dedicatoria.

Te lo prometí de niño, luché día a día, me esforcé y di lo máximo en cada etapa de mi vida, hice muchas promesas conmigo mismo, compromisos para que llegaras a este día tan importante conmigo.

No sé en qué momento fallé, pero sé que en donde quiera que estés siempre me estarás cuidando, siempre estarás orgulloso de mí, como lo estás de toda la familia que tú forjaste y nos heredaste, esa familia que tanto me gusta presumir, que tanto me gusta decir "Por él somos quien somos", no me alcanzarían las gracias para terminar de agradecerte todos los valores y amor que inculcaste en mi padres, en mis hermanos, en mis tíos y tías y en todos mis primos. Porque con cinco días de escuela, creaste una familia de profesores comprometidos con la educación de la sociedad.

Por eso y por mucho más, te admiro, te extraño y te amo, abuelo.

- José Eleuterio Estrada Martínez (1926 – 2014)

Los cimientos y fortalezas que nos dan los padres surgen de todas las bases que fueron inculcadas por los abuelos, tengo el gusto de poder contar con todo lo necesario para llegar a este punto y para salir adelante en la vida y mucho de ello es gracias a ustedes, que como pareja me enseñaron a valorar muchos aspectos de ser una mejor persona y que sé que juntos siempre estarán para mí, apoyándome en todas mis decisiones y cuidándome donde quiera que estén.

Cada día que pasa, realmente extraño el amor de abuelos que siempre tuvieron para mí.

- Juan Padilla Figueroa (1942 -2016)
- Osvelia Padilla Andoney Góngora (1943 – 2016)

El tiempo de convivencia realmente no importa, nunca me importó que pudiese verte 3 veces al año, pero el tiempo que tuvimos juntos, el que me enseñaras a valorar lo hermoso del campo, de los animales, a vivir y disfrutar como niño en todo momento, pero siempre cuidándome. Me haces mucha falta en mi vida, en mis vacaciones, y siempre te tendré en mi mente. Te quiero tía.

- Blasa Soto Ávila (1932 – 2009)

La fortaleza de cada ser humano nace y se desarrolla con base en los valores inculcados por lo seres más importantes en la vida de cada individuo, afortunadamente, en mi vida he tenido mucha gente que me ha brindado experiencias, fuerza, amor y cariño para poder llegar lo más lejos posible.

A mis padres, José y Ofelia, los pilares de mi crecimiento, cimientos de mi formación, bases de conocimiento y, sobre todo, mi vida. Por ustedes he llegado hasta aquí y por ustedes llegaré más lejos, los amo.

A mis hermanos *Pepos* y Joyce, la confianza y apoyo que he recibido de ustedes han influido y especialmente, han marcado mi vida para bien.

A mis tías Felisa y Teresa, prácticamente mis otras madres, el cariño, apoyo y confianza que siempre han tenido en mí ha sido tanto que nunca en la vida podré expresarles ni un poco de todo lo que ustedes representan en mi vida.

A la familia Morales Estrada, Martín, Guadalupe, mis otros padres, Osvaldo, Aurea y Aline, mis otros hermanos, que me han recibido en su familia y me han apoyado como uno de ustedes, el agradecimiento que tengo hacia ustedes es infinito, los amo.

A mis tíos Margarito e Isabel, el cariño y respeto hacia ustedes siempre ha sido y será muy grande, gracias por todo.

A mis primos, Adriana, Aurelio, Rodrigo y ahora Fernando, a mi sobrina Regina, por todos los momentos felices que hemos compartido.

A mi tío Pablo, más que un tío, un amigo, en quien sé que podré confiar toda mi vida, quien me enseñó muchas cosas sobre esta y sobre todo que ha marcado quién quiero ser en un futuro.

A mi primo Juan Pablo, mi hermano pequeño, el más rebelde y conflictivo, pero que ha aportado mucho a mi vida, siempre contarás conmigo.

A mi tío Pedro, un camarada, una base sólida en mi formación humana.

A la profesora Silvia González Brambila, mi maestra, coordinadora de carrera, amiga y mi otra madre, con quien he reído y llorado, muchas gracias por ser la persona más interesada en apoyarnos.

A Karla Cuellar, mi mejor amiga, mi confidente, mi hermana, porque siempre has estado ahí, en el momento justo, donde y cuando más te he necesitado, te quiero.

A mi amiga Aimeé, la persona más odiosa, pero que siempre está preocupada por mí, por ti he logrado mucho en mi vida académica, social y personal, gracias por haber llegado a mi vida.

A mi amiga Alejandra, por ti el título de mi portada dice Licenciatura en Ingeniería en Computación, y por eso, la paciencia, la amistad incondicional, los consejos, la sinceridad y confianza que me has tenido y el apoyo que me has brindado en muchas situaciones, te lo agradezco profundamente, te quiero comadre.

A mi amiga Tania, llegaste a mi vida y la marcaste de una forma muy especial, te agradezco todas tus palabras, enojos y consejos. Te admiro por todo lo que has logrado y superado en ti y también en mí, por el poco tiempo que hemos compartido juntos, solamente tú sabes realmente cuanto te adoro.

A mis amigos Jesús, Alejandro, Freddy, Jorge, Aruni, Federico y Mario, por representar el valor de la amistad, las risas y enseñanzas que pudieron compartir conmigo, gracias.

A mis amigas Karla, Andrea, Lupita, Mariel e Iris por los mejores momentos que hemos pasado, confianza y consejos, apoyo y cariño que me han tenido en todos estos años.

A mis amigas Norma y Julia, en tan poco tiempo se han convertido en personas muy especiales en mi vida, muchas gracias por las enseñanzas que me han dado, por los momentos de alegría que tenemos.

A la profesora Margarita Chávez Martínez, mi maestra, mi madre académica, siempre estuvo dispuesta a confiar en mí, en ayudarme y por usted hoy soy una persona con más valores.

A los profesores Cyntia Gómez y Jesús Olivares, profesores y amigos que gracias a su confianza pude elegir el mejor camino para mi formación universitaria.

A mi jefa, Gabriela Del Valle, muchas gracias por aguantarme, por apoyarme, por confiar en mí, por recibirme tan cálidamente al Departamento de Ciencias Básicas, muchas gracias por todo.

A Alejandra, Ismael, Rosy, Alejandrina y Soco, mis compañeros de trabajo, quienes se han convertido día con día en mi familia laboral, les agradezco todo su apoyo.

A los profesores Marco Antonio Gutiérrez Villegas, Josué Figueroa González, Alejandro Cruz Sandoval y Jorge Alfonso Quevedo Martínez, por ser grandes profesores en mi vida académica, por convertirse en mis amigos y tenerme la confianza de que llegaré muy lejos, gracias.

A todos mis profesores de educación básica, media y superior, por desarrollar esta tan importante labor de la docencia, de compartir sus conocimientos para tener una sociedad mejor, en especial, a los profesores Cesareo García Martínez, Alejandro Kunold Bello, Jesús Isidro González Trejo, Rogelio Herrera Aguirre, Víctor Cuauhtémoc García, Samuel Alcántara Montes, Judith Araos Hernández, muchas gracias y admiraciones.

Resumen

Este trabajo presenta todas las actividades realizadas sobre el proyecto asignado y que está basado en el software de monitoreo Zabbix, el cual se instaló la versión más reciente que es 3.4.1 y el monitoreo fue a través de los protocolos ICMP y SNMP versión 2, utilizando herramientas de ayuda como son los *proxies* en distintos equipos como *firewalls*, *router*, *Switch* y computadoras. Todas las actividades de monitoreo se realizaron a través de un entorno de máquina.

Objetivos

1. Objetivo General

   - Diseñar e implementar un sistema para el monitoreo de una red corporativa a través del Protocolo Simple de Administración de Red (SNMP).

2. Objetivos Particulares

   - Diseñar e implementar un módulo para el envío de alertas vía correo electrónico.
   - Diseñar e implementar un módulo de monitoreo que aplique dos técnicas de monitorización basadas en las políticas de seguridad de red de la empresa.
   - Diseñar e implementar un modelo de solicitud de información a los dispositivos que tengan habilitado el protocolo SNMP.

Introducción

Hoy en día, Internet ha llegado a ser para las empresas una herramienta de trabajo que les permite generar ganancias económicas. Por ello, la protección a las redes que tales empresas manejan es una tarea prioritaria.

El empleo de sistemas para el monitoreo de redes facilita a los administradores de estas la búsqueda y detección de aquellos componentes de red tales como computadoras, *Switch, router,* teléfonos ip, entre otros, que no cumplan con su especificación. Por ello, el monitoreo de una red corporativa puede ayudar a prevenir las caídas del servicio de internet o, en el peor de los casos, cuando ocurre un siniestro, ayuda a identificar por qué ha ocurrido; esto se traduce en la minimización de pérdidas económicas por la ausencia de esta herramienta llamada internet. La realización de un buen monitoreo depende en gran medida del software a emplear, de las políticas de seguridad diseñadas por y para la empresa y de las acciones a tomar de acuerdo con los problemas considerados en las políticas de seguridad.

Zabbix es un software que permite el monitoreo de una amplia cantidad de equipos y cuenta con características tales que lo hacen ideal para ser empleado en redes corporativas. Además, cuenta con una particularidad que comercialmente lo hacen atractivo: es un software código abierto.

En este proyecto, se propone el diseño e implementación de un sistema que permita asegurar el buen funcionamiento de una red corporativa mediante su monitorización con base en la implementación y administración de un servidor Zabbix en un ambiente CentOS 7 de Linux. Adicionalmente se contempla la creación de políticas de seguridad aplicados tanto al *software* como a aquellos dispositivos y elementos de red. Para ello se emplearían, entre otros protocolos, el Protocolo Simple de Monitoreo de Red (SNMP) en sus tres distintas versiones.

Justificación

Aquellas empresas en México que diariamente utilizan internet como una herramienta laboral para obtener ganancias económicas, tales como los bancos o corporativos que ofrecen servicios de facturación, atención al cliente y soporte técnico vía remota, no pueden permitirse tener una interrupción de este servicio debido a las pérdidas económicas que se pueden generar.

En muchas ocasiones, el proveedor del servicio de internet no es el culpable ya que pueden existir un sinnúmero de razones que pueden provocar fallos en dicho servicio, por ejemplo, dispositivos de red dañados, saturación del servicio, entre otros.

Por esta razón, es necesaria la realización de un monitoreo de la red corporativa de manera tal que permita al administrador, con base en las políticas de seguridad de la empresa, el diagnóstico oportuno para actuar lo más pronto posible en la presencia de factores de riesgo en materia de redes.

Antecedentes

El Protocolo Simple de Administración de Red (SNMP) es el principal encargado de solicitar y mostrar la información de los equipos deseados, pero a nivel macro, es decir, en una red corporativa el aplicar una sentencia por cada elemento de cada dispositivo no es para nada práctico.

Actualmente existen diversas herramientas y programas de monitoreo que funcionan de forma local, es decir, el dispositivo encargado de monitorear debe estar en la misma red. Teniendo esta limitante, hay que añadir que los costos de licenciamiento son costos en su mayoría.

Zabbix, al ser un software gratis y que continuamente se sigue innovando con actualizaciones que mejoran y atacan las necesidades de una empresa.

Con base en los Proyectos Terminales consultados se pudo innovar ya la parte de monitoreo de Red en un software que utiliza las diferentes versiones del SNMP y escalarlo a un monitoreo indirecto, es decir, a través de un servidor proxi.

Marco Teórico

Zabbix es un software diseñado para el monitoreo en tiempo real, es de código abierto y totalmente gratuito, lo que es un gran diferenciador en comparación con otros softwares como N-Top que sus licencias se disparan hasta los 500 euros con solamente un año de actualizaciones.

A nivel mundial Zabbix ha tenido un gran auge en países como Inglaterra, Rusia, China, Brasil principalmente, por lo que la presencia de este software en México no ha sido tan reveladora por lo que el comenzar a utilizarlo sería una gran herramienta que se propondría a empresas para seguir colaborando al desarrollo tecnológico y la expansión de Zabbix.

1. Servicios de Zabbix.

Zabbix además ofrece un excelente servicio de graficación sobre los parámetros de monitoreo y guarda esta información el tiempo que el usuario desea, e incluso dentro de una gráfica se pueden varios parámetros que pueden ser comparados dependiendo de las necesidades que se tengan. Su vista puede ser incrementada desde rangos de 5 minutos hasta la vista de 1 año, lo que al momento del análisis ayuda mucho el rango de tiempo que se desea analizar.

Además, incluye un sistema de alertas que hay configurar, Zabbix maneja sistemas de alertas a través de correo electrónico, sistema de mensajes SMS, o aplicaciones que incluyan las de un sistema de mensajes como Telegram.

Por defecto, Zabbix incluye plantillas de monitoreo de todos los protocolos que soporta, estos no son tan especializados ya que cada proveedor brinda objetos de monitoreo específicos para cada dispositivo. Sin embargo, se pueden crear distintas plantillas a gusto del usuario y con los objetos que requiera. Una plantilla consta de aplicaciones, ítems, disparadores (*Triggers),* Ítems Dinámicos (*Discovery Rules),* y gráficas.

a) Ítems

Estos son los encargados de realizar las tareas de monitoreo para los cuales son creados, son creados de manera manual por el administrador o bien por algún ítem dinámico.

b) Disparadores (*Triggers*)

Estos disparadores, notifican cuando ciertas condiciones sobre los resultados que obtienen los ítems se cumplen y envían alertas tanto al panel principal como al sistema de alertas que se tenga configurado, dependiendo del grado de alerta. Existen 4 distintos grados de alerta (Nulo, medio, alto, muy alto) el administrador configura en que nivel de alerta se activan estos disparadores. Todas estas alertas se realizan a través de expresiones regulares.

c) Ítem dinámicos (*Discovery Rules*).

Este tipo de ítems se activan a través de *Scripts* que se hayan creado directamente en Zabbix o se hayan agregado a la carpeta de *Scripts* externos en el servidor donde se instaló Zabbix. Su función es aplicar un código basado en PHP para cargar ciertos ítems con datos específicos, como pueden ser nombres de interfaces o bien para agregar una gran cantidad de ítems de forma automática. Así mismo es posible agregar disparadores y gráficas automáticamente.

El panel principal desde la versión 3.4.0 puede ser modificado a gusto del administrador, colocar las gráficas de interés e incluye un panel donde se visualizan todas las alertas que se han tenido en orden cronológico descendente, las alertas que no se han atendido y las que ya se han rescatado, dando una visión general de todo lo que el servidor Zabbix se encuentra monitoreando, recalcando que ahora el administrador decide que ver.

Finalmente, existe una sección de reportes, la cual almacena en orden cronológico descendente únicamente todos los problemas que se han tenido y pudiendo desplegar los detalles de que ha pasó.

2. Protocolo ICMP y SNMP

2.1. **I**nternet **C**ontrol **M**essage **P**rotocol

Es un protocolo que se utiliza para la verificación de errores de comunicación entre dispositivos que se encuentren en una red, la instrucción más famosa es el Ping.

Realizan un Ping a una dirección IP dentro de una Red sirve principalmente para verificar que podamos llegar a esta red en cuestión, es decir, podernos comunicar para el envío de información. Principalmente envía 4 paquetes de 32 bits por defecto con la instrucción (esto en el Sistema Operativo Windows):

$$ping\ < IP >.$$

Y envía ‘n’ cantidad de paquetes de 32 bits en el Sistema Operativo Linux.

El resultado muestra la cantidad y porcentaje de paquetes que se recibieron, perdieron o no llegaron, así como el tiempo de cada paquete en llegar y contestar.

Realizar un ping es la prueba más sencilla y común de saber si un dispositivo se encuentra visible en la red, así es fácil determinar cuándo un equipo “cayó”. Este monitoreo es tan fácil y tan esencial que cualquier sistema de monitoreo debe tener.

2.2. **S**imple **N**etwork **M**anagement **P**rotocol.

Es un protocolo dedicado especialmente al monitoreo de dispositivos en una red, su principal requerimiento es que el dispositivo que se desea monitorear tenga asociada una IP.

Existen tres versiones de este protocolo.

a) Primera Versión.

Nace para administrar y supervisar las redes de computadora, incluye su propio agente (Agente SNMP v1) que realiza la petición al dispositivo que se monitoreará quien debe tener también un agente SNMP el cual devolverá la información solicitada si es que la puede obtener.

b) Segunda Versión.

La versión 2, mejora algunos problemas que se mostraron en la primera versión, estos incluyen la muy limitada información que se podía obtener y algunos problemas de seguridad. Esta versión es la más usada actualmente entre todos los protocolos de monitoreo ya que ofrece una estabilidad enorme.

c) Tercera Versión

La tercera versión se enfoca en mejorar plenamente la seguridad de este protocolo, sin embargo, esta no ha sido bien recibida entre las empresas que utilizan este protocolo, por lo que la versión 2 sigue siendo la más usada por su sencillez y eficacia y este ámbito de seguridad se cubre a través de dispositivos externos como un *firewall* de última generación.

3. Herramientas y elementos de monitoreo.

3.1. Árboles MIB y hojas OID.

El protocolo SNMP maneja árboles MIB los cuales gráficamente se pueden representan como árboles de búsqueda (Fig. 1). Las hojas que tienen hijos también se consideran sub-árboles que también son árboles MIB, las hojas que ya no tienen hijos se les llama OID (*Object IDentifier*) que son los objetos que los agentes interpretan para saber qué información se requiere del dispositivo monitoreado.

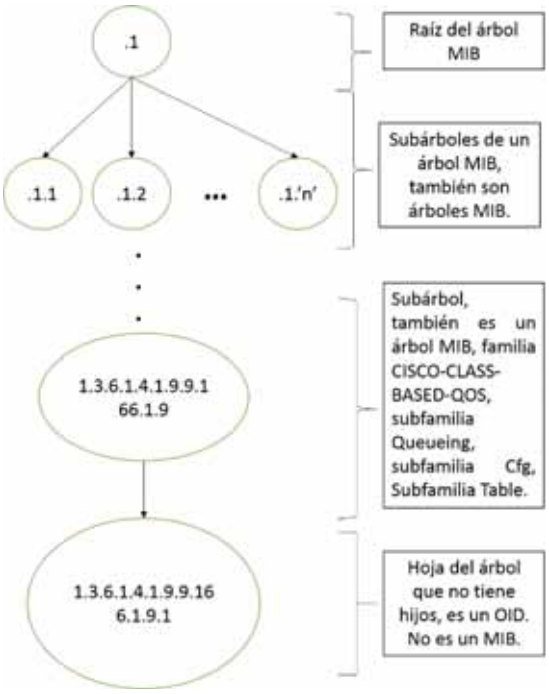

Fig. 1, muestra la representación gráfica de árboles y sub-árboles MIB y una hoja OID

3.2. Representante Proxy.

Un proxy es un intermediario que en general su uso es quien sale y conecta a internet para obtener la información del solicitante como una página web, la almacena en una memoria caché y regresa esa información al solicitante, al haber guardado la información en memoria, si otro usuario utiliza es proxy para obtener la misma información este ya no irá a internet, le regresará la información de la memoria caché.

El proxy, en general, es el representante de buscar información, no necesariamente en internet. En el monitoreo, se utilizan para obtener información sobre equipos que se encuentran protegidos por un *firewall*, ya que este solamente permitirá la salida de la información necesaria, dando confiabilidad y seguridad al monitoreo.

Material y Equipo

Los siguientes materiales y equipos fueron los que se utilizaron particularmente para esta estancia profesional.

- 2 máquinas Virtuales con las siguientes características:
  - Sistema Operativo Linux CentOs7.
  - 80 Gb de memoria.
  - 2 Gb de RAM.
  - 1 tarjeta de Red.
  - Servidor de Base de Datos “MariaDB”.
  - Conexión a internet con IPv4 estática.

Desarrollo del Proyecto

1. Requerimientos e Instalación Zabbix 3.4.1

1.1. Requerimientos

Una ventaja de Zabbix, es el poco espacio que requiere para monitorear a una gran cantidad de dispositivos y en caso de requerir un monitoreo más grande, la memoria debe crecer según los requerimientos de memoria oficiales de Zabbix (Tabla 1).

Se instalará la versión 3.4.1 y la versión 3.0.10, para poder comparar en un futuro.

1.2. Instalación

Seguir la guía de instalación, (Anexo A).

Tabla 1, muestra los requerimientos de Zabbix

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

2. Primer monitoreo con ICMP en Zabbix.

Como ya se mencionó el Protocolo ICMP solamente comprueba la conectividad entre 2 dispositivos en una red. Este apartado incluirá el agregar un host, agregar plantillas, y gráficas.

2.1. Localizar el Host a monitorear.

Del host que necesitamos monitorear necesitamos saber principalmente la dirección IP, no importa el protocolo a usar, la dirección IP es fundamental.

Para este protocolo en particular, es necesario habilitar las reglas necesarias de ICMP IPv4 del Firewall de Windows (solamente para dispositivos con sistema operativo Windows).

Para esta representación y una mejor visualización en imágenes se monitorearán los siguientes equipos:

- IP a monitorear: 10.11.11.145 (Linux)
- IP a monitorear: 10.11.11.140 (Windows)

a) Se comenzará desde el inicio de la interfaz de Zabbix, se deberá ingresar en un usuario con permisos, en este caso el admin.
b) Se procederá a ingresar a la sección de "Configuración" en el apartado de Host. Y en el lado superior derecho se dará clic en la opción agregar host (Fig. 2).

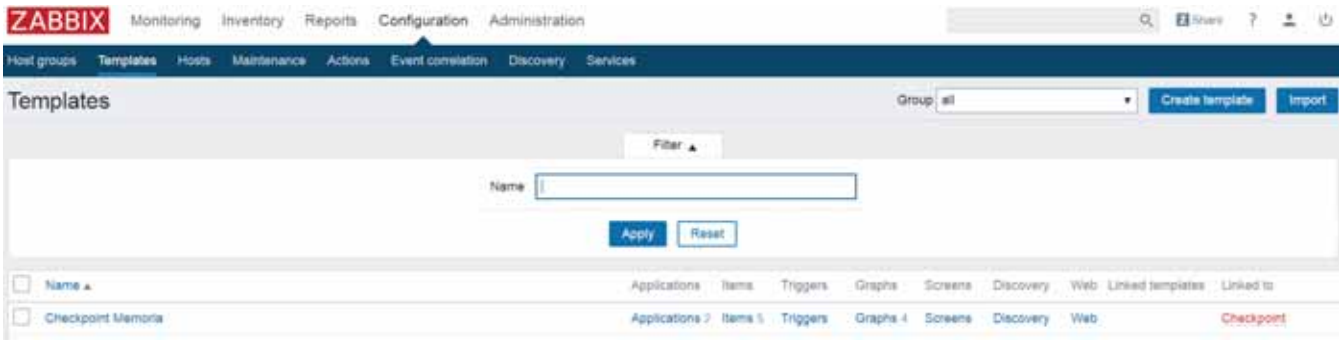

Fig. 2, muestra la sección de Configuración en el apartado Host.

c) Dentro de esta nueva ventana tenemos una gran cantidad de campos a llenar (Fig.3):
   a. Nombre: Debemos dar nombre al dispositivo que queremos monitorear; P.E. Computadora de Pepito, Firewall de la Empresa, Etc.
   b. Grupo: Todos los dispositivos tienen que ir en algún grupo, de lado derecho son los creados por defectos de Zabbix y también los creados, si queremos crear uno en

la barra de abajo indica si queremos agregar un nuevo grupo coloquemos el nombre, P.E: Computadoras Casa, Empresa, Computadoras Empresa, etc.

Zabbix Agent, SNMP, JMX, IPMI**:** Estos espacios significan con qué agente queremos monitorear, para este casi de ICMP se puede utilizar cualquiera, sin embargo, se realizará con el Agente Zabbix.

c. Hay tres barras de opciones, las cuales piden la dirección IP, el servidor DNS y el número de puerto por el cual irá. Se modificará la dirección IP que queremos monitorear solamente.
d. En la parte final de la ventana, existe una opción de monitorear por proxy, por el momento solo debe monitorear por el agente, es decir, se llenará la opción con "Sin Proxy".
e. Finalmente, se dará clic en agregar.

d) Ya guardado el nuevo host, se dará clic y nos regresará a la ventana del paso c) pero con la configuración ya guardada, ahora se dará clic en la parte superior en la opción *Templates*.

e) Los *Templates*, como se mencionó en el Marco Teórico, son plantillas que pueden incluir distintas cosas como Ítems, Triggers, Gráficas, Ítems Dinámicos. El protocolo ICMP ya viene cargado en una plantilla por defecto de Zabbix, ya que es un monitoreo básico.

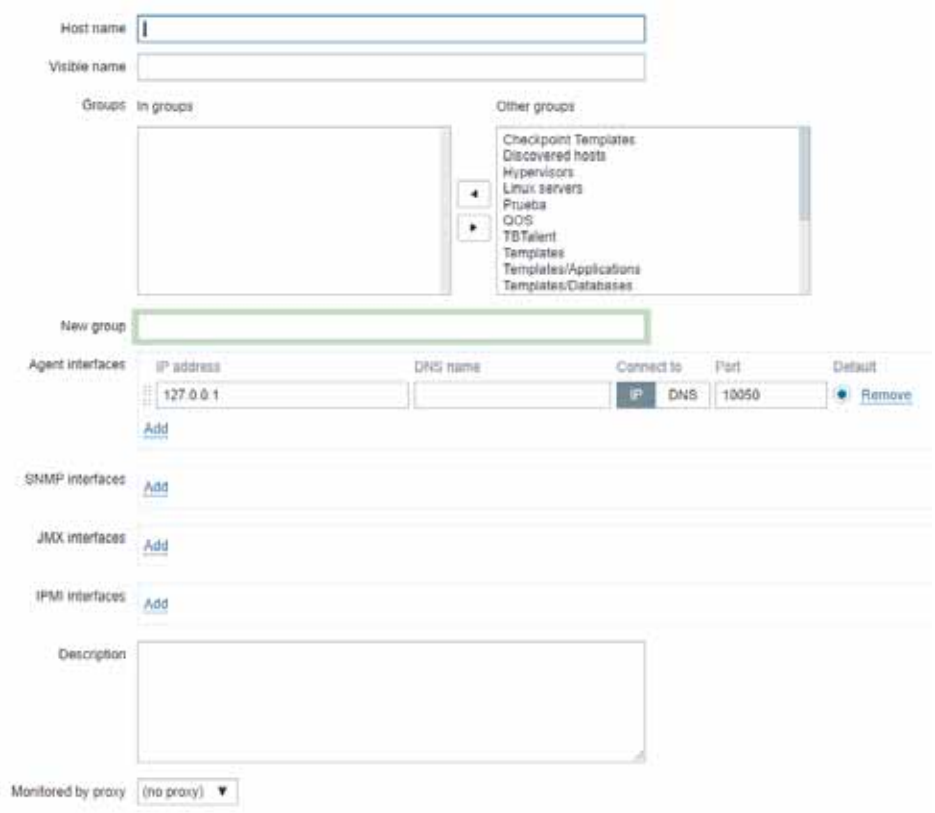

Fig. 3, muestra la ventada correspondiente a agregar un nuevo host.

f) En esta nueva ventana (Fig. 4), se agregará el nombre de plantilla que

necesitemos, en general, estas pueden ser las que estén cargadas por defecto y las que se crean.

a. Escribiremos el nombre del protocolo y nos aparecerán las plantillas disponibles.
b. En el caso de ICMP solamente existe una, se seleccionará y se dará clic en el botón agregar.

g) Una vez agregado, se dará clic en actualizar (*update*). Al haber agregado la plantilla, se agregaron ítems, Triggers, etc. Y ya se encuentra monitoreando el servidor Zabbix al equipo.
h) Para agregar otro dispositivo, hay que repetir todos los pasos. (Se agregará el equipo con IP 10.11.11.140).

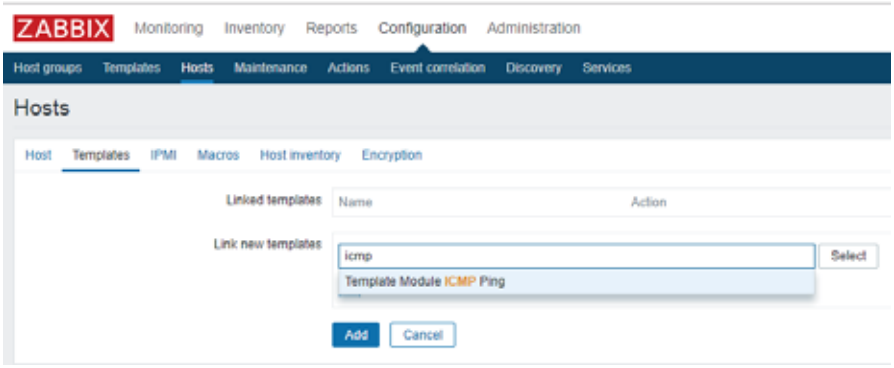

Fig. 4, muestra la pantalla correspondiente a añadir una nueva plantilla.

Para agregar gráficas y empezar a visualizar resultados cabe mencionar que esto se realiza para el host que está siendo monitoreado por ICMP, pero esto sirve para todo tipo de protocolo siempre y cuando cumplan los requisitos que se describirán.

2.2. Gráficas.

Una gráfica 'G' es una representación visual de los datos en un intervalo 'I', el cual en su mayoría de veces suele ser un tiempo 'T'.

Ayudan mucho a analizar el comportamiento de los datos en un periodo de tiempo, ya que con ello se pueden obtener muchos detalles como la hora exacta en que se presentó algún problema o fenómeno de interés y comenzar un análisis estadístico sobre algún tema en particular, por ejemplo, saber en que hora del día se encuentra mayor ancho de banda en uso.

a) Crear una nueva gráfica.

Las gráficas en Zabbix dependen de dos cosas esenciales; resultados numéricos de los ítems y el tiempo en que se comienza a monitorear.

Es importante destacar que algunos ítems que devuelven un resultado como el nombre del equipo, el nombre de los QoS creados, en general, datos estáticos que regresan resultados de tipo texto (cadena o *string*), no pueden ser graficados, ya que no podemos tener una gráfica Texto vs Tiempo, no tiene lógica, pero estos de forma automática generan un historial de cambios que ha tenido.

Una vez señalado este punto, podemos concluir que solamente los ítems que regresen un valor numérico (con signo, sin signo, reales, enteros) podrán ser graficados.

Generalmente las plantillas por defecto de Zabbix, ya incluyen las gráficas incluidas, sin embargo, se partirá como si no existieran gráficas.

1. Debemos entrar a la sección donde se encuentran todos los host y seleccionar al que se desea crear una gráfica.
2. Se podrá apreciar la configuración del host completa, en la barra superior de herramientas en donde se encuentra la

sección de ítems, macros, hay una sección de gráficas. Se ingresará.

3. En esta sección aparecerán todas las gráficas creadas para este host, algunas pueden haber sido creadas por ítems dinámicos o ya vienen incluidas en las plantillas. En la parte superior derecha hay un botón “Crear una nueva Gráfica”, ingresaremos ahí.
4. Dentro de nueva ventana, hay campos para llenar, necesariamente se tiene que dar un nombre a la gráfica, altura y anchura (que las medidas por defecto son bastantes buenas).
    a. Tipo de gráfica.

Normal: Es una gráfica de líneas que cambian dependiendo del valor que arroje el ítem. (Fig. 5).

Fig. G1, muestra la representación de la gráfica tipo normal.

Stacked: Es la tradicional gráfica rellena, que colorea del color señalado todo lo que está debajo de su límite. (Fig. G2)

Fig. 5, muestra la representación de la gráfica tipo *stacked*

Pie: Es la gráfica de tipo pastel, en donde convierte los resultados a porcentajes. (Fig. 6).

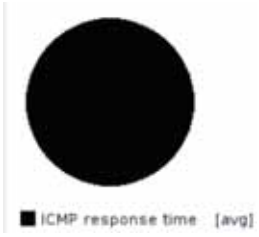

Fig. 6, muestra la representación de la gráfica tipo pie.

b) Visualizar una gráfica.

Una vez creada la gráfica al gusto de usuario se puede empezar a monitorear, en la barra principal en la sección de “Monitoreo” en el apartado de Gráfica (Fig. 7), en la parte superior se escoge el grupo del host que se desea graficar y el nombre del host y el nombre de la gráfica que se quiera mostrar, posteriormente aparecerá la gráfica que se creó anteriormente.

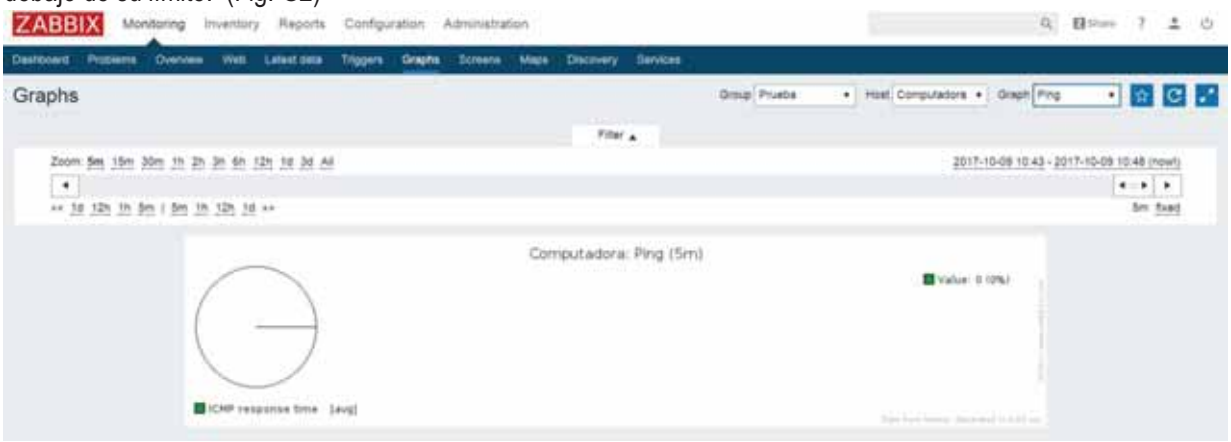

Fig. 7, muestra la gráfica creada monitoreando.

2.3. Última información Monitoreada.

En ocasiones, únicamente importará el estado actual o la información más reciente que se tiene sobre un dispositivo, dejando de lado el comportamiento que ha presentado en un cierto tiempo. Por ello Zabbix tiene incorporado un apartado de última información (*Latest Data*), donde se podrá visualizar un Grupo completo o dispositivos que nos interesen.

Para acceder a esta apartado, en la barra principal hay una sección de monitoreo (*Monitoring*), el cual despliega opciones como el Tablero Principal (*Dashboard)*, Triggers, Eventos, Gráficas y el que interesa en este caso Última Información (*Latest Data*). (Fig. 8).

Dentro de esta sección se tiene un apartado de filtro, en el cual podemos escoger el/los grupos o el/los dispositivos que se quiere visualizar su última información, esta última información incluye el nombre del ítem del cual está obteniendo la información (*Name*), la última fecha de actualización (*Last Check*), el valor que regresó (*Last Value*) y el cambio que se tuvo respecto al último valor (Change).

En la sección del filtro (Fig. 9), muestra principales opciones; Grupo de Host (*Host group*), (*Hosts), (Application), (Name),* y dos casillas para obtener un mejor filtrado (*Show ítems without data y Show Details).*

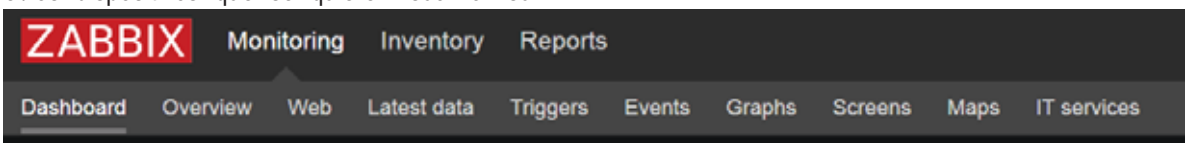

Fig. 8, muestra la barra principal y los apartados de la sección de Monitoreo.

.

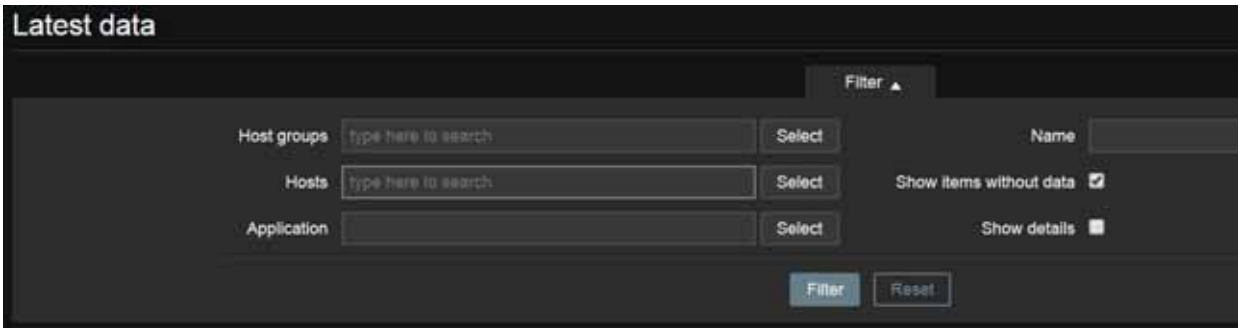

Fig. 9, muestra la sección de filtrado del apartado de Última Información.

a) *Host Groups* (Fig. 10)

Escogiendo la opción de *Select* se abrirá una nueva ventana en donde se podrá escoger el/los grupos que se quieran monitorear, solamente se necesita seleccionar la casilla.

Una vez seleccionados, en la parte inferior de esta nueva pantalla se encontrará un botón de nombre *Select*, el cual confirmará a los elementos señalados.

Una vez cerrada la ventana, en la sección de filtrado se selecciona el botón de filtrar y debajo de bajo aparecerá una nueva sección con los grupos seleccionados llenando los campos mencionados anteriormente sobre monitoreo. (Fig. 11).

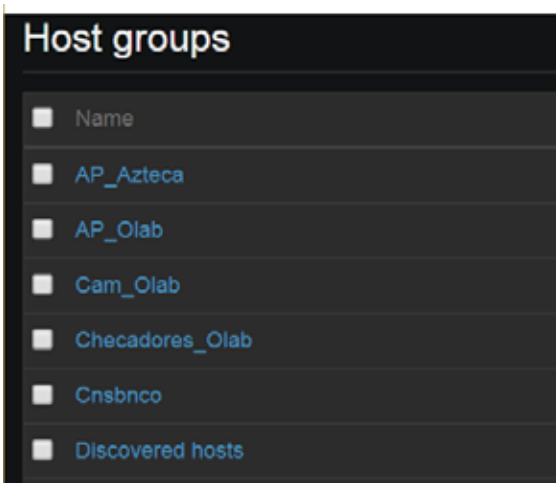

Fig. 10, muestra la ventana de grupos de hosts

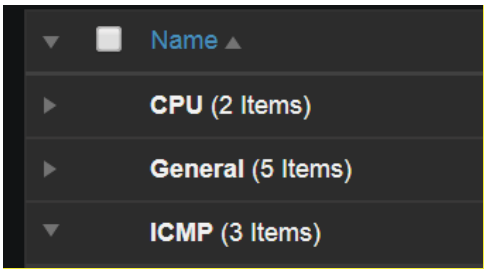

Fig. 11, muestra los campos de monitoreo.

Aunque exista una opción de graficación, esta mostrará una gráfica por defecto y no con todas las características de una gráfica creada como en el punto número 2.

b) Hosts (Fig. 12)

Para abrir la nueva ventana se realiza el mismo proceso de *Host Groups,* analizando esta ventana, es muy parecida a la de *Host Groups,* sin embargo, en la parte superior derecha se tiene una barra desplegable con el nombre de los grupos. Escogiendo uno aparecerán todos los hosts de ese grupo y se podrá seleccionar el que se desee monitorear. Una vez hecho, se seleccionará el botón *Select* en la parte inferior de la ventana.

Para agregar a otro host que no pertenezca al mismo grupo, se repite el proceso.

De igual forma, en la parte inferior de a sección de filtrado aparecerán.

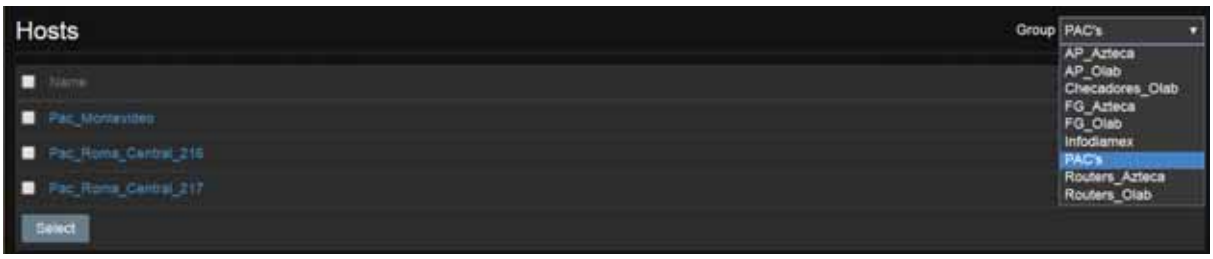

Fig. 12, muestra la ventana de Hosts.

c) *Application* (Fig. 13)

Aquí se monitoreará únicamente las aplicaciones creadas, por ejemplo, la aplicación ICMP que viene cargada en la plantilla, escogiendo esa monitoreará la aplicación ICMP de todos los equipos que se tengan dados de alta en Zabbix.

Su ventana, en la parte superior derecha al igual que la de *Host,* tiene un grupo para escoger la aplicación y otra para escoger *Host*.

d) Name

Solamente una palabra que se desee filtrar, por ejemplo, *router*, todos los dispositivos que tengan la palabra *router* aparecerán.

Fig. 13, muestra la ventana de Aplicaciones.

3. Introducción al SNMP v2

Como se describió en la teoría, el Protocolo Simple de Administración de Red (SNMP) funciona con 2 agentes, un agente que va hacia otro dispositivo a solicitar información y una vez obtenida regresa al solicitante y entrega la información, mientras que el otro cuando llega la petición del agente es el encargado de buscar en su dispositivo esta información y entregarla.

También se tienen 3 versiones de este protocolo, esto porque a través del tiempo se ha ido mejorando algunos aspectos, sobre todo en el de seguridad.

La segunda versión de SNMP incluye nuevas operaciones respecto a la versión 1, mejora aspectos de seguridad que eran graves en la versión 1 y a pesar de que ya existe la versión 3, la versión 2 sigue siendo la más utilizada a nivel mundial.

En general, el protocolo SNMP trabaja con árboles MIB y objetos OID, que, como se describieron en el marco teórico, tiene semejanza con árboles de búsqueda. Cabe resaltar que para que un dispositivo pueda soportar SNMP debe tener MIB's por defecto (Fig. 14) y cada empresa como CISCO, CheckPoint realizan a demás nuevos MIB especiales para sus dispositivos e incluyen nuevos objetos, lo que hace atractivo para utilizar este protocolo.

Realmente, el monitoreo que hacen estos softwares como Zabbix lo hacen a través de instrucciones por consola o terminal con la siguiente estructura:

$$snmpwalk - v\ 2c - c\ COMUNIDAD\ IP\ OID$$

Donde:

- -v indica que a continuación se escribirá la versión.
- 2c es la versión 2 de SNMP
- -c indica que a continuación se escribirá la comunidad

Es necesario una comunidad para poder acceder a la información monitoreada, dentro de esta comunidad se encuentran dispositivos que soportan SNMP, por ejemplo, se tiene una comunidad llamada "*DeptoSistemas*" y en ella se encuentran todas las computadoras del Departamento de Sistemas, específicamente, si se quiere monitorear una o varias computadoras de este departamento, se tiene que acceder a esta comunidad.

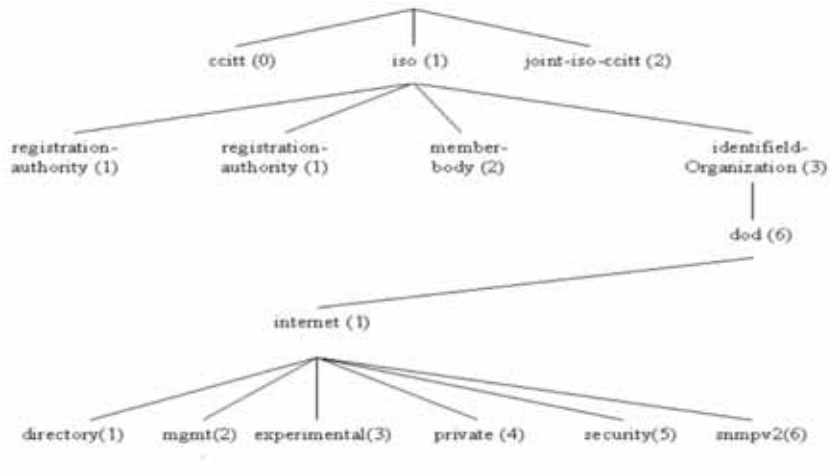

Fig. 14, muestra el árbol MIB principal.

4. Monitoreo con SNMP.

Para monitoreo con SNMP se requiere:

- Servidor Zabbix funcionando.
- Dispositivo a monitorear con SNMP habilitado.
- IP del Dispositivo.
- Nombre de la comunidad a la cual pertenece el dispositivo a monitorear.

Se realizará el monitoreo con el siguiente ejemplo:

- IP: 10.11.11.145
- Comunidad: TBTalent

Desde el *Dashboard*, en la barra principal en la parte de General, en el apartado de monitoreo se agregará un host.

El único detalle será que no se utilizará el agente Zabbix, ahora se utilizará el agente SNMP, solicitará la misma información (Fig. 15).

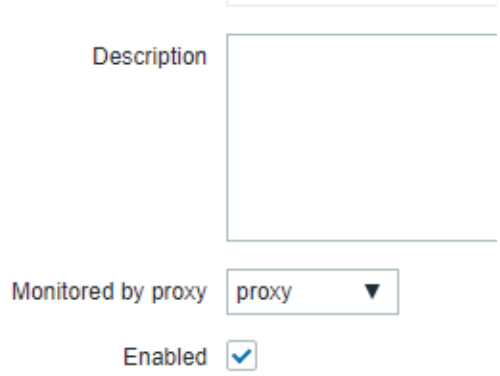

Fig. 15, muestra el cambio de configuración de monitoreo por proxy.

En las plantillas, Zabbix incluye por defecto algunas plantillas de SNMP, se agregarán las plantillas SNMP Device, el cual, devuelve información como interfaces ocupadas, sus nombres, y algunas otras cosas, como se hizo en el monitoreo con SNMP

En el apartado de Macros es importante, ya que se utilizan a una Expresión Regular {$SNMP_COMMUNITY}, esta expresión casi viene por defecto en todas las plantillas de SNMP y con ello se puede sustituir esta expresión regular por el nombre de la comunidad “TBTalent”, (un macro) (Fig. 15).

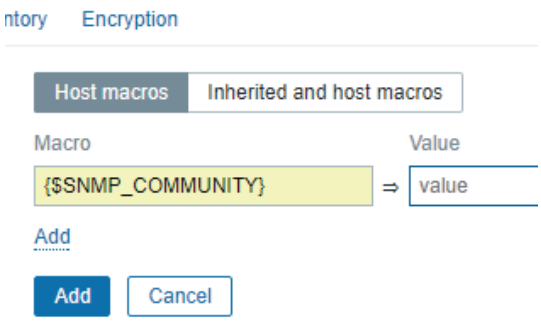

Fig. 16, muestra el macro SNMP_COMMUNITY

Finalmente, se colocarán las gráficas deseadas y se actualizará el host.

En la sección de última información se actualizará la información.

4.1. Crear Plantillas.

En la sección de *Templates* se puede crear nuevas plantillas con los MIBs que uno quiere, solamente se tiene que respetar que **NO** se repitan objetos, ya que no se podrá utilizar la plantilla.

En la parte superior derecha de esta sección existe un botón de crear plantilla, al acceder a él vienen las siguientes opciones (Fig. 16).

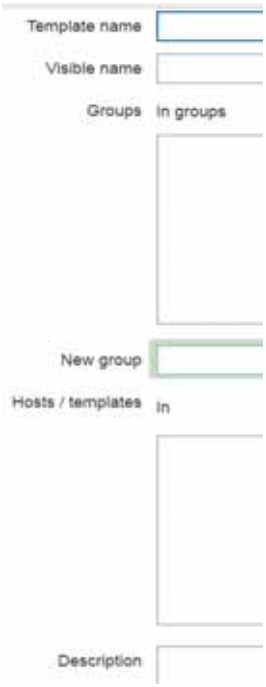

Fig. 17, muestra los campos a llenar para crear una nueva plantilla.

1. Template name: Nombre de la plantilla a crear
2. Nombre visible: Apodo de la plantilla.
3. Grupos en grupos: Grupo en donde se quiere colocar la platilla para un futuro filtrado mejor.
4. Nuevo Grupo: Crear un nuevo grupo.
5. Host / Templates: Agregar la plantilla en algunos hosts.
6. Descripción: Descripción de la plantilla.

4.2. Importar Plantillas

Incluso cualquier plantilla creada desde otro Zabbix se puede importar, la plantilla a importar debe estar en un archivo XML, en la parte superior derecha se encuentra un botón de importar plantilla (*Import Template).* Se selecciona y se escoge el archivo, posteriormente Zabbix carga la plantilla y la añade a la biblioteca.

4.3. Exportar Plantillas

Al igual que la importación, la exportación también tiene un botón especial, se escoge la plantilla o plantillas seleccionando un *checkbox* y en la parte

final de la ventana seleccionar el botón de exportar, se descargará un archivo XML.

4.4. Crear ítems

Para agregar un nuevo ítem SNMP, se requiere:

- OID.
- Key.
- Versión del Agente.
- Saber que devuelve.

Utilizando ***PuTTy*** para conectarse a través de SSH al dispositivo para monitorear, se usará la instrucción:

snmpwalk -v 3c -c TBTalent 10.11.11.145 + OID

y regresará un valor

la llave (Key) será:

Así para cualquier OID que se quiere agregar como ítem.

5. Introducción a los Proxies.

Como se describió en el Marco Teórico, un proxy sirve como un intermediario de conexión, que al momento de ingresar a una página de internet, el proxy es quien solicita la información y la entrega.

Para este servicio de monitoreo, el proxy es quien obtendrá la información de monitoreo cada 60 segundos a un servidor proxy y el servidor proxy lo entregará al servidor Zabbix, como se muestra en la Fig. 18, a diferencia del monitoreo que hace Zabbix (Fig. 19).

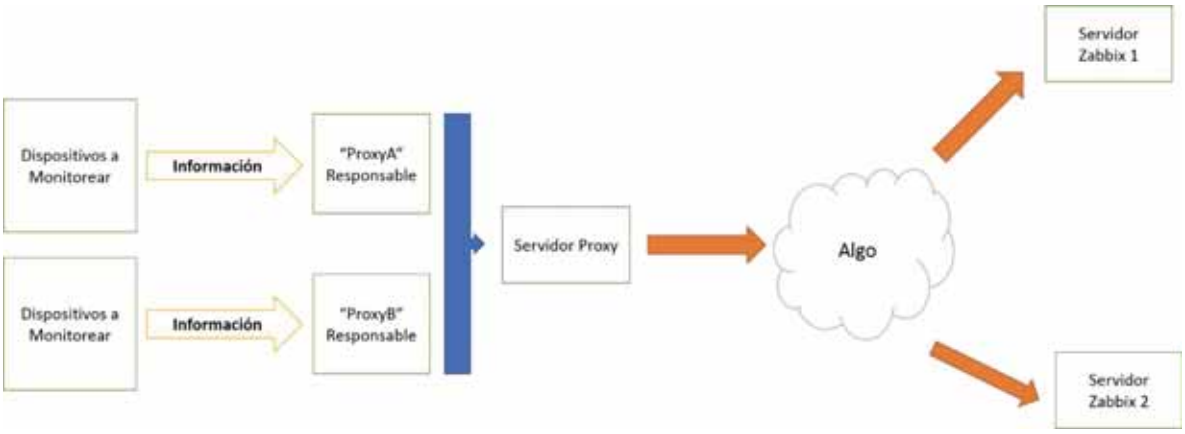

Fig. 18 , muestra el funcionamiento de un monitoreo con Proxy.

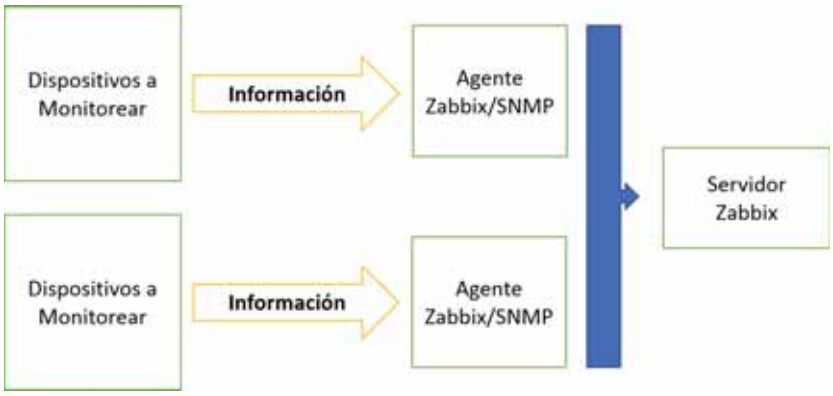

Fig. 19, muestra el funcionamiento de un monitoreo sin Proxy.

En general, se puede deducir, que para hacer un monitoreo sin proxy se debe estar directamente conectado a los dispositivos, e incluso en términos de seguridad, no es tan viable que ocurra este fenómeno.

Una ventaja con un proxy, es que el recolecta la información dentro de distintas redes, por ejemplo, detrás de un FW, con una red distinta a la del Zabbix.

6. Monitoreo con Proxy.

Se requiere:

- Servidor Zabbix funcionando.
- Servidor proxy instalado y configurado.

Para la instalación del Servidor Proxy, seguir el manual (Apéndice B).

Cabe resaltar que la instalación debe ser estrictamente en una máquina distinta a donde se tiene que la del servidor Zabbix.

Dentro de Zabbix,

7. Monitoreo con ICMP, SNMP con Proxy.

El monitoreo es exactamente igual, únicamente se debe tener creado el proxy y configurado.

Zabbix busca al servidor proxy con la dirección IP configurada, una vez ahí, busca al proxy por su nombre y toma la información. Este proceso lo repite cada minuto.

7.1. Crear un proxy desde Zabbix.

En la sección de General y Proxy, existe un botón para crear el proxy, únicamente solicitará el nombre del proxy y su forma de monitoreo “activo” o “pasivo”. Activo se refiere a que el proxy el dará la información por sí solo, mientras que pasivo el servidor Zabbix solicita la información al proxy.

Se puede crear un nuevo host o modificar alguno de los que se tienen, no importa si monitorea por ICMP o SNMP, la única diferencia es que, en la ventana de configuración principal, se modificará en la parte inferior la opción (*Monitoring with proxy)* ahora se seleccionará el proxy.

En el apartado de General y Proxy, ahora con el proxy creado se puede ver detalles como ver si está disponible, sin embargo, también hay un dato de tiempo de vida de proxy, esta información significa la última vez que se actualizó el proxy, por defecto se actualiza cada minuto (Fig. 20). En la sección de último monitoreo se puede apreciar que ya se encuentra monitoreando el dispositivo, y su última fecha de actualización dependerá del tiempo que se tenga por ítem.

Fig. 20, muestra la edad de un proxy.

Si el tiempo de actualización por ítem es mayor a 1 minuto, no actualizará hasta el minuto que es lo que tarda el proxy en actualizarse. Si el tiempo de actualización es mayor a 1 minuto no habrá problema.

Durante la estancia profesional, se realizó el monitoreo con proxy siguiendo el siguiente diagrama (Fig. 21).

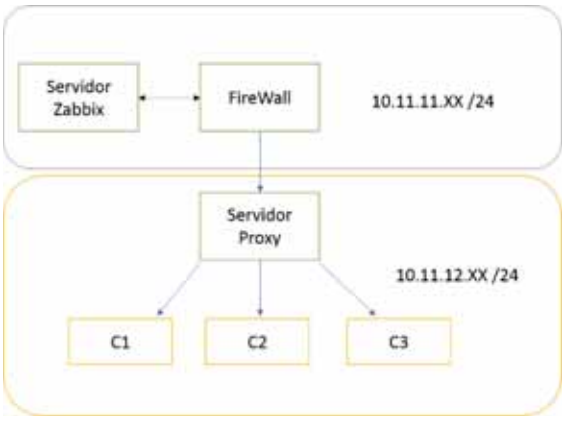

Fig. 21, muestra el monitoreo con proxy realizado en la estancia.

Comparaciones con Zabbix 3.0.10

1. El servidor de base de datos SQLite no es soportado para el Servidor Zabbix 3.4, pero aún soportado para el servidor Proxy.
2. La interfaz gráfica mejora para el dashboard, dando una mejor comodidad de personalizar al gusto de administrador.
3. Da una mejor flexibilidad al uso de SELinux en caso de que no se desee desactivar para su instalación.

Comentarios y Observaciones.

La instalación del servidor Zabbix aplica para cualquier versión a partir de la versión 3.0 hasta la 3.4.1.

Se realizó alrededor de 6 veces la instalación de un servidor Zabbix y 2 la instalación de un servidor Proxy.

Durante la estancia profesional, se realizó monitoreo de dispositivos como *Switches, Routers, Firewall Checkpoint, Firewall Fortinet,* Computadoras Personales.

Estas pruebas se realizaron una gran variedad de veces, así mismo, se tuvo la aplicación en la empresa CARPERMOR, donde se tuvo una colaboración con la supervisión del Ing. Daniel Ibarra.

Es importante resaltar que, si no se desactiva SELinux, no se podrá acceder a través de una red Wi-Fi desde cualquier otro dispositivo.

Algunos MIB como es el caso de *Routers* CISCO, requieren de un licenciamiento especial para liberar nuevos MIB, o bien, de una configuración especial.

Se recomienda bastante el uso de los softwares descritos en la sección Material y Equipo.

Así mismo, se recomienda un inglés intermedio ya que la mayor parte de la documentación sobre Zabbix se encuentra en inglés y portugués.

Igualmente, se recomienda la búsqueda de información en foros oficiales de Zabbix.

Conclusiones.

Para monitorear, es de suma importancia conocer el protocolo que se usará, para el caso de SNMP, es indispensable saber cómo funciona y cómo se compone.

El monitoreo será más práctico y preciso cuando se utilizan herramienta, como fue el uso de proxy y de ítems especiales. Obviamente, aplicar estas herramientas darán un nivel de complejidad un poco más grande.

El monitoreo con proxy se puede escalar con el uso de una IP Púbica, sin embargo, para efectos prácticos de laboratorio solamente se probó en redes distintas.

Finalmente, esta estancia profesional pudo mostrar la complejidad de problemas en cuestión de redes de computadora, TB&Talent, ha mostrado que dedicarse a un solo tema no es suficiente, es por ello que es importante capacitarse en distintas áreas de las Redes de Computadora, a pesar de que este proyecto únicamente se enfocó en el área de monitoreo, es necesario conocer temas de seguridad para dar un plus a este monitoreo.

Bibliografía

- Zabbix. (2017). Manual Zabbix. septiembre 2017, de Zabbix Sitio web: (https://www.zabbix.com/documentation/3.4/manual)https://www.zabbix.com/documentation/3.4/manual.
- J. Manuel Huidobro. (1997). SNMP. Un protocolo simple de gestión. septiembre 2017, de BIT Sitio web: https://www.coit.es/publicac/publbit/bit102/quees.htm.
- Robert de Bock, Fred Clausen, Nelson Manning. (2007). Add a Zabbix proxy to an existing Zabbix server. septiembre 2017, de Me in IT Sitio web: http://meinit.nl/add-zabbix-proxy-existing-zabbix-server
- Zabbix. (2007). Zabbix Forums. septiembre 2017, de Zabbix Sitio web: https://www.zabbix.com/forum/