UNIVERSIDAD AUTÓNOMA DEL ESTADO DE HIDALGO

INSTITUTO DE CIENCIAS BÁSICAS E INGENIERÍA

ÁREA ACADÉMICA DE COMPUTACIÓN Y ELECTRÓNICA

LICENCIATURA EN CIENCIAS COMPUTACIONALES

Implementación de una Herramienta de Monitoreo de la Red Universitaria

Tesis

Que para obtener el grado de
LICENCIADO EN CIENCIAS COMPUTACIONALES

QUE PRESENTA

P.L.C.C Erick David Mejía Pérez

ASESORES:

M. en C. Luis Heriberto Islas García
M. en C. Gonzalo Alberto Torres Samperio

Mineral de la Reforma, Hgo., octubre de 2019

UNIVERSIDAD AUTÓNOMA DEL ESTADO DE HIDALGO
Instituto de Ciencias Básicas e Ingeniería
Institute of Basic Sciences and Engineering
Área Académica de Computación y Electrónica
Computer Science and Electronics Department

Mineral de la Reforma, Hgo., a 17 de septiembre del 2018

Número de Control: ICBI-AACyE/1590/2018
Asunto: Autorización de impresión

PLCC. Erick David Mejía Pérez

Por este conducto les comunico que el Jurado que les fue asignado a su trabajo de tesis denominado **"Herramienta de monitoreo en tiempo real de la red de fibra óptica universitaria"**, y que después de revisarlo en reunión de sinodales han decidido autorizar la impresión del mismo, hechas las correcciones que fueron acordadas.

A continuación se anotan las firmas de conformidad de los integrantes del Jurado:

Presidente:	M. en C. Gonzalo Alberto Torres Samperio
Primer Vocal:	M. en C. Luis Heriberto García Islas
Segundo Vocal:	MID. Norma Laura Salazar Viveros
Tercer Vocal:	M. en C. Gabriela Medina Nájera
Secretario:	M. en C. Isaías Pérez Pérez
Primer Suplente:	MID. Alberto Suárez Navarrete
Segundo Suplente:	M. en C. Kristell Daniella Franco Sánchez

Sin otro particular, reitero a usted la seguridad de mi atenta consideración.

UNIVERSIDAD AUTÓNOMA DEL ESTADO DE HIDALGO
Atentamente
"Amor, Orden y Progreso"

M. C. C. Luis Islas Hernández
Coordinador de la Licenciatura en Ciencias Computacionales

Instituto de Ciencias Básicas e Ingeniería
Área Académica de Computación y Electrónica

Ciudad del Conocimiento
Carretera Pachuca - Tulancingo km. 4 5
Colonia Carboneras
Mineral de la Reforma, Hidalgo, México, C.P. 42184
Tel. +52 771 7172000 exts. 2250, 2251 . Fax 2109
aacye_icbi@uaeh.edu.mx

www.uaeh.edu.mx

Índice

Ilustraciones

Tablas

I. Introducción

El uso de las redes de computadoras y las telecomunicaciones se han vuelto indispensables en la vida cotidiana de cualquier organización. Su uso ha facilitado tanto el trabajo individual como el colectivo a través del uso compartido de recursos computacionales. Es por tal motivo que es importante contar con las herramientas que permitan administrar y monitorear el correcto uso de los recursos de red para el óptimo desempeño de actividades que hagan uso de esta tecnología.

En el presente trabajo se propone la implementación de una herramienta de monitoreo para la red universitaria, teniendo como principal cometido modificar la actual función de monitoreo que tiene a cargo la Dirección de Información y Sistemas (DIyS), específicamente el Área de Monitoreo y Operación de la Red, mediante la plataforma Zabbix la cual ofrece una mejora en cuanto a los servicios que se tienen con la actual plataforma denominada Orion como lo es la administración del rendimiento, la administración de seguridad y la administración de la configuración, así mismo la simplicidad de usar el protocolo SNMP (Simple Network Management Protocol / Protocolo Simple de Administración de Red) el cual permite el intercambio de información sobre los servicios antes mencionados por medio del puerto 161 UDP del modelo de interconexión de sistemas abiertos más conocido como “modelo OSI”, (en inglés, Open System Interconnection).

En los capítulos posteriores sea aborda el protocolo SNMP, así como sus principales funciones y procesos, a su vez se explica el método de instalación completa de Zabbix y la puesta en marcha, conjuntamente la puesta a punto y configuración de los dispositivos los cuales se destinaron como ejemplo para este trabajo.

II. Antecedentes

En 1993 como parte de la Infraestructura de comunicación existían tres redes locales aisladas en las siguientes dependencias; Dirección General de Planeación (Abasolo 600), Biblioteca Central (C.U.) y CECA (CEUNI). Donde operan aplicaciones exclusivas para sus mismas dependencias.

En 1995 se inician los trabajos y se implementó el sistema de Red de fibra Óptica y red Perimetral para telefonía en Ciudad Universitaria interconectando a todos los edificios al SITE Principal ubicado en el Edificio CEVIDE 3er piso. Este criterio fue unificado en las instalaciones vigentes en ese tiempo Preparatoria No. 1, 2, 3 y 4, CEUNI, Edificio Central, Rancho Universitario e ICAP, Escuela de Medicina (Ramírez Ulloa).

En 1996 se Inaugura la Red Integral de Telecomunicaciones por el Lic. Jesús Murillo Karam, gobernador de Hidalgo, realizando una llamada telefónica desde las instalaciones de la feria al conmutador de la Universidad, dando por inaugurada la primera red LAN Y WAN en Hidalgo. A Finales de 1996 se implementó la primera página web Institucional con el dominio www.reduaeh.mx

En 1997, corren las primeras aplicaciones en red LAN en todas las dependencias Universitarias, como son Control Escolar, Dirección Financiera y el Sistema del Programa Anual Universitario.

En 1998 de manera oficial se crea la Dirección de Telecomunicaciones y en ese mismo año se llevan a cabo las primeras videoconferencias de Intercambio Académico de clase mundial entre alumnos de la UAEH y países como España, Alemania y Argentina.

En 1999 a todos los alumnos y maestros de la UAEH, se les proporciona una cuenta de correo electrónico con el dominio @reduaeh.mx.

En 2001, se desarrolla el proyecto “Todos Internet”, con el objetivo de fortalecer la infraestructura tecnológica para establecer una red conmutada en todas las dependencias de la institución que se integraba con la ampliación de ancho de banda de intranet que paso de 10 Mbps a 1 Gbps en la ciudad universitaria, que soportaba el tráfico de backbone y que incluía los servicios que se distribuían a los tres campus como son: Sahagún, Actopan y Tlahuelilpan.

En 2004, se implanto el Proyecto de “Actualización Tecnológica” con la finalidad de integrar a la institución soluciones convergentes para la trasmisión de voz, datos y video, de manera flexible y escalable, por lo que se adoptó la telefonía IP, equipo carrier class, así también se refuerza la seguridad de la red perimetral y de autentificación, desarrollando una política institucional para el uso de la red universitaria.

En 2008, se inaugura la Red Metropolitana de Fibra óptica y la Red Regional de Microonda WiMax, con un ancho de banda de hasta 10 Gbps, diseñada para soportar aplicaciones en tiempo real como telefonía IP y videoconferencias, también pretende impulsar el uso de Internet 2 y los servicios de banda ancha, buscando extender las capacidades de conectividad en su red.

III. Descripción del problema

Dentro de las Funciones primordiales de la DIyS se encuentra el mantener en operación los sistemas de información existentes, desarrollar un programa de mantenimiento y administración de la infraestructura de telecomunicaciones, así como de las bases de datos de la institución, garantizando la confidencialidad y seguridad de éstas. Para ello, la DIyS y en particular el Área de Monitoreo y Operación de la Red, hacen uso de la plataforma Orion, la cual permite detectar, diagnosticar y resolver problemas de la red, al igual que el rendimiento de los equipos conectados a ella, sin embargo, el licenciamiento de dicha plataforma tiene un costo por lo tanto implica una inversión constante por parte de la Universidad.

Cabe mencionar que la versión actual de Orion que es usada por el área de Monitoreo y Operación de la red no ofrece algunas características como lo es la administración de seguridad y la administración de la configuración, además la información que arrojan los resultados de la administración de rendimiento no contiene información precisa lo cual afecta la toma de decisiones y, por ello la resolución de problemas se ve atenuada. Es por lo anterior que se busca abatir la inversión y de esta forma mejorar el proceso de monitoreo y administración de la red.

IV. Propuesta de Solución

El término administración de redes es definido como la suma total de todas las políticas y procedimientos que intervienen en la planeación, configuración, control y monitoreo de los elementos que conforman a una red con el fin de asegurar el eficiente y efectivo empleo de sus recursos (Untiveros, 2004).Lo anterior se ve reflejado en la calidad de los servicios ofrecidos, es por ello que se propone el uso de la plataforma Zabbix la cual permite la administración de los servicios que ofrece la universidad, además de detectar, diagnosticar y resolver los problemas dentro de la red, y siendo Zabbix de tipo open source permitirá que la universidad adapte la misma a sus necesidades. Por otra parte, en este trabajo se hablará sobre la implementación de Zabbix, así como la puesta a punto de la configuración y de algunos de los dispositivos que se usan, para ello se planea instalar un servidor en el cual se implemente Zabbix además de capacitar a los encargados dentro del Área de Monitoreo y operación de la red sobre el uso correcto del mismo, así como la implementación progresiva y reemplazo de la actual plataforma

V. Justificación

Actualmente las organizaciones deben trabajar 24 horas al día los 7 días de la semana garantizando la calidad en sus servicios, debido a esto la infraestructura de red de las organizaciones debe operar de manera correcta en todas sus actividades, por ese motivo es necesario establecer una adecuada administración de la red, la cual es una de las actividades primordiales y que muchas veces es ignorada.

El monitoreo de la red debe ser una de las labores incesantes dentro de la administración, la cual contempla diferentes fases como es: La administración de la configuración, de la cual, sus principales actividades son la planeación y el diseño de la red donde sus funciones primordiales son satisfacer los requerimientos inmediatos y futuros de la misma, así como expresarlos en su diseño para llegar a una correcta implementación.

Otra actividad que se ve reflejada dentro de esta fase es la selección de la infraestructura de red donde se deberán elegir los equipos idóneos de acuerdo con las necesidades y a la topología que se propone, además otra actividad que se realiza es la instalación y administración del Software, cuyo principal objetivo es conseguir un manejo adecuado de los recursos de hardware y software dentro de la red.

Por otra parte, se encuentra la actividad provisión que permite asegurar la redundancia de los elementos de software y hardware más importantes de la red, que pueden ser a nivel global o de un elemento en específico. Además, siempre deben existir políticas y procedimientos relacionados, donde se recomienda crear los procedimientos de las aplicaciones más utilizadas, además de las políticas de respaldo de configuraciones, así como también el procedimiento de instalación de una nueva versión del sistema operativo.

Otra de las fases que se encuentra dentro de la administración de una red es la administración del rendimiento, la cual tiene como objetivo recolectar y analizar el tráfico que circula en la red para determinar su comportamiento, dentro de esta actividad se tienen dos etapas la primera etapa se enfoca en el monitoreo el cual consiste en observar y recolectar información referente al comportamiento de la red, asimismo esta etapa será la base sobre la cual se enfocará el presente proyecto. La segunda etapa es el análisis, una vez que se ha recolectado la información mediante la etapa de monitoreo, es necesario interpretarla para determinar el comportamiento de la red y tomar decisiones adecuadas que ayuden a mejorar su desempeño.

Una de las actividades más importantes que se deben tomar en consideración al momento de administrar una red es la seguridad de esta, por tal motivo la administración de la seguridad resguarda la exactitud, integridad y protección de todos los datos, procesos, y recursos de los sistemas de información, de este modo se minimizan los errores, fraudes y pérdidas en los sistemas de información que se tienen dentro de la infraestructura de red.

Por último, se encuentra la administración de fallos que tiene como objetivos la detección y resolución oportuna de las situaciones anormales de la red, consta de varias etapas, en las cuales, las más importantes son la notificación de la falla, la determinación del origen, las pruebas de diagnóstico.

Como ya se mencionó anteriormente, dentro de la administración de rendimiento se encuentra la fase de monitoreo en la cual permite conocer el estado de las actividades de las aplicaciones, servicios de red y las actividades que generen los usuarios.

El monitoreo se puede llevar a cabo utilizando aplicaciones construidas a medida las cuales, tienen un costo y se requiere un licenciamiento privado, lo que significa que para hacer uso de algunas de sus características se necesita la inversión de capital para el uso de estas, además de que la mayoría de sus características no están liberadas para todos los usuarios. Por otra parte, existen herramientas alternativas libres y de licenciamiento GNU/GPL que pueden ser instaladas en sistemas estables, y es por este motivo que se busca que la red universitaria implemente esta alternativa.

Para la implementación de este proyecto se utiliza la plataforma Zabbix la cual se soporta en los estándares del protocolo SNMP (Simple Network Management Protocol) el cual es un protocolo muy extendido que trabaja a nivel de Aplicación del modelo OSI (Open System Interconnection) por medio del puerto 161 del protocolo UDP, mediante el cual se pueden realizar las tareas antes mencionadas de monitorización de red.

Zabbix es una plataforma para el monitoreo de la red que ofrece características como por ejemplo el ser open source que esto permite que la Universidad Autónoma del Estado de Hidalgo implemente y ajuste la plataforma a las necesidades de la infraestructura de la red para el correcto funcionamiento.

La importancia de este trabajo radica en el cambio a una plataforma de tipo open source que se adecue a las necesidades que se tienen en la DIyS y así evitar la inversión del software de licencia privada. Dentro de las funcionalidades de Zabbix podemos encontrar como se mencionó anteriormente la administración del rendimiento la cual nos implica una mejor toma de decisiones en el momento que los problemas surjan.

VI. Objetivo General

Mejorar la actual función de monitoreo que tiene a cargo la Dirección de Información y Sistemas (DIyS) en específico el área de Monitoreo y Operación de la Red mediante la instalación y configuración la plataforma Zabbix la cual ofrece una mejora en cuanto a los servicios que se tienen con la actual plataforma denominada Orion para formalizar la administración de los servicios y equipos de la Red Universitaria.

VII. Objetivos Específicos

- Implementar y configurar una herramienta de monitoreo de licencia tipo GNU/GPL y con eso evitar el pago de una licencia de tipo privada
- Implantar una serie de políticas de administración del Centro de Operaciones de Red (NOC) bajo cargo de la Dirección de Administración y Sistemas de la UAEH.
- Establecer procedimientos de detección y recuperación de fallas en concordancia de los resultados de monitoreo recuperado de Zabbix.
- Configurar las políticas de administración en el centro de NOC en caso de alguna falla o imprevisto.

VIII. Alcances y Limitaciones

Los alcances a los cuales aspira este trabajo abarcan desde la implementación de la plataforma dentro de los servidores del área de Monitoreo y Operación de la Red perteneciente a la DIyS, así como la puesta a punto de la configuración general de la red y los dispositivos específicos que se utilizan dentro de la red. Esto con la finalidad del progresivo reemplazo de la actual plataforma.

Las limitaciones de este trabajo se hallan en que para la implementación inicial se harán uso de cierto número de dispositivos de la red con los que cuenta la universidad, apegándose a los puntos que sean necesarios del modelo de administración de la red denominado F.C.A.P.S. el cual separara los proceso en diferentes actividades para llevar un mayor control de esta.

1. Capítulo I Marco Referencial

En el siguiente capítulo describe el marco teórico a utilizar para el desarrollo de la implementación como lo es el Proceso de la administración de una red; así como el modelo F.C.A.P.S. (por sus siglas Fault-Management/Gestión de Fallos, Configuración/Configuration, Accounting/Contabilidad, Performance/Rendimiento y Security/Seguridad), además hablará el Protocolo Simple de Administración de Red (SNMP por sus siglas en ingles de Simple Network Management Protocol). Además de la información general y características de la Plataforma Zabbix.

1.1. Proceso de la administración.

La administración de redes es una disciplina dentro de las Tecnologías de la Información muy demandada debido a la proliferación de las redes informáticas y, derivado de su uso excesivo, ha propiciado que se convierta en una tarea imprescindible para las empresas.

La administración de red involucra personas, software y hardware. Las personas involucradas son los profesionales de TI que garantizan el servicio continuo y efectivo al usuario final. El conjunto de herramientas de gestión de redes forma parte del software que está involucrado en la tarea de administración. Y, por último, el hardware se relaciona con los dispositivos de red que se utilizan para administrar la red. (Untiveros, 2004)

Existen diversos modelos sobre arquitecturas de administración de redes. Tanto el modelo TMN[1] de la Unión Internacional de Telecomunicaciones, como el modelo OSI-NM[2] (Network Management) que son modelos funcionales que dividen la administración de una red en áreas funcionales (configuración, fallas, desempeño, contabilidad y seguridad), definiendo de esta forma una estructura organizacional con funciones bien establecidas. De esto se deriva el nombre de modelos funcionales.

Dentro de las actividades que se contemplan modelo funcional se consideran; la planeación y diseño de la red; la instalación y administración del software; administración de hardware, y el aprovisionamiento.

1.1.1. Planeación y diseño de la red.

La meta de esta actividad es satisfacer los requerimientos inmediatos y futuros de la red, reflejarlos en su diseño hasta llegar a su implementación. El proceso de planeación y diseño de una red contempla varias etapas, algunas son:

a) Reunir las necesidades de la red. Las cuales pueden ser específicas o generales, tecnológicas, cuantitativas, etc.

Entre las necesidades específicas y de índole tecnológico de una red, se pueden mencionar las siguientes:

- Multicast,
- Voz sobre IP (VoIP),
- Calidad de servicio (QoS), etc.

[1] Serie de recomendaciones M.3000 de la ITU-T. http://www.itu.int
[2] ISO/IEC 7498-4: 1989

De igual manera, entre las necesidades cuantitativas se puede listar:

- Cantidad de nodos en un edificio
- Cantidad de switches necesarios para cubrir la demanda de nodos.

Este tipo de requerimientos solamente involucran una adecuación en el diseño de la red, no requiere de un rediseño completo, en el caso de alguna necesidad más general puede requerir de un cambio total en la red ya que en estos casos los cambios afectan a gran parte del diseño. Una necesidad general, por ejemplo, se presenta cuando se desea la implementación de nuevas tecnologías de red como el cambiar de ATM a Gigabit Ethernet, o cambiar los protocolos de ruteo interno.

b) Diseñar la topología de la red

Normalmente, las redes remotas, así como locales, se apoyan en alguna de las topologías siguientes: estrella, malla, anillo, bus o árbol. A estas se les denomina topologías básicas, pero existen por combinación de ellas, las topologías mixtas o combinadas.

Uno de los principales propósitos de las redes de computadoras es el "compartir recursos", mientras que uno de sus objetivos es hacer que todos los programas, datos y equipos estén disponibles para cualquiera que se encuentre dentro de la red que, y los solicite, sin importar la localización física del recurso y del usuario. Un segundo objetivo consiste en proporcionar una alta fiabilidad al contar con fuentes alternativas de suministro. Por otro lado, otro objetivo es el ahorro económico. Un punto muy relacionado es la capacidad para aumentar el rendimiento del sistema en forma gradual a medida que crece la carga.

c) Determinar y seleccionar la infraestructura de red basada en los requerimientos técnicos y en la topología propuesta.
d) Diseñar, en el caso de redes grandes, la distribución del tráfico mediante algún mecanismo de ruteo ya sea estático o dinámico.
e) Si el diseño y equipo propuesto satisfacen la necesidad, se debe proceder a planear la implementación, en caso contrario, repetir los pasos anteriores hasta conseguir el resultado esperado.

1.1.2. Selección de la infraestructura de red

Esta selección se debe realizar de acuerdo con las necesidades y la topología propuesta. Si se propuso un diseño jerárquico, se deben seleccionar los equipos adecuados para las capas de acceso, distribución y núcleo (Core). Además, la infraestructura debe cumplir con la mayoría de las necesidades técnicas de la red.

1.1.3. Instalaciones y Administración del software.

El objetivo de estas actividades es conseguir un manejo adecuado de los recursos de hardware y software dentro de la red.

Instalaciones de hardware.

Las tareas de instalación de hardware contemplan, tanto la agregación como la sustitución de equipamiento, y abarcan un dispositivo completo, como un switch o un ruteador; o solo una parte de estos, como una tarjeta de red, tarjeta procesadora, un módulo, etc. El proceso de instalación consiste en 7 etapas:

1. Realizar un estudio previo para asegurar que la parte que será instalada es compatible con los componentes ya existentes.
2. Definir la fecha de ejecución y hacer un estimado sobre el tiempo de duración de cada paso de la instalación.
3. Notificar anticipadamente a los usuarios sobre algún cambio en la red.
4. Generalmente, a toda instalación de hardware corresponde una instalación o configuración en la parte de software, entonces es necesario coordinar esta configuración.
5. Generar un plan alterno por si la instalación provoca problemas de funcionalidad a la red.
6. Realizar la instalación, procurando cumplir con los límites temporales previamente establecidos.
7. Documentar el cambio para futuras referencias.

Administración del software.

Es la actividad responsable de la instalación, desinstalación y actualización de una aplicación, sistema operativo o funcionalidad en los dispositivos de la red. Además de mantener un control sobre los programas que son creados para obtener información específica en los dispositivos. Antes de realizar una instalación, se debe tomar en cuenta lo siguiente.

- Que las cantidades de memoria y almacenamiento sean suficientes para la nueva entidad de software.
- Asegurarse de que no exista conflicto alguno, entre las versiones actuales y las que se pretenden instalar.

Otra actividad importante es el respaldo frecuente de las configuraciones de los equipos de red ya que son un elemento importante que requiere de especial cuidado. Estos respaldos son de mucha utilidad cuando un equipo se daña y tiene que ser reemplazado ya que no es necesario realizar la configuración nuevamente.

1.1.4. Provisión

Esta tarea tiene la función de asegurar la redundancia de los elementos de software y hardware más importantes de la red. Puede llevarse a cabo en diferentes niveles, por ejemplo, a nivel de la red global o de un elemento particular de la red. Es la responsable de abastecer los recursos necesarios para que la red funcione, elementos físicos como conectores, cables, multiplexores, tarjetas, módulos, elementos de software como versiones de sistema operativo, parches y aplicaciones. Además de hacer recomendaciones para asegurar que los recursos, tanto de hardware como de software, siempre se encuentren disponibles ante cualquier eventualidad.

Algunos elementos de hardware más importantes para la provisión son: tarjetas procesadoras, fuentes de poder, módulos de repuesto, equipos para sustitución y un respaldo de cada uno de ellos. En el caso se software se han mencionado en el apartado Administración del software.

1.1.5. Políticas y procedimientos relacionados.

En este apartado se recomienda realizar, entre otros, los siguientes procedimientos y políticas.

- Procedimiento de instalación de aplicaciones más utilizadas.
- Políticas de respaldo de configuraciones.
- Procedimiento de instalación de una nueva versión de sistema operativo.

1.1.6. Administración del rendimiento

Tiene como objetivo recolectar y analizar el tráfico que circula por la red para determinar su comportamiento en diversos aspectos, ya sea en un momento en particular (tiempo real) o en un intervalo de tiempo. Esto permitirá tomar las decisiones pertinentes de acuerdo con el comportamiento encontrado. La administración del rendimiento se divide en 2 etapas: monitoreo y análisis.

Monitoreo

El monitoreo consiste en observar y recolectar la información referente al comportamiento de la red en aspectos como los siguientes:

a) **Utilización de enlaces:**

Se refiere a las cantidades ancho de banda utilizada por cada uno de los enlaces de área local (Ethernet, Fast Ethernet, Gigabit Ethernet, etc.), ya sea por elemento o de la red en su conjunto.

b) Caracterización de tráfico.

Es la tarea de detectar los diferentes tipos de tráfico que circulan por la red, con el fin de obtener datos sobre los servicios de red, como http, ftp, que son más utilizados. Además, esto también permite establecer un patrón en cuanto al uso de la red.

c) Porcentaje de transmisión y recepción de información.

Encontrar los elementos de la red que más solicitudes hacen y atienden, como servidores, estaciones de trabajo, dispositivos de interconexión, puertos y servicios

d) Utilización de procesamiento.

Es importante conocer la cantidad de procesador que un servidor está consumiendo para atender una aplicación.

En este presente trabajo considera importante un sistema de recolección de datos en un lugar estratégico dentro de la red, el cual puede ser desde una solución comercial como Orion o la solución propia de la infraestructura de red, hasta una solución integrada con productos de software libre, en este caso Zabbix.

Análisis

Una vez recolectada la información mediante la actividad de monitoreo, es necesario interpretarla para determinar el comportamiento de la red y tomar decisiones adecuadas que ayuden a mejorar su desempeño. En el proceso de análisis se pueden detectar comportamientos relacionados a lo siguiente:

a) Utilización elevada:

Si se detecta que la utilización de un enlace es muy alta, se puede tomar la decisión de incrementar su ancho de banda o de agregar otro enlace para balancear las cargas de tráfico. También, el incremento en la utilización, puede ser el resultado de la saturación por tráfico generado maliciosamente, en este caso se debe contar con un plan de respuesta a incidentes de seguridad.

b) Tráfico inusual:

El haber encontrado, mediante el monitoreo, el patrón de aplicaciones que circulan por la red ayudará a poder detectar tráfico inusual o fuera del patrón, aportando elementos importantes en la resolución de problemas que afectan el rendimiento de la red.

c) Elementos principales de la red:

Un aspecto importante de conocer cuáles son los elementos que más reciben y transmiten, es el hecho de poder identificar los elementos a los cuales establecer un monitoreo más constante, debido a que seguramente son de importancia. Además, si se detecta un elemento que generalmente no se encuentra dentro del patrón de los equipos con más actividad, puede ayudar a la detección de posibles ataques a la seguridad de dicho equipo.

d) Calidad de servicio:

Otro aspecto, es la Calidad de servicio o QoS, es decir, garantizar, mediante ciertos mecanismos, las condiciones necesarias, como ancho de banda, retardo, a aplicaciones que requieren de un trato especial, como lo son la voz sobre IP (VoIP), el video sobre IP mediante H.323, etc.

e) Control de tráfico:

El tráfico puede ser reenviado o ruteado por otro lado, cuando se detecte saturación por un enlace, o al detectar que se encuentra fuera de servicio, esto se puede hacer de manera automática si es que se cuenta con enlaces redundantes.

Si las acciones tomadas no son suficientes, éstas se deben reforzar para que lo sean, es decir, se debe estar revisando y actualizando constantemente.

La administración del rendimiento se relaciona con la administración de fallas cuando se detectan anomalías en el patrón de tráfico dentro de la red y cuando se detecta saturación en los enlaces. Con la administración de la seguridad, cuando se detecta tráfico que es generado hacia un solo elemento de la red con más frecuencia que la común. Y con la administración de la configuración, cuando ante una falla o situación que atente contra el rendimiento de la red, se debe realizar alguna modificación en la configuración de algún elemento de la red para solucionarlo.

1.1.7. Administración de fallas

Tiene como objetivo la detección y resolución oportuna de situaciones anormales en la red. Consiste en varias etapas. Primero, una falla debe ser detectada y reportada de manera inmediata. Una vez que la falla ha sido notificada se debe determinar el origen de

esta para así considerar las decisiones a tomar. Las pruebas de diagnóstico son, algunas veces, la manera de localizar el origen de una falla. Una vez que el origen ha sido detectado, se deben tomar las medidas correctivas para restablecer la situación o minimizar el impacto de la falla.

El proceso de la administración de fallas consiste en 5 diferentes fases:

1) *Monitoreo de alarmas.* Se realiza la notificación de la existencia de una falla y del lugar donde se ha generado. Esto se puede realizar con el auxilio de las herramientas basadas en el protocolo SNMP.
2) *Localización de fallas.* Determinar el origen de una falla.
3) *Pruebas de diagnóstico.* Diseñar y realizar pruebas que apoyen la localización de una falla.
4) *Corrección de fallas.* Tomar las medidas necesarias para corregir el problema, una vez que el origen de esta ha sido identificado.
5) *Administración de reportes.* Registrar y dar seguimiento a todos los reportes generados por los usuarios o por el mismo administrador de la red.

Una falla puede ser notificada por el sistema de alarmas o por un usuario que reporta algún problema.

1.1.7.1. Monitoreo de alarmas

Las alarmas son un elemento importante para la detección de problemas en la red. Es por eso por lo que se propone contar con un sistema de alarmas, el cual es una herramienta con la que el administrador se auxilia para conocer que existe un problema en la red. También conocido como sistema de monitoreo, se trata de un mecanismo que permite notificar que ha ocurrido un problema en la red. Esta propuesta se basa en la utilización de herramientas basadas en el protocolo estándar de monitoreo, SNMP (del inglés Simple Network Management Protocol), ya que este protocolo es utilizado por todos los fabricantes de equipos de red. (Untiveros, 2004)

Cuando una alarma ha sido generada, ésta debe ser detectada casi en el instante de haber sido emitida para poder atender el problema de una forma inmediata, incluso antes de que el usuario del servicio pueda percibirla. Las alarmas pueden ser caracterizadas desde al menos dos perspectivas, su tipo y su severidad

Tipo de las alarmas

- ***Alarmas en las comunicaciones***. Son las asociadas con el transporte de la información, como las pérdidas de señal.
- ***Alarmas de procesos***. Son las asociadas con las fallas en el software o los procesos, como cuando el procesador de un equipo excede su porcentaje normal.
- ***Alarmas de equipos.*** Como su nombre lo indica, son las asociadas con los equipos. Una falla de una fuente de poder, un puerto, son algunos ejemplos.
- ***Alarmas ambientales.*** Son las asociadas con las condiciones ambientales en las que un equipo opera. Por ejemplo, alarmas de altas temperaturas.
- ***Alarmas en el servicio.*** Relacionadas con la degradación del servicio en cuanto a límites predeterminados, como excesos en la utilización del ancho de banda, peticiones abundantes de ICMP (por sus siglas en inglés de Internet Control Message Protocol).

Severidad de las alarmas.

- ***Crítica.*** Indican que un evento severo ha ocurrido, el cual requiere de atención inmediata. Se les relaciona con fallas que afectan el funcionamiento global de la red. Por ejemplo, cuando un enlace importante está fuera de servicio, su inmediato restablecimiento es requerido.
- ***Mayor.*** Indica que un servicio ha sido afectado y se requiere su inmediato restablecimiento. No es tan severo como el crítico, ya que el servicio se sigue ofreciendo, aunque su calidad no sea la óptima.
- ***Menor.*** Indica la existencia de una condición que no afecta el servicio pero que deben ser tomadas las acciones pertinentes para prevenir una situación mayor. Por ejemplo, cuando se alcanza cierto límite en la utilización del enlace, no indica que el servicio sea afectado, pero lo será si se permite que siga avanzando.
- ***Indefinida.*** Cuando el nivel de severidad no ha sido determinado por alguna razón.

1.1.7.2. Localización de fallas.

Este segundo elemento de la administración de fallas es importante para identificar las causas que han originado una falla. La alarma indica el lugar del problema, pero las pruebas de diagnóstico adicionales son las que ayudan a determinar el origen de esta. Una vez identificado el origen, se tienen que tomar las acciones suficientes para reparar el daño.

Pruebas de diagnóstico

Las pruebas de diagnóstico son medios importantes para determinar el origen de una falla. Algunas de estas pruebas de diagnóstico que se pueden realizar son:

a) Pruebas de conectividad física.

Son pruebas que se realizan para verificar que los medios de transmisión se encuentran en servicio, si se detecta lo contrario, tal vez el problema es el mismo medio.

b) Pruebas de conectividad lógica.

Son pruebas que ofrecen una gran variedad, ya que pueden ser punto a punto, o salto por salto. Las pruebas punto a punto se realizan entre entidades finales, y las salto por salto se realizan entre la entidad origen y cada elemento intermedio en la comunicación. Los comandos usualmente utilizados son “ping” y “traceroute”.

c) Pruebas de medición.

Esta prueba va de la mano con la anterior, donde, además de revisar la conectividad, se prueban los tiempos de respuesta en ambos sentidos de la comunicación, la pérdida de paquetes, la ruta que sigue la información.

Corrección de fallas.

Es la etapa donde se recuperan las fallas, las cuales pueden depender de la tecnología de red. En esta propuesta solo se mencionan las prácticas referentes a las fallas al nivel de la red.

Entre los mecanismos más recurridos, y que en una red basada en interruptores son aplicables, se encuentran los siguientes.

- ***Reemplazo de recursos dañados.*** Hay equipos de red que permiten cambiar módulos en lugar de cambiarlo totalmente.
- ***Aislamiento del problema.*** Aislar el recurso que se encuentra dañado y que, además, afecta a otros recursos es factible cuando se puede asegurar que el resto de los elementos de la red pueden seguir funcionando.
- ***Redundancia.*** Si se cuenta con un recurso redundante, el servicio se cambia hacia este elemento.
- ***Recarga del sistema.*** Muchos sistemas se estabilizan si son reiniciados.
- ***Instalación de software.*** Sea una nueva versión de sistema operativo, una actualización, un parche que solucione un problema específico, etc.
- ***Cambios en la configuración.*** También es algo muy usual cambiar algún parámetro en la configuración del elemento de la red.

1.1.8. Administración de reportes

Es la etapa de documentación de las fallas. Cuando un problema es detectado o reportado, se le debe asignar un número de reporte para su debido seguimiento, desde ese momento un reporte queda abierto hasta que es corregido. Este es un medio para que los usuarios del servicio puedan conocer el estado actual de la falla que reportaron. El ciclo de vida de la administración de reportes se divide en cuatro áreas, de acuerdo con la recomendación X.790[3] de la ITU-T.

Creación de reportes

Un reporte es creado después de haber recibido una notificación sobre la existencia de un problema en la red, ya sea por una alarma, una llamada telefónica de un usuario, por correo electrónico o por otros medios. Cuando se crea un reporte debe contener al menos la siguiente información:

- El nombre de la persona que reportó el problema.
- El nombre de la persona que atendió el problema o que creó el reporte de este.
- Información técnica para ubicar el área del problema.
- Comentarios acerca de la problemática.
- Fecha y hora del reporte.

Seguimiento a reportes

La administración de reportes debe permitir al administrador dar seguimiento de cada acción tomada para solucionar el problema, y conocer el estado histórico y actual del reporte. Para cada reporte debe mantenerse un registro de toda la información relacionada al mismo: pruebas de diagnóstico, como fue solucionado el problema, tiempo que llevó la solución, etc., y ésta debe poder ser consultada en cualquier momento por el administrador.

Manejo de reportes

El administrador debe ser capaz de tomar ciertas acciones cuando un reporte está en curso, como escalar el reporte, solicitar que sea cancelado un reporte que no ha sido cerrado aún, poder hacer cambios en los atributos del reporte, como lo es el teléfono de algún contacto, poder solicitar hora y fecha de la creación o finalización de un reporte, etc.

[3] Serie de recomendaciones X.790 de la ITU-T. https://www.itu.int/rec/T-REC-X.790-199511-I/es

Finalización de reportes

Una vez que el problema reportado ha sido solucionado, el administrador o la gente responsable del sistema de reportes, debe dar por cerrado el reporte. Una práctica importante, es que antes de cerrar un reporte el administrador debe asegurarse que efectivamente el problema reportado ha sido debidamente corregido.

1.1.9. Administración de la contabilidad

Es el proceso de recolección de información acerca de los recursos utilizados por los elementos de la red, desde equipos de interconexión hasta usuarios finales. Esto se realiza con el objetivo de realizar los cobros correspondientes a los clientes del servicio mediante tarifas establecidas. Este proceso, también llamado tarificación, es muy común en los proveedores de servicio de Internet (ISP por sus siglas en inglés de Internet Service Provider).

1.1.10. Administración de la seguridad

Su objetivo es ofrecer servicios de seguridad a cada uno de los elementos de la red, así como a la red en su conjunto, creando estrategias para la prevención y detección de ataques, así como para la respuesta ante incidentes de seguridad.

Prevención de ataques

El objetivo es mantener los recursos de red fuera del alcance de potenciales usuarios maliciosos. Una acción puede ser la implementación de alguna estrategia de control de acceso. Obviamente, los ataques solamente se reducen, pero nunca se eliminan del todo.

Detección de intrusos

El objetivo es detectar el momento en que un ataque se está llevando a cabo. Hay diferentes maneras en la detección de ataques, tantas como la variedad de ataques mismo. El objetivo de la detección de intrusos se puede lograr mediante un sistema de detección de intrusos que vigile y registre el tráfico que circula por la red apoyado en un esquema de notificaciones o alarmes que indiquen el momento en que se detecte una situación anormal en la red.

Respuesta a incidentes

El objetivo es tomar las medidas necesarias para conocer las causas de un compromiso de seguridad en un sistema que es parte de la red, cuando éste hay sido detectado, además de tratar de eliminar dichas causas.

Políticas de Seguridad

La meta principal de las políticas de seguridad es establecer los requerimientos recomendados para proteger adecuadamente la infraestructura de cómputo y la información ahí contenida. Una política debe especificar los mecanismos por los cuales estos requerimientos deben cumplirse. El grupo encargado de esta tarea debe desarrollar todas las políticas después de haber hecho un análisis profundo de las necesidades de seguridad. Entre otras, algunas políticas necesarias son:

- Políticas de uso aceptable.
- Políticas de cuentas de usuario.
- Políticas de configuración de ruteadores.
- Políticas de listas de acceso.
- Políticas de acceso remoto.
- Políticas de contraseñas.
- Políticas de respaldos.

Servicios de seguridad

Los servicios de seguridad definen los objetivos específicos a ser implementados por medio de mecanismos de seguridad. Identifica el “que”. De acuerdo con la Arquitectura de Seguridad OSI, un servicio de seguridad es una característica que debe tener un sistema para satisfacer una política de seguridad.

La arquitectura de seguridad OSI identifica cinco clases de servicios de seguridad:

1) Confidencialidad
2) Autenticación
3) Integridad
4) Control de acceso
5) No repudio

Un paso importante es definir cuáles de estos servicios deben ser implementados para satisfacer los requerimientos de las políticas de seguridad.

Mecanismos de seguridad

Se deben definir las herramientas necesarias para poder implementar los servicios de seguridad dictados por las políticas de seguridad. Algunas herramientas comunes son: herramientas de control de acceso, cortafuegos (firewall), TACACS+ o RADIUS; mecanismos para acceso remoto como Secure Shell o IPSec; Mecanismos de integridad como MD5, entre otras. Todos estos elementos en su conjunto conforman el modelo de seguridad para una red de cómputo.

Proceso.

- Para lograr el objetivo perseguido se deben, al menos, realizar las siguientes acciones: Elaborar las políticas de seguridad donde se describan las reglas de administración de la infraestructura de red. Y donde además se definan las expectativas de la red en cuanto a su buen uso, y en cuanto a la prevención y respuesta a incidentes de seguridad.
- Definir, de acuerdo con las políticas de seguridad, los servicios de necesarios y que pueden ser ofrecidos e implementados en la infraestructura de la red.
- Implementar las políticas de seguridad mediante los mecanismos adecuados.

1.2. F.C.A.P.S. (Fault, Configuration, Accounting, Performance, Security)

En 1996 la ITU-T introdujo el M.3010 [4] que introducía la estructura del Telecommunications Management Network (TMN) para que los operadores gestionen su Plataforma de Servicios de Red. En 1997 el M.3400[5] introdujo F.C.A.P.S. La ISO aplicada de F.C.A.P.S. a redes de datos en el modelo OSI.

F.C.A.P.S. es el modelo y framework de red de gestión de telecomunicaciones de ISO para la gestión de redes. F.C.A.P.S. es un acrónimo de Fault, Configuration, Accounting, Performance, Security (Falla, Configuración, Contabilidad, Desempeño, Seguridad Ilustración 1-1) que son las categorías en las cuales el modelo ISO define las tareas de gestión de redes. En algunas redes Contabilidad se reemplaza con Administración (International Organization for Standardization, 2017)

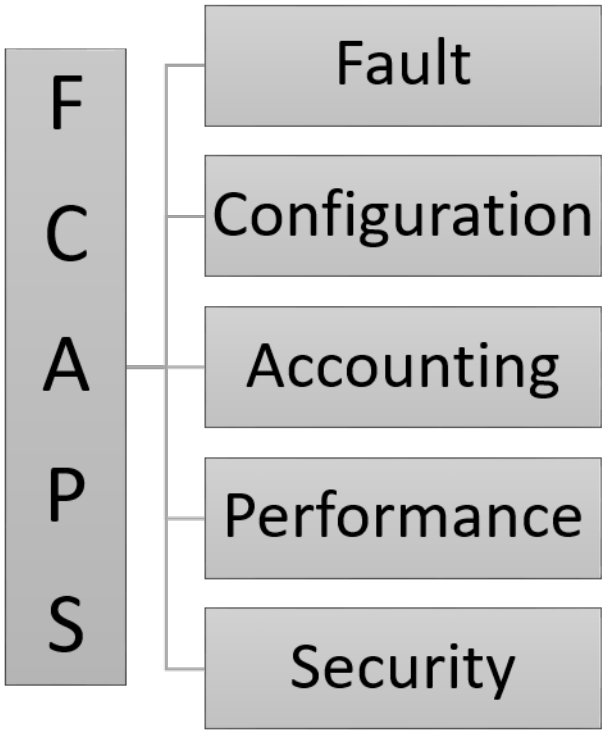

ILUSTRACIÓN 1-1 FASES DEL MODELO F.C.A.P.S.

[4] (ITU-T, 1996)
[5] (ITU-T, 1997)

1.2.1. Fault Management / Administración de Fallas

Una de las áreas de administración asociadas al modelo de F.C.A.P.S. es la administración de fallas.

Una falta es un evento que tiene un significado negativo. El objetivo de la falta es reconocer, aislar, corregir y registrar fallos que ocurren en las redes de telecomunicaciones. Además, utiliza análisis de tendencias para predecir errores de tal manera que la red siempre está disponible. Esto puede ser establecido monitorizando cosas diferentes para un comportamiento anormal.

Cuando ocurre una falta o un evento, frecuentemente un componente de la red enviará una notificación al operador de la red utilizando un protocolo propietario o abierto como SNMP o al menos escribir un mensaje en su consola para un servidor de consola para capturar un log/página. Esta notificación se supone que se lanza automáticamente o mediante actividades manuales. Por ejemplo, la recopilación de más datos para identificar la naturaleza y la gravedad del problema o poner el equipo de backup on-line.

Los principales sistemas de Gestión de Fallos son HP OpenView, IBM Tivoli Netcool, TTI Telecom Netrac, Clarity, etc. Las herramientas de aislamiento de fallos como Delphi que también están disponibles son básicamente utilizadas para aislar fallos en cualquier red de telecomunicación.

El modelo F.C.A.P.S. identificada doce tareas de administración necesarias para un sistema de “Fault management”:

1) Detección de falla.
2) Corrección de falla.
3) Aislamiento de la falla.
4) Recuperación de la red.
5) Manejo de alarmas.
6) Filtrado de alarmas.
7) Generación de alarmas.
8) Borrado de correlación.
9) Pruebas de diagnóstico.
10) Error de registros.
11) Manejo de errores.
12) Estadísticas de errores.

1.2.2. Configuration Management / Administración de Configuración

Es el concepto de asegurar una consistencia, repetición, y auditable configuración en todos los equipos de la red, basados en una política de configuración.

Es el proceso mediante el cual todas las operaciones diarias son monitoreadas y controladas.

Es el proceso de obtener información de la red y usarla para hacer ajustes a la configuración de los dispositivos de la red

Todos los cambios de hardware y de software son coordinados a través de este proceso.

Nuevos programas o equipamiento, la modificación de sistemas existentes y la eliminación de sistemas y programas obsoletos también son coordinados a través de la Administración de la configuración.

Los objetivos de la administración de la configuración son:

- Recolectar información.
- Modificar la configuración.
- Generación de reportes.
- Gestión de cambios.

Según las redes incrementan su tamaño, una tarea importante es la configuración automatizada. Algunos ejemplos de esta tarea son el DNS, histórico de cambios de configuración RANCID[6] (Really Awesome New Cisco config Differ), Archivos manejados en Compact flash, control de versiones.

Este proceso debe tener en cuenta:

- Permitir el acceso rápido a la información sobre configuraciones.
- Facilitar la configuración remota de los dispositivos.
- Proporcionar inventario actualizado de los componentes de la red.

Para recopilar y almacenar las configuraciones de los dispositivos de la red (esto se puede hacer a nivel local o remota).

- Para simplificar la configuración del dispositivo.
- Hacer un seguimiento de los cambios que se hacen a la configuración.
- Para configurar “provisión” a través de circuitos de caminos o redes no conmutadas.

[6] https://wiki.opennms.org/wiki/RANCID_RWS

- Como aumento de tamaño de las redes, una tarea importante es la configuración automática.

El modelo F.C.A.P.S. identificada doce tareas de administración necesarias para un sistema de “Configuration management”:

1) Recursos de inicialización
2) Provisionamiento de red
3) Autodescubrimiento
4) Copia de seguridad y restauración
5) Apagado de recursos
6) Gestión del cambio
7) Pre-provisión
8) Inventario/gestión de activos
9) Copia de configuración
10) Configuración remota
11) Automatización de distribución de software
12) Iniciación de Job, tracking, y ejecución

1.2.3. Accounting Management / Administración de la Contabilidad

La gestión de las cuentas es a menudo conocida como la gestión de la tarifación. El objetivo es reunir las estadísticas de los usuarios. Utilizando las estadísticas, los usuarios pueden ser tarifados y utilizando el límite pueden ser forzados. Por ejemplo:

- Utilización de disco.
- Enlace de utilización.
- Tiempo de CPU.

RADIUS, TACACS y DIAMETER son ejemplos de protocolos comúnmente utilizados para gestión de tarificación.

Para redes no tarificadas, "administración" reemplaza a "cuentas". Los objetivos de la administración son gestionar el conjunto de usuarios autorizados estableciendo usuarios, contraseñas y permisos y administrar las operaciones de los equipos como realizar backups de software y la sincronización.

La siguiente lista destaca las ocho consideraciones para las herramientas que permiten a la contabilidad de gestión:

1) Realizar un seguimiento de servicio o el uso de los recursos.
2) Costo de los servicios.
3) Contabilidad límite.
4) Uso de las cuotas.
5) Auditorías.
6) Reporte de Fraudes.
7) Combine los costos de múltiples recursos.
8) Apoyo a diferentes modos de Gestión del Rendimiento.

1.2.4. Performance Management / Administración del Rendimiento

Gestión del rendimiento implica la vigilancia efectiva del tiempo de respuesta de la red y la gestión proactiva de las actualizaciones necesarias para apoyar a sus usuarios.

La gestión del rendimiento permite al gestor preparar la red para el futuro, así como a determinar la eficiencia de la red actual, por ejemplo, en relación con las inversiones realizadas para establecerla. El rendimiento de la red se mide con el throughput, el porcentaje de utilización, las tasas de error y los tiempos de respuesta.

Recolectando y analizando los datos de rendimiento, el estado de la red puede ser monitorizado. Las tendencias pueden indicar la capacidad o cuestiones de fiabilidad que se convierten en servicios afectados.

Los umbrales de rendimiento pueden ser establecidos para lanzar una alarma. La alarma sería manejada por el proceso de gestión de fallos habitual. Las alarmas varían dependiendo de la severidad.

Cuando se mira un sistema de gestión del rendimiento, se buscan los siguientes ocho atributos:

1) Utilización y tasas de error.
2) El performance y recolección de datos.
3) Niveles consistentes de performance.
4) Realización de análisis de datos.
5) Reporte de problemas.
6) Capacidad de planificación.
7) Generación de informes de rendimiento.
8) Mantener y examinar los registros históricos.

1.2.5. Security Management / Administración de la Seguridad

La gestión de la seguridad es el proceso de controlar el acceso a recursos en la red. La seguridad de datos puede ser conseguida principalmente con la autenticación, el cifrado y la autorización configurada con el sistema operativo y la configuración de control de acceso del sistema de gestión de base de datos.

Considere las siguientes ocho actividades fundamentales para un eficaz sistema de gestión de seguridad:

1) Acceso restrictivo a los recursos.
2) Registros de acceso.
3) Protección de datos.
4) Control de los derechos de acceso de usuario.
5) Seguridad de auditoría de registro.
6) Seguridad de alarma / Reporte de eventos.
7) Tenga cuidado de las violaciones de la seguridad y los intentos.
8) Seguridad de información relacionada con las distribuciones.

1.3. Protocolo Simple de Administración de Red o SNMP

Dado que la tendencia natural de una red cualquiera es a crecer, conforme se añaden nuevas aplicaciones y más y más usuarios hacen uso de esta, los sistemas de gestión empleados han de ser lo suficientemente flexibles para poder soportar los nuevos elementos que se van añadiendo, sin necesidad de realizar cambios drásticos en la misma (Huidobro, 1997).

Este punto, el de gestión de red, es uno de los más controvertidos en teleinformática, ya que, prácticamente, no existe una solución única, aceptada por todos y que sea fácilmente implantable. Las soluciones existentes suelen ser propietarias -Netview de IBM, OpenView de HP, etc.- lo que hace que, en una red compleja, formada por equipos multi-fabricante, no exista un único sistema capaz de realizar la gestión completa de la misma, necesitándose varias plataformas -una por cada fabricante-, lo que dificulta y complica enormemente la labor del gestor de red.

Con la idea de presentar una solución única, válida para cualquier tipo de red, varios grupos de normalización están trabajando en ello y, aunque hay dos tendencias claras (SNMP para redes de empresa y CMIS/CMIP (Common Management Information Service/Protocol) para redes públicas), sólo SNMP es la que está consiguiendo una aceptación e implantación amplia, a lo que ha contribuido su sencillez y rapidez de desarrollo. (NET-SNMP, 2017)

El Protocolo Simple de Administración de Red o SNMP (del inglés Simple Network Management Protocol) es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red como se observa en la Ilustración 1-2. Los dispositivos que normalmente soportan SNMP incluyen Routers, switches, servidores, estaciones de trabajo, impresoras, bastidores de módem y muchos más. Permite a los administradores supervisar el funcionamiento de la red, buscar y resolver sus problemas, y planear su crecimiento.

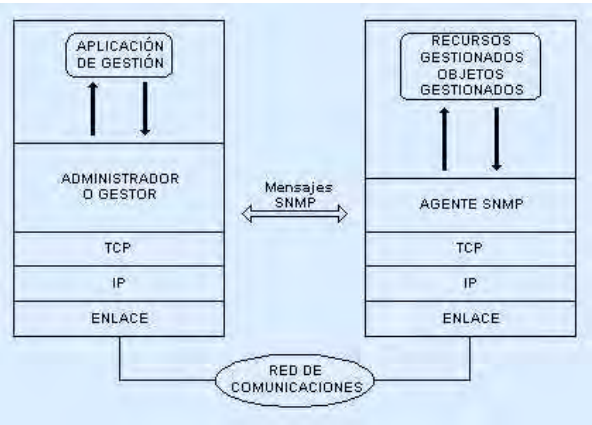

ILUSTRACIÓN 1-2 MODELO DE COMUNICACIÓN SNMP

Surge a raíz del interés mostrado por la IAB (Internet Activities Board) en encontrar un protocolo de gestión que fuese válido para la red Internet, dada la necesidad de este debido a las grandes dimensiones que estaba tomando. Los tres grupos de trabajo que inicialmente se formaron llegaron a conclusiones distintas, siendo finalmente el SNMP (RFC 1098 (The Internet Engineering Task Force, 1989)) el adoptado, incluyendo éste algunos de los aspectos más relevantes presentados por los otros dos: HEMS (High-Level Management System) y SGMP (Simple Gateway Monitoring Protocol).

SNMP es un componente de la suite de protocolo de Internet como se define por el IETF[7]. Se compone de un conjunto de normas para la gestión de la red, incluyendo una capa de aplicación del protocolo, una base de datos de esquema, y un conjunto de objetos de datos. Las versiones de SNMP más utilizadas son SNMP versión 1 (SNMPv1) y SNMP versión 2 (SNMPv2).

SNMP en su última versión (SNMPv3) posee cambios significativos con relación a sus predecesores, sobre todo en aspectos de seguridad; sin embargo, no ha sido mayoritariamente aceptado en la industria.

En usos típicos SNMP, uno o más equipos administrativos, llamados gerentes, tienen la tarea de supervisión o la gestión de un grupo de hosts o dispositivos de una red informática. En cada sistema gestionado se ejecuta, en todo momento, un componente de software llamado agente que reporta la información a través de SNMP con el gerente. Los agentes SNMP exponen los datos de gestión en los sistemas administrados como variables. El protocolo también permite realizar tareas de gestión de activos, tales como la modificación y la aplicación de una nueva configuración a través de la modificación remota de estas variables. Las variables accesibles a través de SNMP están organizadas en jerarquías. Estas jerarquías y otros metadatos (tales como el tipo y la descripción de la variable), se describen por Bases de Información de Gestión (MIB).

1.3.1. Componentes básicos

Una red administrada a través de SNMP consta de tres componentes clave:

1. Sistemas administradores de red (Network Management Systems, NMS).
2. Dispositivos administrados.
3. Agentes.

Estos componentes tienen las siguientes funciones:

Un sistema administrador de red (NMS) ejecuta aplicaciones que supervisan y controlan a los dispositivos administrados. Los NMS's proporcionan el volumen de recursos de procesamiento y memoria requeridos para la administración de la red. Uno o más NMS's deben existir en cualquier red administrada.

Un dispositivo administrado es un dispositivo que contiene un agente SNMP y reside en una red administrada. Estos recogen y almacenan información de administración, la cual es puesta a disposición de los NMS's usando SNMP. Los dispositivos administrados, a veces llamados elementos de red, pueden ser Routers, servidores de acceso, switches, bridges, hubs, computadores o impresoras.

Un agente es un módulo de software de administración de red que reside en un dispositivo administrado. Un agente posee un conocimiento local de información de

[7] The Internet Engineering Task Force (IETF®) https://www.ietf.org

administración (memoria libre, número de paquetes IP recibidos, rutas, etcétera), la cual es traducida a un formato compatible con SNMP y organizada en jerarquías.

1.3.2. Comandos básicos

Los dispositivos administrados son supervisados y controlados usando cuatro comandos SNMP básicos: lectura, escritura, notificación y operaciones transversales.

El comando de lectura es usado por un NMS para supervisar elementos de red. El NMS examina diferentes variables que son mantenidas por los dispositivos administrados.

El comando de escritura es usado por un NMS para controlar elementos de red. El NMS cambia los valores de las variables almacenadas dentro de los dispositivos administrados.

El comando de notificación es usado por los dispositivos administrados para reportar eventos en forma asíncrona a un NMS. Cuando cierto tipo de evento ocurre, un dispositivo administrado envía una notificación al NMS.

Las operaciones transversales son usadas por el NMS para determinar qué variables soporta un dispositivo administrado y para recoger secuencialmente información en tablas de variables, como, por ejemplo, una tabla de rutas.

1.3.3. Base de información de administración SNMP (MIB)

Una Base de Información de Administración (Management Information Base, MIB) es una colección de información que está organizada jerárquicamente. Las MIB's son accedidas usando un protocolo de administración de red, como, por ejemplo, SNMP.

Un objeto administrado (algunas veces llamado objeto MIB, objeto, o MIB) es uno de cualquier número de características específicas de un dispositivo administrado. Los objetos administrados están compuestos de una o más instancias de objeto, que son esencialmente variables.

Existen dos tipos de objetos administrados: Escalares y tabulares. Los objetos escalares definen una simple instancia de objeto. Los objetos tabulares definen múltiples instancias de objeto relacionadas que están agrupadas conjuntamente en tablas MIB.

Un ejemplo de un objeto administrado es *atInput*, que es un objeto escalar que contiene una simple instancia de objeto, el valor entero que indica el número total de paquetes AppleTalk de entrada sobre una interfaz de un router. (NET-SNMP, 2017)

Un identificador de objeto (object ID) identifica únicamente a un objeto administrado en la jerarquía MIB. La jerarquía MIB puede ser representada como un árbol con una raíz como se observa en la Ilustración 1-2 anónima y los niveles, que son asignados por diferentes organizaciones.

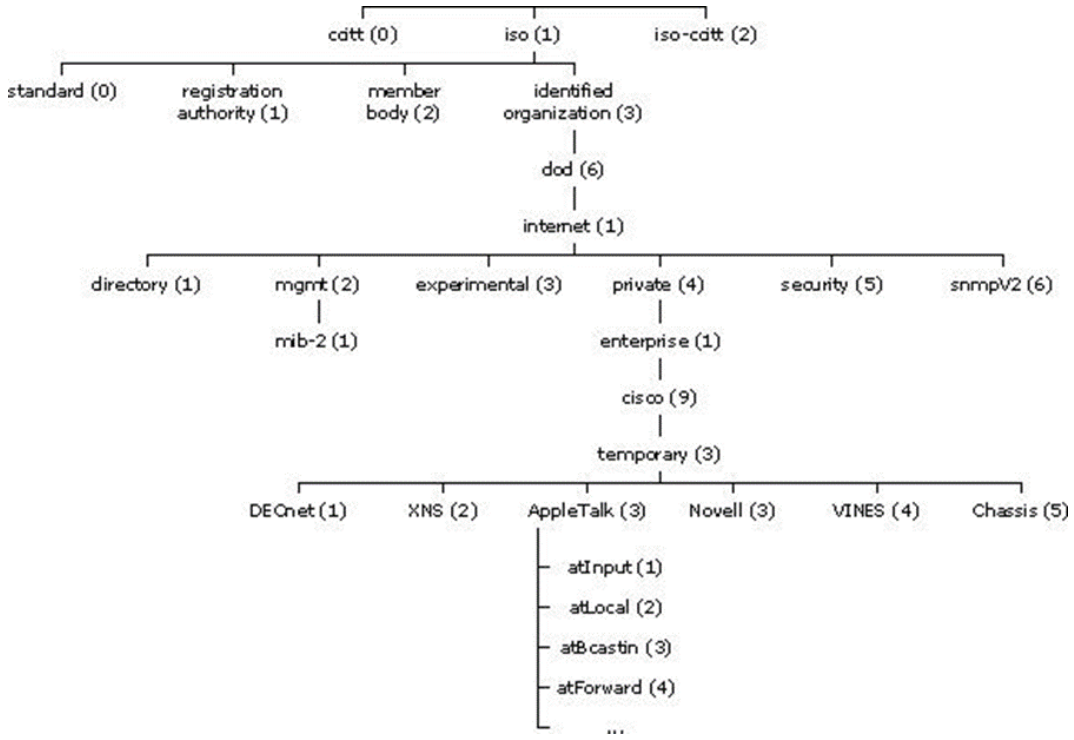

ILUSTRACIÓN 1-3 ÁRBOL DE JERARQUÍA MIB

El árbol MIB ilustra las variadas jerarquías asignadas por las diferentes organizaciones

Los identificadores de los objetos ubicados en la parte superior del árbol pertenecen a diferentes organizaciones estándares, mientras los identificadores de los objetos ubicados en la parte inferior del árbol son colocados por las organizaciones asociadas.

Los fabricantes pueden definir ramas privadas que incluyen los objetos administrados para sus propios productos. Las MIB's que no han sido estandarizadas típicamente están localizadas en la rama experimental.

El objeto administrado atInput podría ser identificado por el nombre de objeto *iso.identified-organization.dod.internet.private.enterprise.cisco.temporary.AppleTalk.atInputo* por el descriptor de objeto equivalente *1.3.6.1.4.1.9.3.3.1.*

El corazón del árbol MIB se encuentra compuesto de varios grupos de objetos, los cuales en su conjunto son llamados mib-2. Los grupos son los siguientes:

- System (1);
- Interfaces (2);
- AT (3);
- IP (4);
- ICMP (5);
- TCP (6);
- UDP (7);
- EGP (8);
- Transmission (10);
- SNMP (11).

Es importante destacar que la estructura de una MIB se describe mediante el estándar Notación Sintáctica Abstracta 1 (Abstract Syntax Notation One)[8]

1.3.4. Detalles del Protocolo

SNMP opera en la capa de aplicación del conjunto de protocolos de Internet (capa 7 del modelo OSI). El agente SNMP recibe solicitudes en el puerto UDP 161. El administrador puede enviar solicitudes de cualquier puerto de origen disponible para el puerto 161 en el agente. La respuesta del agente será enviada de vuelta al puerto de origen en el gestor. El administrador recibe notificaciones (Trampas e InformRequests) en el puerto 162. El agente puede generar notificaciones desde cualquier puerto disponible. Cuando se utiliza con Transport Layer Security las solicitudes se reciben en el puerto 10161 y trampas se envían al puerto 10162. SNMPv1 especifica cinco unidades de datos de protocolo (PDU) centrales. Otros dos PDU, GetBulkRequest e InformRequests se añadieron en SNMPv2 y prorrogados a SNMPv3. (NET-SNMP, 2017)

Todas las PDU SNMP se construyen de la siguiente manera:

- Cabecera IP
- Encabezado UDP versión comunidad
- Tipo de PDU
- Petición-ID
- Error de estado
- Índice de errores
- Enlaces de variables

[8] https://es.wikipedia.org/wiki/ASN.1

1.3.5. Mensajes SNMP

Para realizar las operaciones básicas de administración anteriormente nombradas, el protocolo SNMP utiliza un servicio no orientado a la conexión (UDP) para enviar un pequeño grupo de mensajes (*unidades de protocolo de datos o PDUs*) entre los administradores y agentes. La utilización de un mecanismo de este tipo asegura que las tareas de administración de red no afectarán al rendimiento global de la misma, ya que se evita la utilización de mecanismos de control y recuperación como los de un servicio orientado a la conexión, por ejemplo, TCP.

Los puertos UDP comúnmente utilizados para SNMP se encuentran en la

Número	Descripción
161	SNMP
162	SNMP - trap

TABLA 1-1 PUERTOS SNMP

Los paquetes utilizados para enviar consultas y respuestas SNMP poseen el formato que se muestra en la Ilustración 1-4:

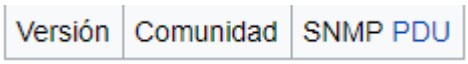

ILUSTRACIÓN 1-4 FORMATO DE CONSULTAS Y RESPUESTAS SNMP

- Versión: Número de versión de protocolo que se está utilizando (por ejemplo 0 para SNMPv1, 1 para SNMPv2c, 2 para SNMPv2p y SNMPv2u, 3 para SNMPv3, ...);
- Comunidad: Nombre o palabra clave que se usa para la autenticación. Generalmente existe una comunidad de lectura llamada "public" y una comunidad de escritura llamada "private";
- SNMP PDU: Contenido de la Unidad de Datos de Protocolo, el que depende de la operación que se ejecute.

Los mensajes GetRequest, GetNextRequest, SetRequest y GetResponse utilizan la estructura que se muestra en la Ilustración 1-5 en el campo SNMP PDU:

Tipo	Identificador	Estado de error	Índice de error	Enlazado de variables

ILUSTRACIÓN 1-5 ESTRUCTURA SNMP PDU

- Identificador: Es un número utilizado por el NMS y el agente para enviar solicitudes y respuesta diferentes en forma simultánea;
- Estado e índice de error: Sólo se usan en los mensajes GetResponse (en las consultas siempre se utiliza cero). El campo "índice de error" sólo se usa cuando "estado de error" es distinto de 0 y posee el objetivo de proporcionar información adicional sobre la causa del problema. El campo "estado de error" puede tener los siguientes valores:
  - 0: No hay error;
  - 1: Demasiado grande;
  - 2: No existe esa variable;
  - 3: Valor incorrecto;
  - 4: El valor es de solo lectura;
  - 5: Error genérico.
- Enlazado de variables: Es una serie de nombres de variables con sus valores correspondientes (codificados en ASN.1).

GetRequest

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

GetNextRequest

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

SetRequest

Este tipo de mensaje es utilizado por el NMS para solicitar a un agente modificar valores de objetos. Para realizar esta operación el NMS envía al agente una lista de nombres de objetos con sus correspondientes valores.

GetResponse

Este mensaje es usado por el agente para responder un mensaje GetRequest, GetNextRequest, o SetRequest. En el campo "Identificador de Request" lleva el mismo identificador que el "Request" al que está respondiendo.

Trap

Una trap es generado por el agente para reportar ciertas condiciones y cambios de estado a un proceso de administración. El formato de la PDU se muestra en la

ILUSTRACIÓN 1-6 ESTRUCTURA PDU DE UN TRAP

- Enterprise: Identificación del subsistema de gestión que ha emitido el trap;
- Dirección del agente: Dirección IP del agente que ha emitido el trap;
- Tipo genérico de trap:
    - Cold start (0): Indica que el agente ha sido inicializado o reinicializado;
    - Warm start (1): Indica que la configuración del agente ha cambiado;
    - Link down (2): Indica que una interfaz de comunicación se encuentra fuera de servicio (inactiva);
    - Link up (3): Indica que una interfaz de comunicación se encuentra en servicio (activa);
    - Authentication failure (4): Indica que el agente ha recibido un requerimiento de un NMS no autorizado (normalmente controlado por una comunidad);
    - EGP neighbor loss (5): Indica que en sistemas en que los Routers están utilizando el protocolo EGP, un equipo colindante se encuentra fuera de servicio;
    - Enterprise (6): En esta categoría se encuentran todos los nuevos traps incluidos por los vendedores.
- Tipo específico de trap: Es usado para traps privados (de fabricantes), así como para precisar la información de un determinado trap genérico;
- Timestamp: Indica el tiempo que ha transcurrido entre la re-inicialización del agente y la generación del trap;
- Enlazado de variables: Se utiliza para proporcionar información adicional sobre la causa del mensaje.

GetBulkRequest

Este mensaje es usado por un NMS que utiliza la versión 2 o 3 del protocolo SNMP típicamente cuando es requerida una larga transmisión de datos, tal como la recuperación de largas tablas. En este sentido es similar al mensaje GetNextRequest usado en la versión 1 del protocolo, sin embargo, GetBulkRequest es un mensaje que implica un método mucho más rápido y eficiente, ya que a través de un solo mensaje es posible solicitar la totalidad de la tabla.

InformRequest

Un NMS que utiliza la versión 2 o 3 del protocolo SNMP transmite un mensaje de este tipo a otro NMS con las mismas características, para notificar información sobre objetos administrados, utilizando el protocolo de nivel 4(OSI) TCP, y enviara el InformRequest hasta que tenga un acuse de recibo.

1.3.6. Desarrollo y Uso

Versión 1

SNMP versión 1 (SNMPv1) es la implementación inicial del protocolo SNMP. SNMPv1 opera a través de protocolos como el User Datagram Protocol (UDP), Protocolo de Internet (IP), servicio de red sin conexión OSI (CLNS), AppleTalk Protocolo de datagramas de entrega (DDP), y Novell Internet Packet Exchange (IPX). SNMPv1 es ampliamente utilizado y es el de facto protocolo de gestión de red en la comunidad de Internet.

Los primeros RFCs para SNMP, ahora conocido como SNMPv1, aparecieron en 1988:

- RFC 1065 - Estructura e identificación de información de gestión para internet basadas en TCP / IP (The Internet Engineering Task Force, 1988)
- RFC 1066 - Base de información de gestión para la gestión de la red de internet basadas en TCP / IP. (The Internet Engineering Task Force, 1988)
- RFC 1067 - Un protocolo simple de administración de red. (The Internet Engineering Task Force, 1988)

Estos protocolos estaban obsoletos por:

- RFC 1155 - Estructura e identificación de información de gestión para internet basadas en TCP / IP. (The Internet Engineering Task Force, 1990)
- RFC 1156 - Base de información de gestión para la gestión de la red de internet basadas en TCP / IP. (The Internet Engineering Task Force, 1990)
- RFC 1157 - Un protocolo simple de administración de red. (The Internet Engineering Task Force, 1990)

Después de un corto tiempo, RFC 1156 (MIB-1) fue reemplazada por la más habitual:

- RFC 1213 - Versión 2 de la base de información de gestión (MIB-2) para la gestión de la red de internet basadas en TCP / IP. (The Internet Engineering Task Force, 1991)

Versión 1 ha sido criticado por su falta de seguridad. La autenticación de los clientes se realiza sólo por una "cadena de comunidad", en efecto, un tipo de contraseña, la cual transmite en texto plano. El diseño de los años 80 de SNMPv1 fue realizado por un grupo de colaboradores que vieron que el producto patrocinado oficialmente (HEMS/CMIS/CMIP) por OSI (Open System Interconnection) / IETF (Internet Engineering Task Force/) NSF (National Science Foundation) eran tanto inaplicable en las plataformas informáticas de la época, así como potencialmente inviable. SNMP se aprobó basándose en la creencia de que se trataba de un Protocolo provisional necesario para la toma de medidas del despliegue a gran escala de Internet y su comercialización. En esos tiempos, estándares de internet de autenticación y seguridad eran un sueño, a la vez desalentado por los grupos de diseño enfocados en protocolos.

Versión 2

SNMPv2 RFC 1441 (The Internet Engineering Task Force, 1993) - RFC 1452 (The Internet Engineering Task Force, 1993), revisa la versión 1 e incluye mejoras en las áreas de comunicaciones de rendimiento, la seguridad, confidencialidad e-manager-a gerente. Introdujo GetBulkRequest, una alternativa a GetNextRequests iterativos para recuperar grandes cantidades de datos de gestión en una sola solicitud. Sin embargo, el nuevo sistema de seguridad basado en partidos en SNMPv2, visto por muchos como demasiado complejo, no fue ampliamente aceptada. Esta versión de SNMP alcanzado el nivel de madurez de Norma, pero se consideró obsoleto por las versiones posteriores.

Simple basada en la comunidad la version Network Management Protocol 2, o SNMPv2c, se define en el RFC 1901 (The Internet Engineering Task Force, 1996) - RFC 1908 (The Internet Engineering Task Force, 1989). SNMPv2c comprende SNMPv2 sin el nuevo modelo de seguridad de SNMP v2 controversial, utilizando en su lugar el sistema de seguridad basado en la simple comunidad de SNMPv1. Esta versión es una de las relativamente pocas normas para cumplir con el proyecto de nivel de madurez estándar del IETF, y fue considerado el de facto estándar SNMPv2. Es también estaba obsoleto después, por SNMPv3. (Huidobro, 1997)

Simple de usuario basada en la versión Network Management Protocol 2, o SNMPv2u, se define en el RFC 1909 (The Internet Engineering Task Force, 1996) - RFC 1910 (The Internet Engineering Task Force, 1996). Este es un compromiso que pretende ofrecer una mayor seguridad que SNMPv1, pero sin incurrir en la alta complejidad de

SNMPv2. Una variante de este se comercializó como SNMP v2, y el mecanismo fue finalmente adoptado como uno de los dos marcos de seguridad de SNMP v3.

SNMPv1 y SNMPv2c interoperabilidad

Tal como está actualmente especificada, SNMPv2c es incompatible con SNMPv1 en dos áreas clave: los formatos de mensajes y operaciones de protocolo. Mensajes SNMPv2c utilizan diferentes cabeceras y la unidad de datos de protocolo (PDU) formatos de mensajes SNMPv1. SNMPv2c también utiliza dos operaciones de protocolo que no están especificados en SNMPv1. Además, RFC 2576 (The Internet Engineering Task Force, 2000) define dos posibles estrategias de coexistencia SNMPv1/v2c: agentes de proxy y sistemas de gestión de red bilingües.

Agentes de proxy

Un agente SNMPv2 puede actuar como un agente proxy en nombre de dispositivos SNMPv1 administrados, de la siguiente manera:

- Un SNMPv2 NMS emite un comando destinado a un agente SNMPv1.
- El NMS envía el mensaje SNMP para el agente proxy SNMPv2.
- El agente proxy reenvía Cómo, GetNext y Set mensajes al agente SNMPv1 sin cambios.
- Mensajes GetBulk son convertidas por el agente proxy de GetNext mensajes y luego se envían al agente SNMPv1. El agente proxy mapas de mensajes de captura SNMPv1 a SNMPv2 mensajes de captura y luego las envía al NMS.

Sistema de gestión de la red bilingüe

Sistemas de gestión de red SNMPv2 Bilingües soportan tanto SNMPv1 y SNMPv2. Para apoyar este entorno de gestión dual, una aplicación para la gestión del NMS bilingües debe ponerse en contacto con un agente. El NMS examina la información almacenada en una base de datos local para determinar si el agente es compatible con SNMPv1 o SNMPv2. Sobre la base de la información en la base de datos, el NMS se comunica con el agente utilizando la versión adecuada de SNMP.

Versión 3

Aunque SNMPv3 no realiza cambios en el protocolo, aparte de la adición de seguridad criptográfica, da la impresión de ser muy diferente debido a las nuevas convenciones textuales, los conceptos y la terminología.

SNMPv3 añadió principalmente la seguridad y mejoras de configuración remota SNMP. Debido a la falta de seguridad de las versiones previas de SNMP, los administradores de red usaban otros medios, tales como SSH para la configuración, contabilidad y gestión de fallos.

SNMPv3 se ocupa de cuestiones relacionadas con el despliegue a gran escala de SNMP, contabilidad y gestión de fallos. Actualmente, SNMP se utiliza principalmente para el control y la gestión del rendimiento.

SNMPv3 define una versión segura de SNMP y también facilita la configuración remota de las entidades SNMP. SNMPv3 ofrece un entorno seguro para la gestión de sistemas que abarcan los siguientes:

- Identificación de las entidades SNMP para facilitar la comunicación sólo entre entidades SNMP conocidas - Cada entidad SNMP tiene un identificador llamado snmpEngineID y comunicación SNMP es posible sólo si la entidad SNMP conoce la identidad de su interlocutor. Trampas y notificaciones son excepciones a esta regla.
- Soporte para los modelos de seguridad - Un modelo de seguridad puede definir la política de seguridad dentro de un dominio administrativo o una intranet. SNMPv3 contiene las especificaciones para USM.

Definición de los objetivos de seguridad, donde los objetivos del servicio de autenticación de mensajes incluyen la protección contra lo siguiente:

- Modificación de la información - Protección contra algunos no autorizados entidad que altera SNMP en tránsito mensajes generados por un principal autorizado.
- Masquerade - Protección contra intentar operaciones de gestión no autorizadas por algún director al asumir la identidad de otra principal que cuenta con las autorizaciones correspondientes.
- Mensaje Corriente Modificación - Protección contra mensajes que consiguen maliciosamente reordenado, retrasado, o reproducido para efectuar las operaciones de gestión autorizadas.
- Divulgación - Protección contra escuchas en los intercambios entre los motores de SNMP.

Especificación para USM - USM (Modelo de seguridad basada en el usuario) consiste en la definición general de los siguientes mecanismos de comunicación disponibles:

- Comunicación sin autenticación y privacidad (noAuthNoPriv).
- La comunicación con la autenticación y sin privacidad (authNoPriv).
- La comunicación con la autenticación y la privacidad (authpriv).
- Definición de diferentes protocolos de autenticación y privacidad - Actualmente, los protocolos de autenticación MD5 y SHA y los protocolos de privacidad y CBC_DES CFB_AES_128 se admiten en la USM.
- Definición de un procedimiento de descubrimiento - Para encontrar el snmpEngineID de una entidad SNMP para una dirección de transporte común y dirección de punto final de transporte.
- Definición del procedimiento de sincronización de hora - Para facilitar la comunicación autenticado entre las entidades SNMP.
- Definición del marco MIB SNMP - Para facilitar la configuración remota y administración de la entidad SNMP.
- Definición de las MIB USM - Para facilitar la configuración remota y administración del módulo de seguridad.
- Definición de las MIB VACM - Para facilitar la configuración remota y administración del módulo de control de acceso.

El SNMPv3 se centra en dos aspectos principales, a saber, la seguridad y la administración. El aspecto de seguridad se dirige, ofreciendo tanto una sólida autenticación y cifrado de datos para la privacidad. El aspecto de la administración se centra en dos partes, a saber, los originadores de notificación y agentes proxy. SNMPv3 define una serie de capacidades relacionadas con la seguridad. Las especificaciones iniciales definen la USM y VACM, que más tarde fueron seguidos por un modelo de seguridad de transporte que proporciona apoyo a través de SSH y SNMPv3 en TLS y DTLS.

- USM (Modelo de Seguridad basado en Usuarios) proporciona funciones de autenticación y privacidad (encriptación) y opera en el nivel de mensaje.
- VACM (Modelo de Control de Acceso basado en Vista) determina si se permite a un director dado acceso a un objeto MIB particular, para realizar funciones específicas y opera en el nivel de PDU.
- TSM (Modo de Seguridad del Transporte) proporciona un método para la autenticación y el cifrado de mensajes a través de los canales externos de seguridad. Dos transportes, SSH y TLS/DTLS, han definido que hacen uso de la especificación de TSM.

La seguridad ha sido la mayor debilidad de SNMP desde el principio. La autenticación en las versiones de SNMP 1 y 2 consiste sólo en una contraseña (cadena de comunidad) enviada en texto claro entre un gerente y agente. Cada mensaje SNMPv3 contiene los parámetros de seguridad que están codificados como una cadena de octetos. El significado de estos parámetros de seguridad depende del modelo de seguridad que se utiliza. SNMPv3 proporciona características de seguridad importantes:

- Confidencialidad - El cifrado de paquetes para impedir la escucha por una fuente no autorizada.
- Integridad - Integridad de los mensajes para asegurar que un paquete no ha sido alterado durante el tránsito que incluye un mecanismo opcional por repetición de paquetes.
- Autenticación - para comprobar que el mensaje es de una fuente válida.

A partir de 2004 el IETF reconoce el Protocolo de Gestión de Red Simple versión 3 como se define en el RFC 3411 (The Internet Engineering Task Force, 2002) - RFC 3418 (también conocido como STD0062 (The Internet Engineering Task Force, 2002)) como la versión estándar actual de SNMP. El IETF ha designado SNMPv3 un completo estándar de Internet, el más alto nivel de madurez de un RFC. Considera versiones anteriores sean obsoletos (designándolos diversamente "Histórico" u "Obsoleto"). En la práctica, las implementaciones de SNMP a menudo soportan múltiples versiones: Típicamente SNMPv1, SNMPv2c y SNMPv3.

Dificultades de implementación

Las implementaciones del protocolo SNMP pueden variar entre diferentes fabricantes. En algunos casos, el SNMP es incorporado como una característica adicional en el sistema y no como un elemento fundamental del mismo. Algunos fabricantes tienden a ampliar en exceso su interfaz de línea de comandos (CLI) propietaria para configurar y controlar sus sistemas.

La estructura tipo árbol aparentemente simple y el indexado lineal del SNMP pueden no ser interpretados suficientemente bien por las estructuras de datos que son elementos del diseño básico de una plataforma. En consecuencia, el procesamiento de consultas SNMP en ciertos conjuntos de dato pueden exigir más uso del CPU del necesario. Por ejemplo, se crearían tablas de enrutamiento más grandes de lo normal, como BGP y IGP.

Algunos valores de SNMP (como los valores tabulares) requieren conocer específicamente los esquemas de los índices, los cuales no son necesariamente consistentes en todas las plataformas. Esto puede causar problemas de correlación entre los valores de diferentes equipos que no usan el mismo esquema en sus índices (por ejemplo, al recopilar métricas sobre la utilización del disco cuando un "identificador de disco" específico sea diferente entre plataformas.

1.4. Zabbix

Zabbix fue creado por Alexei Vladishev, y actualmente es desarrollado y apoyado activamente por Zabbix SIA. Es una solución de monitoreo distribuido de código abierto de clase empresarial.

Zabbix es un software que supervisa numerosos parámetros de una red y la integridad y salud de los servidores. Zabbix utiliza un mecanismo de notificación flexible que permite a los usuarios configurar alertas basadas en correo electrónico para prácticamente cualquier evento. Esto permite una reacción rápida a los problemas del servidor. Zabbix ofrece excelentes funciones de generación de informes y visualización de datos basadas en los datos almacenados. Esto hace que Zabbix sea ideal para la planificación de la capacidad.

Zabbix soporta tanto sondeo como captura. Todos los informes y estadísticas de Zabbix, así como los parámetros de configuración, se acceden a través de un web front-end. Un front-end basado en web asegura que el estado de su red y la salud de sus servidores se pueden evaluar desde cualquier ubicación. Configurado correctamente, Zabbix puede desempeñar un papel importante en el monitoreo de la infraestructura de TI. Esto es igualmente cierto para las pequeñas organizaciones con algunos servidores y para las grandes empresas con una multitud de servidores.

Zabbix está libre de costo. Zabbix está escrito y distribuido bajo la licencia GPL General Public License versión 2. Esto significa que su código fuente está libremente distribuido y disponible para el público en general. (Zabbix SIA, 2016)

1.4.1. Información General

Arquitectura

Zabbix se compone de varios componentes de software importantes, cuyas responsabilidades se describen a continuación.

Servidor

El servidor Zabbix es el componente central al que los agentes informan la disponibilidad y la integridad de la información y las estadísticas. El servidor es el repositorio central en el que se almacenan todos los datos de configuración, estadísticos y operacionales.

Almacenamiento de base de datos

Toda la información de configuración, así como los datos recogidos por Zabbix se almacenan en una base de datos.

Interfaz web

Para un fácil acceso a Zabbix desde cualquier lugar y desde cualquier plataforma, se proporciona la interfaz basada en web. La interfaz es parte del servidor de Zabbix, y normalmente (pero no necesariamente) se ejecuta en la misma máquina física que la que ejecuta el servidor.

Proxy

El proxy Zabbix puede recopilar datos de rendimiento y disponibilidad en nombre del servidor Zabbix. Un proxy es una parte opcional del despliegue de Zabbix; sin embargo, puede ser muy beneficioso distribuir la carga de un solo servidor Zabbix.

Agente

Los agentes Zabbix se implementan en objetivos de monitoreo para monitorear activamente los recursos y las aplicaciones locales y reportar los datos recopilados al servidor Zabbix.

Flujo de datos

Además, es importante dar un paso atrás y echar un vistazo al flujo de datos general dentro de Zabbix. Para crear un elemento que reúne datos, primero debe crear un host. Al pasar al otro extremo del espectro Zabbix, primero debe tener un elemento para crear un disparador. Debe tener un disparador para crear una acción. Por lo tanto, si desea recibir una alerta de que su CPU lo carga demasiado alto en el servidor X, primero debe crear una entrada de host para el servidor X seguida de un elemento para supervisar su CPU, luego un disparador que se activa si la CPU es demasiado alta por una acción que le envía un correo electrónico. Mientras que puede parecer un montón de pasos, con el uso de plantillas realmente no lo es. Sin embargo, debido a este diseño es posible crear una configuración muy flexible. (Zabbix SIA, 2016)

1.4.2. Características de Zabbix

Zabbix es una solución de monitorización de red altamente integrada, que ofrece una multiplicidad de características en un solo paquete.

- Recolección de datos
- Comprobaciones de disponibilidad y rendimiento
- Soporte para SNMP (captura y sondeo), IPMI, JMX, supervisión de VMWare
- Controles personalizados
- Recopilación de datos deseados a intervalos personalizados
- Realizada por servidor / proxy y por agentes

Definiciones de umbrales flexibles

Puede definir umbrales de problemas muy flexibles, llamados disparadores, referenciando valores desde la base de datos de back-end

Alarmas altamente configurables

- Las notificaciones de envío se pueden personalizar para el calendario de escalado, el destinatario, el tipo de medio
- Las notificaciones pueden ser significativas y útiles usando variables macro
- Las acciones automáticas incluyen comandos remotos

Gráficos en tiempo real

Los elementos supervisados se grafican de inmediato utilizando la funcionalidad gráfica incorporada

Capacidades de monitorización web

Zabbix puede seguir un camino de clics simulados del ratón en un sitio web y comprobar la funcionalidad y el tiempo de respuesta

Amplias opciones de visualización

Capacidad de crear gráficos personalizados que pueden combinar varios elementos en una sola vista

Mapas de red

Pantallas personalizadas y presentaciones de diapositivas para una vista general del cuadro de mandos

Informes

Vista de alto nivel (empresarial) de los recursos supervisados

Almacenamiento de datos históricos

- Datos almacenados en una base de datos
- Historial configurable
- Procedimiento de limpieza incorporado

Fácil configuración

- Agregar dispositivos supervisados como hosts
- Los hosts son recogidos para el seguimiento, una vez en la base de datos
- Aplicar plantillas a dispositivos supervisados

Uso de plantillas

- Agrupación de controles en plantillas
- Las plantillas pueden heredar otras plantillas

Detección de redes

- Descubrimiento automático de dispositivos de red
- Registro automático de agente
- Descubrimiento de sistemas de archivos, interfaces de red y OID SNMP

Interfaz web rápida

- Un front-end basado en web en PHP
- Accesible desde cualquier lugar
- Puede hacer clic en el registro de auditoría

API de Zabbix

Zabbix API proporciona una interfaz programable para Zabbix para manipulaciones masivas, integración de software de terceros y otros propósitos.

Sistema de permisos

- Autenticación segura de usuarios
- Ciertos usuarios pueden limitarse a ciertas vistas

Agente ampliamente extenso y fácilmente disponible

- Desplegado en objetivos de monitoreo
- Puede desplegarse tanto en Linux como en Windows

Demonios binarios

- Escritos en C, para rendimiento y huella de memoria pequeña
- Fácilmente portátil

Listo para entornos complejos

Monitoreo remoto facilitado mediante el uso de un proxy Zabbix.

1.4.3. Requerimientos de Zabbix

Hardware

Zabbix requiere de ambas memorias tanto memoria física como espacio en disco duro; 128 Mb en memoria física y 256 Mb libres en disco duro para punto de inicio. Independientemente la cantidad requerida en espacio de disco duro dependerá del número de hosts y paramentos que serán monitoreados si se planea mantener un largo historial de parámetros monitoreados es posible que se necesiten un par de gigabytes para mantener un espacio suficiente para almacenar el historial en la base de datos. (Zabbix SIA, 2016)

CPU

Zabbix y en especial la base de datos de Zabbix pueden requerir recursos significantes de CPU dependiendo del número de parámetros monitoreados y el motor de base de datos elegida.

Otro tipo de hardware

Para el soporte de notificaciones vía SMS es requerido un puerto de comunicación Serial y un modem GSM serial, un convertidor USB-to-serial también puede funcionar.

En la 40Tabla 1-2 se puede apreciar las diferentes configuraciones de hardware que se ocupará Zabbix dependiendo de la cantidad de Host a monitorear.

Tamaño	Sistema Operativo	CPU/Memoria RAM	Base de datos	Host Monitoreados
Pequeña	CentOS	Virtual Appliance	MySQL InnoDB	100
Mediana	CentOS	2 CPU cores / 2GB	MySQL InnoDB	500
Grande	RedHat Enterprise Linux	4 CPU cores/ 8GB	RAID10 MySQL InnoDB or PostgreSQL	>1000
Enorme	RedHat Enterprise Linux	8 CPU cores/ 16GB	Fast RAID10 MySQL InnoDB or PostgreSQL	>10000

TABLA 1-2 CONFIGURACIÓN DEL HARDWARE DE ZABBIX

La configuración actual depende mucho del número de hosts activos y de la tasa de actualización. Es altamente recomendado correr la base de datos por separado para grandes cantidades de hosts.

Plataformas Soportadas.

Debido a los requerimientos de seguridad y la naturaleza indispensable de monitorear un servidor, UNIX es el único sistema operativo que puede dar consistentemente el rendimiento, la tolerancia a fallos y la adaptabilidad necesarios. Zabbix opera en las versiones líderes del mercado.

Zabbix es probado en las siguientes plataformas:

- Linux
- IBM AIX
- FreeBSD
- NetBSD
- OpenBSD
- HP-UX
- Mac OS X
- Solaris
- Windows: Todas las versiones de escritorio y servidores desde 2000 (Únicamente el Agente de Zabbix)

Zabbix puede trabajar en otro tipo sistemas operativos UNIX también.

Nota: Zabbix deshabilita el volcado de memoria sí es configurado con cifrado y no se iniciará sí el sistema no permite la desactivación de volcado de memoria.

Software

Zabbix es desarrollado alrededor del moderno servidor web Apache, motores de bases de datos líderes y un lenguaje de scripting PHP.

Sistemas Manejadores de bases de datos

En la Tabla 1-3 se pueden observar los diferentes motores de base de dato utilizados por Zabbix, así como la versión mínima requerida

Software	Versión	Comentarios
MySQL	**5.0.3 o Superior**	**Necesario sí MySQL es utilizado por Zabbix como servidor de base de datos Necesario InnoDB engines**
Oracle	**10g o superior**	**Necesario sí Oracle es utilizado por Zabbix como servidor de base de datos¡**
PostgreSQL	**8.1 o superior**	**Necesario sí PostgreSQL es utilizado por Zabbix como servidor de base de datos NOTA* se sugiere el uso de al menos PostgreSQL 8.3, el cual introduce mucho mejor el rendimiento del comando VACUUM**
SQLite	**3.3.5 o superior**	**Necesario sí SQLite es utilizado por Zabbix como servidor de base de datos**
IBM DB2	**9.7 o superior**	**Necesario sí IBM DB2 es utilizado por Zabbix como servidor de base de datos NOTA * El soporte de IBM DB2 es experimental**

TABLA 1-3 SMBD SOPORTADOS POR ZABBIX

Nota: Mientras que SQLite3 puede ser usado con Zabbix proxies sin ningún problema, no se recomienda el uso de SQLite3 en el servidor de Zabbix desde la versión 2.4.0, el acceso simultaneo del servidor y del front-end a la base de datos puede llevar a la corrupción de la base de datos.

Front-end

Para poder ejecutar la interfaz gráfica o front-end en la Tabla 1-4 se especifica el software necesario, así como los complementos para una correcta visualización de este.

Software	Versión	Comentarios
Apache	1.3.12 o superior	
PHP	5.4.0 o superior	
Extensiones de PHP:		
Gb	2.0 o superior	PHP GD extension must support PNG images (--with-png-dir), JPEG (--withjpeg-dir) images and FreeType 2 (--with-freetype-dir).
Bcmath		php-bcmath (--enable-bcmath)
Ctype		php-ctype (--enable-ctype)
libXML	2.6.15 o superior	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		xmlwriter php-xmlwriter, if provided as a separate package by the distributor.
Sesión		session php-session, if provided as a separate package by the distributor.
Sockets		sockets php-net-socket (--enable-sockets). Required for user script support.
Mbstring		mbstring php-mbstring (--enable-mbstring)
Gettext		gettext php-gettext (--with-gettext). Required for translations to work.
Ldap		ldap php-ldap. Required only if LDAP authentication is used in the frontend.
Ibm_db2		ibm_db2 Required if IBM DB2 is used as Zabbix backend database.
Mysqli		mysqli Required if MySQL is used as Zabbix backend database.
Oci8		oci8 Required if Oracle is used as Zabbix backend database.
Pgsql		pgsql Required if PostgreSQL is used as Zabbix backend database.
Sqlite3		sqlite3 Required if SQLite is used as Zabbix backend database.

TABLA 1-4 APLICACIONES NECESARIAS PARA LA INTERFAZ GRÁFICA

Nota: Zabbix puede trabajar con versiones anteriores de Apache, MySQL, Oracle y PostgreSQL

Navegador WEB en el lado del cliente

Cookies y Java Script deben estar habilitados.

Las últimas versiones de Google Chrome, Mozilla Firefox, Microsoft Internet Explorer, Microsoft Edge y Opera son compatibles. Otros navegadores (Apple Safari, Konqueror) también pueden funcionar con Zabbix.

Server

En la Tabla 1-5 se muestran las librerías necesarias para ejecutar el servidor

Requisito	Requisito Descripción
OpenIPMI	Requiere soporte para IPMI.
Libevent	Requerido para monitoreo IPMI y métricas masivas. Versión 1.4 o superior.
libssh2	Requerido para la compatibilidad con SSH. Versión 1.0 o superior.
Fping	Requerido para elementos de ping de ICMP.
Libcurl	Requiere para la supervisión web, la supervisión de VMWare y la autenticación SMTP. Para la autenticación SMTP, se requiere la versión 7.20.0 o superior.
Libiksemel	Requerido para el soporte de Jabber.
libxml2	Requerido para la supervisión de VMWare.
net-snmp	Necesario para la compatibilidad SNMP.
Librería	PCRE necesaria para soporte de expresiones regulares PCRE.

TABLA 1-5 LIBRERÍAS NECESARIAS PARA EL SERVIDOR

Java Gateway

Si obtuvo Zabbix desde el repositorio de origen o un archivo, las dependencias necesarias ya están incluidas en el árbol de origen.

Si obtuvo Zabbix desde el paquete de su distribución, entonces las dependencias necesarias ya están proporcionadas por el sistema de empaquetado.

En ambos casos, el software está listo para ser utilizado y no son necesarias descargas adicionales.

Sí, sin embargo, desea proporcionar sus versiones de estas dependencias (por ejemplo, si está preparando un paquete para alguna distribución de Linux), a continuación, se muestra la lista de versiones de la biblioteca con las que Java Gateway funciona. Zabbix puede trabajar con otras versiones de estas bibliotecas, también.

En la Tabla 1-6 se enumeran los archivos JAR que están actualmente agrupados con el Java gateway en el código original:

Library	License	Website	Comments
logback-core-0.9.27.jar	EPL 1.0, LGPL 2.1	http://logback.qos.ch/	Tested with 0.9.27, 1.0.13, and 1.1.1.
logback-classic-0.9.27.jar	EPL 1.0, LGPL 2.1	http://logback.qos.ch/	Tested with 0.9.27, 1.0.13, and 1.1.1.
slf4j-api-1.6.1.jar	MIT License	http://www.slf4j.org/	Tested with 1.6.1, 1.6.6, and 1.7.6.
android-json-4.3_r3.1.jar	Apache License 2.0	https://android.googlesource.com/platform/libcore/+/master/json	Tested with 2.3.3_r1.1 and 4.3_r3.1. See src/zabbix_java/lib/README for instructions on creating a JAR file.

TABLA 1-6 ARCHIVOS JAR NECESARIOS PARA EL GATEWAY

Tamaño de la base de datos

Los datos de configuración de Zabbix requieren una cantidad fija de espacio en disco y no crecen mucho.

El tamaño de la base de datos Zabbix depende principalmente de estas variables, que definen la cantidad de datos históricos almacenados:

a) Número de valores procesados por segundo

Este es el número medio de nuevos valores que el servidor Zabbix recibe cada segundo. Por ejemplo, si tenemos 3000 elementos para la supervisión con una frecuencia de actualización de 60 segundos, el número de valores por segundo se calcula como 3000/60 = 50.

Esto significa que se añaden 50 nuevos valores a la base de datos Zabbix cada segundo.

b) Configuración de la ama de llaves para la historia

Zabbix mantiene valores durante un período fijo de tiempo, normalmente varias semanas o meses. Cada nuevo valor requiere una cierta cantidad de espacio en disco para los datos y el índice.

Por lo tanto, si nos gustaría mantener 30 días de historia y recibimos 50 valores por segundo, el número total de valores estará alrededor de (30 * 24 * 3600) * 50 = 129.600.000, o unos 130M de valores.

Dependiendo del motor de base de datos utilizado, el tipo de valores recibidos (flotantes, enteros, cadenas, archivos de registro, etc.), el espacio en disco para mantener un valor único puede variar de 40 bytes a cientos de bytes. Normalmente es alrededor de 90 bytes por valor para los elementos numéricos. En nuestro caso, significa que 130M de valores requerirá 130M * 90 bytes = 10.9GB de espacio en disco. (Zabbix SIA, 2016)

1.4.4. Procesos de Zabbix

Server

Información general

El servidor Zabbix es el proceso central del software Zabbix.

El servidor realiza el sondeo y captura de datos, calcula disparadores, envía notificaciones a los usuarios. Es el componente central al que los agentes y proxies de Zabbix informan sobre disponibilidad e integridad de los sistemas. El servidor puede revisar remotamente los servicios en red (como servidores web y servidores de correo) mediante simples comprobaciones de servicio.

El servidor es el repositorio central en el que se almacenan todos los datos de configuración, estadísticos y operativos, y es la entidad de Zabbix la que alertará activamente a los administradores cuando surjan problemas en cualquiera de los sistemas supervisados.

El funcionamiento de un servidor básico de Zabbix se divide en tres componentes distintos; son: servidor Zabbix, front-end web y almacenamiento de bases de datos.

Toda la información de configuración de Zabbix se almacena en la base de datos, con la que interactúan tanto el servidor como el interfaz web. Por ejemplo, cuando crea un elemento nuevo utilizando el front-end web (o API), se agrega a la tabla de elementos de la base de datos. A continuación, aproximadamente una vez por minuto, el servidor Zabbix consultará la tabla de elementos para obtener una lista de los elementos activos que se almacenarán en un caché dentro del servidor Zabbix. Esta es la razón por la que puede tardar hasta dos minutos para que los cambios realizados en Zabbix front-end aparezcan en la última sección de datos. (Zabbix SIA, 2016)

Proceso del servidor

Si está instalado como paquete

El servidor Zabbix se ejecuta como un proceso de daemon. El servidor se puede iniciar ejecutando:

shell> service zabbix-server start

Esto funcionará en la mayoría de los sistemas GNU / Linux. En otros sistemas puede que tenga que ejecutar:

shell> /etc/init.d/zabbix-server start

Del mismo modo, para detener / reiniciar / ver el estado, utilice los siguientes comandos:

shell> service zabbix-server stop
shell> service zabbix-server restart
shell> service zabbix-server status

Inicio manual

Si lo anterior no funciona, debe iniciarlo manualmente. Encuentre la ruta al binario zabbix_server y ejecute:

shell> zabbix_server

Puede utilizar los parámetros que se muestran en la Tabla 1-7 en la línea de comandos con el servidor Zabbix:

Parámetro	Descripción
-c --config <file>	ruta al archivo de configuración (el valor predeterminado es /usr/local/etc/zabbix_server.conf)
-R --runtime-control <option>	realizar funciones administrativas
-h –help	Obtener ayuda
-V --version	Muestra en pantalla la versión

TABLA 1-7 PARÁMETROS DEL COMANDO ZABBIX_SERVER

Nota: El control de tiempo de ejecución no es compatible con OpenBSD y NetBSD.

Ejemplos de ejecución del servidor Zabbix con parámetros de línea de comandos:

shell> zabbix_server -c /usr/local/etc/zabbix_server.conf
shell> zabbix_server --help
shell> zabbix_server -V

Control de tiempo de ejecución

En la Tabla 1-8 se muestran las opciones de control de tiempo de ejecución:

Opción	Descripción	Objetivo
config_cache_reload	Recargar la caché de configuración Se ignora si se está cargando la caché.	
housekeeper_execute	Inicie el procedimiento de limpieza y se ignora si el procedimiento de limpieza está en curso.	
log_level_increase[=<target>]	Aumentar el nivel de registro, afecta a todos los procesos si no se especifica el destino.	pid - Identificador de proceso (1 a 65535) tipo de proceso - Todos los procesos de tipo especificado (por ejemplo, poller) tipo de proceso, N - Tipo de proceso y número (por ejemplo, poller, 3)
log_level_decrease[=<target>]	Disminuir el nivel de registro, afecta a todos los procesos si no se especifica el destino.	

TABLA 1-8 OPCIONES DEL CONTROL DE EJECUCIÓN DEL SERVIDOR

El intervalo permitido de PID para cambiar el nivel de registro de un único proceso Zabbix es de 1 a 65535. En sistemas con opciones PID grandes <tipo de proceso, N> se puede usar para cambiar el nivel de registro de un solo proceso.

Ejemplo de uso del control de tiempo de ejecución para recargar la configuración del servidor

shell> zabbix_server -c /usr/local/etc/zabbix_server.conf -R config_cache_reload

Ejemplo de uso del control de tiempo de ejecución para activar la ejecución de la ama de llaves:

shell> zabbix_server -c /usr/local/etc/zabbix_server.conf -R housekeeper_execute

Ejemplos de uso del control de tiempo de ejecución para cambiar el nivel de registro:

Aumentar el nivel de registro de todos los procesos:

shell> zabbix_server -c /usr/local/etc/zabbix_server.conf -R log_level_increase

Aumentar el nivel de registro del segundo proceso de poller:

shell> zabbix_server -c /usr/local/etc/zabbix_server.conf -R log_level_increase = poller, 2

Aumentar el nivel de registro del proceso con PID 1234:

s*hell> zabbix_server -c /usr/local/etc/zabbix_server.conf -R log_level_increase = 1234*

Disminuir el nivel de registro de todos los procesos de poller de http:

shell> zabbix_server -c /usr/local/etc/zabbix_server.conf -R log_level_decrease = "http poller"

proceso de usuario

El servidor Zabbix está diseñado para ejecutarse como un usuario no root. Se ejecutará como cualquier usuario no root que se inicie como. Por lo que puede ejecutar el servidor como un usuario no root sin ningún problema.

Si va a intentar ejecutarlo como 'root', cambiará a un usuario zabbix 'codificado', el cual debe estar presente en su sistema. Sólo puede ejecutar servidor como 'root' si modifica el parámetro 'AllowRoot' en el archivo de configuración del servidor.

Si el servidor y el agente Zabbix se ejecutan en el mismo equipo, se recomienda utilizar un usuario diferente para ejecutar el servidor que para ejecutar el agente. De lo contrario, si ambos se ejecutan como el mismo usuario, el agente puede acceder al archivo de configuración del servidor y cualquier usuario de nivel *Admin* en Zabbix puede recuperar fácilmente, por ejemplo, la contraseña de la base de datos.

scripts de arranque

Los scripts se utilizan para iniciar / detener automáticamente los procesos de Zabbix durante la puesta en marcha / apagado del sistema. Los scripts se encuentran en directorio misc / init.d.

Plataformas soportadas

Debido a los requisitos de seguridad y al carácter crítico de la operación del servidor, UNIX es el único sistema operativo que puede ofrecer consistentemente el rendimiento necesario, la tolerancia a fallos y la resistencia. Zabbix opera en versiones líderes del mercado.

El servidor Zabbix se prueba en las siguientes plataformas:

- Linux
- Solaris
- AIX
- HP-UX
- Mac OS X
- FreeBSD
- OpenBSD
- NetBSD
- SCO Open Server
- Tru64/OSF1

Agente

Información general

El agente Zabbix se implementa en un objetivo de supervisión para supervisar activamente los recursos y aplicaciones locales (discos duros, memoria, estadísticas de procesadores, etc.).

El agente reúne localmente la información operacional y reporta los datos al servidor Zabbix para su posterior procesamiento. En caso de fallos (como un disco duro en ejecución o un proceso de servicio bloqueado), el servidor Zabbix puede alertar activamente a los administradores de la máquina en particular que informó del fallo.

Los agentes de Zabbix son extremadamente eficientes debido al uso de llamadas del sistema nativo para recopilar información estadística.

Controles pasivos y activos

Los agentes Zabbix pueden realizar comprobaciones pasivas y activas.

En una comprobación pasiva, el agente responde a una solicitud de datos. El servidor Zabbix (o proxy) pide datos, por ejemplo, carga de la CPU, y el agente de Zabbix devuelve el resultado.

Los controles activos requieren un procesamiento más complejo. El agente debe recuperar primero una lista de elementos del servidor Zabbix para un procesamiento independiente. A continuación, periódicamente enviar nuevos valores al servidor.

Si se realizan comprobaciones pasivas o activas se configura seleccionando el tipo de elemento de supervisión respectivo. El agente Zabbix procesa elementos del tipo 'Agente Zabbix' o 'Agente Zabbix (activo)'.

Plataformas soportadas

El agente Zabbix es compatible con:

Linux

- IBM AIX
- FreeBSD
- NetBSD
- OpenBSD
- HP-UX
- Mac OS X
- Solaris: 9, 10, 11
- Windows: todas las versiones de escritorio y Windows Server desde XP

Agente en sistemas tipo UNIX

El agente Zabbix en sistemas tipo UNIX se ejecuta en el host que se está supervisando.

Si está instalado como paquete

El agente Zabbix se ejecuta como un proceso de daemon. El agente se puede iniciar ejecutando:

shell> service zabbix-agent inicio

Esto funcionará en la mayoría de los sistemas GNU / Linux. En otros sistemas puede que tenga que ejecutar:

shell> /etc/init.d/zabbix-agent start

Del mismo modo, para detener / reiniciar / ver el estado del agente Zabbix, utilice los siguientes comandos:

shell> service zabbix-agent stop
shell> service zabbix-agent restart
shell> service zabbix-agent status

Inicio manual

Si lo anterior no funciona, debe iniciarlo manualmente. Encuentre la ruta al binario zabbix_agentd y ejecute:

shell> zabbix_agentd

Agente en sistemas Windows

El agente Zabbix en Windows se ejecuta como un servicio de Windows, el cual se distribuye como un archivo zip. Después de descargar el archivo necesita descomprimirlo. Elija cualquier carpeta para almacenar el agente Zabbix y el archivo de configuración, ejemplo:

C: \ zabbix

Copie los archivos *bin \ win64 \ zabbix_agentd.exe* y *conf \ zabbix_agentd.win.conf* a *C: \ zabbix.*

Edite el archivo *c:\zabbix\zabbix_agentd.win.conf* según sus necesidades, asegurándose de especificar un parámetro "Hostname" correcto.

Instalación

Después de hacer esto, use el siguiente comando para instalar el agente de Zabbix como servicio de Windows:

C: \> c:\ zabbix\zabbix_agentd.exe -c c:\zabbix\zabbix_agentd.win.conf -i

Ahora debe ser capaz de configurar el servicio "agente Zabbix" normalmente como cualquier otro servicio de Windows.

Otras opciones de agente

Es posible ejecutar varias instancias del agente en un host. Una sola instancia puede utilizar el archivo de configuración predeterminado o un archivo de configuración especificado en la línea de comandos. En caso de múltiples instancias, cada instancia del agente debe tener su propio archivo de configuración (una de las instancias puede usar el archivo de configuración predeterminado).

Los parámetros de línea de comandos que se muestran en la Tabla 1-9 se pueden utilizar con el agente Zabbix:

Parámetro	Descripción
Agentes en UNIX y Windows	
-c –config <config-file>	Ruta de acceso al archivo de configuración. Puede utilizar esta opción para especificar un archivo de configuración que no sea el predeterminado. En UNIX, el valor predeterminado es /usr/local/etc/zabbix_agentd.conf o como se establece en variables de compilación --sysconfdir o --prefix En Windows, el valor predeterminado es c: \ zabbix_agentd.conf
-p –print	Imprimir los elementos conocidos y salir. Nota: Para devolver los resultados de los parámetros de usuario también, debe especificar el archivo de configuración (si no está en la ubicación predeterminada).
-t –test <ítem key>	Prueba de producto y de salida especificado. Nota: Para devolver los resultados de los parámetros de usuario también, debe especificar el archivo de configuración (si no está en la ubicación predeterminada).
-h –help	Muestra la información de ayuda
-V --version	Muestra la Información de la Versión
Agente en UNIX	
-R –runtime-control <option>	Realizar funciones administrativas. Consulte el control de tiempo de ejecución.
Agente en Windows	
-m –multiple-agents	Utilizar múltiples instancias de agente (con funciones -i, -d, -s, -x). Para distinguir los nombres de servicio de instancias, cada nombre de servicio incluirá el valor Hostname del archivo de configuración especificado.
Funciones del Agente en Windows	
-i –install	Instale el agente de Zabbix Windows como servicio
-d –uninstall	Desinstale el agente de Zabbix Windows como servicio
-s –start	Iniciar servicio de agente de Zabbix Windows
-x --stop	Detener servicio de agente de Zabbix Windows

TABLA 1-9 PARÁMETROS DEL AGENTE DE ZABBIX

Ejemplos específicos de uso de parámetros de línea de comandos:

- impresión de todos los elementos integrados del agente con valores:

shell> zabbix_agentd --print

- probar un parámetro de usuario con la clave "mysql.ping" definida en el archivo de configuración especificado

shell> zabbix_agentd -t "mysql.ping" -c /etc/zabbix/zabbix_agentd.conf

- instalar un servicio de "Agente Zabbix" para Windows utilizando la ruta de acceso predeterminada al archivo de configuración c: \ zabbix_agentd.conf

shell> zabbix_agentd.exe –i

- instalar un servicio "Agente Zabbix [Hostname]" para Windows utilizando el archivo de configuración zabbix_agentd.conf ubicado en la misma carpeta que el agente ejecutable y hacer que el nombre del servicio sea único extendiéndolo por el valor Hostname del archivo de configuración

shell> zabbix_agentd.exe -i -m -c zabbix_agentd.conf

Control de tiempo de ejecución

Con las opciones de control de tiempo de ejecución que se muestran en la **¡Error! No se encuentra el origen de la referencia.**, puede cambiar el nivel de registro de los procesos del agente:

Opción	Descripción	Target
log_level_increase[=<target>]	Aumentar el nivel de registro. Si no se especifica el destino, todos los procesos se ven afectados.	El objetivo se puede especificar como: identificador de proceso pid (1 a 65535) tipo de proceso - todos los procesos de tipo especificado (por ejemplo, poller) tipo de proceso, tipo de proceso N y número (por ejemplo, poller, 3)
log_level_decrease[=<target>]	Aumentar el nivel de registro. Si no se especifica el destino, todos los procesos se ven afectados.	

TABLA 1-10 OPCIONES DEL CONTROL DE EJECUCIÓN DEL AGENTE DE ZABBIX

Nota: Tenga en cuenta que el rango utilizable de PID para cambiar el nivel de registro de un proceso de agente único es de 1 a 65535. En sistemas con PID grandes, el <tipo de proceso, N> destino se puede utilizar para cambiar el nivel de registro de un solo proceso.

Ejemplos:

- aumentando el nivel de registro de todos los procesos

shell> zabbix_agentd -R log_level_increase

- aumento del nivel de registro del segundo proceso de escucha

shell> *zabbix_agentd -R log_level_increase=listener,2*

- aumentando el nivel de registro del proceso con PID 1234

shell> zabbix_agentd -R log_level_increase=1234

- disminución del nivel de registro de todos los procesos de comprobación activa

shell> zabbix_agentd -R log_level_decrease="active checks"

Proceso del Usuario

El agente Zabbix en UNIX está diseñado para ejecutarse como un usuario no root. Se ejecutará como cualquier usuario no root que se inicie como. Así que puede ejecutar el agente como cualquier usuario no root sin ningún problema.

Si va a intentar ejecutarlo como 'root', cambiará a un usuario Zabbix 'codificado', el cual debe estar presente en su sistema. Sólo puede ejecutar el agente como 'raíz' si modifica el parámetro 'AllowRoot' en el archivo de configuración del agente.

2. Capitulo II FCAPS UAEH

En el capítulo número dos, explicaremos el uso el modelo F.C.A.P.S. dentro del proceso de administración de la red dentro de la Universidad Autónoma del Estado de Hidalgo sobre el cual está fundamentado este trabajo.

2.1. Modelo F.C.A.P.S. Dentro de la U.A.E.H.

De acuerdo con el “Plan de Desarrollo Institucional” de la Universidad Autónoma del estado de Hidalgo en el “Capítulo VII. Infraestructura física” hasta el año 2017 se cuentan con 21 Institutos, Escuelas Superiores y Escuelas Preparatorias con un total de 78 Aulas de computo, 777 Cubículos y 21 bibliotecas (Universidad Autónoma del Estado de Hidalgo, 2017), los cuales ofrecen el acceso a internet de forma alámbrica e inalámbrica por medio de la red universitaria de datos a una población total de 56,908 estudiantes de los diferentes niveles educativos que ofrece la U.A.E.H. (Universidad Autónoma del Estado de Hidalgo, 2018).

En el punto 12.1.5 Del tema “Programas rectores e institucionales” menciona que se debe tener una planeación estratégica participativa en los diferentes sistemas de información y telecomunicaciones para ello la DIyS dentro de su manual de organización establece que las funciones principales del Área de Monitoreo y Operación de la Red son (Dirección de Información y Sistemas, 2007):

- El mantenimiento de la infraestructura tecnológica de forma física y lógica brindando seguridad, redundancia, confiabilidad, integridad, confidencialidad y disponibilidad de la información resguardada.
- La administración lógica de la red de datos alámbrica e inalámbrica (wifi y microondas) y telefonía de la UAEH.
- Monitorear el estado de los equipos de comunicaciones en producción.
- implementación de políticas de seguridad en los Firewall´s institucionales

Para realizar las funciones antes mencionadas se debe llevar un proceso de administración de la red para ello en el presente trabajo aplicara las diferentes actividades que se exponen dentro del modelo F.C.A.P.S. el cual esta estandarizado por la ISO/IEC 10040:1998[9] aplicada a las redes de datos en el modelo OSI.

2.1.1. Fault Management / Administración de Fallas

Una de las principales áreas de administración asociadas al modelo FCAPS es la administración de fallas.

La Universidad Autónoma del Estado de Hidalgo de las doce tareas de administración necesarias para un eficiente sistema de administración de fallas hace uso de las siguientes tareas:

1. Detección de falla.
    - Para este punto se apoya del Software denominado Orion, el cual hace uso del protocolo SNMP para verificar la integridad de la red.
2. Generación de alarmas.

[9] Visión general de la gestión de sistemas

- Cuando la falla ha sido detectada por el sistema, inmediatamente se genera una alarma, en este punto las alarmas se clasifican debido a su tipo y a su severidad.

3. Error de Registros
   - Una vez que la alarma se ha generado y clasificado se llevan a cabo una serie de pruebas de diagnóstico para verificar el tipo de falla que pueden ser de tipo física, lógica o de medición
4. Corrección de falla
   - En este punto se usan los mecanismos más recurridos los cuales pueden ser desde cambios a la configuración, la recarga de sistema o instalación/actualización del software hasta el remplazo parcial o total del recurso dañado
5. Recuperación de la red
   - Una vez que la falla ha sido solucionada, se regresa la alarma y un reporte en el cual se detalla el tipo de falla y la solución realizada

2.1.2. Configuration Management / Administración de Configuración

Es el proceso mediante el cual todas las operaciones diarias son monitoreadas y controladas asegurando una consistencia, repetición y auditable configuración en todos los equipos de red, basándose en una política de configuración.

La Universidad Autónoma del Estado de Hidalgo a través de la Dirección de Información y Sistemas y en particular en el Área de operación mantienen un proceso mediante el cual todas las operaciones son monitoreadas diariamente, para ello utilizan algunas de las tareas que el modelo FCAPS menciona las cuales son las siguientes:

1. Provisionamiento de red.
   - La Universidad Autónoma del Estado de Hidalgo tiene dentro de las tareas de la administración de configuración el tener el aprovisionamiento de todos los dispositivos de las cuales se usan dentro de la red universitaria.
2. Configuración Remota.
   - Una vez que los equipos de red han sido instalados y configurados básicamente se hace una configuración remota desde el NOC (Network Operation Center por sus siglas en ingles).
3. Copia de Configuración.
   - Una vez que se han configurado completamente se deben guardas las configuraciones realizadas para en algún caso falla posterior, la recuperación sea más rápida y eficaz
4. Copia de Seguridad y restauración.
   - La Universidad Autónoma del Estado de Hidalgo, dentro de sus equipos de red manejan los servidores, por este hecho, se tiene una política de en la

cual se establece que se deben tener copias de seguridad cada determinado tiempo.

5. Inventario y/o Gestión de activos.
    - El tener un control de todos los dispositivos de red tanto activos como en almacén

2.1.3. Accounting Management / Administración de la Contabilidad

La gestión de las cuentas es a menudo conocida como la gestión de la tarifación. El objetivo es reunir las estadísticas de los usuarios de los siguientes parámetros.

- Utilización de disco.
- Enlace de utilización.
- Tiempo de CPU.

Para ello la Universidad mantiene un seguimiento de los servicios de red, así como los recursos de cada dispositivo para administrar las operaciones de los equipos y de esta manera asignar permisos y contraseñas, así como la planificación de copias de seguridad del software y la sincronización.

2.1.4. Performance Management / Administración del Rendimiento

La gestión del rendimiento implica una vigilancia efectiva del tiempo de respuesta de la red, además permite preparar la red para un futuro.

Una ventaja de la gestión de rendimiento es que al recolectar los datos del rendimiento la red puede ser monitorizada y así indicar la capacidad o cuestiones de fiabilidad.

Para la Universidad Autónoma del Estado de Hidalgo la gestión de rendimiento se basa en 3 atributos principales los cuales permiten una correcta administración.

1. El Performance y recolección de datos
2. Los reportes de problemas
3. Mantener y examinar los registros históricos

2.1.5. Security Management / Administración de la Seguridad

La gestión de la seguridad es el proceso de controlar el acceso a recursos en la red. La seguridad de datos puede ser conseguida principalmente con la autenticación, el cifrado y la autorización configurada con el sistema operativo y la configuración de control de acceso del sistema de gestión de base de datos.

Por esto mismo las actividades que lleva a cabo la Universidad Autónoma del Estado de Hidalgo son las siguientes:

1. Protección de datos
   - Para esta actividad los datos se clasifican debido a su contenido
2. Acceso restrictivo a los recursos
   - Esta actividad tiene como objetivo la prevención de intrusos que puedan robar, alterar o eliminar información que pueda ser primordial a la institución
3. Registro de accesos
   - Con esta actividad se puede tener un mayor control al momento de accesos a los sistemas y/o dispositivos
4. Seguridad de alarma/Reporte de eventos

3. Capítulo III Requisitos e Instalación de Zabbix

En el capítulo II se especificarán los Prerrequisitos que necesitan para la instalación del servidor Zabbix, además de la instalación paso a paso en el servidor, así como la puesta a punto de las configuraciones y políticas de seguridad del servidor hasta llegar a la configuración de la interfaz gráfica

3.1. Prerrequisitos.

Antes de poder instalar Zabbix se deberá tener instalado y configurado LAMP en nuestro servidor.

LAMP es el acrónimo usado para describir un sistema de infraestructura de internet que usa las siguientes herramientas:

- **Linux**, el sistema operativo; En algunos casos también se refiere a LDAP.
- **Apache**, el servidor web;
- **MySQL/MariaDB**, el gestor de bases de datos;
- **Perl, PHP, o Python**, los lenguajes de programación.

La combinación de estas tecnologías es usada principalmente para definir la infraestructura de un servidor web, utilizando un paradigma de programación para el desarrollo (Universo Digital, 2016).

3.1.1. Apache

El servidor web Apache es uno de los servidores web más populares y potentes del mundo, debido a su facilidad de administración y flexibilidad además de ser un servidor web multi plataforma, de código abierto con una gama completa de características como CGI, SSL y dominios virtuales. (Liquid Web, 2015) Para instalar apache dentro de CentOS 7 se ejecutarán las siguientes instrucciones:

Paso 1: Como se observa en la Ilustración 3-1 se ejecutará el administrador de software “yum” y se instalará el paquete httpd el cual contiene los archivos necesarios para el servidor apache.

```
[root@localhost Desktop]# yum install httpd
```

ILUSTRACIÓN 3-1 COMANDO DE INSTALACIÓN DE APACHE

Paso 2: Se permitirá el acceso por medio de los puertos predeterminados para http y https a través del firewall de CentOS con los comandos que se muestran en la Ilustración 3-2 y se procederá a reiniciar el servicio del firewall.

```
[root@localhost emejia]# firewall-cmd --permanent --add-port=80/tcp
success
[root@localhost emejia]# firewall-cmd --permanent --add-port=443/tcp
success
[root@localhost emejia]# firewall-cmd --reload
success
```

ILUSTRACIÓN 3-2 COMANDOS PARA AGREGAR APACHE AL FIREWALL

Paso 3: Una vez instalado el servidor y actualizado los permisos necesarios en el firewall, se deberá habilitar e iniciar el servicio de apache, para ello se ejecutarán los comandos que aparecen en la Ilustración 3-3

```
[root@localhost Desktop]# systemctl enable httpd.service
Created symlink from /etc/systemd/system/multi-user.target.wants/httpd.service
o /usr/lib/systemd/system/httpd.service.
[root@localhost Desktop]# systemctl start httpd.service
```

ILUSTRACIÓN 3-3 COMANDO PARA HABILITAR E INICIAR EL SERVICIO DE APACHE

Una vez realizados los pasos anteriores se procederá a realizar una verificación del estado actual del servicio de apache, para ello se deberá ejecutar el comando que aparece en la Ilustración 3-4 el cual nos mostrará el número de identificación del proceso, así como la información detallada del proceso.

```
[root@localhost Desktop]# systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor preset
: disabled)
   Active: active (running) since Wed 2017-10-04 09:06:22 PDT; 19s ago
     Docs: man:httpd(8)
           man:apachectl(8)
 Main PID: 4122 (httpd)
   Status: "Total requests: 0; Current requests/sec: 0; Current traffic:   0 B/s
ec"
   CGroup: /system.slice/httpd.service
           ├─4122 /usr/sbin/httpd -DFOREGROUND
           ├─4129 /usr/sbin/httpd -DFOREGROUND
           ├─4130 /usr/sbin/httpd -DFOREGROUND
           ├─4131 /usr/sbin/httpd -DFOREGROUND
           ├─4132 /usr/sbin/httpd -DFOREGROUND
           └─4133 /usr/sbin/httpd -DFOREGROUND

Oct 04 09:06:22 localhost.localdomain systemd[1]: Starting The Apache HTTP Se...
Oct 04 09:06:22 localhost.localdomain httpd[4122]: AH00558: httpd: Could not ...
Oct 04 09:06:22 localhost.localdomain systemd[1]: Started The Apache HTTP Ser...
Hint: Some lines were ellipsized, use -l to show in full.
[root@localhost Desktop]#
```

ILUSTRACIÓN 3-4 COMANDO PARA VER EL ESTADO DEL SERVICIO DE APACHE

Otra manera para verificar el estado del servicio de apache es poder visualizar el contenido por medio de un navegador, para ello en una pestaña del navegador introduciremos la dirección *http:///localhost/* si nos encontramos dentro del servidor, o *http://<ip-del-servidor>/* si nos encontramos en una computadora dentro de la misma red.

3.1.2. MySQL/MariaDB

MariaDB Server es uno de los servidores de bases de datos más populares del mundo. Está hecho por los desarrolladores originales de MySQL. Es un reemplazo directo y mejorado para MySQL. MariaDB se usa porque es rápido, escalable y robusto, con un rico ecosistema de motores de almacenamiento, complementos y muchas otras herramientas que lo hacen muy versátil para una amplia variedad de casos de uso. (MariaDB, 2014)

MariaDB se desarrolla como software de código abierto y como base de datos relacional, proporciona una interfaz SQL para acceder a los datos. Para instalar MariaDB dentro de CentOS 7 se ejecutarán las siguientes instrucciones:

***Paso 1**:* Como se observa en la Ilustración 3-5 se ejecutará el administrador de software "yum" y se instalará el paquete mariadb-server el cual contiene los archivos necesarios para el servidor de base de datos, para este caso MariaDB.

ILUSTRACIÓN 3-5 COMANDO PARA LA INSTALACIÓN DE MARIADB

Paso 2: Una vez terminada la instalación del servidor de base de datos, es necesario habilitar e inicia el servicio, para ello se deberá ejecutar los comandos que aparecen en la Ilustración 3-6

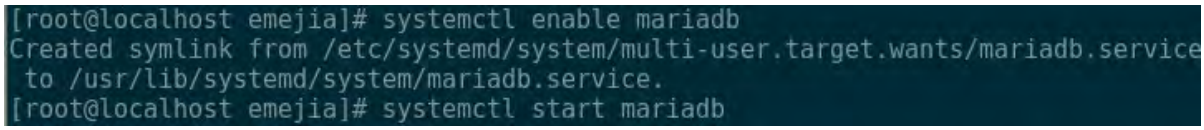

ILUSTRACIÓN 3-6 COMANDO PARA HABILITAR E INICIAR MARIADB

Nota: Por defecto en MySQL/MariaDB el usuario "root" viene sin contraseña, entonces, para prevenir accesos no autorizados a la base de datos, para ello pasaremos al siguiente paso.

Paso 3: Para ejecutar el script de configuración se escribirá el comando que aparece en la Ilustración 3-7 el cual nos guiará paso por paso.

ILUSTRACIÓN 3-7 SCRIPT PARA CONFIGURACIÓN DE SEGUIRDAD

El script proporciona una explicación detallada de cada paso como se muestra en la Ilustración 3-8 Las primeras instrucciones solicitarán la nueva contraseña del usuario root, una vez ingresada nos pedirá que confirmemos ingresando la misma contraseña.

Una vez actualizada la contraseña, aceptaremos las sugerencias de seguridad de MariaDB, y de la misma manera eliminará los usuarios anónimos y la base de datos de prueba y refrescará los privilegios de las tablas actuales.

```
NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
      SERVERS IN PRODUCTION USE!  PLEASE READ EACH STEP CAREFULLY!

In order to log into MariaDB to secure it, we'll need the current
password for the root user.  If you've just installed MariaDB, and
you haven't set the root password yet, the password will be blank,
so you should just press enter here.

Enter current password for root (enter for none):
OK, successfully used password, moving on...

Setting the root password ensures that nobody can log into the MariaDB
root user without the proper authorisation.

Set root password? [Y/n] Y
New password:
Re-enter new password:
Password updated successfully!
Reloading privilege tables..
 ... Success!
```

ILUSTRACIÓN 3-8 CONTENIDO DE SCRIPT DE SEGURIDAD DE MARIADB

3.1.3. PHP

PHP es un acrónimo recursivo de "PHP: Hypertext Preprocessor" es un lenguaje de programación de propósito general, altamente usado, especialmente apto para el desarrollo web y puede ser incorporado en HTML. (The PHP group, 2017)

PHP es el componente de nuestra configuración que procesará el código para mostrar contenido dinámico. Puede ejecutar scripts, conectarse a nuestras bases de datos MySQL para obtener información, y entregar el contenido procesado a nuestro servidor web para mostrar.

Para instalar PHP dentro de CentOS 7 se ejecutarán las siguientes instrucciones (Digital Ocean, 2014):

Paso 1: Como se observa en la Ilustración 3-9 se ejecutará el administrador de software “yum” y se instalarán los paquetes necesarios para el correcto funcionamiento de PHP en el servidor de CentOS.

```
[root@localhost Desktop]# yum install php php-cli php-common php-devel php-pear
php-gd php-mbstring php-mysql php-xml –y
```

ILUSTRACIÓN 3-9 COMANDO PARA INSTALAR PHP

Paso 2: Se verificará que la versión instalada sea la correcta, para ello se deberá crear un archivo llamado *"testphp.php"* dentro de la carpeta de publicaciones de apache, con el comando que aparece en la Ilustración 3-10, una vez creado se añadirán las líneas de código que aparecen en la Ilustración 3-11

```
[root@localhost Desktop]# vim /var/www/html/testphp.php
```

ILUSTRACIÓN 3-10 COMANDO Y UBICACIÓN DEL ARCHIVO "TESTPHP.PHP"

```
<?php
phpinfo();
?>
~
```

ILUSTRACIÓN 3-11 CONTENIDO DEL ARCHIVO TESTPHP.PHP

Una vez creado el archivo anterior, nos dirigiremos al navegador y si nos encontramos de manera local en nuestro servidor teclearemos la siguiente dirección *http://localhost/testphp.php* o *http://ip-del-servidor/testphp.php* si nos encontramos en una computadora dentro de la misma red, una vez cargada la página se mostrara una pantalla parecida a la Ilustración 3-12 donde nos arrojara un informe detallado acerca de la versión que se tiene instalado de php.

PHP Version 5.4.16

System	Linux localhost.localdomain 3.10.0-327.el7.x86_64 #1 SMP Thu Nov 19 22:10:57 UTC 2015 x86_64
Build Date	Nov 6 2016 00:30:05
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini
Scan this dir for additional .ini files	/etc/php.d
Additional .ini files parsed	/etc/php.d/curl.ini, /etc/php.d/dom.ini, /etc/php.d/fileinfo.ini, /etc/php.d/gd.ini, /etc/php.d/json.ini, /etc/php.d/mbstring.ini, /etc/php.d/mysql.ini, /etc/php.d/mysqli.ini, /etc/php.d/pdo.ini, /etc/php.d/pdo_mysql.ini, /etc/php.d/pdo_sqlite.ini, /etc/php.d/phar.ini, /etc/php.d/posix.ini, /etc/php.d/sqlite3.ini, /etc/php.d/sysvmsg.ini, /etc/php.d/sysvsem.ini, /etc/php.d/sysvshm.ini, /etc/php.d/wddx.ini, /etc/php.d/xmlreader.ini, /etc/php.d/xmlwriter.ini, /etc/php.d/xsl.ini, /etc/php.d/zip.ini
PHP API	20100412
PHP Extension	20100525
Zend Extension	220100525

ILUSTRACIÓN 3-12 VERSIÓN DE PHP

3.2. Instalación de Zabbix

Los paquetes oficiales de Zabbix están disponibles para RHEL 7, CentOS 7 y Oracle Linux 7, para ello se importará el paquete de configuración del repositorio oficial con el comando que se observa en la Ilustración. Este paquete contiene archivos de configuración necesarios para yum (software package manager).

```
[root@localhost Desktop]# rpm --import http://repo.zabbix.com/RPM-GPG-KEY-ZABBIX
[root@localhost Desktop]# rpm -ivh http://repo.zabbix.com/zabbix/3.4/rhel/7/x86_
64/zabbix-release-3.4-1.el7.centos.noarch.rpm
Retrieving http://repo.zabbix.com/zabbix/3.4/rhel/7/x86_64/zabbix-release-3.4-1.
el7.centos.noarch.rpm
Preparing...                          ################################# [100%]
Updating / installing...
   1:zabbix-release-3.4-1.el7.centos  ################################# [100%]
[root@localhost Desktop]#
```

ILUSTRACIÓN 3-13 COMANDO PARA IMPORTAR EL PAQUETE DE ZABBIX

Una vez importados los paquetes se procederá a instalar los paquetes con el administrador de software “yum” con el comando que aparece en Ilustración 3-14:

```
[root@localhost Desktop]# yum install zabbix-server-mysql zabbix-web-mysql zabbi
x-agent zabbix-get zabbix-sender zabbix-java-gateway -y
```

ILUSTRACIÓN 3-14 COMANDO PARA LA INSTALACIÓN DE ZABBIX

3.2.1. Crear base de datos

Para servidores Zabbix y daemons proxy se requiere una base de datos, que a su vez no es necesaria para ejecutar el agente Zabbix.

Para la creación de dicha base de datos se deberán seguir las siguientes instrucciones:

Paso 1: Antes de comenzar, se deberá accesar a la línea de comando de MariadDB como usuario privilegiado o root seguidamente se creará una base de datos con el nombre de Zabbix con el comando que aparece en la Ilustración 3-15

```
[root@localhost Desktop]# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 10
Server version: 5.5.56-MariaDB MariaDB Server

Copyright (c) 2000, 2017, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> create database zabbix character set utf8 collate utf8_bin;
Query OK, 1 row affected (0.03 sec)
```

ILUSTRACIÓN 3-15 COMANDO PARA CREAR UNA BASE DATOS.

Paso 2: Una vez que se ha creado la base de datos se procederá a crear el usuario "Zabbix" y al mismo tiempo se le otorgarán privilegios en la base de datos creada en el paso anterior, para ello se utilizará el comando que se observa en la Ilustración 3-16

```
[root@localhost ~]# zcat /usr/share/doc/zabbix-server-mysql-3.4.2/create.sql.gz
| mysql -uzabbix -p zabbix
Enter password:
[root@localhost ~]#
```

ILUSTRACIÓN 3-16 COMANDO PARA CREAR UN USUARIO

Paso 3: Una vez creada base de datos y el usuario, se deberá importar el esquema base para el llenado de la base con los datos iniciales del servidor, para ello se necesitará un archivo que se importa junto a los paquetes del ***Paso 1*** el cual se ejecutara con el comando que aparece en la Ilustración 3-17.

```
[root@localhost ~]# zcat /usr/share/doc/zabbix-server-mysql-3.4.2/create.sql.gz
| mysql -uzabbix -p zabbix
Enter password:
[root@localhost ~]#
```

ILUSTRACIÓN 3-17 COMANDO Y UBICACIÓN PARA EL ESQUEMA DE ZABBIX

Paso 4: Una vez creada y configurada la base de datos, se deberá editar el archivo de configuración llamado "Zabbix_server.conf" el cual se ubica en "*/etc/Zabbix/Zabbix_server-conf*" dentro de dicho archivo se encuentran las opciones para crear la conexión entre el servidor y la base de datos como lo es "*DBHost (en este caso será local), DBName, DBUser y DBPassword*" lo cuales se obtendrán de los ***Paso 1*** y ***Paso 2*** y deberá quedar como el la Ilustración 3-18

```
### Option: DBHost
# Mandatory: no
# Default:
 DBHost=localhost

### Option: DBName
# Mandatory: yes
# Default:

DBName=zabbix

### Option: DBUser
# Mandatory: no
# Default:

DBUser=zabbix

### Option: DBPassword
# Mandatory: no
# Default:
 DBPassword=zabbix2017
```

ILUSTRACIÓN 3-18 CONFIGURACIONES DE SERVIDOR DE ZABBIX

3.2.2. Configuración de PHP para la interfaz gráfica de Zabbix

Algunos ajustes de PHP ya están configurados por default. Pero es necesario activar la configuración "date.timezone" y establecer la zona horaria correcta.

El archivo para editar contiene la configuración de Apache para la interfaz gráfica de Zabbix el cual se ubica en *"/etc/httpd/conf.d/zabbix.conf"* en el cual solo se activará la línea antes comentada y se le agregará la zona horaria para este caso será "America/Mexico_City" quedando como en la Ilustración 3-19

```
Alias /zabbix /usr/share/zabbix

<Directory "/usr/share/zabbix">
    Options FollowSymLinks
    AllowOverride None
    Require all granted

    <IfModule mod_php5.c>
        php_value max_execution_time 300
        php_value memory_limit 128M
        php_value post_max_size 16M
        php_value upload_max_filesize 2M
        php_value max_input_time 300
        php_value always_populate_raw_post_data -1
        php_value date.timezone America/Mexico_City
    </IfModule>
</Directory>

<Directory "/usr/share/zabbix/conf">
    Require all denied
</Directory>
```

ILUSTRACIÓN 3-19 CONTENIDO DEL ARCHIVO ZABBIX.CONF

3.2.3. Configuración de SELinux

Security-Enhanced Linux (SELinux) es un módulo de seguridad para el kernel Linux que proporciona el mecanismo para soportar políticas de seguridad para el control de acceso, incluyendo controles de acceso obligatorios. Se trata de un conjunto de modificaciones del núcleo y herramientas de usuario que pueden ser agregadas a diversas distribuciones Linux. Su arquitectura se enfoca en separar las decisiones de las aplicaciones de seguridad de las políticas de seguridad mismas y racionalizar la cantidad de software encargado de las aplicaciones de seguridad. (CentOS, 2017)

Al tener SELinux habilitado y ejecutándose, se deberá habilitar la comunicación entre Zabbix y el servidor apache, para ello se deberán ejecutar los comandos que aparecen en la Ilustración 3-20

```
[root@localhost emejia]# setsebool -P httpd_can_network_connect=1
[root@localhost emejia]# setsebool -P httpd_can_connect_zabbix=1
[root@localhost emejia]# setsebool -P zabbix_can_network=1
[root@localhost emejia]#
```

ILUSTRACIÓN 3-20 COMANDOS PARA AGREGAR A ZABBIX A LAS POLÍTICAS DE SEGURIDAD

Una vez que se ha permitido la comunicación de deberá permitir el acceso de los puertos predeterminados de Zabbix a través del firewall con los comandos que se muestran en la Ilustración 3-21

```
[root@localhost ~]# firewall-cmd --permanent --add-service=http
success
[root@localhost ~]# firewall-cmd --permanent --zone=public --add-port=10051/tcp
success
[root@localhost ~]# firewall-cmd --permanent --zone=public --add-port=10050/tcp
success
```

ILUSTRACIÓN 3-21 AGREGAR LOS PUERTOS DE ZABBIX AL FIREWALL

Ya que se han actualizado los permisos dentro del firewall y de SElinuxse deberá habilitar e iniciar el servicio del servidor de Zabbix, para ellos se utilizarán los comandos que se encuentran en la Ilustración 3-22

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

ILUSTRACIÓN 3-22 COMANDOS PARA HABILITAR Y ACTIVAR EL SERVICIO DE ZABBIX

A partir de la versión 3.4 de Zabbix introduce IPC (del inglés Inter-Process Communication o Comunicanción entre procesos) utilizando sockets, por lo que puede ser necesario aplicar reglas adicionales de SELinux, para ellos descargaremos un archivo del siguiente enlace:

https://support.zabbix.com/secure/attachment/53320/53320_zabbix_server_add.te

Una vez descargado el archivo necesario se deberán importar las nuevas reglas, para ello se harán uso de los comandos que se muestran dentro de la Ilustración 3-23.

```
[root@localhost emejia]# yum install policycoreutils-python
[root@localhost emejia]# checkmodule -M -m -o zabbix_server_add.mod zabbix_serve
r_add.te
checkmodule:  loading policy configuration from zabbix_server_add.te
checkmodule:  policy configuration loaded
checkmodule:  writing binary representation (version 17) to zabbix_server_add.mo
d
[root@localhost emejia]# semodule_package  -m zabbix_server_add.mod -o zabbix_se
rver_add.pp
[root@localhost emejia]# semodule -i zabbix_server_add.pp
```

ILUSTRACIÓN 3-23 IMPORTAR LAS NUEVAS POLÍTICAS DE SEGURIDAD

3.2.4. Instalación de la interfaz gráfica

Una vez finalizada la instalación del servidor y todos sus componentes es momento de proceder con los pasos de instalación de la interfaz gráfica de Zabbix que le permitirán acceder a todas las funcionalidades de Zabbix.

Paso 1: Si nos encontramos de manera local en nuestro servidor teclearemos en el navegador la siguiente dirección *http://localhost/zabbix* o *http://ip-del-servidor/zabbix* si nos encontramos en una computadora dentro de la misma red y una vez dentro deberá aparecer una pantalla de bienvenida como la que se muestra en la Ilustración 3-24 la cual nos guiara por el asistente de instalación y configuración de la interfaz gráfica. Para continuar se deberá dar clic en el botón “Next step”.

ILUSTRACIÓN 3-24 PANTALLA DE BIENVENIDA DE ZABBIX

Paso 2: En la pantalla que se muestra a continuación nos muestra los prerrequisitos necesarios para poder poner en marcha a Zabbix, en caso de que todos los requisitos se cumplan se mostraran todas las leyendas en verde como en la Ilustración 3-25 seguidamente se procederá a dar clic en el botón Next step

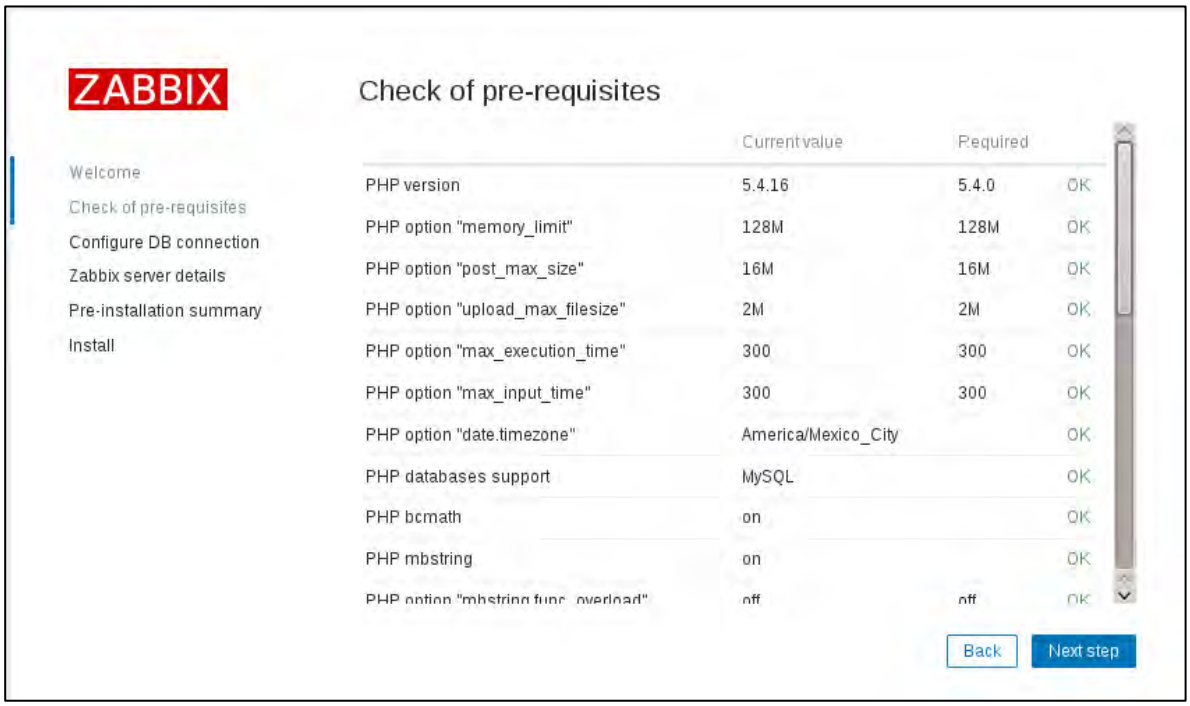

ILUSTRACIÓN 3-25 PRERREQUISITOS DE ZABBIX

Paso 3: Una vez finalizado el paso anterior, deberá mostrar una pantalla como en la Ilustración 3-26 donde nos pedirá los detalles de nuestra base de datos, como lo es el motor de base de datos, la ubicación de nuestra base de datos (en caso que la base de datos se haya creado en otro host), el puerto, así como el nombre de la base de datos, el usuario y la contraseña del mismo, estos últimos datos se pueden obtener de la configuración creada en la sección Crear base de datos y una vez que se han introducido los datos se procederá a dar clic en el botón “Next step” para continuar con la configuración.

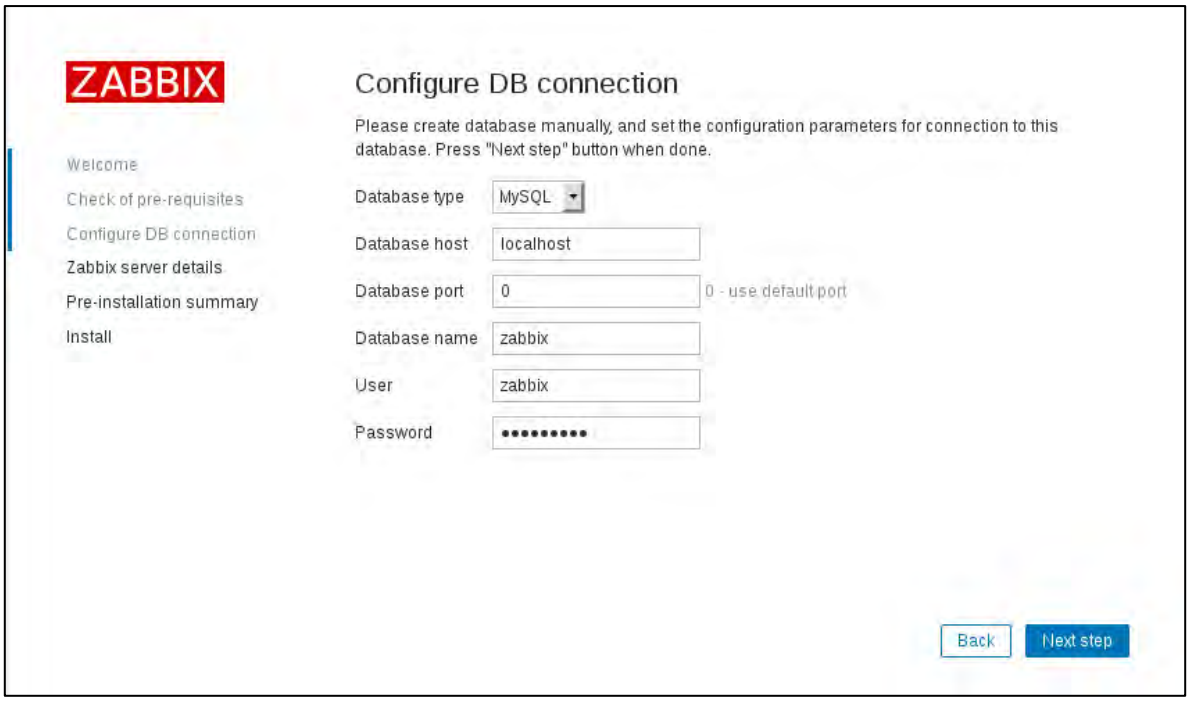

ILUSTRACIÓN 3-26 PANTALLA DE CONEXIÓN A LA BASE DE DATOS

Paso 4: En la pantalla siguiente nos pedirá que se introduzcan los datos básicos del servidor de Zabbix como lo es el host en el cual se encuentra alojado, el puerto que utilizará y el nombre que se le proporcionará al servidor como se puede observar en la Ilustración 3-27 el asistente traer por defecto la dirección del host y el puerto solo se deberá agregar el nombre del servidor, una vez realizado lo anterior, se procederá a dar clic en el botón “Next step”.

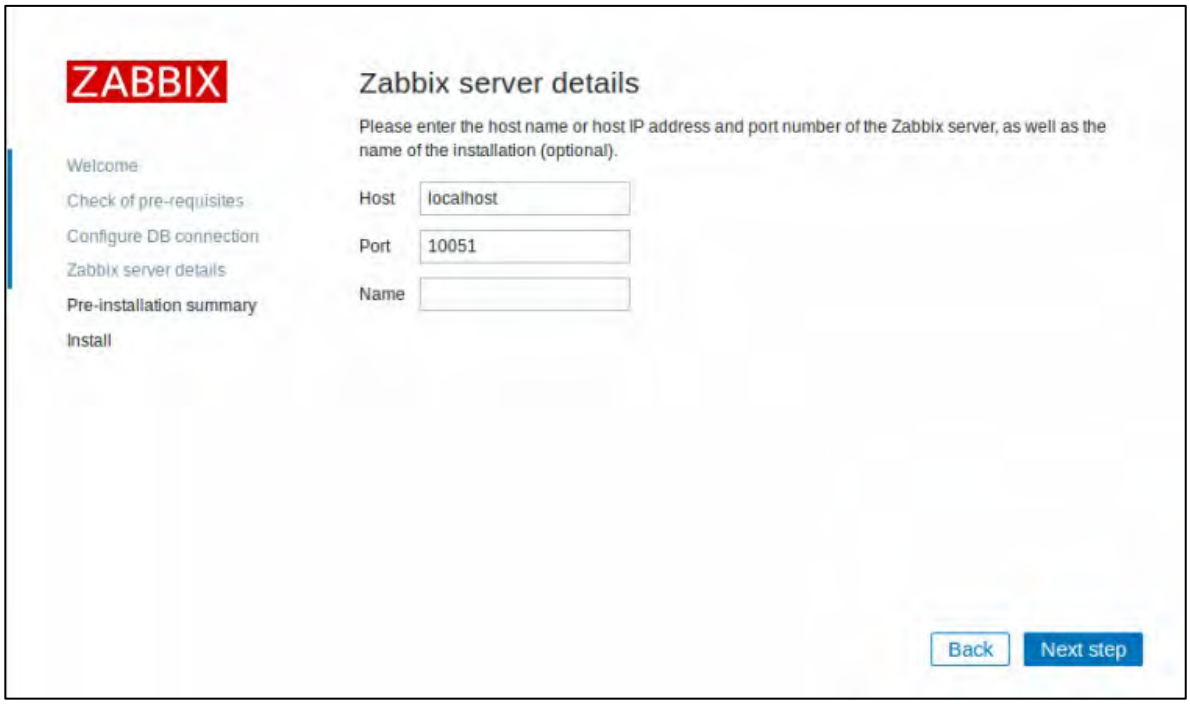

ILUSTRACIÓN 3-27 DETALLES DEL SERVIDOR DE ZABBIX

Paso 5: Una vez terminadas las configuraciones anteriores se mostrará un resumen como en la Ilustración 3-28 en caso de observar un dato erróneo se podrá cambiar dando clic en el botón back, en caso contrario continuaremos la configuración dando clic en el botón Next step y se aplicará la configuración

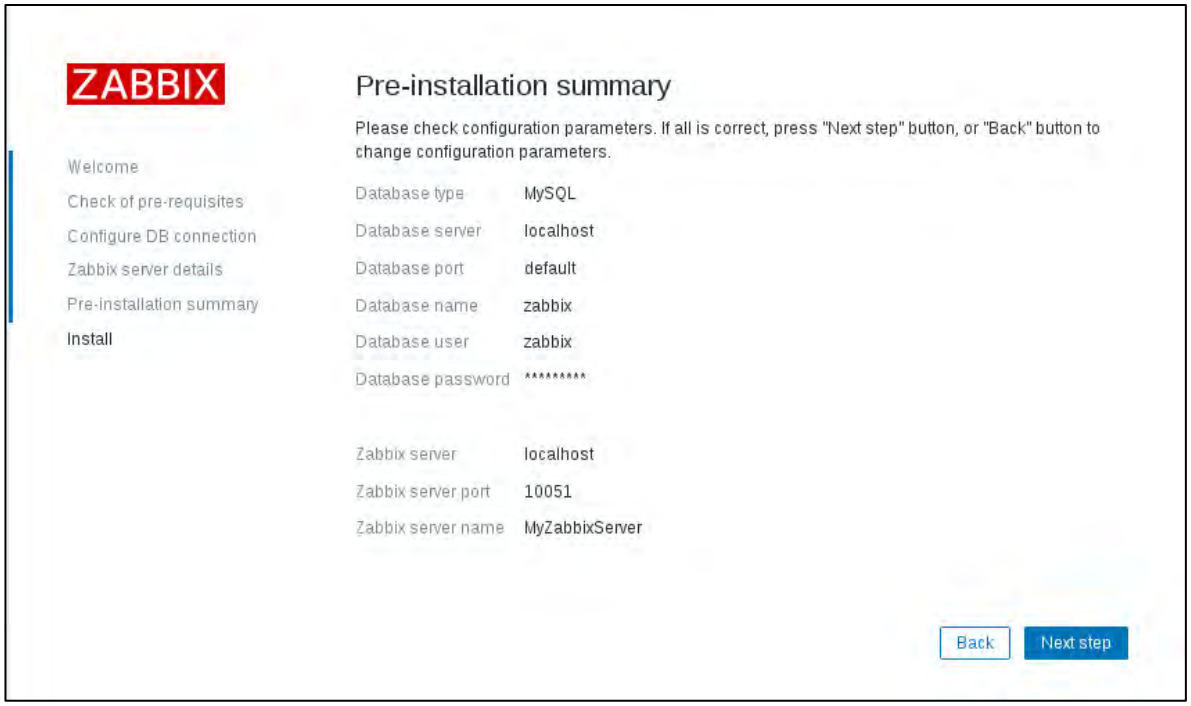

ILUSTRACIÓN 3-28 RESUMEN DE CONFIGURACIÓN

Paso 6: Para dar por finalizada la instalación se mostrará una pantalla como la Ilustración 3-29 donde se mostrará un mensaje en el cual confirma la finalización satisfactoriamente, para terminar y salir del asistente daremos clic en el botón Finish.

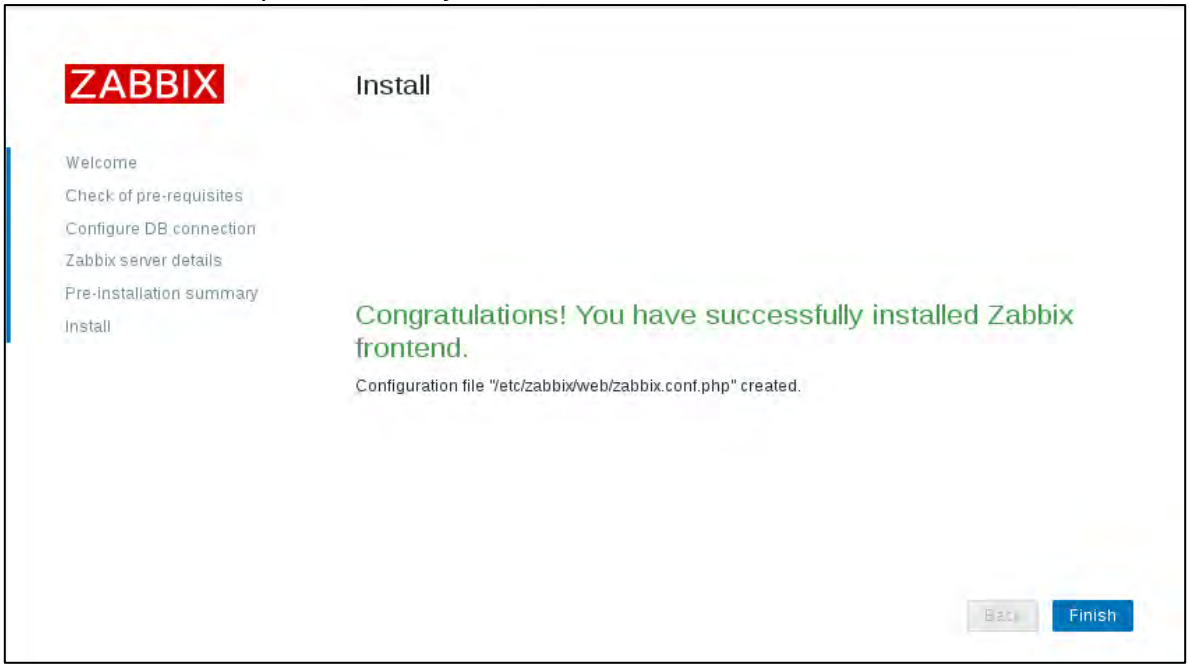

ILUSTRACIÓN 3-29 PANTALLA DE FINALIZACIÓN

Paso 8: Una vez terminada la instalación se presentará la pantalla de Inicio de Sesión como se observa en la Ilustración 3-30 en la cual se deberá iniciar sesión con el usuario por efecto que es Admin con la contraseña Zabbix, se recomienda que después del primer inicio de sesión se cambien inmediatamente las credenciales antes mencionadas

ILUSTRACIÓN 3-30 PANTALLA DE INICIO DE SESIÓN DE ZABBIX

4. Capítulo IV Pruebas de Zabbix

En el tercer capítulo se tocará el tema de las diferentes pruebas a las que se sometió la plataforma Zabbix para el monitoreo de los distintos dispositivos designados para las mismas, los resultados obtenidos serán mostrados de manera gráfica.

4.1. Supervisión y resolución de problemas de la red

Supervisar una red en funcionamiento puede proporcionar información a un administrador de red para administrar la red de forma proactiva e informar estadísticas de uso de la red a otros. La actividad de los enlaces, las tasas de error y el estado de los enlaces son algunos de los factores que contribuyen a que un administrador de red determine el estado y el uso de una red. Recopilar y revisar esta información en el transcurso del tiempo permite que un administrador de red vea y proyecte el crecimiento, y puede contribuir a que el administrador detecte y reemplace una parte defectuosa antes de que falle por completo.

Si una red o una parte de una red queda fuera de servicio, esto puede tener un impacto negativo importante en la empresa. Cuando ocurren problemas en la red, los administradores deben usar un enfoque sistemático de resolución de problemas a fin de que la red vuelva a funcionar completamente lo antes posible.

La capacidad de un administrador de red para resolver problemas de red de manera rápida y eficaz es una de las habilidades más buscadas en TI. Las empresas necesitan personas con habilidades sólidas de resolución de problemas de red, y la única forma de obtener estas habilidades es a través de la experiencia práctica y el uso de métodos sistemáticos de resolución de problemas. (Cisco Networking Academy, 2017)

Al trabajar en un entorno de producción, el uso de técnicas eficaces de resolución de problemas reduce el tiempo total dedicado a esta tarea. Hay tres etapas principales en el proceso de resolución de problemas Ilustración 4-1:

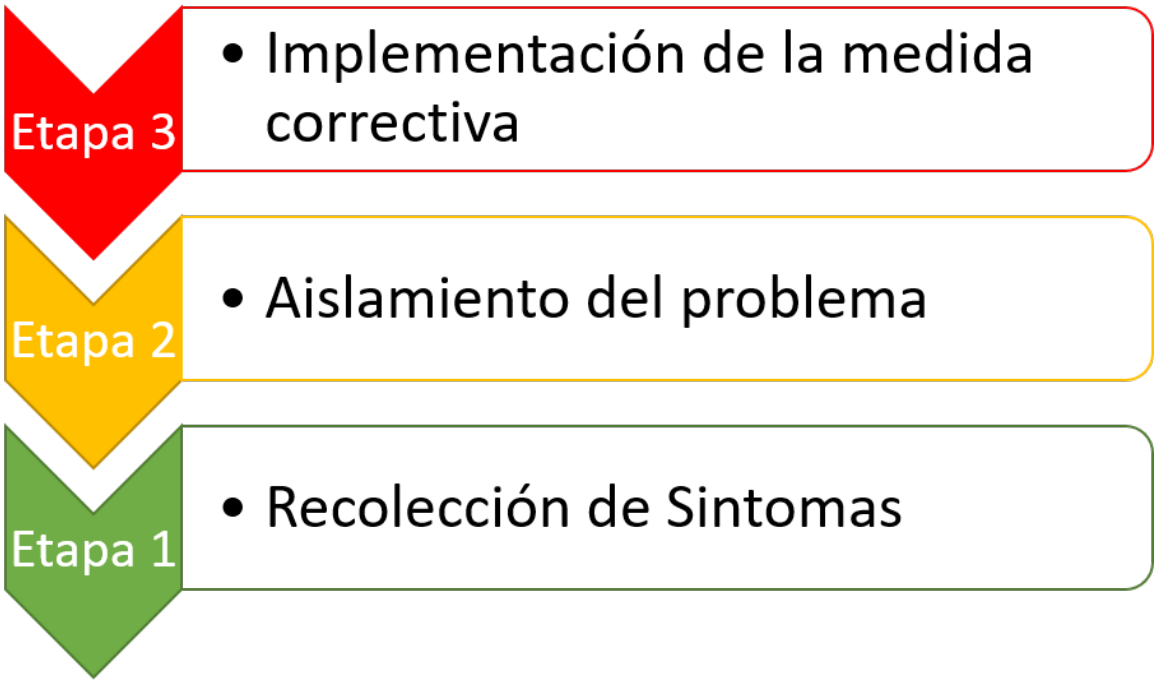

ILUSTRACIÓN 4-1 ETAPAS DE RESOLUCIÓN DE PROBLEMAS

Etapa 1. Recolección de síntomas: la resolución de problemas comienza con la recolección y el registro de los síntomas de la red, los sistemas finales y los usuarios. Además, el administrador de red determina qué componentes de la red se vieron afectados y de qué forma cambió la funcionalidad de la red en comparación con la línea de base. Los síntomas pueden aparecer de distintas maneras, que incluyen alertas del sistema de administración de red, mensajes de la consola y quejas de los usuarios. Mientras se recolectan los síntomas, es importante que el administrador de red realice preguntas e investigue el problema para restringirlo a una variedad de posibilidades más reducida.

Etapa 2. Aislamiento del problema: el aislamiento es el proceso mediante el que se eliminan variables hasta que se identifica como la causa a un único problema o a un conjunto de problemas relacionados. Para realizar esto, el administrador de red examina las características de los problemas en las capas lógicas de la red para poder seleccionar la causa más probable.

Etapa 3. Implementación de la medida correctiva: una vez que se identificó la causa del problema, el administrador de red trabaja para corregir el problema mediante la implementación, la puesta a prueba y el registro de posibles soluciones. Después de encontrar el problema y determinar una solución, es posible que el administrador de red deba decidir si la solución se puede implementar inmediatamente o si se debe posponer. Esto depende del impacto de los cambios en los usuarios y en la red. La gravedad del problema se debe ponderar en comparación con el impacto de la solución. A veces, se puede crear una solución alternativa hasta que se resuelva el problema real. Por lo general, esto forma parte de los procedimientos de control de cambios de una red.

Si la medida correctiva implementada no da solución al problema o genera un problema nuevo, el administrador se encarga de registrar la solución probada, se eliminan los cambios y el administrador de red vuelve a recolectar síntomas y a aislar el problema.

Para cada etapa, se debe establecer una política de resolución de problemas que incluya procedimientos de control de cambios. Una política proporciona una forma coherente de llevar a cabo cada etapa. Parte de la política debe incluir el registro de cada dato importante.

4.2. Supervisión en Zabbix

Antes de poder supervisar Cualquier red es necesario dar de alta a los dispositivos que se van a monitorear en el servidor de Zabbix y, además, en el dispositivo que se desee monitorear se deberá permitir la conexión por medio de la dirección ip del servidor de Zabbix, además, en caso de usar el protocolo SNMP se deberá de crear la comunidad específica para Zabbix.

Para dar de alta un host por medio de la interfaz de Zabbix, de deberá dirigir a la pestaña de “Configuration”, y se activaran las opciones de esta pestaña como se muestra en la Ilustración 4-2, daremos clic en la opción “Hosts”

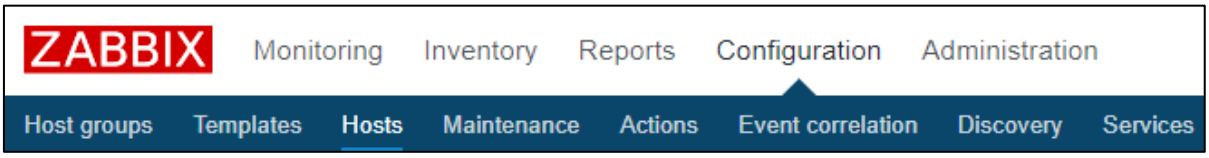

ILUSTRACIÓN 4-2 OPCIONES DE LA PESTAÑA "CONFIGURATION"

Una vez ingresada a la interfaz nos deberá aparecer una tabla con los hosts que se han dado de alta como se muestra en la Ilustración 4-3 . Para ingresar un nuevo host se deberá dar clic en el botón “Create host” que se ubica en la esquina superior derecha, en caso de querer editar un host ya existente solo se deberá dar clic en nombre de este.

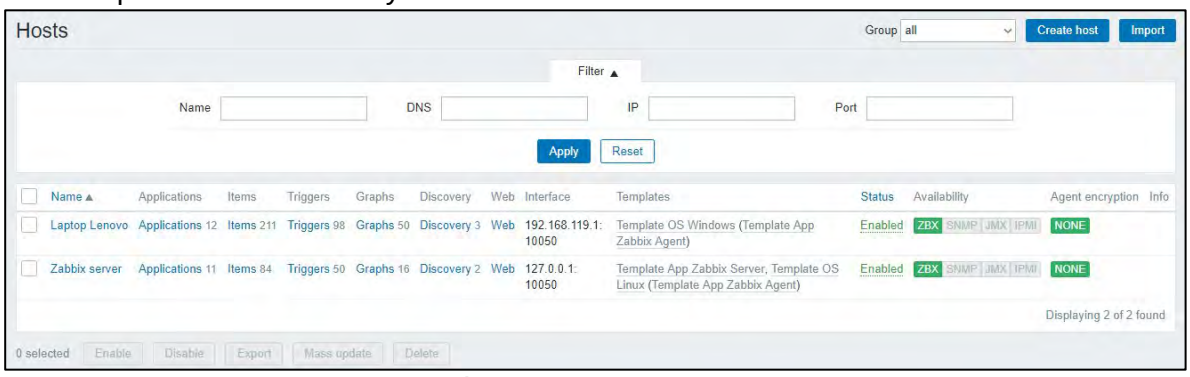

ILUSTRACIÓN 4-3 ADMINISTRADOR DE HOST

Una vez que se ha ingresado a la interfaz para crear un nuevo host nos aparecerá una barra de opciones como la que se muestra en la Ilustración 4-4 para empezar se deberá accesar a la opción que dice hosts

ILUSTRACIÓN 4-4 OPCIONES AL MOMENTO DE CREAR UN HOST

Host

Dentro de la opción Host nos mostrara una interfaz un formulario como se puede apreciar en la Ilustración 4-5 el cual contiene diferentes parámetros de configuración para el nuevo host los cuales se describen a continuación en la Tabla 4-1.

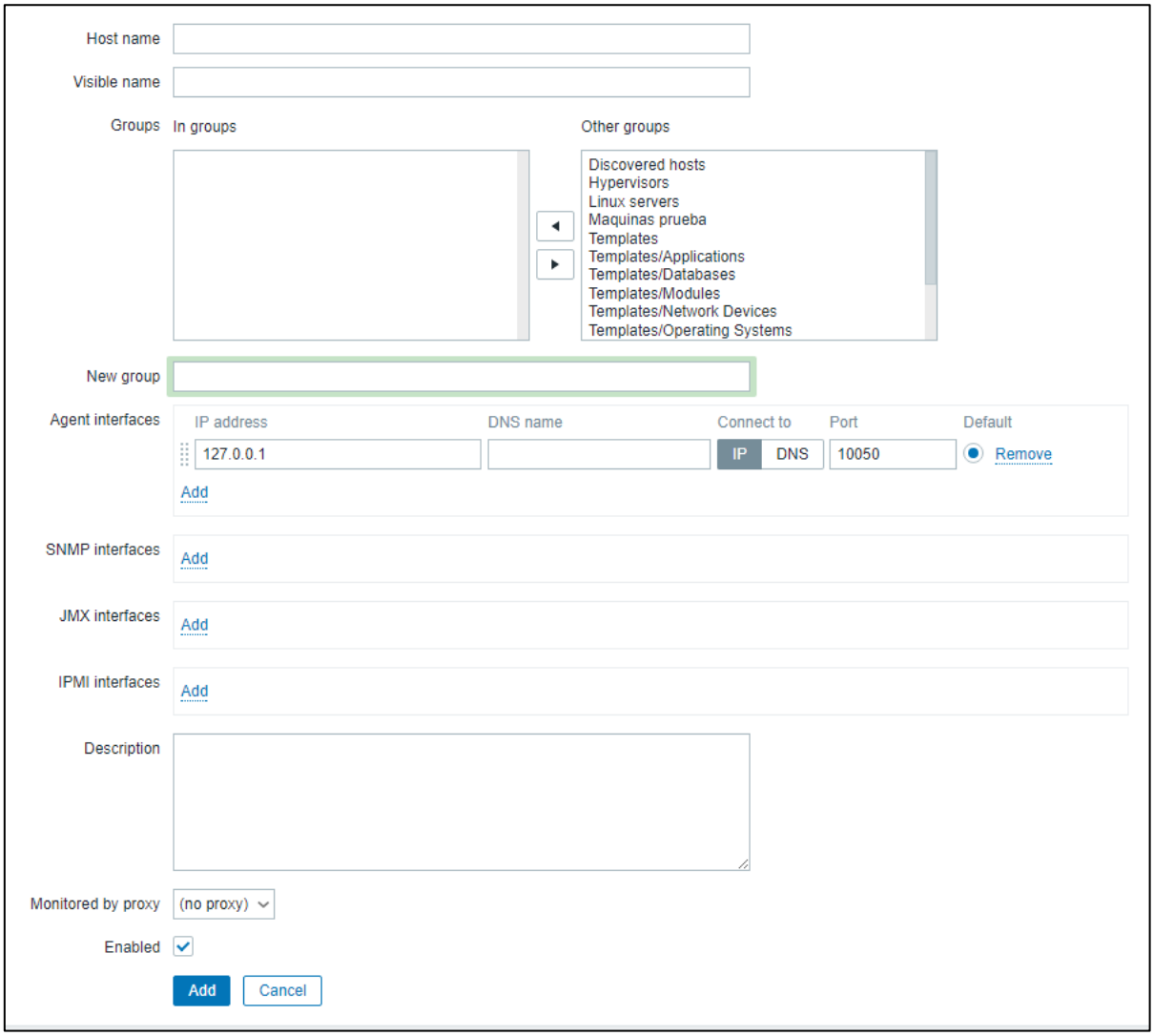

ILUSTRACIÓN 4-5 FORMULARIO DE CONFIGURACIÓN DE UN NUEVO HOST

Parámetro	Descripción
Host name	Ingrese un nombre de host único. Se permiten alfanuméricos, espacios, puntos, guiones y guiones bajos. Nota: Con el agente Zabbix ejecutándose en el host que está configurando, el parámetro del archivo de configuración del agente Nombre de host debe tener el mismo valor que el nombre de host ingresado aquí. El nombre del parámetro es necesario en el procesamiento de las verificaciones activas.
Visible name	Si configura este nombre, será visible en listas, mapas, etc. Este atributo tiene soporte UTF-8.
Groups	Seleccione los grupos de host a los que pertenece el host. Un host debe pertenecer al menos a un grupo de hosts
New host group	Se puede crear un nuevo grupo y vincularlo con el host. Ignorado, si está vacío.
Interfaces	Se admiten varios tipos de interfaz de host para un host: Agent, SNMP, JMX e IPMI. Para agregar una nueva interfaz, haga clic en Agregar en el bloque Interfaces e ingrese IP / DNS, Conectarse e Información de puerto. Nota: las interfaces que se utilizan en cualquier elemento no se pueden eliminar y el enlace Quitar está en gris para ellas. La opción Usar solicitudes masivas para interfaces SNMP permite habilitar / deshabilitar el procesamiento masivo de solicitudes SNMP por interfaz.
IP address	Dirección IP del host (opcional).
DNS name	Nombre del DNS del host (opcional).
Connect to	Al hacer clic en el botón correspondiente le dirá al servidor Zabbix qué usar para recuperar datos de los agentes: IP: se conecta a la dirección IP del host (recomendado) DNS: se conecta al nombre DNS del host
Port	Número de puerto TCP / UDP. Los valores predeterminados son: 10050 para agente de Zabbix, 161 para agente de SNMP, 12345 para JMX y 623 para IPMI.
Default	Marque el botón de opción para configurar la interfaz predeterminada.
Description	Ingrese la descripción del host.
Monitored by proxy	El host puede ser monitoreado por el servidor Zabbix o por uno de los proxies de Zabbix: (sin proxy): el host es monitoreado por el servidor Zabbix Nombre del proxy: el host es supervisado por el proxy Zabbix "Nombre del proxy"
Enable	Marque la casilla para activar el host, listo para ser monitoreado. Si no está marcado, el host no está activo, por lo tanto, no se controla.

TABLA 4-1 PARÁMETROS DE UN HOST

Templates

Otra de las opciones que se nos muestra en la Ilustración 4-4 más atrás es la de poder configurar un Template, Un template es un conjunto de entidades que se pueden aplicar de forma conveniente a múltiples hosts, estas entidades pueden ser ítems, Triggers, gráficas, aplicaciones y pantallas. Como muchos hosts en la vida real son idénticos o bastante similares, naturalmente se deduce que el conjunto de entidades que ha creado para un host puede ser útil para muchos. Por supuesto, podría copiarlos a cada nuevo host, pero eso sería mucho trabajo manual. En cambio, con las plantillas puede copiarlas en una plantilla y luego aplicar la plantilla a tantos hosts como sea necesario. (Zabbix SIA, 2016)

Una ventaja es que los templates pueden ser creados desde cero, utilizar los que vienen por defecto en la instalación de Zabbix o en dado caso utilizar aquellos que han sido creados por la comunidad que utiliza Zabbix y los comparte en el foro oficial que se encuentra en la siguiente dirección URL:

https://share.zabbix.com

Para agregar un template a nuestro host daremos clic en la opción Templates y nos mandara a un formulario como el que aparece a continuación. En él se deberá escribir el nombre el template deseado en el cuadro de texto con título “Link new templates” donde se mostrarán las diferentes opciones que contengan el nombre ingresado, una vez que se hayan elegido todos los templates daremos clic en el botón que dice “Add” y si se ha seguido el proceso correctamente deberán aparecer vinculados como en la Ilustración 4-6

ILUSTRACIÓN 4-6 CONFIGURACIÓN DE TEMPLATE DE UN HOST

Para desvincular un template, se deberá usar una de las dos opciones disponibles en el bloque de “Linked templates”:

Link/Desvincular: Desvincula el template, pero conserva todos los ítems, Triggers y gráficos.

Unlink and Clear/Desvincular y borrar: Desvincula completamente el template eliminando todos los ítems, Triggers y gráficos.

Intelligent Platform Management Interface / Interfaz de gestión de plataforma inteligente (IMPI)

Otra opción configurable dentro de las opciones de la Ilustración 4-4 (más atrás) es la interfaz IPMI (por sus siglas en ingles de Intelligent Platform Management Interface o Interfaz de gestión de plataforma inteligente), que pueden supervisar el estado y la disponibilidad de los dispositivos estandarizados para la administración remota de "luces apagadas" o "fuera de banda" de los sistemas informáticos. Permite controlar el estado del hardware directamente desde las llamadas tarjetas de administración.

Para configurar daremos clic en la opción IMPI de la Ilustración 4-4 y se mostrara un formulario como que aparece en la Ilustración 4-7 en el cual nos aparecen 3 bloques, el primer bloque nos muestra el tipo de algoritmo con el cual nos autenticaremos, mientras que el segundo el nivel de privilegios que tenemos en sistema a monitorear, por último, el 3er bloque nos pedirá que se introduzcan las credenciales para ingresar al sistema.

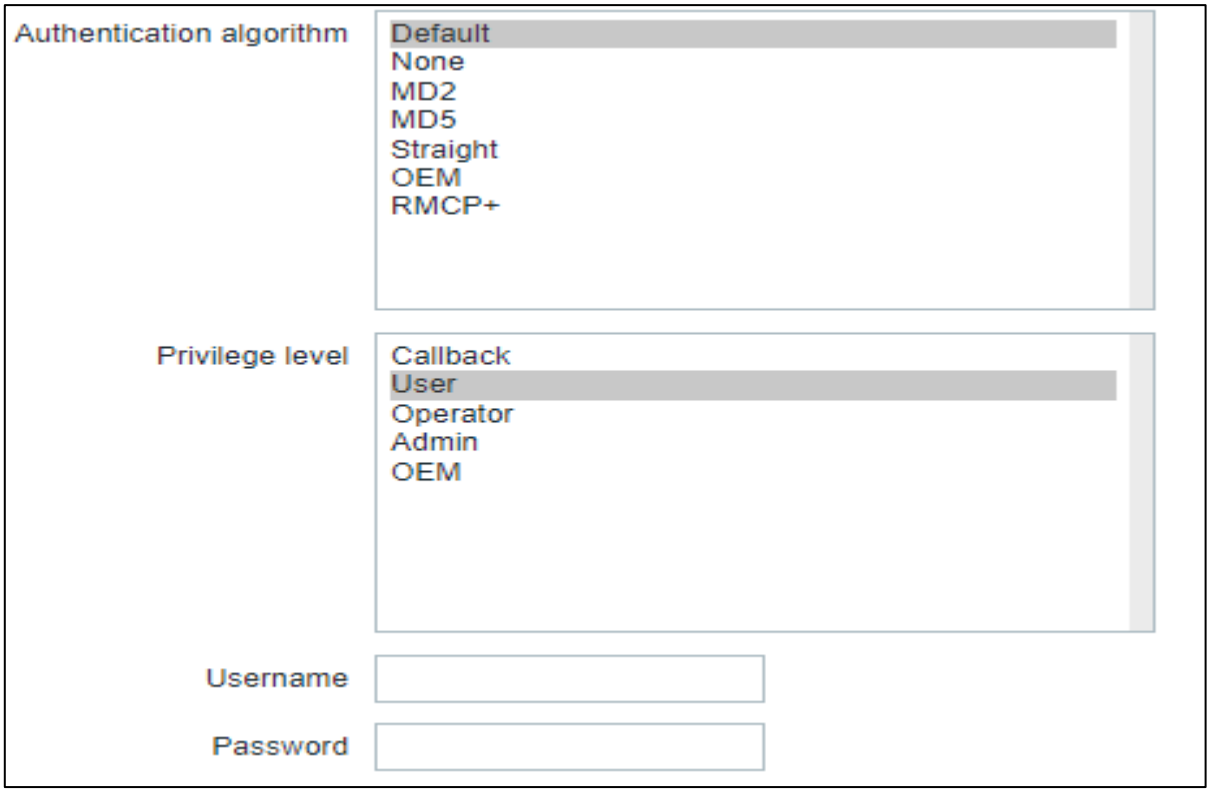

ILUSTRACIÓN 4-7 INTERFAZ DE CONFIGURACIÓN DE IMPI

Macros

La pestaña Macros de la Ilustración 4-4 le permite definir macros de usuario de nivel de host. También puede ver aquí macros globales y de nivel de template si selecciona la opción Macros heredadas y de host . Ahí es donde todas las macros de usuario definidas para el host se muestran con el valor que resuelven, así como su origen.

Por conveniencia, se proporcionan enlaces a los templates respectivos y a la configuración de macro global. También es posible editar un template / macro global en el nivel de host, creando de manera efectiva una copia de la macro en el host. (Zabbix SIA, 2016)

Para agregar una macro a nuestro host deberemos ingresar a la opción “Macros” en esta interfaz se muestran dos opciones, las cuales son “Host macros” y “Inhererited and host macros” esta última podemos heredar de los templates ya vinculados. En este caso se usará la macro más utilizada cuando se use el protocolo SNMP, por medio la cual se dará de alta la comunidad a la que pertenece el dispositivo y quedara como se aprecia en la Ilustración 4-8

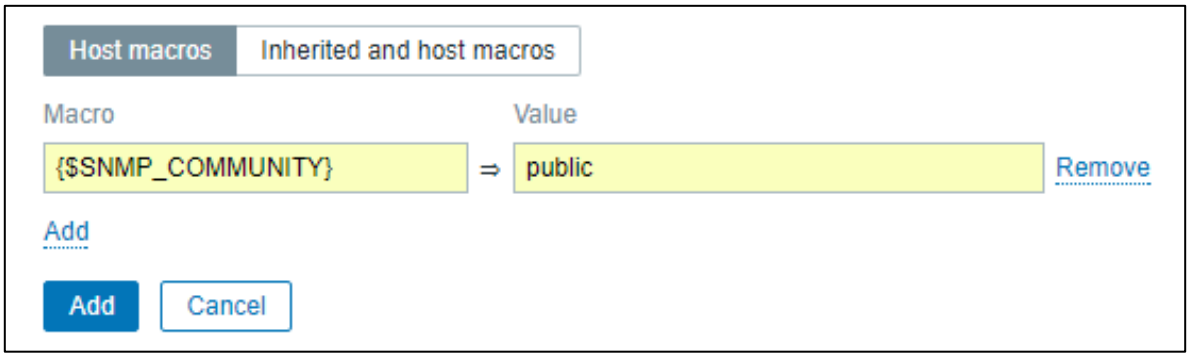

ILUSTRACIÓN 4-8 INTERFAZ DE MACROS

Host Invetory / Inventario de Host

Dentro de las opciones que se muestran en la Ilustración 4-4 se encuentra Host Invenotry la cual nos permite ingresar la información específica (como por ejemplo el tipo de dispositivo, el nombre, el sistema operativo, la dirección MAC) dentro de un formulario como se aprecia en el Ilustración 4-9, una de las opciones que Zabbix nos ofrece, es el poder habilitar un inventario automático, para que al momento que empiece a recolectar información rellene los campos de manera automática, o en dado caso deshabilitar la información

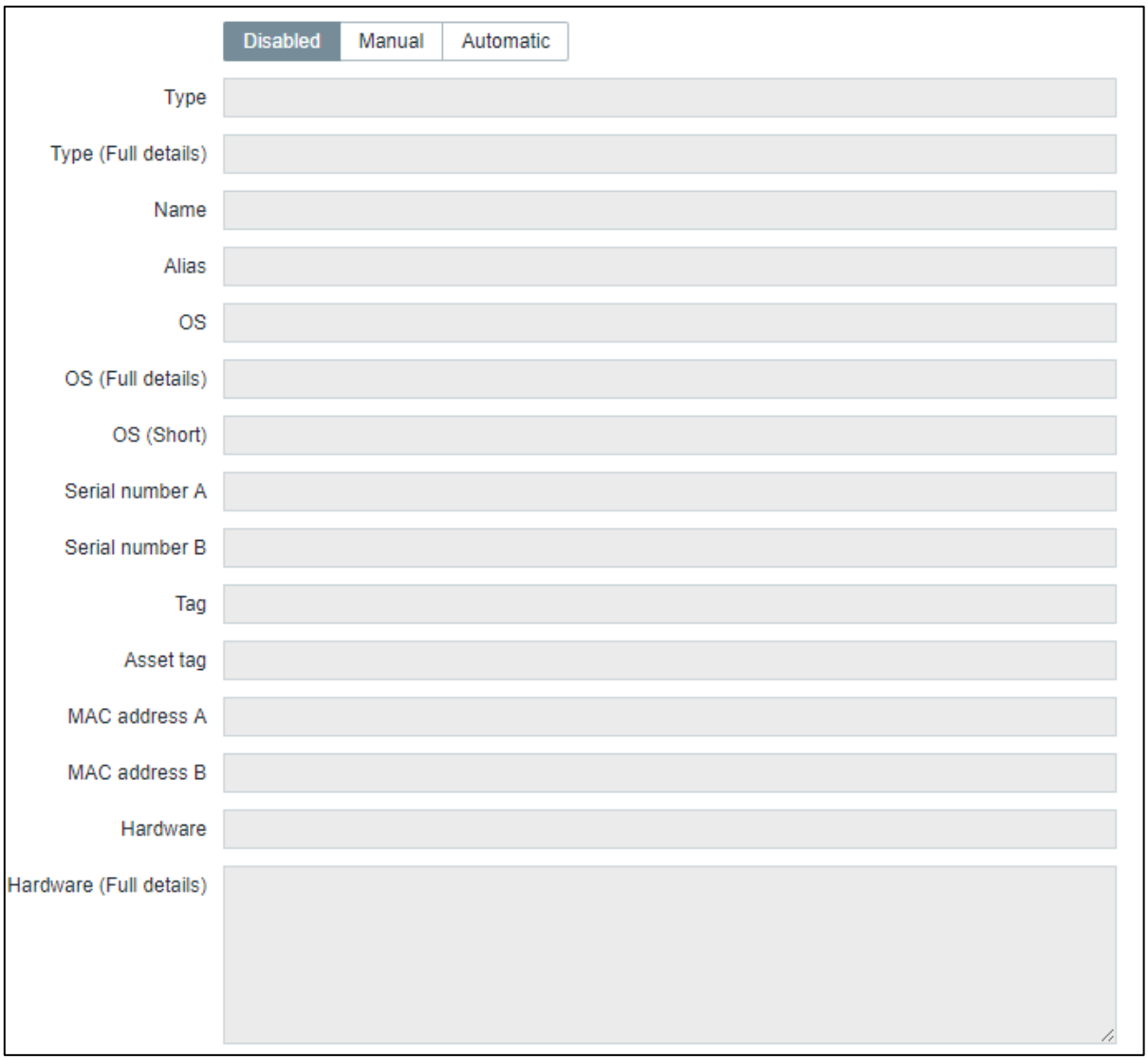

ILUSTRACIÓN 4-9 INTERFAZ DE HOST INVENTORY

Encryption / Encriptación

Zabbix admite comunicaciones encriptadas entre el servidor Zabbix, el agente Zabbix, las utilidades zabbix_sender y zabbix_get utilizando el protocolo Transport Layer Security (TLS) v.1.2.

El cifrado es opcional y configurable para componentes individuales para ellos nos iremos a la opción Encryption de la Ilustración 4-4 Una vez en la interfaz se nos mostrara un formulario como el de la Ilustración 4-10 en el cual dependiendo el tipo de encriptación que se utilice mostrara los cuadros de texto, los cuales se definen en la Tabla 4-2

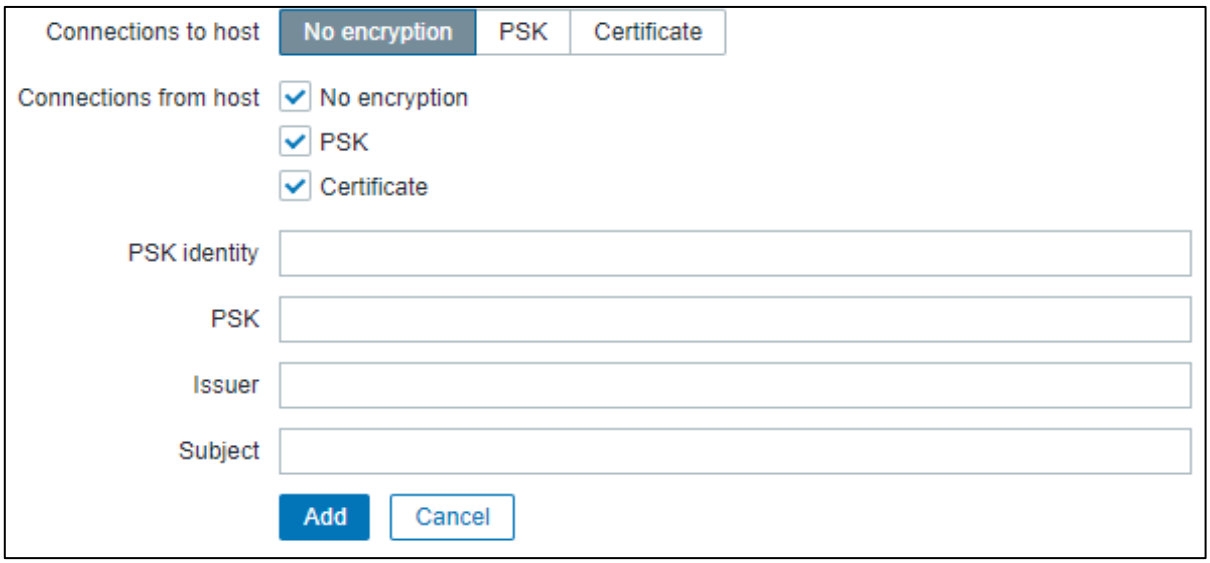

ILUSTRACIÓN 4-10 INTERFAZ DE ENCRIPTACIÓN

Parámetros	Descripción
Connections to host	Cómo se conecta el servidor o proxy de Zabbix al agente de Zabbix en un host: sin cifrado (predeterminado), utilizando PSK (clave pre compartida) o certificado.
Connections from host	Seleccione qué tipo de conexiones están permitidas desde el host (es decir, desde el agente de Zabbix y el remitente de Zabbix). Se pueden seleccionar varios tipos de conexión al mismo tiempo (útil para probar y cambiar a otro tipo de conexión). El valor predeterminado es "Sin cifrado".
Issuer	Permite al emisor del certificado. El certificado se valida primero con CA (autoridad de certificación). Si es válido, firmado por la CA, entonces el campo Emisor se puede usar para restringir aún más la CA permitida. Este campo está destinado a utilizarse si su instalación de Zabbix utiliza certificados de varias CA. Si este campo está vacío, se acepta cualquier CA.
Subject	Tema permitido del certificado. El certificado se valida primero con CA. Si es válido, firmado por la CA, entonces el campo Asunto puede usarse para permitir solo un valor de la cadena Asunto. Si este campo está vacío, se acepta cualquier certificado válido firmado por la CA configurada
PSK indentity	Cadena de identidad de clave pre compartida.
PSK	Clave pre compartida (cadena hexadecimal). Longitud máxima: 512 dígitos hexadecimales (PSK de 256 bytes) si Zabbix usa la biblioteca GnuTLS o OpenSSL, 64 dígitos hexadecimales (PSK de 32 bytes) si Zabbix usa la biblioteca mbed TLS (PolarSSL)

TABLA 4-2 OPCIONES DE LA ENCRIPTACIÓN

Una vez que se han ingresado todos los datos del nuevo host, se procederá a presionar el botón “Add” en caso de que sea un nuevo host o en el botón “Update” cuando se haya editado un host ya existente.

Una vez completado el proceso se agregará el nuevo host a la interfaz que aparece en la Ilustración 4-3 (más atrás) con la diferencia que el nuevo host mostrará en rojo la columna “Availability” como aprecia en la Ilustración 4-11, esta columna nos indica el tipo de protocolo por el cual se estará comunicando el servidor y el host que está en espera de que el nuevo host responda las peticiones del servidor.

Name ▲	Applications	Items	Triggers	Graphs	Discovery	Web	Interface	Templates	Status	Availability
CentOS 7 VM	Applications 10	Items 50	Triggers 19	Graphs 11	Discovery 2	Web	192.168.87.132: 10050	Template OS Linux (Template App Zabbix Agent)	Enabled	ZBX SNMP JMX IPMI

ILUSTRACIÓN 4-11 HOST EN ESPERA DE COMUNICACIÓN CON EL SERVIDOR

Una vez que exista una comunicación mutua entre el nuevo host y el servidor la columna cambiará a un color verde, a partir de ese momento el administrador podrá recibir notificaciones en caso de algún problema con el mismo.

4.3. Monitoreo con Zabbix

En el presente trabajo se realizaron algunas pruebas de medición en cuatro diferentes dispositivos de red, en este caso switch en diferentes ubicaciones y de diferentes modelos, las especificaciones completas se encuentran en el Apéndice A

, los switches utilizados son los siguientes:

- Switch Cisco Catalyst 2950
- Switch Cisco Catalyst 2960
- Switch Cisco Catalyst 3750E
- Switch Cisco Catalyst 3560

Las pruebas realizadas consistieron en la obtención de datos por medio del protocolo SNMP y se mostraran de una manera gráfica al usuario en la interfaz de Zabbix. Los datos que se obtuvieron se conforman de: Nombre o “Alias” con el cual se identifica dentro de la red, Una descripción breve la cual contiene el modelo del switch, la versión de Cisco IOS que se tiene instalado. Un tercer dato que se obtuvo es la cantidad de Memoria usada y libre, estableciendo un máximo y mínimo para ambas y tener un rango de funcionamiento correcto, además se obtienen datos del uso de CPU teniendo un mínimo, un promedio y un máximo, el último dato que se obtiene es un monitoreo del tráfico de las vlan’s que tienen cada uno de los dispositivos, mostrando detalles como velocidad, uso mínimo, uso máximo y promedio de entrada y salidas de datos en los dispositivos.

Todos los datos recabados son procesados al instante y se muestran en una pantalla diseñada para presentarse de manera amigable al usuario, esto con la finalidad de otorgarle herramientas que faciliten la tarea de monitorear y de igual manera una toma de decisiones más eficaz sobre la administración de la red universitaria, con la finalidad de cumplir con las tareas que se presentan en el modelo F.C.A.P.S. dentro de la administración del rendimiento.

Los resultados y las pantallas se muestran a continuación:

Switch Cisco C2950

En la Ilustración 4-12 se pueden observar los datos obtenidos de un Switch Cisco C2950 dentro de un rango de 1 hora de monitoreo.

Uso de memoria:

Usada

Min: 3.42 Mb

Max: 3.51 Mb

Promedio: 3.48 Mb

Libre

Min: 1.44 Mb

Max: 1.54 Mb

Promedio: 1.48 Mb

Uso de CPU

Min: 29%

Max: 38%

Promedio: 33.35%

Tráfico en la VLAN1

Entrada

Min: 50.94 Kbps

Max: 56.69 Kbps

Promedio: 53.82 Kbps

Salida

Min: 187.82 Kbps

Max: 342.02 Kbps

Promedio: 257.82 Kbps

Información del dispositivo:

Cisco IOS Software C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA12, RELEASE SOFTWARE (fc1)

ILUSTRACIÓN 4-12 RESULTADOS SWITCH C2950

Switch Cisco C2960

En la Ilustración 4-6Ilustración 4-13 se pueden observar los datos obtenidos de un Switch Cisco C2960 dentro de un rango de 1 hora de monitoreo.

Uso de memoria:

Usada

Min: 10.44 Mb

Max: 10.44 Mb

Promedio:10.44 Mb

Libre

Min: 19.83 Mb

Max: 19.84 Mb

Promedio:19.83 Mb

Uso de CPU

Min: 5%

Max: 7%

Promedio:5.76%

Tráfico en la VLAN1

Entrada

Min: 720 bps

Max: 2.51 Kbps

Promedio: 1.29 Kbps

Salida

Min: 176 bps

Max: 2.51 Kbps

Promedio: 1.15 Kbps

Información del dispositivo:

Cisco IOS Software, C2960 Software (C2960-LANLITEK9-M), Version 12.2(55)SE10, RELEASE SOFTWARE (fc2)

ILUSTRACIÓN 4-13 RESULTADOS SWITCH C2960

Switch Cisco C3750E

En la Ilustración 4-6Ilustración 4-14 se pueden observar los datos obtenidos de un Switch Cisco C3750E dentro de un rango de 1 hora de monitoreo.

Uso de memoria:

Usada

Min: 46.31 Mb

Max: 46.33 Mb

Promedio: 46.32 Mb

Libre

Min: 401.92 Mb

Max: 401.94 Mb

Promedio: 401.93 Mb

Uso de CPU

Min: 10%

Max: 13%

Promedio: 10.16%

Tráfico en la VLAN1

Entrada

Min: 1.88 Kbps

Max: 7.48 Kb

Promedio: 3.12 Kbps

Salida

Min: 2.08 kbps

Max: 4.25 kbps

Promedio: 2.54 kbps

Información del dispositivo:

Cisco IOS Software, C3750E Software (C3750E-UNIVERSALK9-M), Version 12.2(58)SE2, RELEASE SOFTWARE (fc1)

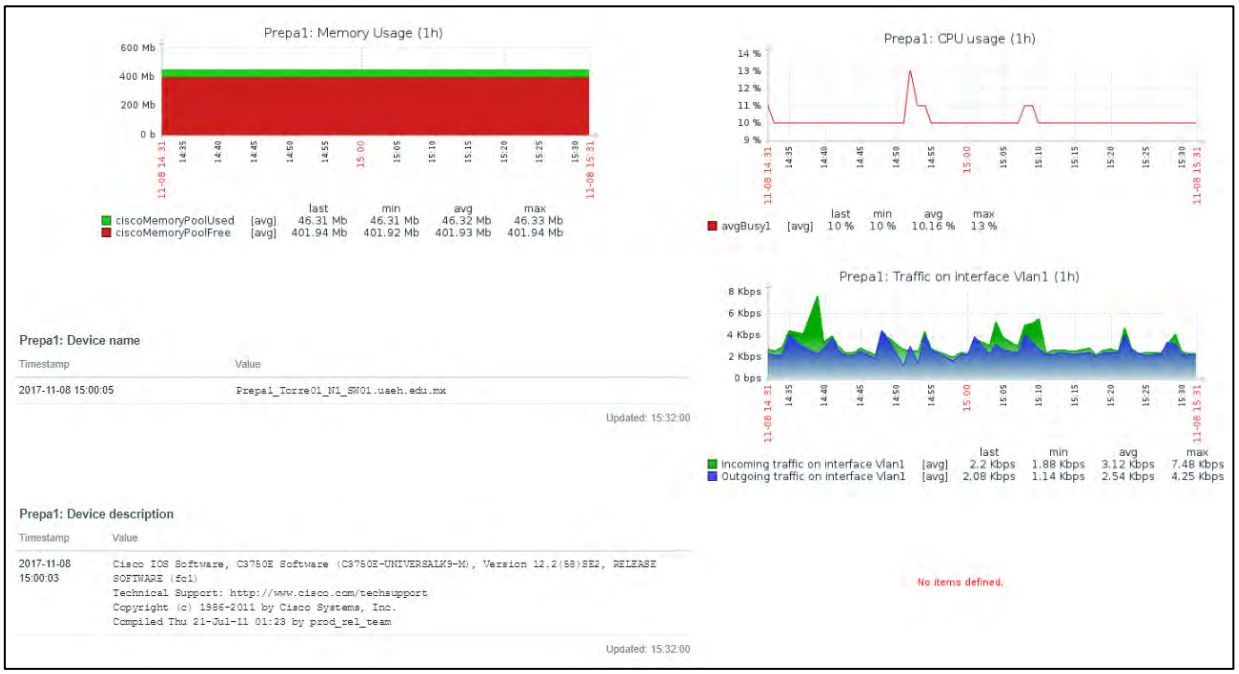

ILUSTRACIÓN 4-14 RESULTADOS SWITCH C3750E

Switch Cisco C3560

En la Ilustración 4-15 se pueden observar los datos obtenidos de un Switch Cisco C3560 dentro de un rango de 1 hora de monitoreo.

Uso de memoria:

Usada

Min: 13.99 Mb

Max: 14.01 Mb

Promedio: 13.99 Mb

Libre

Min: 83.17 Mb

Max: 83.19 Mb

Promedio: 83.19 Mb

Uso de CPU

Min: 6%

Max: 7%

Promedio: 6.03%

Tráfico en la VLAN1

Entrada

Min: 888 bps

Max: 3.78 Kbps

Promedio: 1.52 Kbps

Salida

Min: 552 bps

Max: 3.67 Kbps

Promedio: 1.25 Kbps

Información del dispositivo:

Cisco IOS Software, C3560 Software (C3560-IPBASE-M), Version 12.2(35)SE5, RELEASE SOFTWARE (fc1)

ILUSTRACIÓN 4-15 RESULTADOS SWITCH C3560

5. Capítulo V Resultados en un entorno real

En este apartado se mostrarán algunos resultados durante el proceso de adecuación y reemplazo de la actual plataforma Orión a la nueva plataforma Zabbix.

Desde la implementación hasta el momento en el cual se presenta este trabajo se ha estado trabajando en paralelo a la plataforma Orión, dando resultados favorables a cualquier cambio o problema que surgieran dentro de la red universitaria, a continuación, hago mención de algunos de ellos.

Una vez configurados los grupos de trabajo con los cuales identificar los diferentes dispositivos de red y ubicaciones los cuales por medio de la pantalla de “Host Status” muestra los grupos que llegaran a tener problemas como se muestra en la Ilustración 5-1

ILUSTRACIÓN 5-1 GRUPOS DE TRABAJO

Cuando se desea conocer el detalle del grupo de trabajo y los problemas que se presentan en el mismo grupo se da clic en el nombre del grupo el cual nos llevara a una pantalla como la que se muestra en la Ilustración 5-2, por seguridad de la información de la res universitaria solo se muestra el apartado con la cantidad de errores mas no el detalle.

Esta pantalla nos muestra un pequeño resumen con la siguiente información: Hora del problema, Severidad, Hora de recuperación, status, Host, Problema, duración y conocimiento del problema.

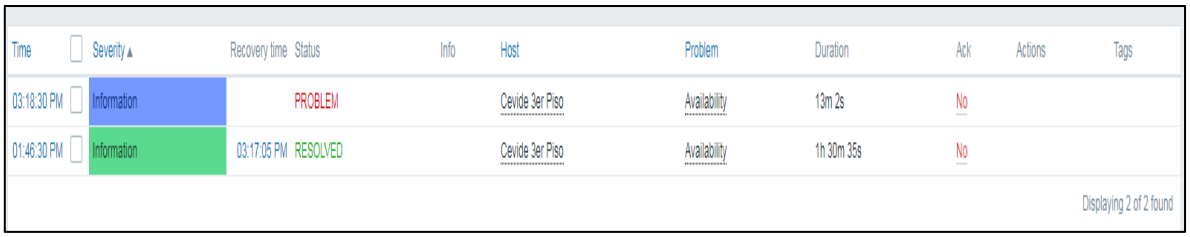

ILUSTRACIÓN 5-2 PANTALLA DE PROBLEMAS DE HOST

Otra de las mejoras que presento la plataforma Zabbix es la posibilidad de mandar una notificación en cuanto se detecte una anomalía dentro de la red, esta es un gran apoyo para el área de monitoreo de la red ya que estas notificaciones tienen la posibilidad de ser enviadas por correo electrónico al administrador como se puede ver en la Ilustración 5-3 ya que si por algún motivo no se encuentra monitoreando pueda tener conocimiento y así actuar de ser necesario.

Action log

Time ▾	Action	Type	Recipient	Message	Status	Info
04/18/2018 06:20:20 AM	Report problems to Zabbix administrators	Alertas	admrnoc (admrnoc monitoring) g @uaeh.edu.mx	**Resolved: Biblioteca ICAP SW3 - Free memory too low** Problem has been resolved at 06:20:17 on 2018.04.18 Problem name: Biblioteca ICAP SW3 - Free memory too low Host: Biblioteca ICAP SW3 Severity: Average Original problem ID: 27869	Sent	
04/16/2018 10:33:09 PM	Report problems to Zabbix administrators	Alertas	admrnoc (admrnoc monitoring) g @uaeh.edu.mx	**Problem: Biblioteca ICAP SW3 - Free memory too low**	Sent	

ILUSTRACIÓN 5-3 MUESTRA DE CORREOS ENVIADOS

Así mismo realizando el monitoreo a detalle del estado general de los equipos activos en la plataforma zabbix, se lograron obtener gráficas con mayor detalle que las obtenidas en el tema Monitoreo con Zabbix (más atrás) las cuales se muestran a continuación con un ejemplo de un equipo que se monitorea ubicado en Prepa 1, el cual por seguridad de la red no se muestra el detalle de la misma.

Uso de CPU: Ilustración 5-4

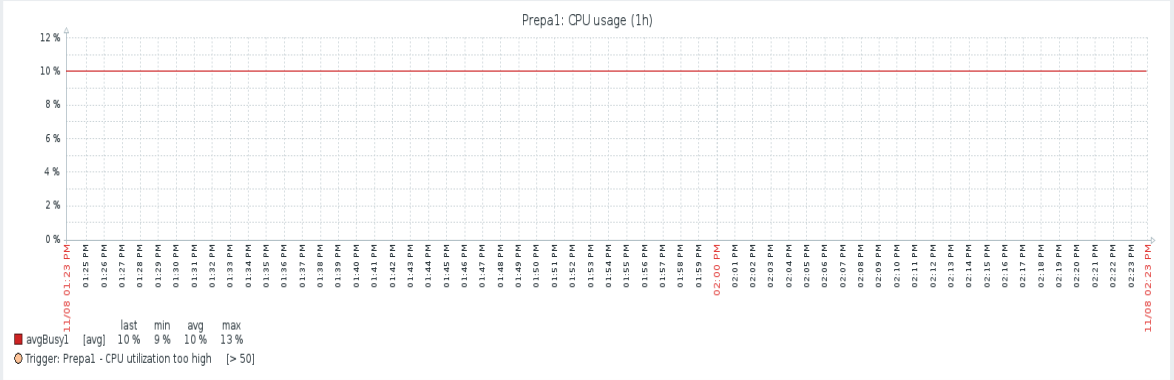

ILUSTRACIÓN 5-4 GRÁFICA USO CPU

Uso en Memoria:

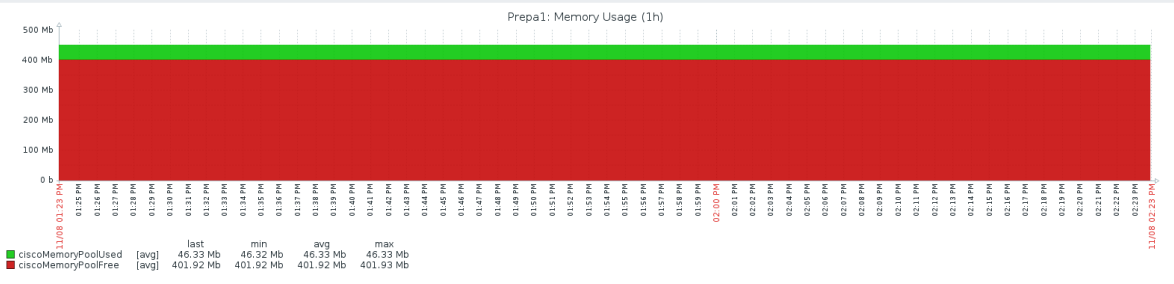

ILUSTRACIÓN 5-5 GRÁFICA USO DE MEMORIA

Trafico de entrada y salida en la interface g1/0/1(Interface de ejemplo): Ilustración 5-6

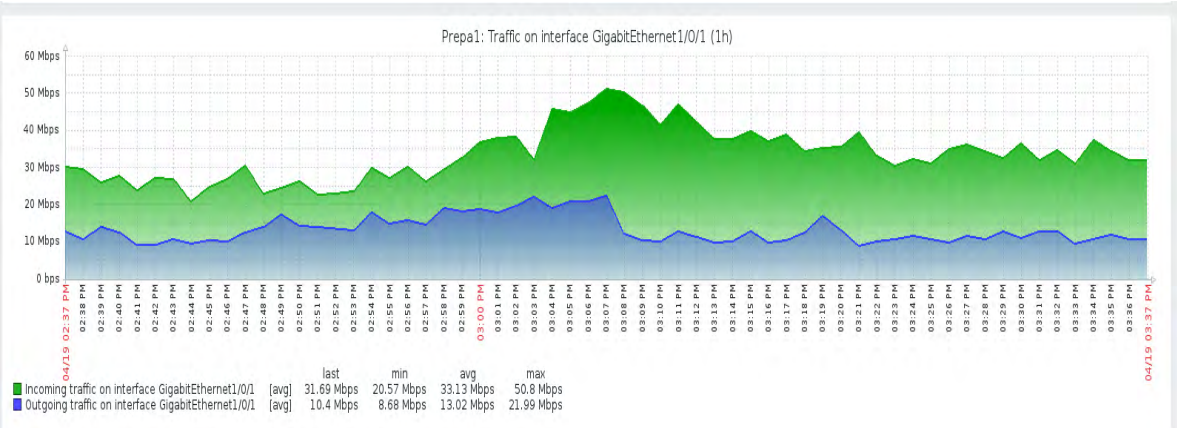

ILUSTRACIÓN 5-6 GRÁFICA DE TRAFICO DE E/S

Gracias a la representación de la información de manera gráfica para el encargado de la administración y monitoreo de la red le ayuda a mantener un control detallado del uso y comportamiento tanto de la red como de la información que se maneja dentro de ella, y de esta manera reaccionar de una manera proactiva ante cualquier situación que se presente.

Conclusiones

Dentro de la “POLÍTICA GENERAL PARA EL USO ADECUADO DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES EN LA UAEH” declara lo siguiente:

> *“Preservar la integridad de la información y contrarrestar las interrupciones en las actividades productivas críticas de la Universidad Autónoma del Estado de Hidalgo en concordancia con los estándares internacionales y las mejores prácticas en seguridad de la información, para evitar fallas mayores o desastres, controlar el acceso a la información y a las instalaciones de activos informáticos y de comunicaciones, utilizar los sistemas de información de manera segura para reducir el riesgo de error humano y prevenir pérdida, robo, abuso o modificación del software, los datos o los bienes informáticos, evitar infringir cualquier norma civil o penal, ley, obligación contractual o cualquier reglamento sobre el uso de la información y derechos de autor, detectar actividades no autorizadas, proteger la información y los activos informáticos contra terceros.” (Dirección de Información y Sistemas, 2018)*

El objetivo fundamental del presente trabajo es la mejoría del actual del monitoreo que tiene a su cargo la DIyS específicamente en Área de Monitoreo y Operación de la red, lo cual se logró por medio de la implementación de la plataforma Zabbix como remplazo parcial de la actual plataforma Orión, mejorando así el tiempo de respuesta ante problemas que puedan suscitarse dentro de la red universitaria.

Otro de los objetivos es el mejoramiento de las políticas de calidad mencionadas anteriormente, lo cual se logró con la implementación de Zabbix, ya que al tener control del monitoreo en tiempo real de los equipos de red se puede tener un mayor tiempo de respuesta ante incidentes los cuales lleven a la perdida de la integridad de la información y alteración o robo de la misma.

El resultado de este trabajo es por tanto la implementación parcial de la plataforma Zabbix permitiendo la mejoría en el monitoreo con ayuda de la recopilación de datos de manera eficiente, además ayudando a que toda la información recabada sea procesada de manera visual con ayuda de las gráficas que muestra Zabbix.

Como continuación de este trabajo de tesis y como en cualquier otro proyecto, existen diversas labores inconclusas y en las que es posible continuar trabajando. Durante el desarrollo de esta tesis han surgido algunos trabajos futuros que se han dejado abiertas y que se esperan completar en un futuro.

A continuación, se presentan algunos trabajos futuros que pueden desarrollarse como resultado de este proyecto o que, por exceder el alcance de esta tesis, no han podido ser tratados con la suficiente profundidad.

- El remplazo completo de la actual plataforma Orion a Zabbix.
- La puesta a punto de todos los dispositivos a monitorear por Zabbix.
- Capacitación del personal sobre el uso de Zabbix.
- Elaboración de un manual de usuario e instalación para futuras referencias dentro del Área de Monitoreo y Operación

Referencias

CentOS. (06 de Julio de 2017). *HowTos/SELinux.* Obtenido de https://wiki.centos.org/HowTos/SELinux

Cisco Networking Academy. (10 de Octubre de 2017). *CCNA4.* Obtenido de http://ecovi.uagro.mx/ccna4/index.html

Digital Ocean. (21 de Julio de 2014). *How To Install Linux, Apache, MySQL, PHP (LAMP) stack On CentOS 7.* Obtenido de https://www.digitalocean.com/community/tutorials/how-to-install-linux-apache-mysql-php-lamp-stack-on-centos-7

Dirección de Información y Sistemas. (15 de Enero de 2007). *Manual de Organización.* Obtenido de Documentos Administrativos: http://sgc.uaeh.edu.mx/sistemas/images/documentosAdministrativos/ManualOrganizacion.doc

Dirección de Información y Sistemas. (26 de Octubre de 2016). *Manual de Procedimientos DIyS.* Obtenido de Documentos Administrativos: http://sgc.uaeh.edu.mx/sistemas/images/documentosAdministrativos/ManuaProcedimientosDIyS.doc

Dirección de Información y Sistemas. (1 de 01 de 2018). *Política General.* Obtenido de http://sgc.uaeh.edu.mx/sistemas/index.php?option=com_content&view=article&id=7&Itemid=136

Huidobro, J. M. (1997). SNMP. Un protocolo simple de gestión. *BIT*.

International Organization for Standardization. (22 de Agosto de 2017). *FCAPS.* Obtenido de https://www.iso.org/standard/24406.html

ITU-T. (1996). *M.3010 Principio para lagestión de una red de telecomunicaciones.* Obtenido de https://www.itu.int/rec/T-REC-M.3010/es

ITU-T. (1997). *M.3400 Funciones de gestión TMN.* Obtenido de https://www.itu.int/rec/T-REC-M.3400-200002-I

Liquid Web. (12 de Enero de 2015). *How to Install Apache on CentOS 7.* Obtenido de https://www.liquidweb.com/kb/how-to-install-apache-on-centos-7/

MariaDB. (10 de Octubre de 2014). *Installing MariaDB 10 on CentOS 7 / RHEL 7.* Obtenido de https://mariadb.com/resources/blog/installing-mariadb-10-centos-7-rhel-7

NET-SNMP. (26 de Febrero de 2013). Obtenido de http://net-snmp.sourceforge.net

NET-SNMP. (30 de Agosto de 2017). *Simple Network Management Protocol.* Obtenido de http://www.net-snmp.org/about/history.html

Rosales Briceño, C. (1994). Protocolo snmp (protocolo sencillo de administración de redes) . *Télématique*, 106. Obtenido de TELEMATIQUE.

The Internet Engineering Task Force. (Enero de 1996). *Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework RFC 1908.* Obtenido de https://tools.ietf.org/html/rfc1908

The Internet Engineering Task Force. (Agosto de 1988). *A Simple Network Management Protocol RFC 1067.* Obtenido de https://tools.ietf.org/html/rfc1067

The Internet Engineering Task Force. (Agosto de 1988). *Management Information Base for Network Management of TCP/IP-based internets RFC 1066.* Obtenido de https://tools.ietf.org/html/rfc1066

The Internet Engineering Task Force. (Agosto de 1988). *Structure and Identification of Management Information for TCP/IP-based internets RFC 1065.* Obtenido de https://tools.ietf.org/html/rfc1065

The Internet Engineering Task Force. (Abril de 1989). *A Simple Network Management Protocol (SNMP) RFC 1098.* Obtenido de https://tools.ietf.org/html/rfc1098

The Internet Engineering Task Force. (Mayo de 1990). *A Simple Network Management Protocol (SNMP) RFC 1157.* Obtenido de https://tools.ietf.org/html/rfc1157

The Internet Engineering Task Force. (Mayo de 1990). *Management Information Base for Network Management of TCP/IP-based internets RFC 1156.* Obtenido de https://tools.ietf.org/html/rfc1156

The Internet Engineering Task Force. (Mayo de 1990). *Structure and Identification of Management Information for TCP/IP-based Internets RFC 1155.* Obtenido de https://tools.ietf.org/html/rfc1155

The Internet Engineering Task Force. (Marzo de 1991). *Management Information Base for Network Management of TCP/IP-based internets: MIB-II RFC 1213.* Obtenido de https://tools.ietf.org/html/rfc1213

The Internet Engineering Task Force. (Abril de 1993). *Coexistence between version 1 and version 2 of the Internet-standard Network Management Framework RFC 1452.* Obtenido de https://tools.ietf.org/html/rfc1452

The Internet Engineering Task Force. (Abril de 1993). *Introduction to version 2 of the Internet-standard Network Management Framework RFC 1441.* Obtenido de https://tools.ietf.org/html/rfc1441

The Internet Engineering Task Force. (Febrero de 1996). *An Administrative Infrastructure for SNMPv2 RFC 1909.* Obtenido de https://tools.ietf.org/html/rfc1909

The Internet Engineering Task Force. (Enero de 1996). *Introduction to Community-based SNMPv2 RFC 1901.* Obtenido de https://tools.ietf.org/html/rfc1901

The Internet Engineering Task Force. (Febrero de 1996). *User-based Security Model for SNMPv2 RFC 1910.* Obtenido de https://tools.ietf.org/html/rfc1910

The Internet Engineering Task Force. (Marzo de 2000). *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework RFC 2576.* Obtenido de https://tools.ietf.org/html/rfc2576

The Internet Engineering Task Force. (Diciembre de 2002). *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks RFC 3411.* Obtenido de https://tools.ietf.org/html/rfc3411

The Internet Engineering Task Force. (Diciembre de 2002). *Management Information Base (MIB) for the Simple Network Management Protocol (SNMP) RFC 3418.* Obtenido de https://tools.ietf.org/html/rfc3418

The Internet Engineering Task Force. (s.f.). *About the IETF*. Obtenido de https://www.ietf.org

The PHP group. (1 de Octubre de 2017). *¿Qué es PHP?* Obtenido de http://php.net/manual/es/intro-whatis.php

Universidad Autónoma del Estado de Hidalgo. (2017). *Plan de Desarrollo Institucional 2018-2023.* Pachuca de Soto: UAEH.

Universidad Autónoma del Estado de Hidalgo. (2018). *Aunario Estadistico 2017.* Pachuca de Soto: UAEH.

Universo Digital. (22 de Agosto de 2016). *CÓMO INSTALAR LINUX, APACHE, PHP, MYSQL (LAMP).* Obtenido de http://universo-digital.net/instalar-linux-apache-php-mysql-lamp-ubuntu/

Untiveros, S. (Julio de 2004). *Aprenda Redes.* Obtenido de http://www.AprendaRedes.com

Zabbix SIA. (28 de Septiembre de 2016). *Zabbix Documentation 3.4.* Obtenido de https://www.zabbix.com/documentation/3.4/manual

Glosario

Acción

Un medio predefinido para reaccionar a un evento.

Una acción consiste en operaciones (por ejemplo, enviar una notificación) y condiciones (cuando se lleva a cabo la operación)

Agente De Zabbix

Un proceso desplegado en objetivos de monitoreo para monitorear activamente los recursos y aplicaciones locales

Api De Zabbix

La API de Zabbix le permite usar el protocolo JSON RPC para crear, actualizar y recuperar objetos Zabbix (como hosts, elementos, gráficos y otros) o realizar cualquier otra tarea personalizada

Aplicación

Una agrupación de elementos en un grupo lógico

Disparador / Trigger

una expresión lógica que define un umbral de problema y se utiliza para "evaluar" los datos recibidos en los elementos

Cuando los datos recibidos están por encima del umbral, los disparadores pasan de 'Ok' a un estado 'Problema'. Cuando los datos recibidos están por debajo del umbral, los activadores permanecen en / regresan a un estado 'Ok'.

Escalada

Un escenario personalizado para ejecutar operaciones dentro de una acción; una secuencia de enviar notificaciones / ejecutar comandos remotos

Escenario Web

Una o varias solicitudes HTTP para comprobar la disponibilidad de un sitio web

Evento

Una sola ocurrencia de algo que merece atención como un estado de cambio de disparo o un auto -registro de descubrimiento / agente que tiene lugar

Grupo De Hosts

Un agrupamiento lógico de hosts; puede contener hosts y plantillas.

Los hosts y las plantillas dentro de un grupo de acogida no están vinculados entre sí de ninguna manera.

Los grupos de host se utilizan al asignar derechos de acceso a hosts para diferentes grupos de usuarios.

Host

Un dispositivo en red que desea supervisar, con IP / DNS.

Interfaz

La interfaz web provista con Zabbix

Ítem

Una pieza particular de datos que desea recibir fuera de un host, una métrica de datos.

Mando A Distancia

Un comando predefinido que se ejecuta automáticamente en un host supervisado en alguna condición

Medios De Comunicación

Un medio de notificación; canal de entrega

Notificación

Un mensaje sobre algún evento enviado a un usuario a través del canal de medios elegido

Plantilla/Template

Un conjunto de entidades (elementos, disparadores, gráficos, pantallas, aplicaciones, reglas de descubrimiento de bajo nivel, escenarios web) listos para ser aplicados a uno o varios hosts

El trabajo de las plantillas es acelerar el despliegue de tareas de monitoreo en un host; también para facilitar la aplicación de cambios masivos en las tareas de monitoreo.

Las plantillas se enlazan directamente a los hosts individuales.

Problema

Un disparador que está en estado "Problema"

Servidor Zabbix

Un proceso central del software Zabbix que realiza monitoreo, interactúa con los proxies y agentes Zabbix, calcula disparadores, envía notificaciones; un repositorio central de datos

Zabbix Proxy

Un proceso que puede recopilar datos en nombre del servidor Zabbix, eliminando una carga de procesamiento del servidor

Apéndice A

Características de los Switches

Características de los Switches

ILUSTRACIÓN 5-7 CISCO CATALYST 2950

Tipo de dispositivo	Conmutador - 24 puertos – Gestionado 2950
Tipo incluido	Sobremesa 1U
Subtipo	Fast Ethernet
Puertos	24 x 10/100
Tamaño de tabla de dirección MAC	8K de entradas
Protocolo de gestión remota	SNMP 1, SNMP 2, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, HTTP
Método de autentificación	RADIUS, TACACS+, Secure Shell v.2 (SSH2)
Características	Control de flujo, capacidad duplex, concentración de enlaces, soporte VLAN, snooping IGMP, soporte para Syslog, Cola Round Robin (WRR) ponderada, actualizable por firmware
Cumplimiento de normas	IEEE 802.3, IEEE 802.3u, IEEE 802.1D, IEEE 802.1Q, IEEE 802.1p, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s
Memoria Flash	8 MB Flash
Indicadores de estado	Velocidad de transmisión del puerto, modo puerto duplex, ancho de banda utilización %, alimentación, tinta OK, estado, enlace/actividad
Tipo de dispositivo	Conmutador - 24 puertos - Gestionado
Interfaces	1 x consola - RJ-45 - gestión 24 x 100Base-TX - RJ-45

TABLA 5-1 CARACTERÍSTICAS DEL SWITCH C2950

ILUSTRACIÓN 5-8 CISCO CATALYST 2960

Tipo de dispositivo	Conmutador - 24 puertos – Gestionado 2960
Tipo incluido	Montaje en rack 1U
Subtipo	Fast Ethernet
Puertos	24 x 10/100 + 2 x Gigabit SFP combinado
Rendimiento	Capacidad de conmutación: 16 Gbps Rendimiento de reenvío (tamaño de paquete de 64 bytes): 6.5 Mpps
Capacidad	VLAN activas: 64
Admite carcasa Jumbo	9018 bytes
Protocolo de gestión remota	SNMP 1, RMON 1, RMON 2, Telnet, SNMP 3, SNMP 2c, HTTP, TFTP
Método de autentificación	RADIUS, TACACS+
Características	Conmutación Layer 2, auto-sensor por dispositivo, soporte de DHCP, negociación automática, soporte VLAN, señal ascendente automática (MDI/MDI-X automático), snooping IGMP, soporte para Syslog, soporte DiffServ, Broadcast Storm Control, Multicast Storm Control, Unicast Storm Control, admite Rapid Spanning Tree Protocol (RSTP), admite Multiple Spanning Tree Protocol (MSTP), soporte de Dynamic Trunking Protocol (DTP), soporte de Port Aggregation Protocol (PAgP), Quality of Service (QoS), Protocolo de control de adición de enlaces (LACP), Port Security, MAC Address Notification
Cumplimiento de normas	IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s, IEEE 802.3ah, IEEE 802.1ab (LLDP)
Memoria RAM	128 MB
Memoria Flash	64 MB
Indicadores de estado	Estado puerto, velocidad de transmisión del puerto, modo puerto duplex, alimentación, sistema, enlace/actividad
Interfaces	24 x 100Base-TX - RJ-45 2 x SFP (mini-GBIC) 2 x 1000Base-T - RJ-45

TABLA 5-2 CARACTERÍSTICAS DEL SWITCH C2960

ILUSTRACIÓN 5-9 CISCO CATALYST 3560

Tipo de dispositivo	Conmutador - 24 puertos - L3 – Gestionado 3560
Tipo incluido	Sobremesa 1U
Subtipo	Fast Ethernet
Puertos	24 x 10/100 (PoE) + 2 x SFP
Alimentación por Ethernet (PoE)	PoE
Tamaño de tabla de dirección MAC	12k de entradas
Protocolo de direccionamiento	RIP-1, RIP-2, direccionamiento IP estático, RIPng
Protocolo de gestión remota	SNMP 1, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, SNMP 2c, HTTP, SSH-2
Método de autentificación	Kerberos, RADIUS, TACACS+, Secure Shell v.2 (SSH2)
Características	Capacidad duplex, conmutación Layer 3, conmutación Layer 2, auto-sensor por dispositivo, Encaminamiento IP, soporte de DHCP, alimentación mediante Ethernet (PoE), negociación automática, concentración de enlaces, soporte de MPLS, soporte VLAN, señal ascendente automática (MDI/MDI-X automático), snooping IGMP, limitación de tráfico, activable, snooping DHCP, soporte de Dynamic Trunking Protocol (DTP), soporte de Port Aggregation Protocol (PAgP), soporte de Trivial File Transfer Protocol (TFTP), soporte de Access Control List (ACL), Quality of Service (QoS), Servidor DHCP, Virtual Route Forwarding-Lite (VRF-Lite), rastreador MLD, Dynamic ARP Inspection (DAI), Time Domain Reflectometry (TDR)
Cumplimiento de normas	IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3af, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s
Memoria RAM	128 MB
Memoria Flash	16 MB Flash
Indicadores de estado	Estado puerto, velocidad de transmisión del puerto, modo puerto duplex, alimentación, tinta OK, sistema
Interfaces	24 x 100Base-TX - RJ-45 - PoE 1 x consola - RJ-45 - gestión 2 x SFP (mini-GBIC)

TABLA 5-3 CARACTERÍSTICAS DEL SWITCH C3560

ILUSTRACIÓN 5-10 CISCO CATALYST 3750E

Tipo de dispositivo	Conmutador - 24 puertos - L3 - Gestionado – apilable 3750E
Tipo incluido	Montaje en rack - 1U
Puertos	24 x 10/100/1000 + 2 x X2
Alimentación por Ethernet (PoE)	Sí
Tamaño de tabla de dirección MAC	12k de entradas
Protocolo de direccionamiento	RIP-1, RIP-2, EIGRP, direccionamiento IP estático, RIPng
Protocolo de gestión remota	SNMP 1, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, SNMP 2c, SSH
Características	Conmutación Layer 3, conmutación Layer 2, auto-sensor por dispositivo, soporte de DHCP, alimentación mediante Ethernet (PoE), negociación automática, soporte ARP, soporte VLAN, señal ascendente automática (MDI/MDI-X automático), snooping IGMP, soporte para Syslog, limitación de tráfico, Broadcast Storm Control, soporte IPv6, snooping DHCP, soporte de Dynamic Trunking Protocol (DTP), soporte de Port Aggregation Protocol (PAgP), soporte de Trivial File Transfer Protocol (TFTP), soporte de Access Control List (ACL), Quality of Service (QoS), compatibilidad con Jumbo Frames

TABLA 5-4 CARACTERÍSTICAS DEL SWITCH C3560