2019

SISTEMA DE MONITOREO DE REDES LAN CON ENFASIS EN LABORATORIO DE REDES USM

CASTELLON ZUÑIGA, SIMON CRISTIAN

UNIVERSIDAD TÉCNICA FEDERICO SANTA MARÍA
SEDE VIÑA DEL MAR – JOSÉ MIGUEL CARRERA

“SISTEMA DE MONITOREO DE REDES LAN CON ÉNFASIS EN LABORATORIO DE REDES USM”

Trabajo de Titulación para optar al Título de Técnico Universitario en Telecomunicaciones y Redes

Alumnos:
Simón Cristian Castellón Zúñiga
Bastián Sánchez Méndez

Profesor Guía:
Dr. Ing. Cristian Ahumada Vera

Profesor Correferente:
Ing. Víctor Cárdenas Schweiger

2019

RESUMEN

KEYWORDS: DISPONIBILIDAD - SNMP - MÉTRICA - AGENTE - MAPA TOPOLÓGICO - BASE DE DATOS - PLANTILLA.

El presente proyecto abarca varios aspectos, los cuales son principalmente donde y porqué es importante implementar un buen monitoreo de red, en este caso el énfasis será uno de los laboratorios de la USM, en cada uno de los distintos capítulos de este proyecto se abordarán diversos aspectos.

El capítulo 1; El cual se titula “Problemática a resolver y Alternativas de solución”, está basado en plantear la problemática en base a la ubicación, las posibles soluciones, además de escoger el equipamiento más adecuado que se adapte para un correcto desarrollo del proyecto y entender la importancia de cada una de las herramientas escogiendo también la más adecuada, principalmente basándose en las necesidades de donde se quiera llevar a cabo la instalación.

El capítulo 2; “Implementación del sistema” con la herramienta seleccionada, se trata sobre llevar a cabo un elaborado mapa de solución paso a paso, incluyendo la topología de red.

El capítulo 3; “Evaluación de costos” abarca todos los costos de todo el equipamiento requerido para llevar a cabo la implementación, además del costo de la mano de obra requerida para implementarlo y mantenerlo.

ÍNDICE

RESUMEN

INTRODUCCIÓN 1

CAPÍTULO 1: PROBLEMA A RESOLVER Y ALTERNATIVAS DE SOLUCIÓN 2

1.1 DEFINICIÓN DE MONITOREO DE RED 2

1.2 OBJETIVOS DEL PROYECTO 3

1.2.1 Objetivo Global 3
1.2.2 Objetivos Específicos 3

1.3 RAZONES PARA IMPLEMENTAR UN MONITOREO DE RED 3

1.3.1 Adelantarse a las interrupciones de la red 3
1.3.2 Solucionar problemas con mayor facilidad 3
1.3.3 Mejorar la seguridad de la red 4
1.3.4 Gestionar redes cada vez más cambiantes 4
1.3.5 Vigilar el cumplimiento de las reglas 4
1.3.6 Ayuda en el aprendizaje 4
1.3.7 Ahorro en costos de electricidad e implementos 5

1.4 TIPOS DE MONITOREO 5

1.4.1 Monitoreo Activo 5
1.4.2 Monitoreo Pasivo 5

1.5 PASOS PREVIOS AL MONITOREO DE RED 6

1.5.1 Analizar el sistema 6
1.5.2 Categorizar el inventario 6
1.5.3 Definir elementos con alerta 6
1.5.4 Definir canales de comunicación 6
1.5.5 Establecer el protocolo de actuación 6
1.5.6 Elegir herramienta de monitorización 6

1.6 IMPORTANCIA DE LAS HERRAMIENTAS DE MONITOREO DE RED 7

1.7 HERRAMIENTAS DE MONITOREO DE RED 8

1.7.1 Características de Pandora FMS 8
1.7.2 Características de Nagios 8
1.7.3 Características de Zenoss 8
1.7.4 Características de Zabbix 9

1.8 ¿POR QUÉ UTILIZAR ZABBIX Y NO LOS DEMÁS? 13

1.9 ¿CÓMO FUNCIONA ZABBIX? 13

1.9.1 Funcionamiento general 13
1.9.2 Triggers y plantillas 14

CAPÍTULO 2: IMPLEMENTACIÓN DEL SISTEMA 15

2.1 RECONOCIMIENTO DEL HARDWARE 16

2.1.1 Inventario del sistema 16
2.1.2 Topología del sistema 17

2.2 INSTALACIÓN PREVIA DE SERVICIOS REQUERIDOS 18

2.2.1 Instalación de NTP 18
2.2.2 Instalación de MySQL 18
2.2.3 Instalación de Apache 19

2.3 PREPARACIÓN DE SERVIDOR 20

2.3.1 Instalación del software Zabbix 20
2.3.2 Configuración de monitoreo al servidor 24

2.4 PREPARACIÓN DE AGENTES 25

2.4.1 Configuración en Host Windows 25
2.4.2 Configuración en Servidor 28

2.5 PREPARACIÓN DE SWITCH CISCO 30

2.5.1 Configuración en Switch 30
2.5.2 Configuración en Servidor 31

2.6 MONITOREO TCP/UDP 32

2.7 MONITOREO ICMP 34

2.8 NOTIFICACIONES/ALERTAS 36

2.8.1 Configuración en Gmail 36
2.8.2 Configuración en Zabbix 37
2.8.3 Prueba de las Notificaciones 40

2.9 AUTO DESCUBRIMIENTO 41

2.9.1 Configuración de regla de descubrimiento 41
2.9.2 Configuración de acciones post descubrimiento 42

2.10 GRÁFICOS PERSONALIZADOS 44

2.11 MAPAS TOPOLÓGICOS DE RED 45

2.11.1 Configuración previa 45
2.11.2 Adición de elementos 47
2.11.3 Selección de elementos 47
2.11.4 Elementos de enlace 48

CAPÍTULO 3: EVALUACIÓN DE COSTOS 50

3.1 ESPECIFICACIONES DEL INVENTARIO **50**

3.1.1 Router LAN 50
3.1.2 Switch 51
3.1.3 Router WLAN 52
3.1.4 Teléfono IP 53
3.1.5 PBX IP 54
3.1.6 Cámara IP 55

3.2 COSTOS DEL INVENTARIO 56

3.2.1 Costos generales 56
3.2.2 Cotizaciones 56
3.2.3 Software y SO 56
3.2.4 Componentes de PC 57

3.3 COSTOS MANO DE OBRA 57

3.3.1 Investigación 57
3.3.2 Implementación 58
3.3.3 Mantención 58

3.4 SUMARIO DE COSTOS 58

CONCLUSIONES Y RECOMENDACIONES 60

BIGLOGRAFÍA 61

ANEXOS 62

SIMBOLOGÍA Y SIGLAS

SIGLA

- **yBASExx:** Velocidad en Mbit/s (y), técnica codificación de señal (BASE), tipo de cable (xx).
- **HDD:** Unidad de disco rígido.
- **HTTP:** Protocolo de transferencia de hipertexto (WWW).
- **ICMP:** Protocolo de control de mensajes de internet.
- **IEEE:** Instituto de ingeniería eléctrica y electrónica (estándares).
- **IPv4:** Protocolo de internet versión 4.
- **LAN:** Red de área local.
- **Macro:** (Macroinstrucción) instrucción compleja, formada por varias instrucciones sencillas.
- **Netflow:** Protocolo de recolección de información de tráfico IP propiedad de Cisco.
- **NTP:** Protocolo de tiempo de red.
- **PHP:** Preprocesador de hipertexto.
- **POP3:** Protocolo de oficina de correo.
- **Proxy:** Servidor intermediario en las peticiones que realiza un cliente a otro servidor.
- **RAM:** Memoria de acceso aleatorio.
- **RJ45:** Conector 45 registrado de red.
- **RMON:** Protocolo para la monitorización remota de redes.
- **SLA:** Acuerdo de calidad de servicio.
- **SMTP:** Protocolo para transferencia simple de correo.
- **SNMP:** Protocolo simple de manejo de red.
- **SQL:** Lenguaje de consulta estructurada.
- **SSH:** Secure Shell, Protocolo de seguridad de red.
- **SSL:** Capa de sockets seguros
- **TCP:** Protocolo de control de transmisión.
- **TI:** Tecnología de la información.
- **TLS:** Seguridad de la capa de transporte.
- **UDP:** Protocolo de datagrama de usuario.
- **UTP:** Cable de par trenzado.

INTRODUCCIÓN

El objetivo de este proyecto es investigar por qué en una infraestructura es importante monitorear el comportamiento de la red y de los elementos que la conforman, como podría ser un servidor, router y un switch, con el fin de mantener la disponibilidad de estos sin interrupciones en las actividades planeadas en el día a día.

Las redes computacionales generalmente pertenecen a un proveedor de servicios que debe garantizar una buena calidad del servicio, al igual que las empresas. En este caso el enfoque será implementar un monitoreo de red en la Universidad Técnica Federico Santa María Sede Viña del Mar, más en específico en el Edificio M Laboratorio M-207, este contiene prácticamente la mayoría de elementos que se pueden encontrar en empresas como routers, switches, computadores, servidores entre otros, por lo que contar con una buena herramienta de monitoreo sería esencial, permitiendo así configurar, monitorear, evaluar, analizar y controlar los equipos con el fin de lograr mantener niveles de trabajo y de servicio adecuados a los objetivos de la Universidad.

En este laboratorio se podrá detectar, por ejemplo, alguien que dentro esté usando una aplicación que provoque que la red pudiera colapsar como lo sería un juego en línea o un servicio de streaming, también se podrá saber el estado de los componentes internos de los computadores y si se quisiera implementar un servidor; será imprescindible un sistema de monitorización con el cual se pueda saber el estado de este, el uso del disco duro, sus temperaturas, enlaces disponibles, etc.

La importancia de esta propuesta radica en proporcionar una herramienta fácil de usar, administrable desde cualquier computador, de bajo costo, que sea robusta y eficaz. Lo que se hará es compararlas y decidirse por una, la que más convenga para este caso en concreto.

Como dato importante antes de la implementación, cabe mencionar que el laboratorio de redes M-207 posee componentes como router LAN, switch, computadores, teléfonos IP, cámaras IP, PBX IP, rack, router WLAN. El equipamiento de routers y switches es de diversas marcas como 3com, Cisco, Dell y Huawei, sin embargo, en este trabajo se utilizará solo Cisco.

Un objetivo secundario de este proyecto es mejorar el aprendizaje sobre las redes, su funcionamiento, sus componentes, sus riesgos, sus beneficios, etc.

CAPÍTULO 1: PROBLEMA A RESOLVER Y ALTERNATIVAS DE SOLUCIÓN

1: PROBLEMA A RESOLVER Y ALTERNATIVAS DE SOLUCIÓN

En este capitulo se introducirá al proyecto, pasando por secciones como la definición de monitoreo, la importancia y motivos para implementarlo, las herramientas a elegir, etc.

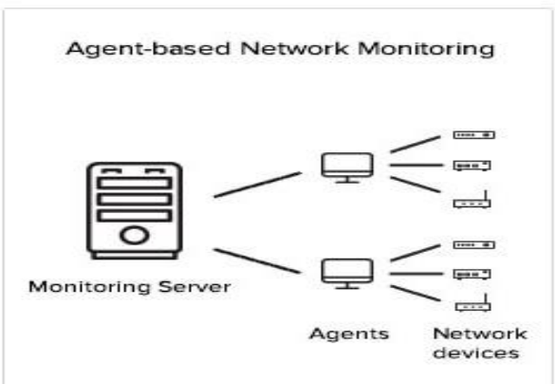
1.1 DEFINICIÓN DE MONITOREO DE RED

El objetivo final de un monitoreo de red es asegurarse de que la red se encuentre funcionando a pleno rendimiento el 100% del tiempo, además de mejorar la optimización mediante análisis de rendimiento. Elegir un software de monitoreo de red adecuado ayudará a detectar posibles problemas antes de que se provoque un colapso o una caída de la red.

El monitoreo de red describe un sistema que constantemente monitoriza una red de computadoras en busca de componentes defectuosos o lentos, para luego informar a los administradores de redes mediante alertas. Ejemplos de problemas que busca son sobrecargas y/o fallas en los servidores y problemas de la infraestructura de red u otros dispositivos.

SNMP (Simple Network Management Protocol) es el estándar de monitoreo más popular, la mayoría de los proveedores lo integran en sus equipos. Este define objetos como lo son parámetros e información que se administran en bases de datos y un protocolo que interactúa con ellos, obteniéndolos y estableciéndolos como variables. SNMP proporciona el marco de trabajo sobre el que se puede implementar una gestión con un software adecuado.

La administración de red abarca el monitoreo y la gestión (aunque en muchos casos, como este, se usa monitoreo de red para referirse a las 2 juntas). Mientras que el monitoreo permite analizar y ver el estado de la red a un nivel básico, la gestión va más allá; permite tomar acciones de gestión además de acciones para paliar los problemas de la red, dando una visión global de todos los sistemas. Otros elementos claves son la estación de trabajo, el agente de base de datos de información (ver figura 1-1) y los protocolos de gestión de red.



Fuente: keil.com

Figura 1-1: Monitoreo de red con Agentes

1.2 OBJETIVOS DEL PROYECTO

Se procederá a presentar los objetivos del proyecto, abarcando los 3 capítulos.

1.2.1 Objetivo Global

Implementar un sistema de monitoreo de redes LAN con énfasis en laboratorio USM.

1.2.2 Objetivos Específicos

- ➢ Describir un monitoreo de red, sus beneficios y componentes.
- ➢ Formular implementación del sistema de monitoreo de red en el laboratorio de redes USM.
- ➢ Ejemplificar herramientas con las cuales se puede implementar para poder elegir la que más se adecue a la ubicación ya establecida.
- ➢ Implementar la herramienta elegida para el monitoreo de red.
- ➢ Evaluar los costos de la implementación.

1.3 RAZONES PARA IMPLEMENTAR UN MONITOREO DE RED

Se enumerarán las razones para implementar un monitoreo de red

1.3.1 Adelantarse a las interrupciones de la red

Los errores en los sistemas informáticos son causados por el error humano, los problemas de configuración y los factores ambientales pueden contribuir. Monitorizar la red ofrece la visibilidad necesaria para mantenerse un paso por delante de posibles problemas, ayudando a identificar interrupciones por ejemplo que podrían causar cuellos de botella y averiguar cuál es el causante. Primero se obtiene una imagen de cómo se ve el rendimiento "normal" en la red, lo que facilita la detección de cualquier evento fuera de lo común.

1.3.2 Solucionar problemas con mayor facilidad

Se realiza un inventario de todos los dispositivos que muestran las conexiones físicas entre ellos, la búsqueda de dispositivos problemáticos conlleva mucho menos tiempo. Con un clic en un dispositivo en particular es posible extraer datos clave de rendimiento, como la disponibilidad, la pérdida de paquetes, el tiempo de respuesta, las tasas de error y otro tipo de métricas. Un ejemplo de problema que se puede presentar pensando en el enfoque específico del laboratorio de redes, es el fallo de algún rack, switch, router, etc., que es crucial en el funcionamiento de la red, implementar un monitoreo permitirá que el inconveniente se resuelva más fácil y rápido.

1.3.3 Mejorar la seguridad de la red

La seguridad de los datos críticos es una cuestión de gran importancia para cualquier red. Los intrusos suelen dirigirse a redes que intuyen que están mal equipadas. Respecto a el caso del laboratorio de redes, se puede ser víctima de robo de información importante para el alumno o el profesor, como credenciales, datos bancarios, proyectos propios, etc., de parte de alguna persona que esté de visita en la universidad y que posea los conocimientos informáticos necesarios para infiltrarse, también puede darse lugar el uso malicioso por personal auxiliar de los computadores en tiempos fuera de la jornada. El aplicar un monitoreo de red constante que arroje alarmas de prevención en caso de comportamiento inusual, va a ayudar a la detección temprana de cualquier ataque y a blindar mejor los datos sensibles. Se podrá detectar cambios sospechosos en el tráfico entrante y saliente, mediante su seguimiento en dispositivos críticos. El saber cuándo y en qué dispositivo ocurrió un evento, es muy importante para tener una seguridad proactiva.

1.3.4 Gestionar redes cada vez más cambiantes

Hoy la innovación tecnológica ha permitido el aumento de la cantidad de dispositivos conectados, sensores con acceso a Internet, dispositivos inalámbricos, tecnologías en la nube, cámaras y teléfonos IP, todo este equipo necesita integrarse adecuadamente a la red con monitorizaciones continuas para detectar fluctuaciones y actividades sospechosas.

1.3.5 Vigilar el cumplimiento de las reglas

Las topologías de red en tiempo real, el monitoreo continuo y la asociación de VLANs con canales seguros pueden ayudar mucho al cumplimiento de un reglamento organizacional. En el laboratorio de redes, una vigilancia en tiempo real con alertas puede evitar pasar malos ratos a profesores debido a posibles alumnos que se distraigan mucho mediante páginas recreacionales como por ejemplo videojuegos online, el hecho de que un alumno ocupe un gran ancho de banda por ejemplo por un videojuego online, puede mermar el desempeño de la red y perjudicar a otros, pasando a llevar el reglamento de la universidad de un ambiente estudiantil adecuado.

1.3.6 Ayuda en el aprendizaje

Respecto al caso específico del laboratorio de redes M-207, la verificación de datos específicos del monitoreo de red puede facilitar el aprendizaje de los alumnos, ejemplo de estos son la disponibilidad, la pérdida de paquetes, el tiempo de respuesta y las tasas de error, con los cuales se puede saber cuál es el error concreto que se está cometiendo en una experiencia y así

evitar momentos de frustración, o casos en que un profesor se quede mucho rato en un solo puesto, descuidando a los otros alumnos.

1.3.7 Ahorro en costos de electricidad e implementos

Un correcto monitoreo de red puede tener como beneficio el ahorro en costos de electricidad en periodos de no uso de la red debido a equipo/s específico/s prendidos, también así se evita que se puedan averiar por el sobrecalentamiento y por ello ahorrar el costo que puede conllevar la compra de un reemplazo de este, ejemplo un caso en que un router del laboratorio de redes este prendido todo el día durante la jornada, sin apagarlos durante las ventanas.

1.4 TIPOS DE MONITOREO

Se procederá a describir los 2 métodos de monitoreo de red

1.4.1 Monitoreo Activo:

Introduce paquetes de pruebas en la red, o los envía a determinadas aplicaciones y midiendo sus tiempos de respuesta. Es empleado para medir el rendimiento de esta. Técnicas (basadas en):

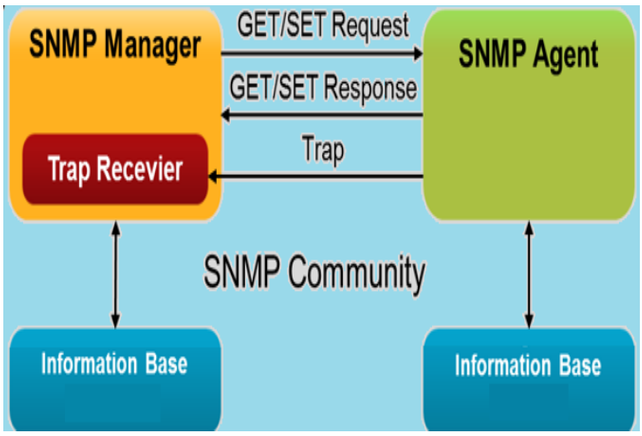
- ICMP: Diagnosticar problemas en la red - Detectar pérdida de paquetes - Tiempo de respuesta - Disponibilidad de host y redes.
- TCP: Tasa de transferencia - Diagnosticar problemas a nivel de aplicación.
- UDP: Pérdida de paquetes en un sentido - Tiempo de respuesta.

1.4.2 Monitoreo Pasivo:

Recolecta y analiza paquetes. Se usa software de análisis de tráfico y en general dispositivos con soporte para SNMP, RMON y Netflow. Es empleado para caracterizar el tráfico de red y para contabilizar su uso. Técnicas:

- SNMP: Genera paquetes llamados “traps” que indican que un evento inusual se ha producido. Ver figura 1-2 para una representación gráfica del funcionamiento de SNMP.
- Captura de tráfico: Mediante la configuración de un puerto espejo en un dispositivo de red o mediante la instalación de un dispositivo intermedio que capture el tráfico.
- Análisis del tráfico: Se utiliza para caracterizar el tráfico de red, es decir, clasificar el tráfico por aplicación, direcciones IP origen y destino, puertos origen y destino, etc.

➢ Flujos: Se utiliza para caracterizar el tráfico de red. Un flujo es un conjunto de paquetes con la misma dirección, puerto TCP origen y destino y tipo de aplicación.



Fuente: manageengine.com

Figura 1-2: Funcionamiento de SNMP.

1.5 PASOS PREVIOS AL MONITOREO DE RED

Se procederá a describir los pasos previos a realizar antes del proceso de monitoreo.

1.5.1 Analizar el sistema: Realizar el inventario por tipo de componente (servidor, router, switch, etc.) elementos dentro del componente (RAM, Tarjeta de Video, HDD, etc.), marca del componente (Intel, Windows, NVIDIA, AMD, etc.), IP y la prioridad de la monitorización. Ver Figura 1-3 como un ejemplo de inventario de red.

1.5.2 Categorizar el inventario: En los diferentes ámbitos de una instalación como los siguientes: sistemas, redes, servidores, seguridad o aplicaciones.

1.5.3 Definir elementos con alerta: Ejemplo procesadores saturados, discos duros próximos a llenarse, ancho de banda limitado, se puede crear una alarma para cada uno de ellos. Existen 5 tipos de alerta: procesamiento, conectividad, ambiental, utilización y disponibilidad.

1.5.4 Definir canales de comunicación: Lugar a donde se enviarán los avisos, como email, SMS, app, chat, etc.

1.5.5 Establecer el protocolo de actuación: Según qué tipo de incidente sea, más grave o menos, requerirá un tipo de actuación y otro.

1.5.6 Elegir herramienta de monitorización: Ejemplo Pandora FMS, Nagios y Zabbix, instalarla y configurarla, manteniendo las medidas de seguridad existentes y siguiendo el análisis inicial y protocolos establecidos.

Una vez se configura el monitor de red en los equipos necesarios, hay que configurar las prioridades para que luego el monitoreo se encargue de analizar constantemente las métricas como el tiempo de respuesta, disponibilidad de recursos, consistencia, confiabilidad, etc. a partir de estos datos, también genera reportes y comienza a categorizar los eventos como frecuentes u ocasionales, así como a asignarles un nivel de gravedad en determinados casos. Adicionalmente, se debe llevar un registro de incidencias. El profesional encargado del monitoreo es un técnico en Administración de sistemas/redes, es él quien configura, administra y hace mantención para garantizar el buen funcionamiento.

Fuente: arandatraining.com

Figura 1-3: Inventario de Red.

1.6 IMPORTANCIA DE LAS HERRAMIENTAS DE MONITOREO DE RED

Dentro de las diversas herramientas de monitoreo de red existen por nombrar algunas Zenoss, Nagios y Zabbix. ¿Qué es lo que se busca en un software de monitoreo? ¿Porque elegir uno por sobre una sobre otras? ¿Qué datos es importantes a tener en cuenta?

- Comunicación de las alertas: Los mensajes deben manejar protocolos que puedan llegar a distintos dispositivos.
- Integraciones con servidores externos: Debe monitorear ejemplo servidores de correo.
- Sencillez de manipulación y presentación de los datos en la interfaz web: Para conocer en tiempo real el estado de la red y otorgar privilegios de acceso.
- Flexibilidad: Debe adaptarse a varios entornos y tecnologías para integrarlos.
- Integraciones con Bases de Datos: El software debe comprender el lenguaje de la base de datos para gestionarla correctamente, como por ejemplo MySQL.
- Multidispositivo: Emplear cualquier dispositivo para gestionar el monitoreo.
- Escalabilidad: Poder adaptarse ante cualquier cambio de crecimiento que sufra la red.
- Soporte: Procurar que cuente con el mayor número de protocolos de adquisición de datos posible, capaces de capturar mensajes de NetFlow, sFlow, jFlow o cualquier otro protocolo.

1.7 HERRAMIENTAS DE MONITOREO DE RED

Existen varias herramientas de Monitoreo de Red como Pandora FMS, Nagios, Zenoss y Zabbix, a continuación, se enumerarán características de cada uno:

1.7.1 Características de Pandora FMS

1. Autodescubrimiento y detección automática de la topología de red.
2. Agentes multiplataforma para Windows, HP-UX, Solaris, BSD, AIX y Linux.
3. Permite virtualización.
4. Monitorización de disponibilidad y rendimiento.
5. Agentes para Android.
6. Gestión de servicios (SNMP, TCP, ICMP, etc.), IPv4 e IPv6.
7. Interfaz web con niveles de acceso totalmente personalizables.
8. Alta escalabilidad.
9. Sistema de informes configurable que evalúa el nivel de cumplimiento de los sistemas (SLA).
10. Versiones no limitadas.

1.7.2 Características de Nagios

1. Fue diseñado para ser ejecutado en GNU/LINUX.
2. Gestión de servicios (SMTP, POP3, HTTP, PING, etc.).
3. Monitorización de recursos de sistemas y gestión de servicios pasivos.
4. Arquitectura simple de integración.
5. Escalado y distribución de servicios, recursos y nodos.
6. Posee un sistema proactivo para la solución de problemas.
7. Soporte de arquitecturas de servidor redundantes y distribuidas.
8. Interfaz de comandos externos (Triggers, web o aplicaciones de terceros) que permitan modificar la administración del sistema.
9. Interfaz intuitiva.
10. Posee muchas variaciones por lo que no es recomendable para cualquier caso.

1.7.3 Características de Zenoss

1. Funciona en sistemas Linux, Unix, sistemas Mac y Windows.
2. Permite exportar e importar datos.
3. Monitorización de disponibilidad y rendimiento.
4. Verificación de los recursos de cada estación y de cómo se está compartiendo la información.

5. Inventario.
6. Disponibilidad de vigilancia de red.
7. Monitoreo sin necesidad de agentes.
8. Monitoreo de servicios de red (HTTP, POP3, NNTP, SNMP y FTP).
9. Extensiones de código abierto.
10. Monitoreo de rendimiento de dispositivos a través de series temporales de datos.

1.7.4 Características de Zabbix

1. Agentes multiplataforma para Linux, OpenBSD, Windows XP o superior.
2. Su alto rendimiento y capacidad de monitoreo permite monitorear en tiempo real la información recopilada de máquinas virtuales, servidores del sistema u otros.
3. La información se puede almacenar en variedad de formatos de base de datos, como MySQL, que se puede analizar después para comprender y mejorar la condición del servidor.
4. Comunicación entre agentes y clientes para recopilar datos y enviarlos al servidor.
5. Los datos están protegidos mediante redes seguras y cifrado, usando por ejemplo SSL/TLS.
6. Interfaz web intuitiva con niveles de acceso totalmente personalizables.
7. Carga de módulos nuevos para aumentar la funcionalidad y el rendimiento.
8. Plataforma para monitorear entornos de TI a gran escala.
9. Autodescubrimiento y detección automática de la topología de red.
10. Gestión de Servicios (SNMP, TCP, UDP, ICMP, etc.).

Las figuras 1-4, 1-5, 1-6 y 1-7 muestran los logos de cada herramienta mencionada.

Fuente: pandorafms.org

Figura 1-4: Logo Zabbix.

Fuente: nagios.org

Figura 1-5: Logo Nagios.

Fuente: nagios.org

Figura 1-6: Logo Zenoss.

Fuente: zabbix.org

Figura 1-7: Logo Zabbix.

La tabla 1-1; muestra una comparativa detallada de distintos aspectos de utilidad para un software de monitoreo de red.

Tabla 1-1: Comparación de características de software de monitorización

	Pandora FMS	**Nagios**	**Zabbix**	**Zenoss**
Gestión y configuración de usuario	Posee una interfaz web de gestión centralizada a través de una base de datos.	Se gestiona a través de ficheros de texto entrelazados, scripts y procesos manuales.	Posee una interfaz web de gestión centralizada a través de una base de datos.	Posee una interfaz web muy centralizada debido a que requiere muchas interacciones diferentes y aplicaciones de terceros.
Monitorización	Monitorización puede realizarse con o sin agentes.	Monitorización con agentes que se encargan de recopilar información y enviarla al servidor.	Monitorización con agentes que se encargan de recopilar información y enviarla al servidor.	La Monitorización sin agentes provoca que se requiera de terceros para extraer la información.
Generación de informes y paneles visuales	Los plugins ya vienen de serie.	Hay que usar un plugin con propia entidad.	Los plugins ya viene de serie.	Los plugins ya vienen de serie.
Escalabilidad	Alta.	Baja.	Muy Alta.	Baja.
Informes SLA	Si, tiempo real.	Si.	Si.	No.
Auto-Descubrimiento	A nivel de aplicación, tomando solo métricas útiles.	Solo de la topología.	Basado en rangos IP, SNMP u otros servicios externos.	Solo de la topología.

Fuente: Elaboración propia

De la tabla 1-1 y la información de características individuales de cada software; podemos deducir que Zabbix es el software de monitoreo más conveniente para usar en este caso en concreto por estar sobre los otros softwares mencionados, este posee una interfaz intuitiva y personalizable, plugins de paneles e informes ya incorporados, informes SLA, cifrado del tráfico de red, buen soporte para SNMP y complementos. Ver punto 1.8 “¿Por qué elegir Zabbix?” para más información.

La tabla 1-2; muestra ponderaciones de las herramientas en cada categoría, correspondientes a las características analizadas en este capítulo, siendo en esta escala, 0 la nota mínima, 1 la nota media y 2 la nota máxima. Esta tabla es un complemento a la tabla 1-1.

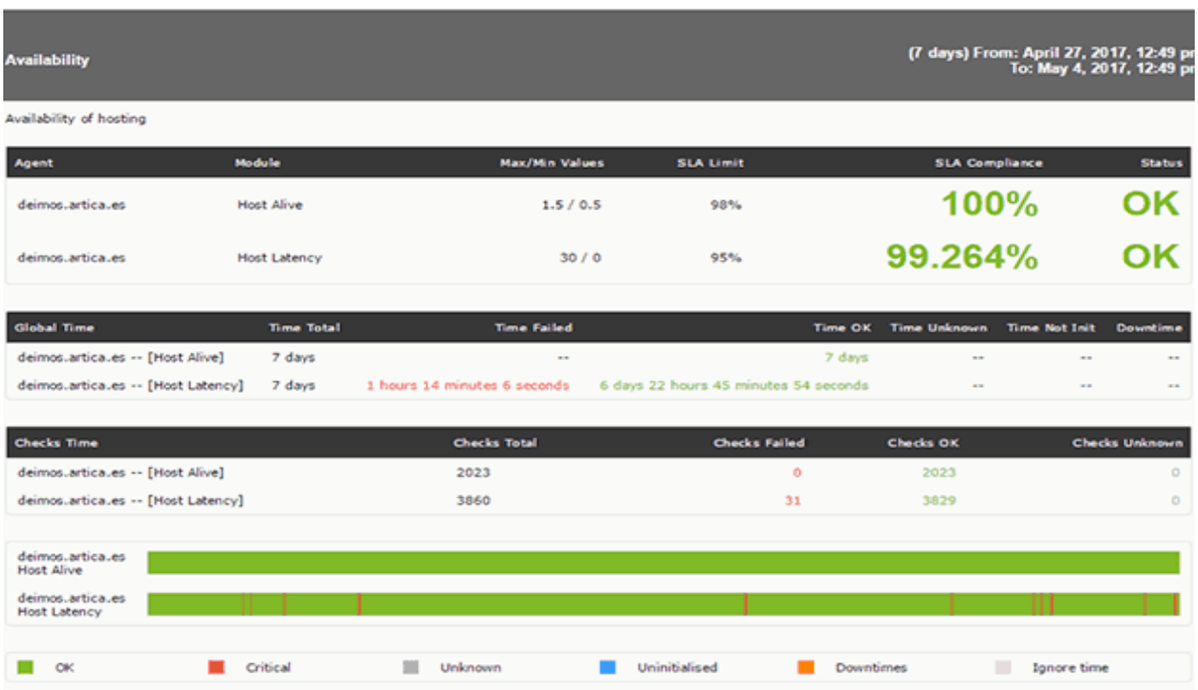
Tabla 1-2: Ponderación de cada herramienta de monitoreo.

	Facilidad	Soporte	Plataf.	Escabilidad	Autodes.	Personaliz.	Costo	Σ
P. FMS	2	2	1	1	1	2	1	10
Nagios	0	1	0	0	0	2	2	5
Zabbix	2	2	2	2	2	2	2	14
Zenoss	1	2	1	0	1	2	1	8

Fuente: Elaboración propia

De la tabla 1-2, se puede concluir que, de acuerdo con la sumatoria de notas, Zabbix es la herramienta más conveniente.

Las figuras 1-8, 1-9 y 1-10; muestran ejemplos de informes generados por distintas herramientas.



Fuente: blog.pandorafms.org

Figura 1-8: Informe de Pandora FMS.

En la figura 1-8; se aprecia un informe SLA que abarca 7 días y que muestra que el porcentaje de disponibilidad y la tasa que latencia están correctos respecto al margen de error del proveedor de servicios, en ese host específico donde está instalado el agente.

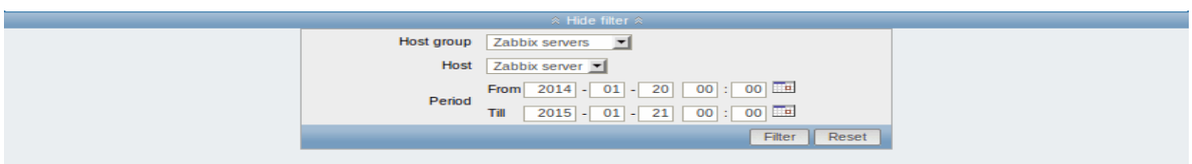
Service Data

Host	Service	Uptime	SLA Status
Nagios Log Server	Check for Elasticsearch	100.000%	PASSED
	Check for Logstash	100.000%	PASSED
	Current Load	100.000%	PASSED
	Current Users	100.000%	PASSED
	Failed SSH logins for NLS1	100.000%	PASSED
	Ping	100.000%	PASSED
	Total Processes	100.000%	PASSED
	Where is my cat_	100.000%	PASSED
Nagios Log Server 2	Check for Elasticsearch	100.000%	PASSED
	Check for Logstash	100.000%	PASSED
	Current Load	100.000%	PASSED
	Current Users	100.000%	PASSED
	Ping	100.000%	PASSED
	Total Processes	100.000%	PASSED
	Where is my cat_	100.000%	PASSED
Nagios XI localhost	Current Users	100.000%	PASSED
	HTTP	100.000%	PASSED
	I/O Wait	100.000%	PASSED
	Load	100.000%	PASSED
	MD5 on /etc/passwd	100.000%	PASSED
	Nagios XI Daemons	100.000%	PASSED
	Nagios XI Jobs	100.000%	PASSED
	Ping	100.000%	PASSED
	Root Partition	100.000%	PASSED
	SSH	100.000%	PASSED
	Swap Usage	100.000%	PASSED
	Total Processes	100.000%	PASSED
	check for httpd	100.000%	PASSED
	Average	100.000%	PASSED

Fuente: blog.pandorafms.org

Figura 1-9: Informe de Nagios.

En la figura 1-9; se muestra un informe que detalla el estado de los datos de servicio de los servidores como lo sería ping, SSH, memoria swap, HTTP, por ejemplo, este funciona a un 100%.



Name	Problems	Ok	Graph
/etc/passwd has been changed on Zabbix server	0.0000%	100.0000%	Show
Configured max number of opened files is too low on Zabbix server	0.0000%	100.0000%	Show
Configured max number of processes is too low on Zabbix server	0.0000%	100.0000%	Show
Disk I/O is overloaded on Zabbix server	0.0108%	99.9892%	Show
Free disk space is less than 20% on volume /	31.8672%	68.1328%	Show
Free inodes is less than 20% on volume /	0.0000%	100.0000%	Show
Host information was changed on Zabbix server	0.0000%	100.0000%	Show
Host name of zabbix_agentd was changed on Zabbix server	0.0000%	100.0000%	Show
Hostname was changed on Zabbix server	0.0000%	100.0000%	Show
Lack of available memory on server Zabbix server	0.0000%	100.0000%	Show
Lack of free swap space on Zabbix server	100.0000%	0.0000%	Show
Less than 5% free in the value cache	0.0000%	100.0000%	Show
Less than 25% free in the configuration cache	0.0000%	100.0000%	Show
Less than 25% free in the history cache	0.0000%	100.0000%	Show

Fuente: blog.pandorafms.org

Figura 1-10: Informe de Zabbix.

En la figura 1-10; se muestran 2 problemas encontrados, uno de ellos es que la memoria swap del servidor está llena, con una gravedad de 100%, siendo el otro problema la falta de memoria en el disco duro (menos del 20%) el cual el programa muestra con una gravedad del 32%.

1.8 ¿POR QUÉ UTILIZAR ZABBIX Y NO LOS DEMÁS?

El único software 100% libre es Zabbix. Tanto Nagios y Zenoss están basados en venta de versiones extendidas del producto, en cambio Zabbix vive de certificaciones a profesionales TI, libros y soporte y también cuenta con manuales de usuario online muy bien detallados, lo cual proporciona una fuente de información adicional para el usuario. Además, Zabbix cuenta con todo lo que se necesita para el monitoreo, una de sus pocas desventajas es que la configuración es un poco más técnica, sin embargo, con dedicación se puede comprender, y su comunicación es bastante activa.

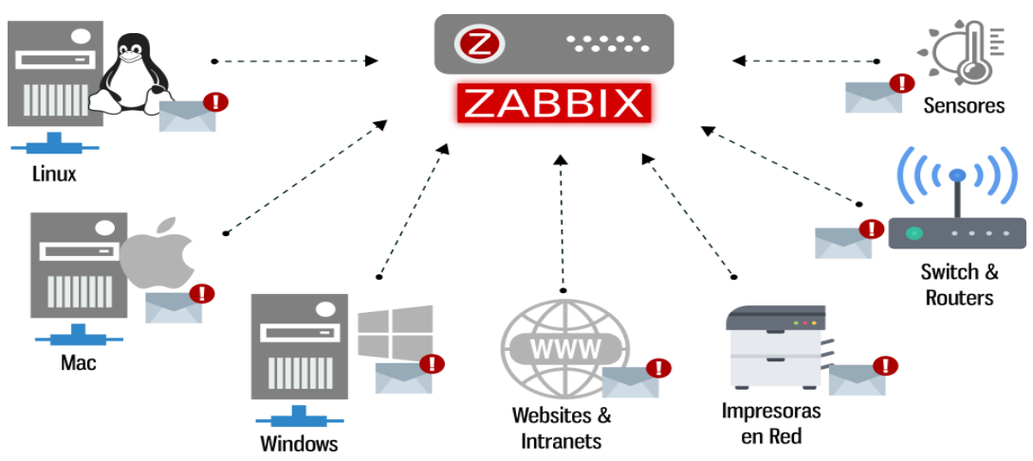
1.9 ¿CÓMO FUNCIONA ZABBIX?

Zabbix es la herramienta elegida, a continuación, se explicará su funcionamiento a grandes rasgos incluyendo uno de sus elementos más importantes: los Triggers, este ítem se profundizará en el capítulo 2.

1.9.1 Funcionamiento general

El funcionamiento de Zabbix ofrece un monitoreo para redes locales (LAN) y redes de área amplia (WAN). El software se puede instalar en un servidor Linux o Ubuntu y luego se dedica a recolectar la información la cual presenta en una interfaz web de forma gráfica.

El servidor monitoriza por SNMP todo router/switch dado de alta y realiza las comprobaciones de ping y latencia, los agentes se encargan del monitoreo mientras sus servicios envían los datos al servidor de monitorización para que luego este se encargue de evaluarlos. Si se cumplen los determinados parámetros SLA, este se encarga de enviar la alerta por medio de por ejemplo un correo electrónico a través de SMTP.



Fuente: quasarbi.com/ZABBIX

Figura 1-11: Topología de Zabbix.

Zabbix cuenta con agentes multiplataforma para las estaciones de trabajo, con estos es posible ver el estado de impresoras, routers, switches, sensores de temperatura y humedad entre otros, como se ve en la figura 1-11. Zabbix almacena la información que recibe de los agentes instalados en los servidores, así como de los dispositivos de red como switch, router, router WLAN, entre otros, que han sido preconfigurados para su monitoreo. Zabbix posee una interfaz web la cual soporta una base de datos y posee un sistema proactivo, permitiendo tomar acciones para solucionar automáticamente los problemas mediante las alertas y las visualizaciones de gráficos.

1.9.2 Triggers y plantillas

El funcionamiento de Zabbix es en base a estos, los Triggers son, como lo sugiere el término, disparadores, son expresiones que evalúan los datos obtenidos de determinados eventos y representan el estado actual del sistema, estos pueden ser de distinto grado de severidad: no clasificado, información, advertencia, común, alto y desastre. La expresión es el componente medular del Trigger, esto es, el momento en que se debe disparar, está formada por distintas funciones. Se pueden crear Triggers propios o usar los que vienen precargados con una plantilla específica, como lo son por ejemplo la plantilla de Windows OS, etc.

Como ejemplo de su funcionamiento, frente a un servicio que no responde, el administrador puede configurar un disparador para emitir un email de notificación dependiendo la severidad de este. En figura 1-12 se puede apreciar un ejemplo donde se pueden ver varios Triggers activados, con grado de severidad variado como lo son cambio de contraseña de usuario Linux (advertencia), demasiados procesos abiertos (advertencia), cambio en la versión del agente (información), el host se ha reiniciado (información), etc.

HOST	TRIGGER	SEVERITY
New host	Disk I/O is overloaded on New host	Warning
Zabbix server 1	Zabbix discoverer processes more than 75% busy	Average
New host	Too many processes on New host	Warning
Zabbix server 1	Zabbix server 1 has just been restarted	Information
New host	New host has just been restarted	Information
New host	Host information was changed on New host	Information
Zabbix server 1	Disk I/O is overloaded on Zabbix server 1	Warning
Zabbix server 1	Version of zabbix-agent(d) was changed on Zabbix server 1	Information
Zabbix server 1	Zabbix http poller processes more than 75% busy	Average
New host	/etc/passwd has been changed on New host	Warning

Fuente: zabbix.com

Figura 1-12: Ejemplos de Triggers accionados.

CAPÍTULO 2: IMPLEMENTACIÓN DEL SISTEMA

2: IMPLEMENTACIÓN DEL SISTEMA

Este capítulo abordará la implementación del monitoreo de red en el laboratorio M-207 USM (LAN), para llevar a cabo este se mezclarán los 2 tipos de monitoreo, el activo y el pasivo, usando los protocolos SNMP e ICMP, además de los agentes, para recabar la información, esta información, como se dijo en el capítulo 1, se categoriza en las áreas: procesamiento, conectividad, ambiental, utilización y disponibilidad.

Refiriéndose el servidor, el sistema operativo elegido será Ubuntu (distribución de Linux), mediante el cual se ingresará a la interfaz web para configurar. Esta configuración, si bien es medianamente técnica, se facilitará con la lectura de manuales de usuario online. Su hardware será el mismo que el de las demás computadoras de la red (ver tabla 2-1), ósea un procesador Intel Core I5, memoria RAM de 8Gb y disco duro de 500 Gb (estos valores pueden variar un poco debido a que el servidor se ejecutará en una máquina virtual).

Ahora se analizará el laboratorio para poder reconocer el hardware de cada uno de los componentes que van a ser objeto del monitoreo de red, realizando para ello un inventario y un mapa topológico, luego, antes de proceder a instalar la herramienta Zabbix, es necesario instalar los servicios necesarios como lo serían NTP, MYSQL, y Apache. El siguiente paso es proceder a instalar el software Zabbix en el servidor y en cada una de las computadoras para que puedan recolectar la información. En cuanto a la preparación del switch Cisco, se debe habilitar y configurar SNMP para su monitoreo, y en cuanto a las cámaras IP y teléfonos IP, se monitorearán por medio de ICMP. El monitoreo de los puertos TCP/UDP también es un punto importante que destacar. Lo siguiente es proceder a configurar las notificaciones de alerta para el administrador, y a configurar el autodescubrimiento y mapas personalizados.

Cabe mencionar que esta implementación se hizo en el software “Oracle VM Virtual Box”, donde, gracias a la tecnología de la virtualización, se pudieron simular las computadoras (hosts) de la red junto con el servidor. La limitancia de este software es que solo soporta la simulación de computadoras, por lo que el proceso de implementación en dispositivos de red y otros dispositivos finales como cámaras y teléfonos, se pudo saber gracias los a manuales de usuario online, quedando pendientes para realizarlos junto a la posterior implementación en físico en el laboratorio.

2.1 RECONOCIMIENTO DEL HARDWARE

El reconocimiento del hardware es el paso previo a la implementación del monitoreo de software (siguientes puntos), este abarca el inventario y topología del sistema.

2.1.1 Inventario del sistema

La tabla 2-1, muestra un inventario el cual corresponde a las etapas previas al monitoreo: análisis del sistema, categorización de inventario y definición de elementos con alerta. Cabe mencionar que las direcciones IP como son varias unidades de cada elemento, ira de 10 en 10 sumándole a la dirección puesta en la tabla.

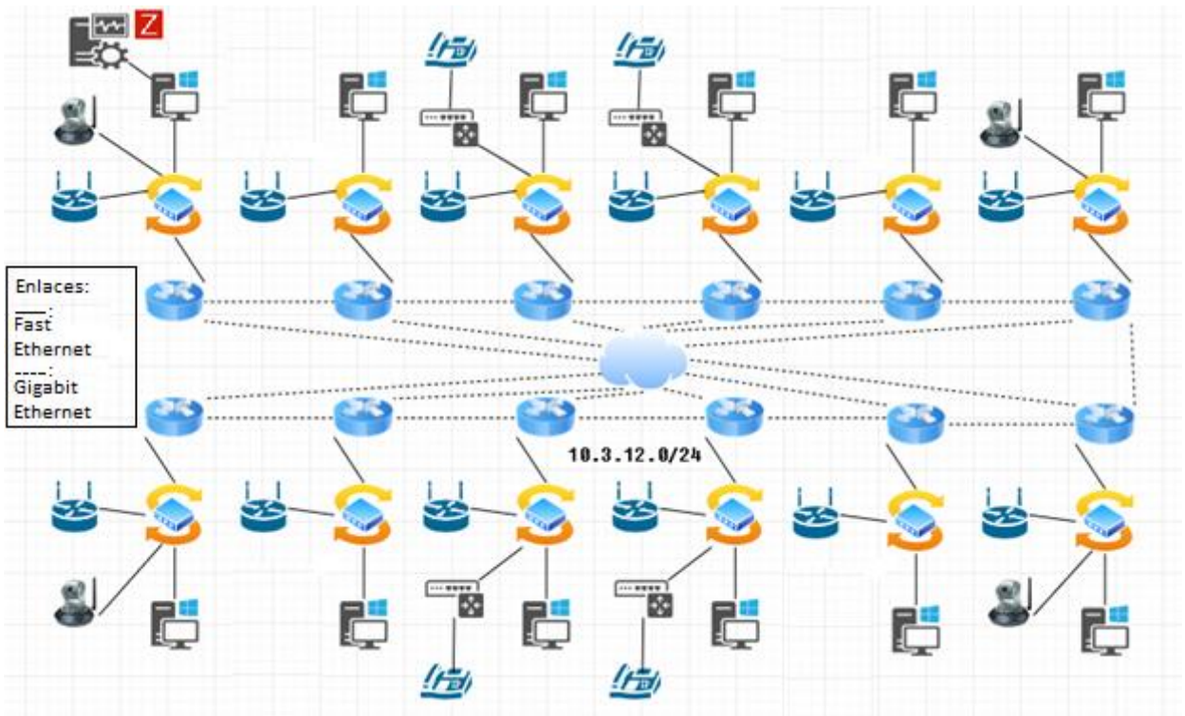
Tabla 2-1: Inventario de Sistema Laboratorio de Redes M-211 USM.

Nombre	**Modelo**	**Cantidad**	**Marca**	**Prioridad**	**Ámbito**	**IP**
Router LAN	2900	12	Cisco	Alta	Redes	10.3.12.1/24
Switch	2960	12	Cisco	Media	Redes	10.3.12.2/24
Procesador (PC)	Core I5	12	Intel	Alta	Sistemas	No aplica
Memoria RAM (PC)	8 gigabytes	12	-	Media	Sistemas	No aplica
Disco Duro (PC)	500 gigabytes	12	-	Media	Sistemas	No aplica
Tarjeta Madre (PC)	-	12	-	Alta	Sistemas	10.3.12.3/24
Router WLAN	EA6500	12	Linksys	Baja	Redes	10.3.12.4/24
Teléfono IP	SPA504G	4	Cisco	Baja	Sistemas	10.3.12.5/24
PBX IP	UC540	4	Cisco	Media	Redes	10.3.12.6/24
Cámara IP	DCS-942L	4	D-Link	Baja	Redes	10.3.12.7/24

Fuente: Elaboración propia.

2.1.2 Topología del sistema

La figura 2-1; muestra un mapa topológico del lugar objeto de trabajo, en él se puede apreciar todos los componentes ya nombrados en el punto anterior (inventario), con los routers de cada host conectados a sus routers contiguos y a la vez a la nube de internet. Como se puede ver, la IP de la red es 10.3.12.0/24 y el servidor Zabbix se ubica en el host de la esquina superior izquierda, funcionando en máquina virtual. Los enlaces a ocupar son Ethernet Cat5e con una velocidad de 100mb.



Fuente: Elaboración Propia.

Figura 2-1: Mapa topológico laboratorio M-207.

La figura 2-2; muestra una fotografía del laboratorio M-207 donde se realizarán las pruebas.

Fuente: Elaboración Propia.

Figura 2-2: Fotografía laboratorio M-207.

2.2 INSTALACIÓN PREVIA DE SERVICIOS REQUERIDOS

Antes de preparar el servidor, es necesario instalar 3 servicios que son la base del funcionamiento de Zabbix, estos se relacionan con la fecha (NTP), base de datos (MySQL) y servidor web (Apache).

2.2.1 Instalación de NTP

Primero se configurará el sistema para usar la fecha y hora correctas usando NTP (protocolo de sincronización de relojes). En la consola de Linux, hay que usar los siguientes comandos para configurar la zona horaria correcta.

 # dpkg-reconfigure tzdata

Instalar el paquete "Ntpdate" y configurar la fecha y hora correctas de inmediato. El comando Ntpdate se usa para establecer la fecha y hora correctas mediante un servidor.

 # apt-get update

 # apt-get install ntpdate

 # ntpdate pool.ntp.br

Instalar el servicio NTP, este es el servicio que mantendrá el servidor actualizado. Luego verificar la fecha y la hora configuradas en el Ubuntu Linux.

 # apt-get install ntp

 # date

2.2.2 Instalación de MySQL

Ahora se procederá con la instalación del servicio de la base de datos. En la consola de Linux, usar los siguientes comandos para instalar los paquetes requeridos.

 # apt-get update

 # apt-get install mysql-server mysql-client

Después de terminar la instalación, usar el siguiente comando para acceder al servidor de base de datos MySQL. Para acceder al servidor de la base de datos, se debe ingresar la contraseña configurada en el asistente de instalación del servidor MySQL.

 # mysql -u root -p

Usar el siguiente comando SQL para crear una base de datos llamada "zabbix".

CREATE DATABASE zabbix CHARACTER SET UTF8 COLLATE UTF8_BIN;

Usar el siguiente comando SQL para crear un usuario de base de datos llamado “zabbix”.

CREATE USER 'zabbix'@'%' IDENTIFIED BY ‘usm’';

Otorgar al usuario de SQL llamado zabbix permiso sobre la base de datos denominada zabbix.

*GRANT ALL PRIVILEGES ON zabbix. * TO 'zabbix'@'%';*

quit;

En la consola de Linux, usar los siguientes comandos para descargar el paquete de instalación de Zabbix.

 # mkdir /downloads

 # cd /downloads

 # wget https://ufpr.dl.sourceforge.net/project/zabbix/ZABBIX%20Latest%20Stable/3.4.12/zabbix-3.4.12.tar.gz

Ahora, es necesario extraer el paquete de instalación de Zabbix e importar la plantilla de base de datos dentro de MySQL. El sistema solicitará la contraseña del usuario de Zabbix SQL cada vez que se intente importar un archivo.

 # tar -zxvf zabbix-3.4.12.tar.gz

 # cd zabbix-3.4.12/database/mysql

 # mysql -u zabbix -p zabbix < schema.sql

 # mysql -u zabbix -p zabbix < images.sql

 # mysql -u zabbix -p zabbix < data.sql

2.2.3 Instalación de Apache

A continuación, es necesario instalar el servidor web “Apache” y todo el software requerido. En la consola de Linux, usar los siguientes comandos para instalar los paquetes requeridos.

 # apt-get install apache2 php libapache2-mod-php php-cli

 # apt-get install php-mysql php-mbstring php-gd php-xml

 # apt-get install php-bcmath php-ldap

Ahora, se debe encontrar la ubicación del archivo “php.ini” en el sistema. Después de encontrarlo, se debe editar.

 # updatedb

 # locate php.ini

 # vi /etc/php/7.2/apache2/php.ini

Se debe tener en cuenta que la versión de PHP y la ubicación del archivo pueden no ser las mismas. Aquí está el archivo luego de configurar.

max_execution_time = 300

memory_limit = 256M

post_max_size = 32M

max_input_time = 300

date.timezone = America/Santiago

Tener en cuenta que se debe configurar la zona horaria de PHP. En este ejemplo, se utilizará la zona horaria América / Santiago. También se debe reiniciar Apache manualmente y verificar el estado del servicio.

 # service apache2 stop

 # service apache2 start

 # service apache2 status

Aquí un ejemplo de la salida del estado del servicio Apache.

apache2.service - LSB: Apache2 web server

Loaded: loaded (/etc/init.d/apache2; bad; vendor preset: enabled)

Drop-In: /lib/systemd/system/apache2.service.d

└─apache2-systemd.conf

Active: active (running) since Mon 2018-04-23 00:02:09 -03; 1min 4s ago

2.3 PREPARACIÓN DE SERVIDOR

La preparación del servidor, del que dependerán los demás equipos a monitorear, se realizara con la instalación de Zabbix y configuración de su auto monitoreo.

2.3.1 Instalación del software Zabbix

Ahora, se tiene que instalar el software Zabbix en Ubuntu Linux. En la consola de Linux, usar los siguientes comandos para instalar los paquetes requeridos.

 # groupadd zabbix

 # useradd -g zabbix -s /bin/bash zabbix

 # apt-get update

 # apt-get install build-essential libmysqlclient-dev libssl-dev libsnmp-dev libevent-dev

 # apt-get install libopenipmi-dev libcurl4-openssl-dev libxml2-dev libssh2-1-dev libpcre3-dev

 # apt-get install libldap2-dev libiksemel-dev libcurl4-openssl-dev libgnutls28-dev

En la consola de Linux, usar los siguientes comandos para acceder a la carpeta del paquete.

 # cd /downloads/zabbix-3.4.12

 # ls

aclocal.m4 build conf configure database include m4 man NEWS src

AUTHORS ChangeLog config.guess configure.ac depcomp INSTALL Makefile.am misc README upgrades

bin compile config.sub COPYING frontends install-sh Makefile.in missing sass

Compilar e instalar el servidor Zabbix usando los siguientes comandos:

#. /configure --enable-server --enable-agent --with-mysql --with-openssl --with-net-snmp --with-openipmi --with-libcurl --with-libxml2 --with-ssh2 --with-ldap

 # make

 # make install

Ahora, se debe encontrar la ubicación del archivo “zabbix_server.conf” en el sistema. Después de encontrarlo, se debe editar.

 # updatedb

 # locate zabbix_server.conf

 # vi /usr/local/etc/zabbix_server.conf

Este es el archivo después de configurar.

LogFile=/tmp/zabbix_server.log

DBHost=localhost

DBName=zabbix

DBUser=zabbix

DBPassword=usm

Timeout=4

LogSlowQueries=3000

Después de terminar la configuración, usar el siguiente comando para iniciar el servidor y el agente Zabbix:

 # /usr/local/sbin/zabbix_server

 # /usr/local/sbin/zabbix_agentd

El paquete de instalación de Zabbix viene con un script de inicio de servicio. Opcionalmente, copiar la secuencia de comandos de inicio con los siguientes comandos.

 # cd /downloads/zabbix-3.4.12/

 # cp misc/init.d/debian/ /etc/init.d/*

Ahora se pueden usar los siguientes comandos para iniciar el servicio del servidor Zabbix.

 # /etc/init.d/zabbix-server start

Mover todos los archivos frontend Zabbix al directorio raíz de la instalación de Apache. Establecer el permiso de archivo correcto en todos los archivos movidos.

 # cd /downloads/zabbix-3.4.12/frontends

 # mkdir /var/www/html/zabbix

 # mv php/ /var/www/html/zabbix*

 # chown www-data.www-data /var/www/html/zabbix/ -R*

Reiniciar el servicio Apache.

 # service apache2 stop

 # service apache2 start

Abrir navegador e ingresar la dirección IP del servidor web más “/zabbix”. En este ejemplo, la siguiente URL se ingresó en el navegador:

http://10.3.12.3/zabbix

La interfaz de instalación web de Zabbix debió ser mostrada (ver figura 2-3). Hacer clic en el botón “Siguiente”.

Fuente: Elaboración Propia.

Figura 2-3: Inicio wizard de Zabbix

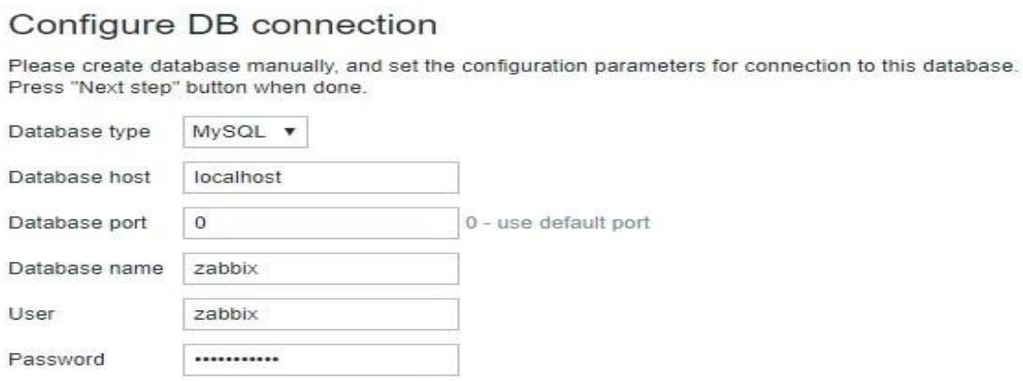
En la pantalla siguiente, se deberá verificar si se cumplieron todos los requisitos (ver figura 2-4). Hacer clic en el botón “Siguiente”.

Fuente: Elaboración Propia.

Figura 2-4: Pantalla de prerrequisitos.

En la siguiente pantalla (ver figura 2-5), ingresar la información de la base de datos requerida para conectarse a la base de datos Zabbix.

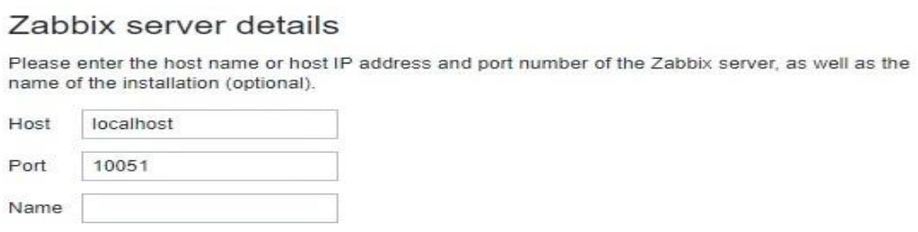
- *Anfitrión: localhost*
- *Nombre de usuario de la base de datos: zabbix*
- *Contraseña de la base de datos: usm*



Fuente: Elaboración Propia.

Figura 2-5: Configuración de base de datos.

En la pantalla de IP/Puerto (ver figura 2-6), se deja igual y siguiente.



Fuente: Elaboración Propia.

Figura 2-6: Pantalla IP/Puerto.

Ahora, revisar el resumen de configuración (ver figura 2-7). Hacer clic en el botón “Siguiente” y luego “Finalizar”.

Fuente: Elaboración Propia.

Figura 2-7: Resumen de configuración.

2.3.2 Configuración de monitoreo al servidor

Luego de los pasos anteriores, se mostrará la pantalla de inicio de sesión de Zabbix (ver figura 2-8).

- *Nombre de usuario predeterminado de Zabbix: admin*
- *Contraseña predeterminada de Zabbix: Zabbix*

Fuente: Elaboración Propia.

Figura 2-8: Pantalla inicio de sesión Zabbix.

Después de un inicio de sesión exitoso, se redirigirá al tablero de la interfaz web de Zabbix. Ahora, es necesario permitir que el servidor Zabbix se monitoree a sí mismo. En el tablero Zabbix acceder al menú “Configuración” y seleccionar la opción “Host” (ver figura 2-9).

Fuente: Elaboración Propia.

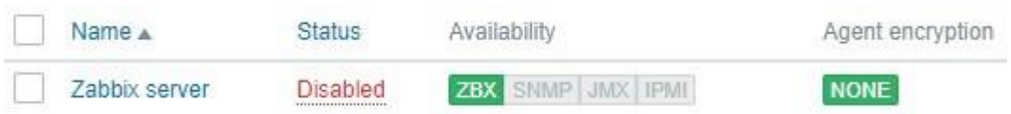
Figura 2-9: Tablero Zabbix - Hosts.

En la esquina superior derecha de la pantalla, seleccionar la opción llamada: “servidores Zabbix” (ver figura 2-10).

Fuente: Elaboración Propia.

Figura 2-10: Grupos de Hosts.

Ubicar el servidor llamado “Zabbix server” y hacer clic en la palabra “DISABLED” (ver figura 2-11). Esto permitirá que el servidor Zabbix se monitoree a sí mismo.



Fuente: Elaboración Propia.

Figura 2-11: Estado de monitoreo al servidor (1).

El estado del servidor Zabbix cambiará de DISABLED a ENABLED (ver figura 2-12).

Fuente: Elaboración Propia.

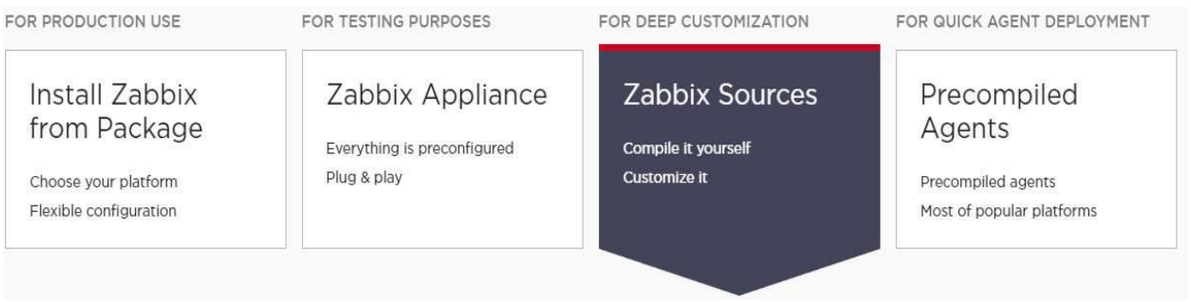
Figura 2-12: Estado de monitoreo al servidor (2).

2.4 PREPARACIÓN DE AGENTES

Aquí vamos a instalar y configurar los agentes de Zabbix en cada uno de los hosts a monitorear para luego agregarlos al servidor.

2.4.1 Configuración en Host Windows

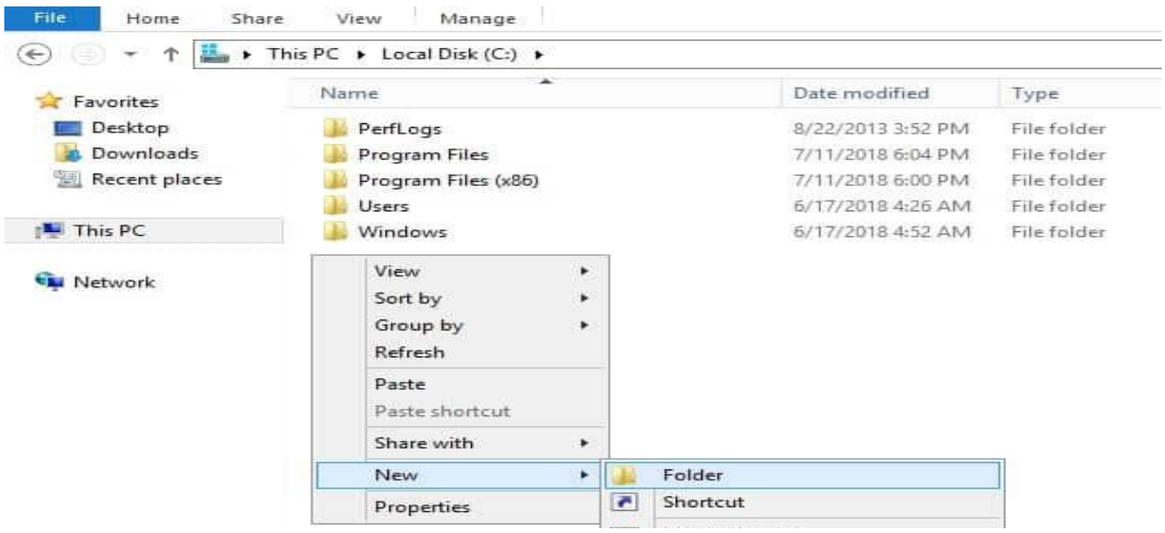
Acceder al sitio web de Zabbix y https://www.zabbix.com/download_sources y descargar la versión “Sources” (ver figura 2-13).



Fuente: Elaboración Propia.

Figura 2-13: Web Zabbix.com.

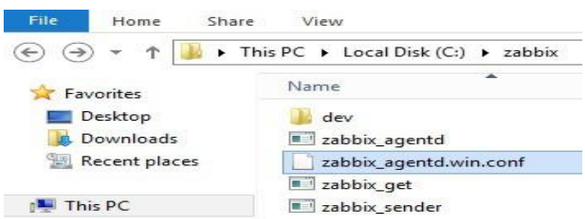
En este ejemplo, se descarga el archivo de Zabbix: zabbix-3.4.12.tar.gz. Abrir la aplicación Windows Explorer, y navegar hasta la raíz de la unidad C y crear un nuevo directorio “Zabbix” (ve figura 2-14).



Fuente: Elaboración Propia.

Figura 2-14: Raíz del disco duro host.

El paquete de instalación de Zabbix generalmente se compacta utilizando una extensión de archivo “tar.gz”, Windows no puede abrir nativamente archivos de esta extensión. Se debe descargar e instalar 7ZIP o WINRAR para abrirlos. Copiar el contenido del siguiente paquete de instalación de Zabbix: zabbix-3.4.12\bin\win64. Pegar el contenido del interior de la carpeta antes creada: C:\zabbix. Hacer lo mismo con el archivo zabbix_agentd.win.conf de la siguiente carpeta del paquete de instalación de Zabbix: zabbix-3.4.12\conf (ver figura 2-15).



Fuente: Elaboración Propia.

Figura 2-15: Carpeta creada Zabbix.

Abrir el programa WORDPAD y editar el archivo de configuración zabbix_agentd.win.conf con este. Eliminar todo el contenido e ingresar las siguientes directivas (luego guardar):

Server=127.0.0.1,10.3.12.3

ServerActive=10.3.12.3

Logfile=C:\zabbix\zabbix_agent.log

En este ejemplo, el agente Zabbix está configurado para permitir la conexión del servidor Zabbix 10.3.12.3. El servidor con la dirección IP 10.3.12.3 puede solicitar y recibir información del agente. El Localhost, 127.0.0.1, tiene permiso para solicitar y recibir información del agente.

Después de finalizar la configuración, abrir un símbolo del sistema. Ingresar el siguiente comando para instalar el servicio del agente Zabbix en Windows.

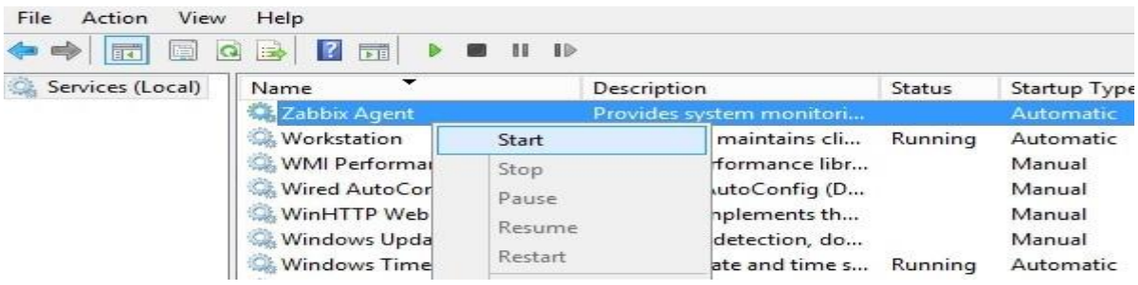
c:\zabbix\zabbix_agentd.exe --config c:\zabbix\zabbix_agentd.win.conf --install

Si todo se hizo correctamente, se deberían ver los siguientes mensajes

zabbix_agentd.exe [4508]: service [Zabbix Agent] installed successfully

zabbix_agentd.exe [4508]: event source [Zabbix Agent] installed successfully

El agente de Zabbix ya está instalado en la computadora, pero se debe comenzar el servicio manualmente. Solo se necesita iniciar el servicio manualmente la primera vez después de la instalación. Abrir la pantalla de administración de servicios de Windows e iniciar el servicio del agente Zabbix (ver figura 2-16).



Fuente: Elaboración Propia.

Figura 2-16: Administrador de servicios Windows.

Abrir el archivo “zabbix_agent.log” para verificar el archivo de registro del agente Zabbix. Si el agente de Zabbix se inició correctamente, se debería ver un mensaje similar a este.

4964:20180808:190920.442 Starting Zabbix Agent [WINDOWS-SERVER-01]. Zabbix 3.4.12 (revision 83216).

*4964:20180808:190920.442 **** Enabled features ****

4964:20180808:190920.442 IPv6 support: YES

4964:20180808:190920.442 TLS support: NO

*4964:20180808:190920.442 **********

4964:20180808:190920.442 using configuration file: c:\zabbix\zabbix_agentd.win.conf

4964:20180808:190920.442 agent #0 started [main process]

4764:20180808:190920.442 agent #2 started [listener #1]

4856:20180808:190920.442 agent #1 started [collector]

4340:20180808:190920.442 agent #3 started [listener #2]

4400:20180808:190920.442 agent #5 started [active checks #1]

5016:20180808:190920.442 agent #4 started [listener #3]

Tener en cuenta que la aplicación de firewall de Windows necesita aceptar conexiones del servidor Zabbix. El firewall de Windows debe aceptar paquetes de red en el puerto TCP: 10050. Ahora se puede usar el tablero del servidor Zabbix para agregar esta computadora al servicio de monitoreo de red.

2.4.2 Configuración en Servidor

Ahora, es necesario acceder al tablero de la interfaz web del servidor Zabbix y agregar la computadora con Windows como un Host. Hay que abrir el navegador e ingresar la dirección IP del servidor web más "/Zabbix". Después de un inicio de sesión exitoso, se redirigirá al tablero de Zabbix. Acceder al menú "Configuración" y seleccionar la opción "Host" (ver figura 2-9). En la esquina superior derecha de la pantalla, hacer clic en el botón "Crear host" (ver figura 2-17).

Fuente: Elaboración Propia.

Figura 2-17: Botón de creación de host.

En la pantalla de configuración de Host, se deberá ingresar la siguiente información:

- *Nombre de host: ingresar un nombre de host para identificar el servidor de Windows.*
- *Nombre de host visible: repetir el nombre de host.*
- *Nuevo grupo: ingresar un nombre para identificar un grupo de dispositivos similares.*
- *Interfaz del agente: ingresar la dirección IP del servidor de Windows.*

A continuación, se debe asociar el host con una plantilla de monitor de red específica. Por defecto, Zabbix viene con una gran variedad de plantillas de monitoreo. Acceder a la pestaña "Plantillas" en la parte superior de la pantalla. Hacer clic en el botón "Seleccionar" y buscar la plantilla llamada: TEMPLATE OS Windows (ver figura 2-18). Hacer clic en el botón Agregar (1). Hacer clic en el botón Agregar (2).

Fuente: Elaboración Propia.

Figura 2-18: Plantilla de Windows OS.

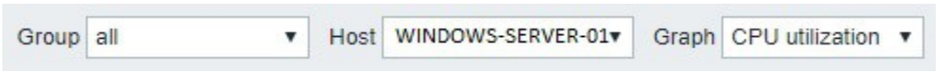
Después de unos minutos, se podrá ver el resultado inicial. El resultado tomará al menos una hora. De forma predeterminada, Zabbix demorara 1 hora en descubrir la cantidad de

interfaces disponibles en la computadora y en recopilar la información. Para probar la configuración, ir al menú “Supervisión” y hacer clic en la opción “Gráficos” (ver figura 2-19).

Fuente: Elaboración Propia.

Figura 2-19: Tablero de Zabbix - Gráficos.

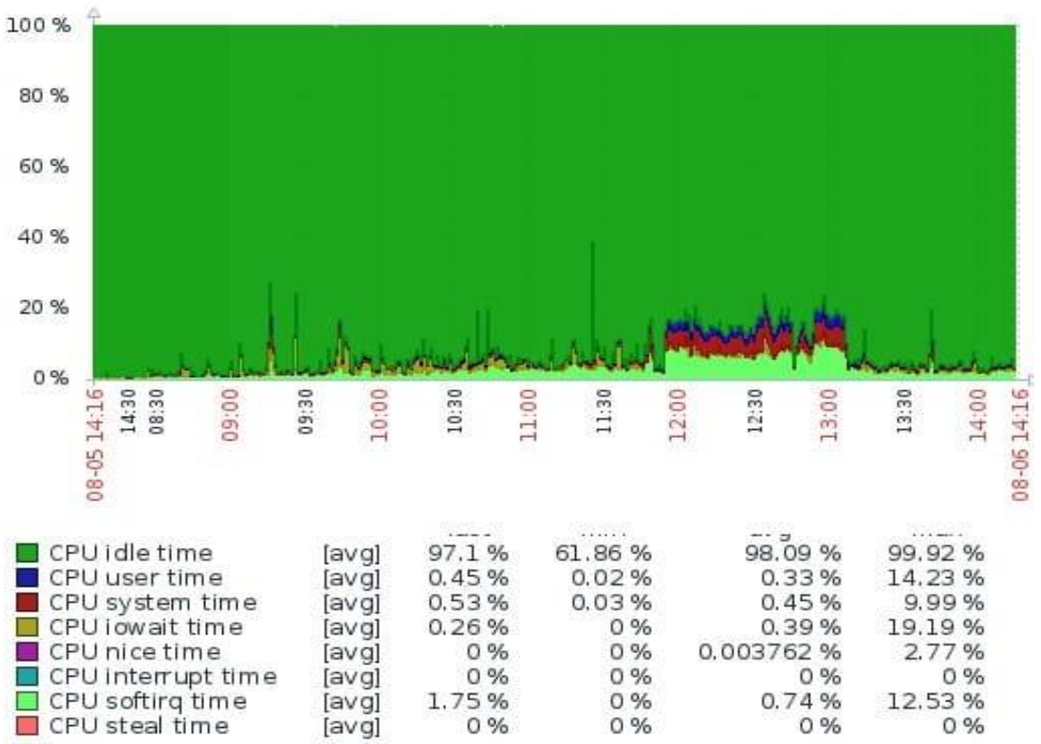
En la esquina superior derecha de la pantalla, seleccionar el grupo llamado “ALL”. Seleccionar el nombre de “host” de la computadora Windows. Seleccionar el gráfico: UTILIZACIÓN DE CPU (ver figura 2-20).



Fuente: Elaboración Propia.

Figura 2-20: Selección de gráficos.

La figura 2-21 muestra el tipo de gráfico seleccionado del host objetivo, donde se pueden ver distintos parámetros de uso de CPU.



Fuente: techexperts.com

Figura 2-21: Gráfico uso CPU.

2.5 PREPARACIÓN DE SWITCH CISCO

Ahora hay que habilitar y configurar el servicio SNMP en el switch, y luego agregarlo al servidor.

2.5.1 Configuración en Switch

Para ello hay que ingresar a la consola, Telnet o SSH, conectarse a la línea de comandos del conmutador e iniciar sesión con un usuario que tenga privilegios administrativos. Después de un inicio de sesión exitoso, se mostrará la línea de comandos de la consola. Usar los comandos para ingresar al modo privilegiado. Usar los siguientes comandos para configurar el servicio SNMP.

Switch> enable

Switch# configure terminal

Switch(config)# snmp-server community comunidad_ejemplo ro

Switch(config)# snmp-server contact Administrador <admin_teleco@gmail.com>

Switch(config)# snmp-server location locación-ejemplo

Switch(config)# exit

Switch# copy running-config startup-config

La Comunidad “comunidad_ejemplo” tiene permiso de solo lectura en Cisco Switch. La persona de contacto responsable de este Switch se configuró como “Administrador”. La ubicación del equipo se configuró como “locación_ejemplo”. Se guardó la configuración de switch.

Ahora se debe que probar la comunicación SNMP entre el servidor Zabbix y Cisco Switch. En la consola del servidor, hay que usar los siguientes comandos para instalar y probar la comunicación SNMP.

 # apt-get install snmp

 # snmpwalk -v2c -c Administrador 192.168.0.200

En este caso Cisco Switch tiene la IP 192.168.0.200. Aquí se muestra una salida SNMPWALK.

iso.3.6.1.2.1.1.1.0 = STRING: “Cisco IOS Software, C2960X Software (C2960X-UNIVERSALK9-M), Version 15.2(2)E6, RELEASE SOFTWARE (fc1)

Technical Support: http://www.cisco.com/techsupport

Copyright (c) 1986-2016 by Cisco Systems, Inc.

iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.9.1.1208

iso.3.6.1.2.1.1.3.0 = Timeticks: (77872563) 9 days, 0:18:45.63

iso.3.6.1.2.1.1.4.0 = STRING: “Administrador <admin_teleco@gmail.com>”

iso.3.6.1.2.1.1.5.0 = STRING: “FKIT-SW01.FKIT. LOCAL”

iso.3.6.1.2.1.1.6.0 = STRING: “Lab M-207 Teleco”

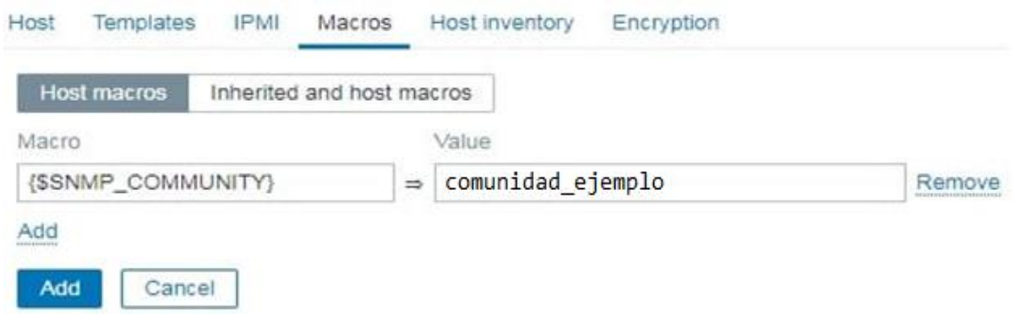
2.5.2 Configuración en Servidor

Se deben repetir los pasos del punto 2.3.2 (adición host Windows) pero en este caso se agregará el switch como host. Además de llenar los datos de nombre, grupo e interfaz agente, para este caso se tendrá que llenar además el campo “Interfaz SNMP” con la dirección IP del switch (ver figura 2-22).

Fuente: Elaboración Propia.

Figura 2-22: Campo de IP SNMP en creación de host.

A continuación, se procede a configurar la comunidad SNMP que Zabbix usa para conectarse al switch. Acceder a la pestaña “Macros” en la parte superior de la pantalla. Crear una macro llamada: {$ SNMP_COMMUNITY}. El valor de la macro {$ SNMP_COMMUNITY} debe ser la comunidad SNMP del switch (ver figura 2-23).



Fuente: Elaboración Propia.

Figura 2-23: Campo macro de comunidad SNMP.

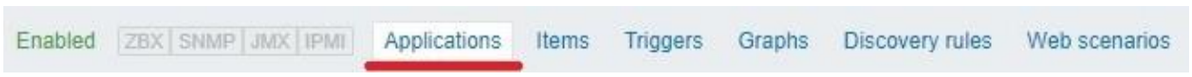
A continuación, se debe asociar el host con una plantilla de monitor de red específica. Acceder a la pestaña “Plantillas” en la parte superior de la pantalla y luego hacer clic en el botón “Seleccionar” seleccionando la plantilla llamada: Plantilla Net Cisco IOS SNMPv2 (ver figura 2-24). Hacer clic en el botón Agregar (1). Hacer clic en el botón Agregar (2).

Fuente: Elaboración Propia.

Figura 2-24: Plantilla de Cisco SNMP.

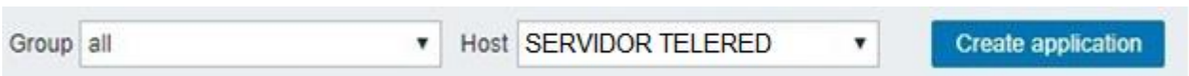
2.6 MONITOREO TCP/UDP

Para continuar se requiere tener ya agregado el host objetivo, esto se puede hacer siguiendo los pasos anteriormente mencionados en el paso 2.3.2 cuando se agregó un host de Windows. En la pantalla del tablero, acceder al menú “Configuración” y seleccionar la opción “Host” (ver figura 2-9). Ubicar y hacer clic en el nombre de host que se creó anteriormente. En este ejemplo, se seleccionó el nombre de host: SERVIDOR TELERED. En la pantalla de propiedades del “Host”, ingresar a la pestaña “Aplicaciones” (ver figura 2-25) y luego, en la parte superior derecha de la pantalla, hacer clic en el botón “Crear aplicación” (ver figura 2-26). En la pantalla de aplicaciones de “Host”, crear una nueva aplicación llamada “TCP Status” (ver figura 2-27).



Fuente: Elaboración Propia.

Figura 2-25: Propiedades de host - Aplicaciones.



Fuente: Elaboración Propia.

Figura 2-26: Creación de aplicación.

Fuente: Elaboración Propia.

Figura 2-27: Campo de nombre de aplicación.

Después de finalizar la creación de la aplicación, acceder a la pestaña “Elementos” (ver figura 2-28).

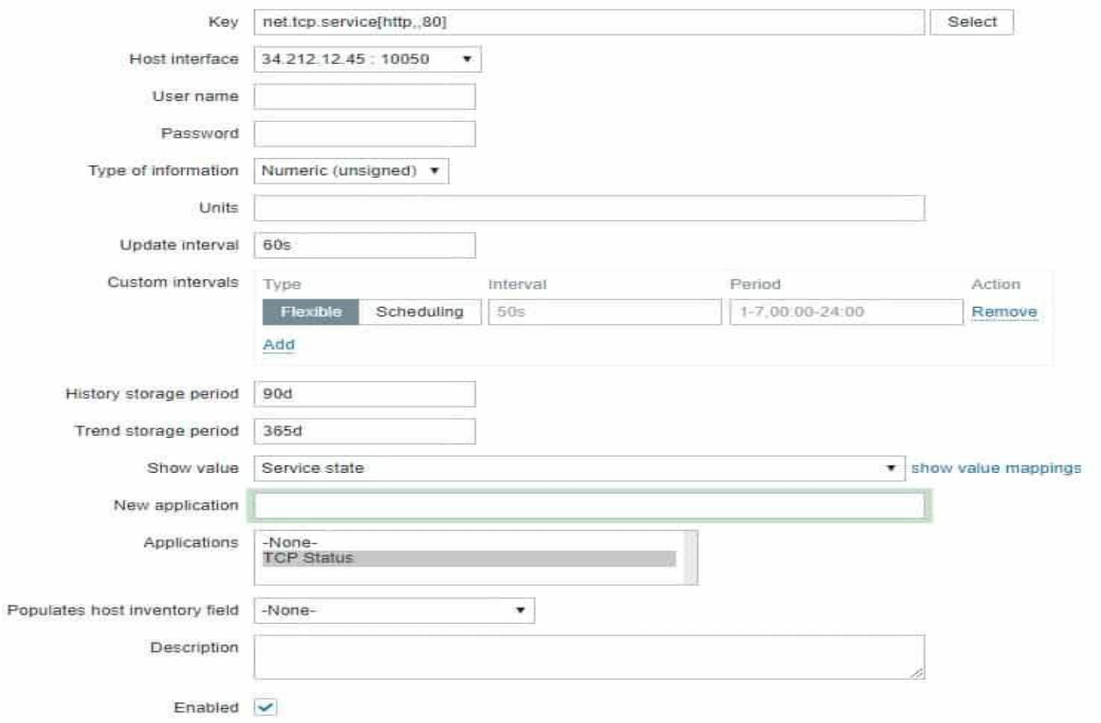
Fuente: Elaboración Propia.

Figura 2-28: Propiedades de host - Elementos.

En la parte superior de la pantalla, hacer clic en el botón “Crear elemento”. En la pantalla de creación de elementos (ver figura 2-29), se debe configurar los siguientes elementos:

- *Nombre: ingresar una identificación en el puerto TCP.*
- *Tipo: verificación simple*
- *Clave: net.tcp.service [http ,, 80]*
- *Tipo de información: numérica (sin signo)*

- *Intervalo de actualización: 60 segundos*
- *Mostrar valor: estado de servicio*
- *Aplicación: TCP Status*



Fuente: Elaboración Propia.

Figura 2-29: Parámetros del monitoreo TCP.

Hacer clic en el botón “Agregar” y finalizar la creación del artículo. Esperar 5 minutos. Para probar la configuración, acceder al menú “Supervisión” y hacer clic en la opción “Últimos datos” (ver figura 2-30).

Fuente: Elaboración Propia.

Figura 2-30: Tablero de Zabbix – Últimos datos.

Usar la configuración del filtro para seleccionar el host deseado. En este ejemplo, el servidor SERVIDOR TELERED (ver figura 2-31). Hacer clic en el botón “Aplicar” y se deberían poder ver los resultados del monitoreo de puerto TCP (ver figura 2-32). En este ejemplo, se monitoreo la disponibilidad del puerto TCP 80 (HTTP) de un host.

Fuente: Elaboración Propia.

Figura 2-31: Filtro de resultados de monitoreo por host.

Fuente: Elaboración Propia.

Figura 2-32: Parámetros del monitoreo TCP.

Nota: Para el monitoreo UDP los pasos a seguir son exactamente los mismos, solo cambia la información a ingresar en algunos campos:

- *Nuevo Grupo: UDP Monitor*
- *Creación de aplicación: UDP Status*
- *Nombre: ingresar una identificación en el puerto UDP.*
- *Clave: net.udp.service [ntp]*
- *Aplicación: UDP Status.*

En este ejemplo, se monitoreo la disponibilidad del puerto UDP 123 (NTP) de un host.

2.7 MONITOREO ICMP

Primero, se debe instalar el paquete "FPING" que permitirá que Zabbix realice comprobaciones ICMP. También se debe tomar nota de la ubicación del programa FPING. Usar el comando "WHICH" para averiguar la ubicación del programa FPING.

 # apt-get update

 # apt-get install fping

 # which fping

/usr/bin/fping

A continuación, se debe editar el archivo de configuración del servidor Zabbix y habilitar la función del monitor ICMP de disponibilidad. En la consola de Linux, usar los siguientes comandos para encontrar la ubicación del archivo zabbix_server.conf. En este ejemplo, el archivo zabbix_server.conf se encuentra en /usr/local/etc. Después de encontrarlo, se debe editar.

 # updatedb

 # locate zabbix_server.conf

 # vi /usr/local/etc/zabbix_server.conf

El archivo debe quedar así:

LogFile=/tmp/zabbix_server.log

DBHost=localhost

DBName=zabbix

DBUser=zabbix

DBPassword=usm

Timeout=4

LogSlowQueries=3000

StartPingers=10

FpingLocation=/usr/bin/fping

El servidor Zabbix se configuró para iniciar automáticamente 10 procesos para recopilar información ICMP PING. Se le dijo al servidor Zabbix que /usr/sbin/fping es la ruta correcta al comando FPING. Ahora, es necesario reiniciar el servicio Zabbix.

 # /etc/init.d/zabbix-server restart

Si el servidor Zabbix se inició correctamente, se debería mostrar un mensaje similar a este en el archivo de registro:

15534:20180807:144646.410 server #36 started [icmp pinger #4]

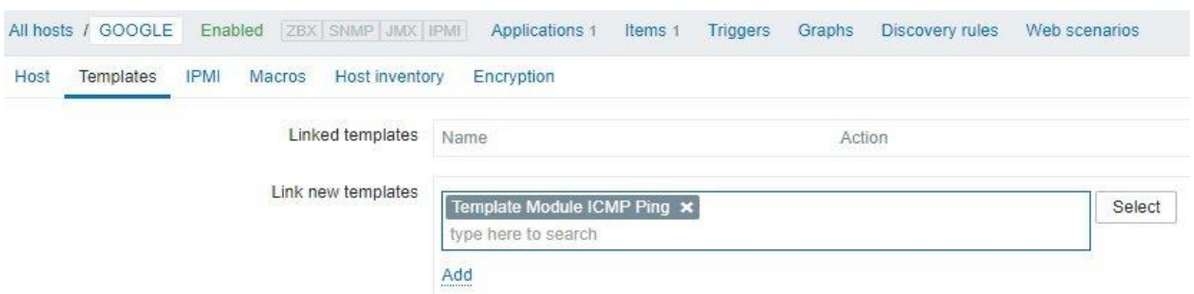
15536:20180807:144646.411 server #38 started [icmp pinger #6]

15538:20180807:144646.411 server #40 started [icmp pinger #8]

15541:20180807:144646.412 server #41 started [icmp pinger #9]

En este ejemplo, el archivo de registro del servidor Zabbix “zabbix_server.log” se encuentra dentro del directorio /tmp.

Luego lo que queda es asociar la plantilla de ICMP de Zabbix al host creado, o a crear, en la interfaz web de Zabbix. Se debe acceder a la pestaña “Plantillas” y asociar la plantilla llamada: “Módulo de plantilla ICMP Ping” (ver figura 2-33).



Fuente: Elaboración Propia.

Figura 2-33: Plantilla de ICMP Ping.

Para probar la configuración, los pasos a seguir son los mismos de cuando se probó el monitoreo TCP/UDP en el paso 5.

2.8 NOTIFICACIONES/ALERTAS

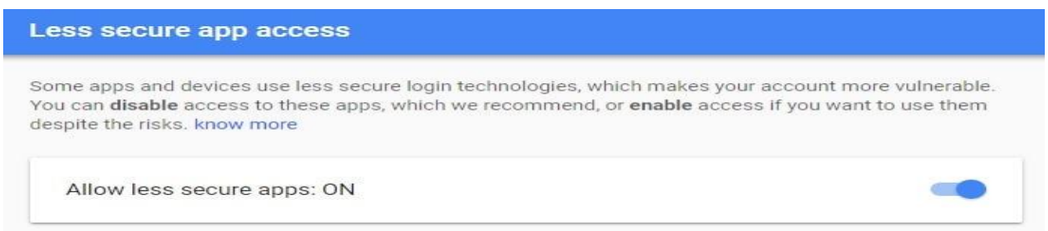
Ahora hay configurar Gmail y el servidor para que exista comunicación entre Zabbix y Gmail y realizar pruebas.

2.8.1 Configuración en Gmail

Primero hay que habilitar la cuenta de Gmail para recibir conexiones de programas externos. En el navegador hay que acceder a la cuenta de Gmail que se usará. Después del inicio de sesión, se debe acceder a la siguiente URL:

- *https://myaccount.google.com/lesssecureapps*

Seleccionar la opción para habilitar el uso de aplicaciones menos seguras (ver figura 2-34).



Fuente: Elaboración Propia.

Figura 2-34: Opciones de seguridad Gmail.

Ahora, se debe probar si se puede usar la línea de comandos de Linux para enviar un correo electrónico usando Gmail. Con el siguiente comando se podrán instalar los paquetes requeridos.

 # sudo apt-get update

 # sudo apt-get install ssmtp

Hay que editar el archivo “ssmtp.conf” para conectarse a la cuenta de Gmail.

 # vi /etc/ssmtp/ssmtp.conf

root=admin_teleco@gmail.com

mailhub=smtp.gmail.com:465

FromLineOverride=YES

AuthUser=admin_teleco@gmail.com

AuthPass=usm1

UseTLS=YES

En este ejemplo se está usando la cuenta de Gmail: admin_teleco@gmail.com con contraseña: usm1. Con el siguiente comando se va a poder enviar un correo electrónico usando la línea de comando.

 # echo "E-Mail using the command-line" | ssmtp admin_teleco@gmail.com

Revisar la bandeja de entrada de Gmail para ver el mensaje de prueba que se acaba de enviar (ver figura 2-35).

Fuente: Elaboración Propia.

Figura 2-35: Correo de prueba recibido.

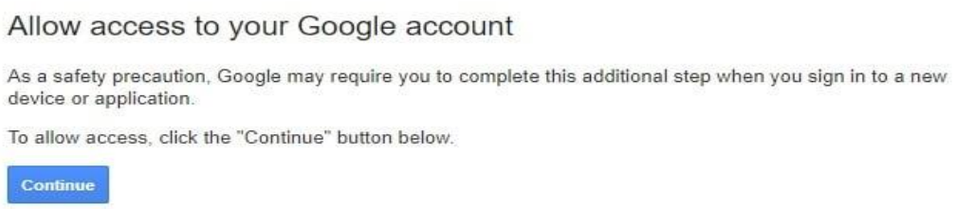
Si la prueba no tuvo éxito, se va a presentar el siguiente mensaje.

- *ssmtp: Autorización fallida (534 5.7.14 https://support.google.com/mail/answer/78754 v24-v6sm2921112pfl.31 - gsmtp)*

Para resolver el problema, se debe acceder a la siguiente URL.

- *https://accounts.google.com/DisplayUnlockCaptcha*

Seleccionar la opción para desbloquear la cuenta (ver figura 2-36) e intentar nuevamente enviar el correo electrónico con la línea de comando.

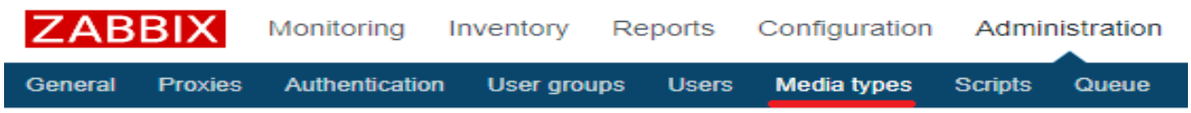


Fuente: Elaboración Propia.

Figura 2-36: Permisos de cuenta Gmail.

2.8.2 Configuración en Zabbix

Hay que abrir el navegador e ingresar la dirección IP del servidor web más "/Zabbix" y luego hacer login. Una vez en la pantalla del panel, hay que acceder al menú "Administración" y seleccionar la opción "Tipos de medios" (ver figura 2-37).



Fuente: Elaboración Propia.

Figura 2-37: Tablero de Zabbix – Tipos de medios.

Hay que ubicarse y hacer clic en la opción llamada Correo electrónico (ver figura 2-38).

Fuente: Elaboración Propia.

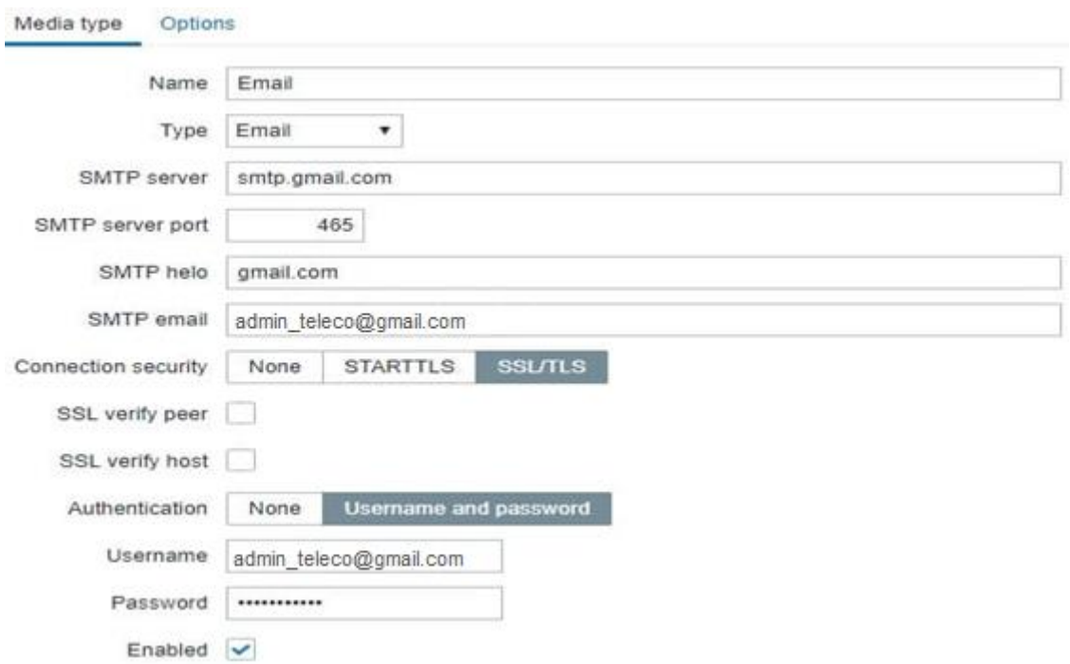
Figura 2-38: Configuración de canales de comunicación.

En la pantalla de propiedades del correo electrónico (ver figura 2-39), hay que ingresar la siguiente configuración.

- *Servidor SMTP: ingresar la dirección IP o el nombre de host del servidor de correo electrónico.*
- *Puerto del servidor SMTP: ingresar el puerto TCP SMTP del servidor de correo electrónico.*
- *SMTP helo: ingresar el nombre de dominio de su dirección de correo electrónico.*
- *Correo electrónico SMTP: la dirección de correo electrónico que enviará las notificaciones Zabbix.*
- *Seguridad de conexión: el protocolo de seguridad que se usará para conectarse al servidor de correo electrónico.*
- *Autenticación: nombre de usuario y contraseña de la cuenta de correo electrónico que enviará las notificaciones de Zabbix.*

Información para escribir:

- *Servidor SMTP - SMTP.GMAIL.COM*
- *Puerto del servidor SMTP - 465*
- *SMTP helo - gmail.com*
- *Correo electrónico SMTP - admin_teleco@gmail.com*
- *Seguridad de conexión: SSL / TLS*
- *Nombre de usuario de autenticación – admin_teleco@gmail.com*
- *Contraseña de autenticación - usm1*



Fuente: Elaboración Propia.

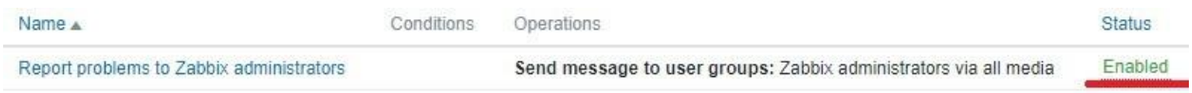
Figura 2-39: Propiedades de correo electrónico.

En la pantalla del tablero, hay que acceder al menú “Configuración” y seleccionar la opción “Acción” (ver figura 2-40).

Fuente: Elaboración Propia.

Figura 2-40: Tablero de Zabbix - Acciones.

Ubicar la opción denominada: Informar problemas a los administradores de Zabbix. Para habilitar esta acción, hay que hacer clic en la palabra Inhabilitado en rojo, esto activará la palabra “Activado” en verde (ver figura 2-41).



Fuente: Elaboración Propia.

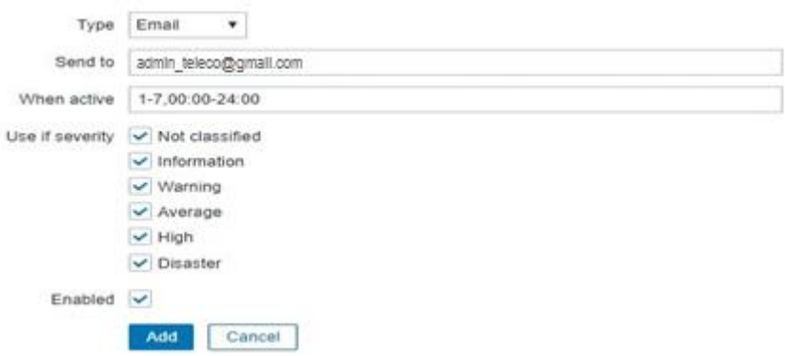
Figura 2-41: Estado de reporte a administradores.

Ahora se procederá a configurar Zabbix para enviar notificaciones por correo electrónico a los usuarios que son miembros del grupo de administradores de Zabbix. De forma predeterminada, solo el usuario Administrador es miembro del grupo de administradores de Zabbix. Ahora, se debe asociar una dirección de correo electrónico a la cuenta de administrador.

En el tablero, en la parte superior derecha de la pantalla se accede a la configuración del perfil de usuario (ver figura 2-42). En la pantalla de perfil de usuario, hay que acceder a la pestaña “Medios” y agregar una nueva configuración de Correo electrónico. La figura 2-43 muestra una imagen con la nueva configuración. Una vez configurado aparecerá una notificación por correo del servidor Zabbix. (ver figura 2-44).

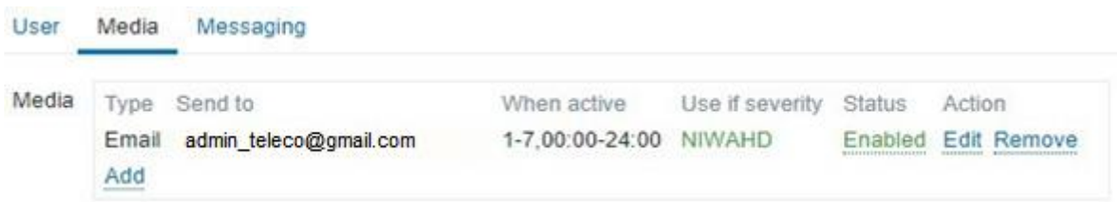
Fuente: Elaboración Propia.

Figura 2-42: Entrada a configuración de perfil.



Fuente: Elaboración Propia.

Figura 2-43: Asociación de correo y alertas a administrador.



Fuente: Elaboración Propia.

Figura 2-44: Sumario de configuración email.

2.8.3 Prueba de las Notificaciones

Hay que probar la configuración de notificación de Trigger. Por lo que se creará un problema falso de ICMP, para esto se creará una configuración de un host inexistente, una vez se esté creando, acceder a la pestaña “Plantillas” y agregar la siguiente plantilla: Módulo de plantilla ICMP Ping (ver figura 2-33).

Después se debe regresar a la pantalla inicial del tablero Zabbix y esperar 5 minutos para que se active la problemática de disponibilidad (ver figura 2-45). Habrá que comprobar si el servidor Zabbix envió una notificación por correo electrónico informando sobre este problema. La figura 2-46 muestra una prueba exitosa.

Fuente: Elaboración Propia.

Figura 2-45: Zabbix detectando el problema.

Fuente: Elaboración Propia.

Figura 2-46: Correo de notificación a Gmail.

2.9 AUTO DESCUBRIMIENTO

Aquí se debe configurar Zabbix para pueda detectar nuevos dispositivos.

2.9.1 Configuración de regla de descubrimiento

Acceder al menú “Configuración” y seleccionar “Descubrimiento” (ver figura 2-47).

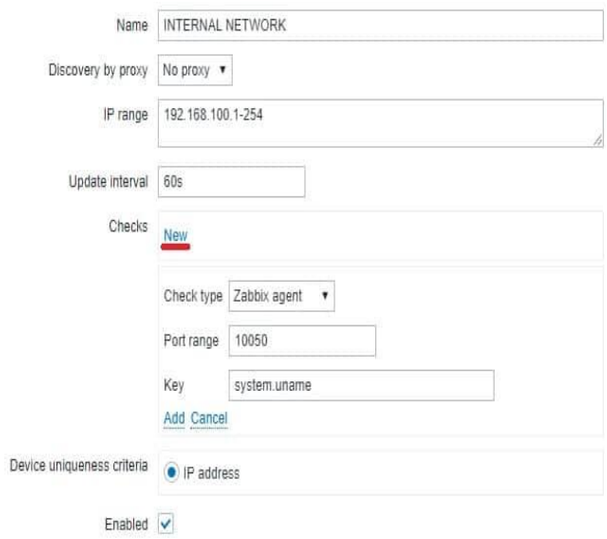
Fuente: Elaboración Propia.

Figura 2-47: Tablero de Zabbix - Descubrimiento.

En la esquina superior derecha de la pantalla, hacer clic en el botón “Crear regla de descubrimiento”. En la pantalla de configuración de descubrimiento de Host, se deberá ingresar la siguiente información:

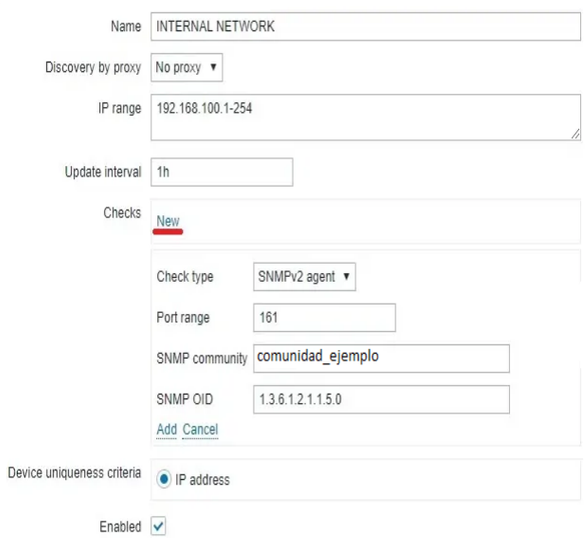
- *Nombre: ingresar una identificación de la regla de descubrimiento.*
- *Descubrimiento por Proxy: Sin proxy.*
- *Rango de IP: ingresar el rango de direcciones IP que debe escanearse.*
- *Intervalo de actualización: intervalo de tiempo entre el escaneo de red.*
- *Chequeos: hacer clic en la opción Nueva.*
- *Criterios de exclusividad del dispositivo: dirección IP o SNMPv2*
- *Habilitado: si*

Las figuras 2-48, 2-50 y 2-52 muestran cómo debe quedar la configuración para descubrimiento con agentes, y las figuras 2-49, 2-51 y 2-53 para descubrimiento con SNMP.



Fuente: Elaboración Propia.

Figura 2-48: Parámetros regla por Agente (1).

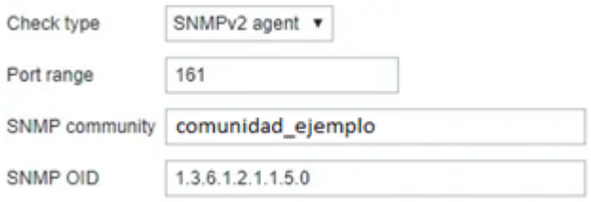


Fuente: Elaboración Propia.

Figura 2-49: Parámetros regla por SNMP (1).

Fuente: Elaboración Propia.

Figura 2-50: Parámetros regla por Agente (2).



Fuente: Elaboración Propia.

Figura 2-51: Parámetros regla por SNMP (2).

Fuente: Elaboración Propia.

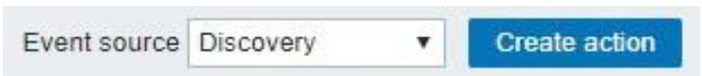
Figura 2-52: Parámetros regla por Agente (3).

Fuente: Elaboración Propia.

Figura 2-53: Parámetros regla por SNMP (3).

2.9.2 Configuración de acciones post descubrimiento

Ahora, se debe configurar las acciones que Zabbix necesita ejecutar después de descubrir un nuevo dispositivo usando el Agente. En la pantalla del tablero, acceder al menú "Configuración" y seleccionar la opción "Acción" (ver figura 2-40). En la esquina superior derecha de la pantalla, seleccionar el origen del evento "Discovery". Hacer clic en el botón "Crear acción" (ver figura 2-54).

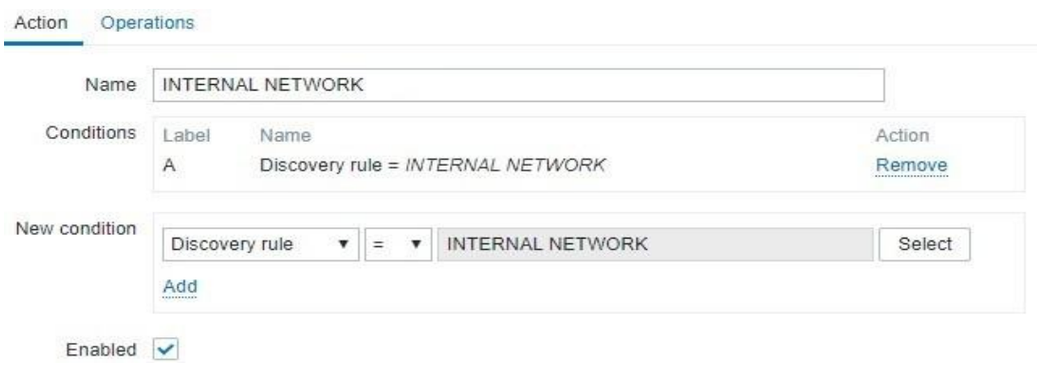


Fuente: Elaboración Propia.

Figura 2-54 Selección de eventos.

En la pantalla de configuración de descubrimiento de Host (ver figura 2-55), se deberá ingresar la siguiente información:

- *Nombre: ingresar una identificación a la acción de descubrimiento.*
- *Condiciones - Regla de descubrimiento = INTERNAL NETWORK*
- *Habilitado: Sí*



Fuente: Elaboración Propia.

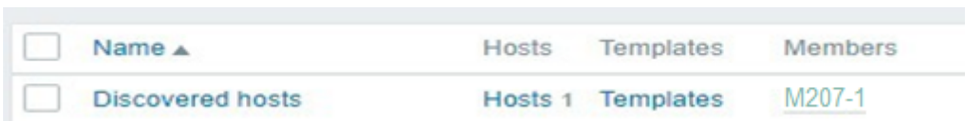
Figura 2-55: Configuración descubrimiento, red interna.

Acceder a la pestaña “Operaciones” y configurar las métricas que Zabbix deberá recabar (ver figura 2-54).

Fuente: Elaboración Propia.

Figura 2-56: Configuración de descubrimiento, acciones.

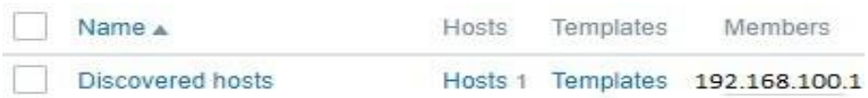
En este ejemplo, el servidor Zabbix escaneará la red 192.168.100.0/24 e intentará encontrar dispositivos con el agente Zabbix instalado cada 1 hora. Si el servidor Zabbix encuentra un dispositivo que usa el agente Zabbix, agregará este dispositivo al grupo de hosts “Descubiertos” (ver figura 2-57).



Fuente: Elaboración Propia.

Figura 2-57: Grupo de host descubiertos por nombre.

Tener en cuenta que el servidor Zabbix debe poder traducir la dirección IP del dispositivo al nombre del dispositivo. Si el servidor Zabbix no puede traducir la dirección IP de la computadora al nombre de host, creará un host usando la dirección IP del dispositivo en lugar de usar el nombre de host (ver figura 2-58).



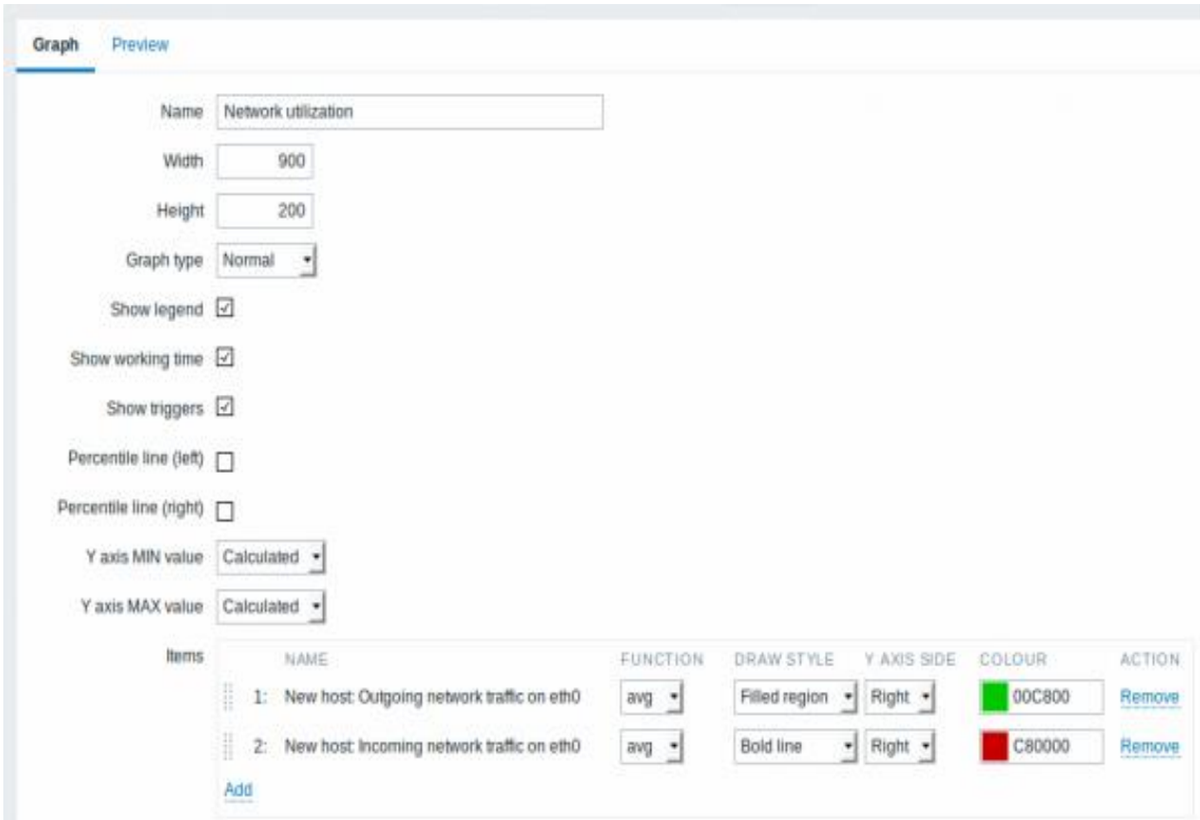
Fuente: Elaboración Propia.

Figura 2-58: Grupo de host descubiertos por IP.

2.10 GRÁFICOS PERSONALIZADOS

Los gráficos personalizados, ofrecen capacidades de personalización, si bien los gráficos simples son buenos para ver datos de un solo elemento, no ofrecen capacidades de configuración, por lo tanto, si desea cambiar el estilo del gráfico o la forma en que se muestran las líneas o comparar varios elementos, por ejemplo, el tráfico entrante y saliente en un solo gráfico, se necesita un gráfico personalizado, y se pueden crear para un host o varios hosts o para una sola plantilla. Para configurar gráficas personalizadas, se debe:

- *Ir a Configuración → Hosts*
- *Hacer clic en Gráficos en la fila junto al host o la plantilla deseada*
- *En la pantalla de Gráficos hacer clic en Crear gráfico.*
- *Editar atributos del gráfico (ver figura 2-59).*



Fuente: Elaboración Propia.

Figura 2-59: Edición atributos del gráfico.

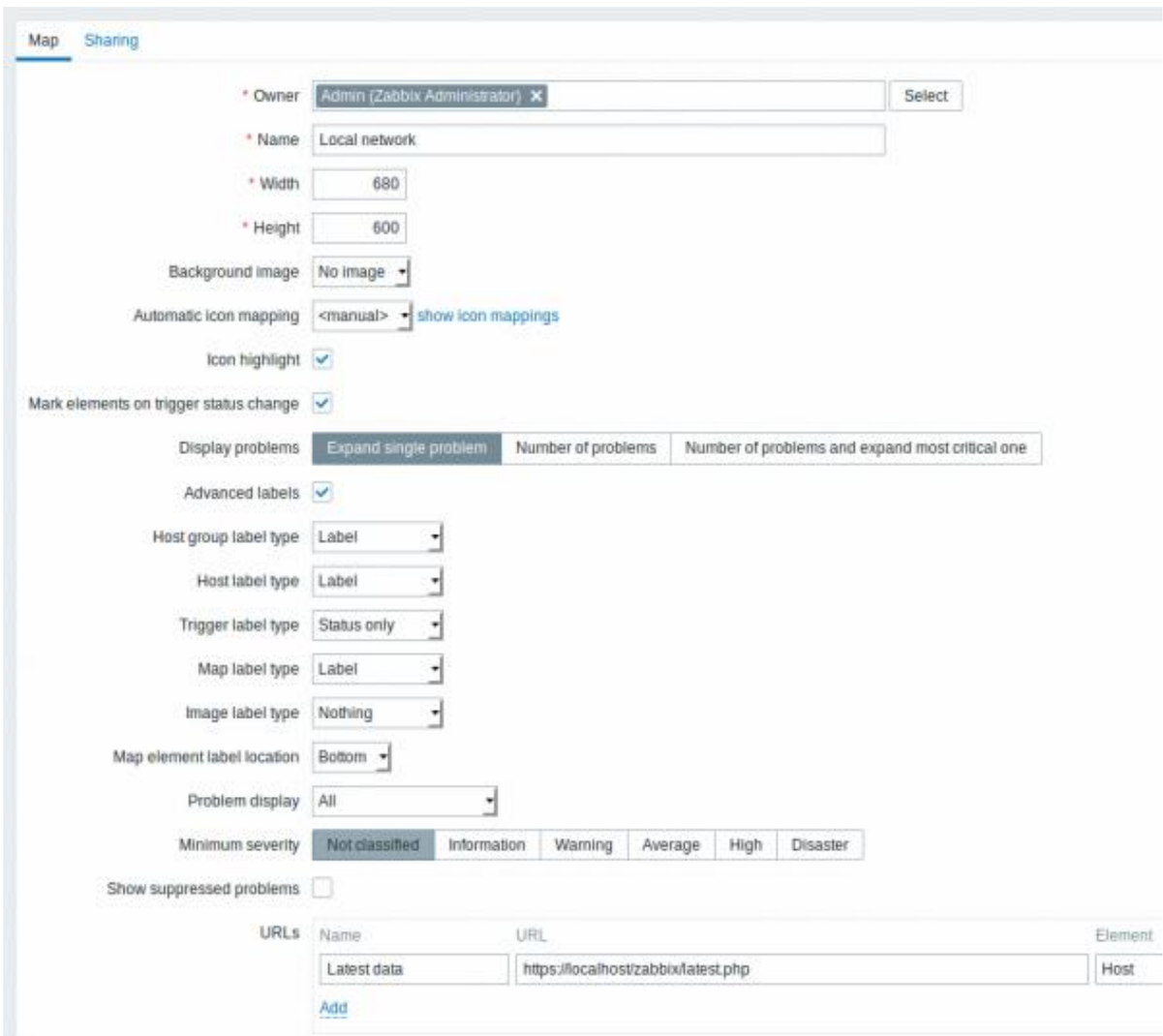
Después de guardar los cambios, ya estará disponible el gráfico para ser consultado, en el apartado de “Gráficos”.

2.11 MAPAS TOPOLÓGICOS DE RED

Los mapas personalizados los cuales nos van a permitir visualizar de mejor manera la topología a monitorear.

2.11.1 Configuración previa

Para crear un mapa se debe ir a Monitoreo → Mapas, luego ir a la vista con todos los mapas, y hacer clic en “Crear mapa”. La pestaña “Mapa” contiene atributos generales del mapa (ver figura 2-60). Todos los campos de entrada obligatorios están marcados con un asterisco.



Fuente: Elaboración Propia.

Figura 2-60: Edición atributos del mapa.

La tabla 2-2 describe los atributos mas importantes en la configuración preliminar de un mapa topológico en Zabbix.

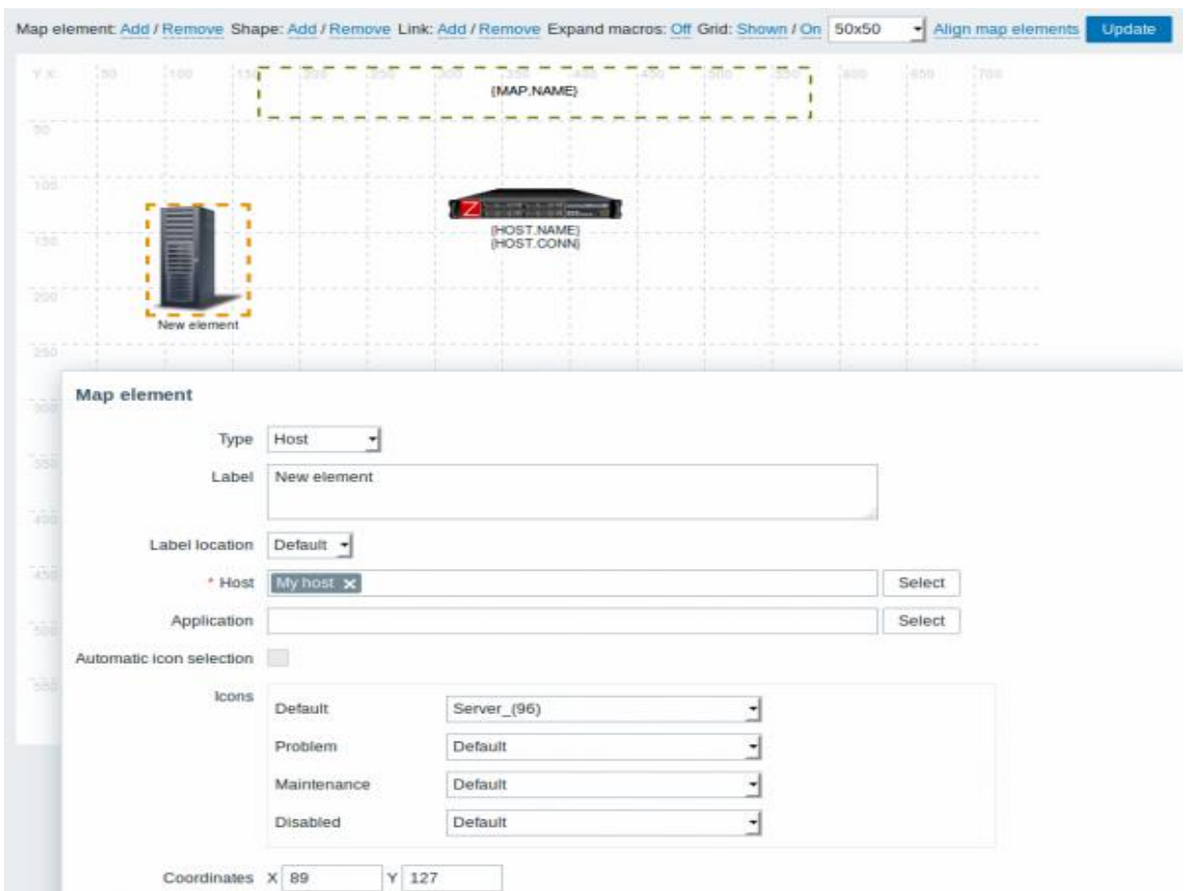
Tabla 2-2: Definición de atributos generales del mapa.

Parámetro	Descripción
Propietario	Nombre del propietario del mapa.
Nombre	Nombre del mapa único.
Anchura	Ancho del mapa en píxeles.
Altura	Altura del mapa en píxeles.
Imagen de fondo	Seleccionar una imagen para utilizar de fondo.
Mapeo automático de iconos	Configurar en Administración → General → Asignación de iconos. La asignación de iconos permite asignar ciertos iconos para ciertos elementos del inventario.
Etiquetas avanzadas	Si se marca esta casilla, se podrá definir distintos tipos de etiquetas para distintos tipos de elementos.
Tipo de etiqueta del elemento del mapa	Dirección IP Nombre del elemento (ejemplo el nombre del host) Estado: solo estado (ok o no) Nada: no se muestran etiquetas
Ubicación de la etiqueta del elemento del mapa	Abajo: debajo del elemento del mapa Izquierda: a la izquierda Derecha: a la derecha Arriba: arriba del elemento del mapa
Pantalla de problemas	Todo: Se muestra una cuenta de problemas completa Separado: Se mostrará cuenta de problemas sin acuse de recibo separado como un número de la cuenta de problemas totales No reconocida solamente: Sólo se mostrará el recuento problema no reconocido.
Gravedad mínima de disparo	Los problemas por debajo del nivel de severidad mínimo seleccionado no se mostrarán en el mapa. Por ejemplo, con “Advertencia” seleccionado, los cambios de “Información” y “No clasificado” no se reflejarán en el mapa.

Fuente: zabbix.com

2.11.2 Adición de elementos

Para agregar un elemento, hay que hacer clic en “Agregar” junto a “Map element”. El nuevo elemento aparecerá en la esquina superior izquierda del mapa, hay que arrastrar y soltar donde se quiera. En la opción de cuadrícula activada, los elementos siempre se alinearán con la cuadrícula, también ocultar o mostrar la cuadrícula. Si se desea colocar elementos en cualquier lugar sin alineación, cambiar la opción a desactivada. También es posible diferenciarlos dándoles nombres, etc. Al hacer clic en el elemento, se muestra un formulario y se puede establecer el tipo de elemento, nombre, icono, etc. (ver figura 2-61).

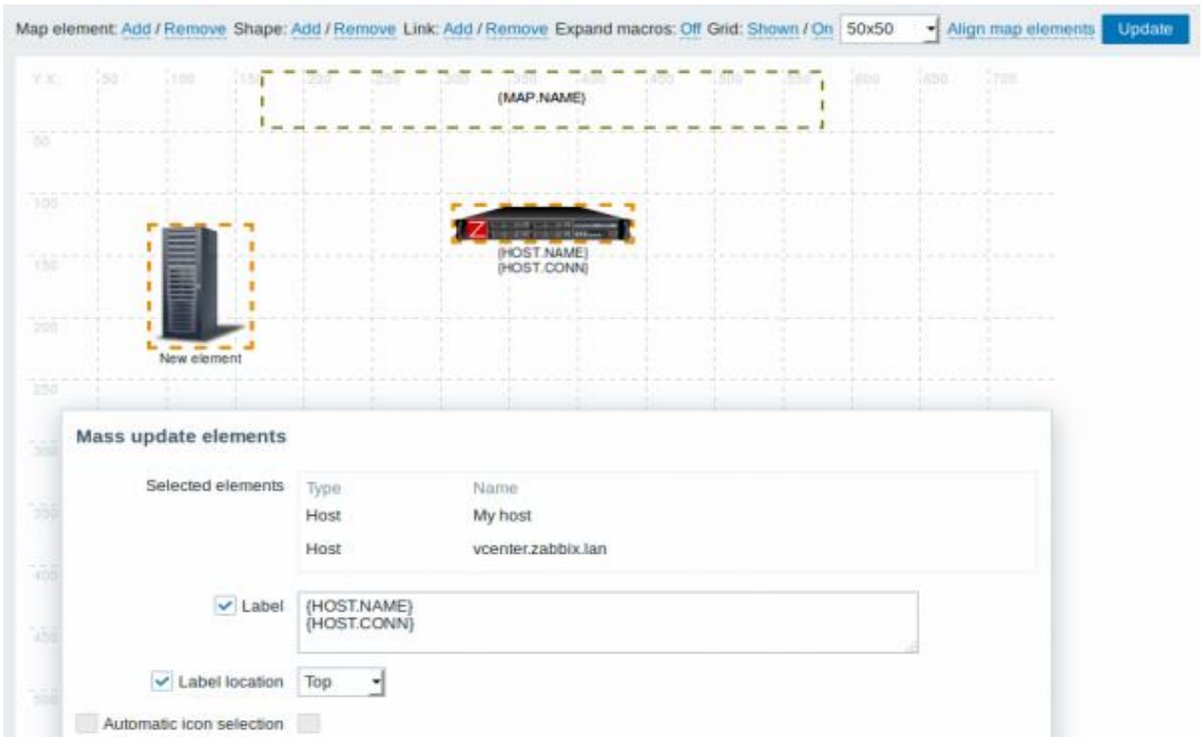


Fuente: Elaboración Propia.

Figura 2-61: Adición de elementos.

2.11.3 Selección de elementos

Para seleccionar elementos, se debe seleccionar uno y luego mantener presionada la tecla Ctrl para seleccionar los otros (ver figura 2-62). Una vez que se selecciona más de un elemento, la forma de propiedad del elemento cambia al modo de actualización masiva para que pueda cambiar los atributos de los elementos seleccionados de una sola vez. Para hacerlo, es necesario marcar el atributo con la casilla de verificación e ingresar un nuevo valor para él.

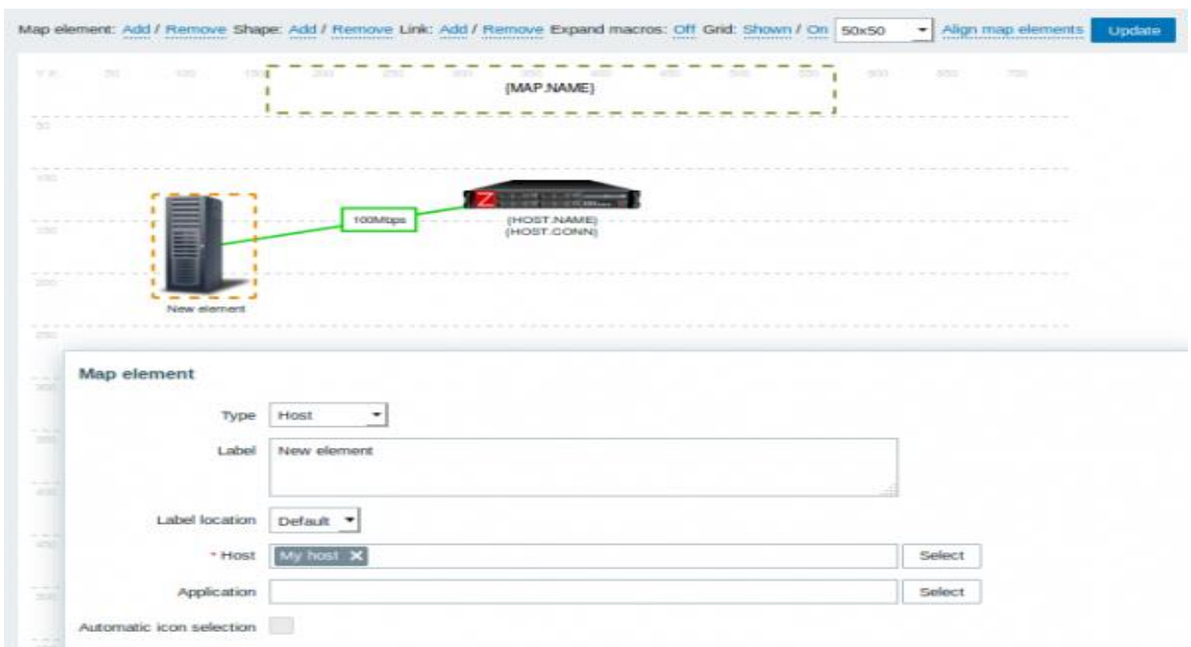


Fuente: Elaboración Propia.

Figura 2-62: Selección de elementos.

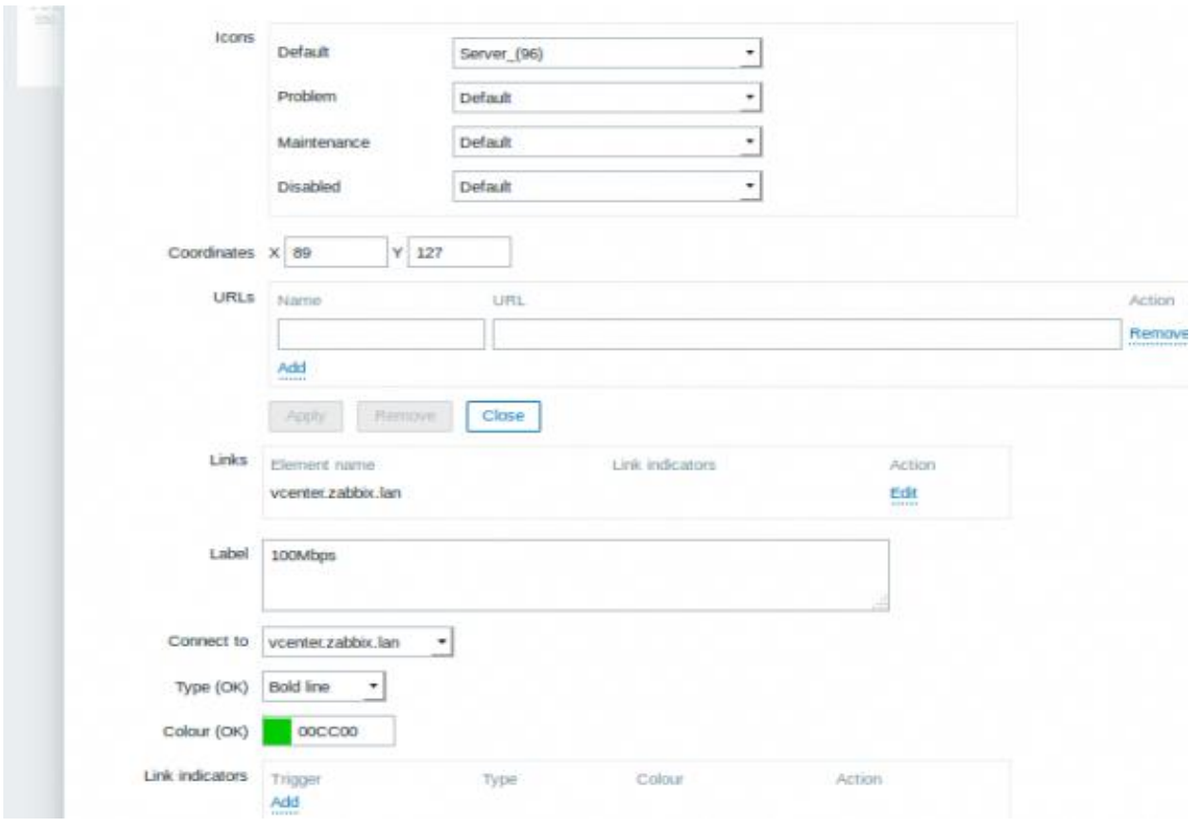
2.11.4 Elementos de enlace

Una vez que se haya puesto algunos elementos en el mapa, habrá que comenzar a vincularlos. Para enlazar dos elementos primero se deben seleccionar. Con los elementos seleccionados, hacer clic en “Agregar” junto a “Enlace”. Con un enlace creado, el formulario de un solo elemento ahora contiene una sección de “Enlaces” adicional. Hacer clic en “Editar” para editar los atributos del enlace (ver figura 2-63).



Fuente: Elaboración Propia.

Figura 2-63: Enlaces de elementos (1).



Fuente: Elaboración Propia.

Figura 2-64: Enlaces de elementos (2).

CAPÍTULO 3: EVALUACIÓN DE COSTOS

3: EVALUACIÓN DE COSTOS

En la evaluación de costos se tomó en cuenta tanto el software como el hardware de cada uno de los elementos a monitorear dentro del laboratorio. Al momento de realizar una correcta evaluación de costos se debe considerar también al número de personas encargadas de trabajar en la implementación, del horario que van a ocupar, cuando lo van a realizar y de las herramientas necesarias para realizar dicho trabajo.

3.1 ESPECIFICACIONES DEL INVENTARIO

Se procederá a listar mediante tablas las especificaciones técnicas de cada uno de los elementos usados para el monitoreo de redes de este proyecto.

Tabla 3-1: Especificaciones técnicas Router LAN.

3.1.1 Router LAN	
Modelo	Cisco 2900
Criptografía y aceleración integradas basadas en hardware	Si
Puertos WAN 10/100/1000	2
Puertos RJ-45	2
Ranuras ISM (Encriptación)	1
Ranuras DSP (PVDM)	2
Memoria DDR2 ECC DRAM (Default)	512 MB
Ranuras de memoria flash USB 2.0 externas (tipo A)	2
Puerto de consola USB (Tipo B)	1
Puertos serial consola	1
Puerto auxiliar serie	1
Dimensiones	44.5 x 438.2 x 439.4 mm
Unidades de Rack	1
Temperatura	-40 a 70ºC
Humedad	5 a 95%
Foto de referencia	 Fuente: westenditstore.com Figura 3-1: Router 2900 series.

Fuente: cisco.com

La tabla 3-1; muestra las características del router LAN, necesario para la realización de este proyecto, siendo monitoreado por Zabbix.

Tabla 3-2: Especificaciones técnicas Switch 2960.

3.1.2 Switch	
Modelo	Cisco 2960
Puerto USB	1
Humedad relativa de funcionamiento	5% de 90% a 40ºC
Temperatura de almacenamiento	–25º de 70ºC
Alimentación	Data, PoE
Voltaje	110 a 220V AC in
Conectores e interfaces	➢ Puertos 10BASE-T: RJ-45, 2 pares, Cat 3, 4, o 5 ➢ Puertos 100BASE-TX: RJ-45, 2 pares Cat 5 UTP ➢ Puertos 1000BASE-T: RJ-45, 4 pares, Cat 5 UTP ➢ Puertos 1000BASE-T SFP: RJ-45, 4 pares, Cat 5 UTP
Cables consola	➢ RJ45 6 ft. con RJ-45 ➢ USB 6 ft. con USB
Poder	Utilizar el cable de alimentación de CA suministrado para conectar el conector de alimentación de CA a una toma de corriente de CA.
Estándares	➢ IEEE 802.1: D STP, p CoS, Q VLAN, s,w, X, ax y ab (LLDP) ➢ IEEE 802.3: ad, af, at, ah, x, 10BASE-T, u 100BASE-TX, ab 1000BASE-T, z 1000BASE-X, az y ae ➢ Estándares RMON I and II ➢ SNMP v1, v2c, and v3
Foto de referencia	

Fuente: cisco.com

Figura 3-2: Switch 2960 series.

Fuente: cisco.com

La tabla 3-2; muestra las características del switch, necesario para la realización de este proyecto, siendo monitoreado por Zabbix.

Tabla 3-3: Especificaciones técnicas Router WLAN.

3.1.3 Router WLAN	
Marca	Linksys EA6540
Tecnología	➢ IEEE 802.11b, g, n y ac ➢ IEEE 802.3 y u
Bandas	2,4 GHz y 5 GHz simultáneas
Interfaces	Puertos 10Base-T/100Base-TX/1000Base-T
Transmisión/recepción	3 x 3
Protocolo de encriptación	WPA2
Antenas	6 (internas)
Características soportadas	IPv6, Calidad de servicio (QoS), tecnología RangeBooster, tecnología SimpleTap, Stateful Packet Inspection Firewall (SPIF), Wi-Fi Protected Setup (WPS).
Puertos	➢ 1 x Gigabit WAN ➢ 4x Gigabit LAN ➢ 1x USB 3.0 y 1x USB 2.0
Leds	Energía, internet y ethernet (1-4)
Temperatura de funcionamiento	0 a 40 ° C
Temperatura de almacenamiento	-20 a 60 ° C
Compatibilidad	IPv6 nativa y IPv6 rapid deployment
Cisco Connect Cloud	Sí
Configuración	CD de instalación Cisco Connect
Dimensiones	256 x 184.3 x 40.1 mm
Máxima Tasa de enlace	867 Mbps
Compatibilidad de plataforma	➢ Windows: XP, Vista, 7, 8, 8.1 y 10 ➢ Mac OS X: 10.5.8 Leopard, 10.6.1 Snow Leopard, 10.7 Lion, 10.8 Mountain Lion y 10.9 Mavericks
Imagen de referencia	 Fuente: linksys.com Figura 3-3: Router WLAN.

Fuente: linksys.com

La tabla 3-3; muestra las características del router WLAN, necesario para la realización de este proyecto, siendo monitoreado por Zabbix.

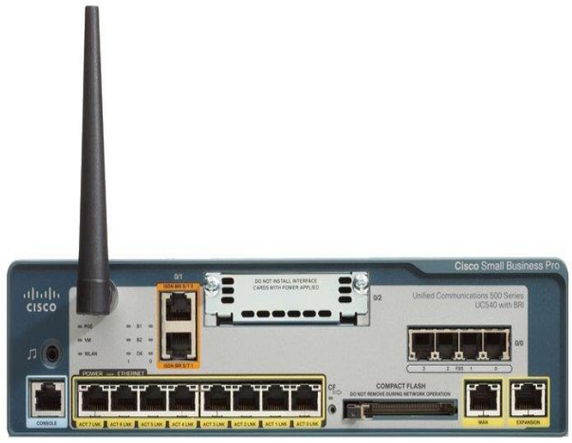
Tabla 3-4: Especificaciones técnicas Teléfono IP.

3.1.4 Teléfono IP	
Marca	Cisco
Modelo	SPA504G
Redes de datos	Dirección MAC (IEEE 802.3) - IPv4 – ARP - DNS: registro y registro SRV – DHCP – ICMP – TCP – UDP - Protocolo de transporte en tiempo real (RTP) - Protocolo de control en tiempo real (RTCP) -Servicios diferenciados (DiffServ) - Protocolo simple de tiempo de red (SNTP)
Pasarela de voz	➢ SIP versión 2 (RFC 3261, 3262, 3263, 3264) ➢ SPCP con Cisco Unified Communications ➢ Llamadas seguras encriptadas con SRTP ➢ Multifrecuencia de doble tono (DTMF) ➢ Soporte de plan de marcado flexible con temporizadores entre dígitos ➢ Dirección IP / soporte de marcado URI ➢ Generación de ruido de confort (GNC) ➢ Detección de actividad de voz (VAD) con supresión de silencio ➢ Soporte de identificación de llamadas
Aprovisionamiento, administración y mantenimiento	➢ El servidor web integrado proporciona administración y configuración ➢ Configuración del teclado del teléfono a través del menú de navegación ➢ Aprovisionamiento y actualización automatizados con HTTPS, HTTP, TFTP ➢ Generación de informes y registro
Fuente de alimentación	Voltaje de salida DC: +5 VDC a 2.0A máximo
Interfaces físicas	➢ 2 puertos Ethernet 10 / 100BASE-T RJ-45 ➢ Auricular: conector RJ-9 ➢ Puerto para auriculares de 2.5 mm
Dimensiones	214 x 212 x 44 mm
T° de funcionamiento	0º - 40ºC
T° de almacenamiento	-20º - 70ºC
Humedad de funcionamiento	5% a 95% sin condensación
Humedad de almacenamiento	5% a 95% sin condensación
Foto de referencia	 Fuente: onedirect.es Figura 3-4: Teléfono IP Cisco.

Fuente: cisco.com

La tabla 3-4; muestra las características del teléfono IP, necesario para la realización de este proyecto, siendo monitoreado por Zabbix.

Tabla 3-5: Especificaciones técnicas PBX IP.

3.1.5 PBX IP	
Marca	Cisco
Modelo	UC540
Admite	Voz, video, inalámbrico, productividad, enrutamiento seguro
Procesamiento de llamadas telefónicas	Si
Correo de voz	Correo de voz integrado y operador automatizado
Cantidad máxima de teléfonos	Hasta 104 teléfonos en múltiples ubicaciones
Capacidades	Básicas del centro de llamadas
Soporte para música en espera	Si
Acceso Inalámbrico	Integrado
Funcionalidad completa para personal remoto y teletrabajadores	Si
Capacidades integradas de correo de voz a correo electrónico	Si
Videollamadas integradas	Si
Funciones de fax a correo electrónico	Si
Alcance	Soporta un solo número entre teléfonos de escritorio, softphones, teléfonos remotos o teletrabajadores y teléfonos móviles
Dimensiones	66.7 x 266.7 x 280.7 mm
	 Fuente: cisco.com Figura 3-5: PBX Cisco.

Fuente: cisco.com

La tabla 3-5; muestra las características de la PBX IP, necesaria para la realización de este proyecto, siendo monitoreada por Zabbix.

Tabla 3-6: Especificaciones técnicas Cámara IP.

3.1.6 Cámara IP	
Modelo	DCS-942L
Marca	D-LINK
Compresión de video	➢ H.264/MPEG4/MJPEG (simultáneos) ➢ JPEG para fotografía
Audio	➢ AAC/ADPCM/mu-Law PCM/LPCM ➢ Sonido bidireccional Full-duplex
Conectividad	➢ Puerto Ethernet 10/100 BASE-TX ➢ Wi-Fi 802.11n ➢ Ranura MicroSD1
Protocolos de red	IPV4, IPv6, ARP, TCP, UDP, ICMP, Cliente DHCP, Cliente NTP (D-Link), Cliente DNS, Cliente DDNS (D-Link), Cliente SMTP, Cliente FTP, Servidor HTTP, HTTPS (para configuración), PPPoE, UPnP Port Forwarding, LLTD, RTP, RTSP, RTCP, Bonjour, Cumple ONVIF
Seguridad	➢ Autenticación por contraseña ➢ Encriptación HTT
Requisitos del sistema para interfaz	Sistema operativo: Microsoft Windows 8/7/Vista y Mac OS X 10.6 o superior
Gestión de eventos	Detección de movimiento y sonido con notificación de eventos y envío de fotos o vídeos por SMTP o FTP
Gestión remota	Configuración accesible vía navegador web
Móviles	App mydlink Lite para iPhone/iPad/iPod touch y Android
Requisitos para la D-ViewCam™	➢ Sistema operativo: Microsoft Windows 8/7/Vista/XP ➢ Navegador: Internet Explorer 7 o superior
Alimentación	5 V DC 1.2 A, 50/60 Hz
Consumo	4.2 watts máximo
Temperatura Funcionamiento	0 a 40°C
Temperatura de Almacenamiento	-20 a 70° C
Humedad Funcionam.	20% a 80% sin condensación
Humedad de Alm.	5% a 95% sin condensación
Foto de referencia	

Fuente: lifeinformatica.com

Figura 3-6: Cámara D-Link DCS-942L.

Fuente: eudlink.com

La tabla 3-6; muestra las características de la cámara IP, necesaria para la realización de este proyecto, siendo monitoreada por Zabbix.

3.2 COSTOS DEL INVENTARIO

Ahora se procederá a revisar los costos asociados al inventario, refiriéndose con esto a los equipos presentes en el laboratorio M-207, con su respectivo hardware y software.

3.2.1 Costos generales

En la tabla 3-7, se muestran los precios de cada uno de los componentes a monitorear, este precio es un precio general, sacado de tiendas de gran tamaño internacionales. *Valor dólar 31 octubre 2019 = $CLP 741,8.

Tabla 3-7: Precio general de componentes.

Componentes	Precio en Dólares
Router LAN	1270,00
Switch	867,00
Router WLAN	129,99
Teléfono IP	114,62
PBX IP	1578,00
Cámara IP	96,50

Fuente: Elaboración propia, basado en equipamiento utilizado.

3.2.2 Cotizaciones

La tabla 3-8, muestra los precios de cada uno de los componentes a monitorear (IVA incluido), este precio se obtuvo por medio de cotizaciones en tiendas nacionales.

Tabla 3-8: Precio de componentes y sus proveedores.

Componentes	Precio en $CLP	Proveedor	Página web
Router LAN	$1.882.930	IPeX	ipexpress.cl
Switch	$1.442.135	Wei Chile S.A.	wei.cl
Router WLAN	$84.990	Falabella	falabella.cl
Teléfono IP	$134.622	Red Cetus	redcetus.cl
PBX IP	$587.790	Clickbox	clickbox.cl
Cámara IP	$76.989	Cintegral	cintegral.cl
Computadora	$426.970	PC Factory	pcfactory.cl

Fuente: Elaboración propia, basado en cotizaciones de productos.

3.2.3 Software y SO

La mayoría del software y sistemas operativos que se utilizaron son gratuitos, sin embargo, vale la pena mencionarlos. La tabla 3-9 muestra lo descrito.

Tabla 3-9: Software y sistemas operativos con sus precios.

Software / SO	Precio en $CLP
MySQL	Gratuito
Apache	Gratuito
Zabbix	Gratuito
Ubuntu Linux	Gratuito
Windows 10 Pro	$126.090

Fuente: Elaboración propia, basado en software utilizado.

3.2.4 Componentes de PC

La tabla 3-10 muestra la cotización pedida en la página pcfactory.cl, contiene el hardware de las computadoras ocupadas, descrito en el capítulo 2, más los periféricos.

Tabla 3-10: Precio componentes de computadora.

Componente	**Precio en $CLP**
Intel ® CPU Core i5-9400F 4.10 GHz 9MB	$151.990
MSI ® Tarjeta Madre Intel H310M PRO-VDH PLUS	$55.990
Kingston ® DDR4 8GB 2400MHz Value RAM	$36.990
Toshiba ® Disco Duro 500GB Sata3	$29.990
DLink ® Tarjeta de Red Interna PCI-E RJ45 10/100/1000	$14.190
Asus ® DVDRW SATA 24x	$11.990
Spektra ® Gabinete mATX 200W	$19.990
Spektra ® Fuente de Poder 500W	$14.990
LG ® Monitor 22MK400H 21,5"	$76.990
Genius ® Mouse DX-110 Óptico USB	$3.290
HP ® Teclado HP 100 USB	$7.590
Spektra ® Cable SATA (Serial-Ata) Datos	$2.980
	Total: $426.970

Fuente: pcfactory.cl

3.3 COSTOS MANO DE OBRA

Estos costos están asociados a la mano de obra necesaria para la investigación, implementación y mantención del monitoreo, el trabajo lo debe hacer idealmente un Técnico en Telecomunicaciones y Redes, sin embargo, también sirve un Ingeniero Informático.

Cabe destacar que la mano de obra aquí puede tener 2 significados distintos, el primero hace alusión a una sala con todos los equipos tal cual están en el laboratorio M-207, la misma cantidad y los mismos modelos, este proyecto no abarca este caso pero vale la pena mencionarlo, y el segundo, el caso de este proyecto, se refiere a una mini red con 3 estaciones de trabajo que se usaría por los creadores de este proyecto para testear el buen funcionamiento de los métodos ya explicados, para su posterior implementación práctica.

3.3.1 Investigación

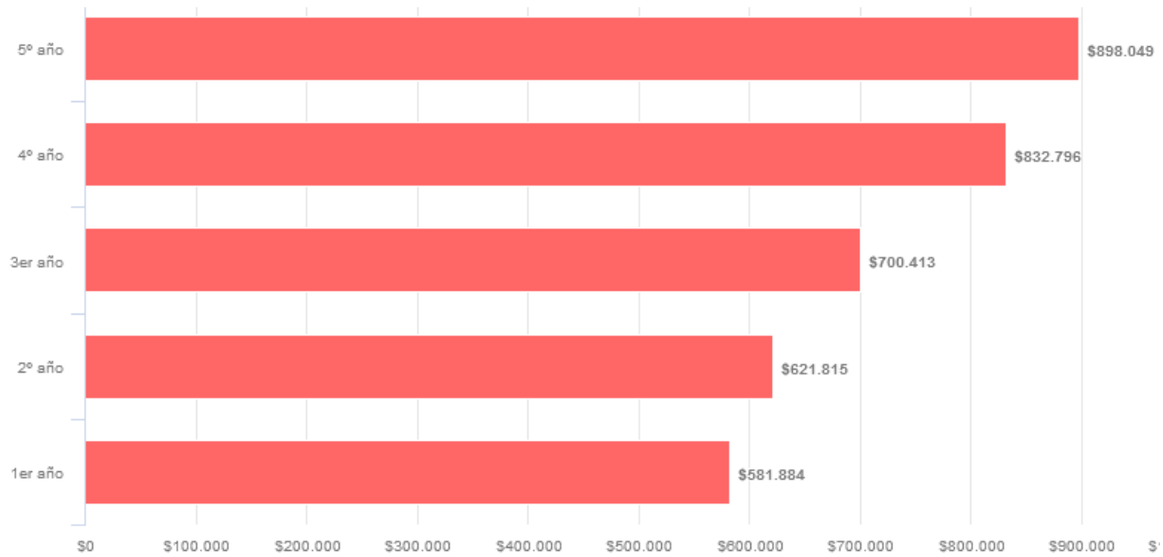
Se refiere a lo necesario para la realización este informe. Tomando en cuenta un total de estimado de 160 horas de investigación invertidas en este proyecto, con las leyes del país que dictan un total máximo de 40 horas semanales de trabajo, se puede deducir que la investigación corresponde a un mes de trabajo y se tomará el valor estimado de $580.000, para más información ver figura 3-7.

3.3.2 Implementación

Suponiendo, por previo estudio de mercado, que la instalación de una estación de trabajo con todos los componentes que conlleva, osea computador, router, switch, y cámara, teléfono y PBX IP cuando corresponda, su cableado y por último su configuración, cuesta unos $15.000 (0,5 UF app.), este valor habría que multiplicarlo por 3 estaciones de trabajo, dando un total de $45.000. El proyecto se llevaría a cabo en un plazo de tiempo estimado de una semana, dando margen de tiempo para realizar las pruebas correspondientes, por las que se cobrarán unos $145.000, correspondiente a la cuarta parte (1 semana) del sueldo de referencia $580.000.

3.3.3 Mantención

La figura 3-7, muestra en detalle el sueldo mensual de un Técnico en Telecomunicaciones de acuerdo con los años que pasaron desde que egresó. Para tener un valor más concreto, se tomará el valor del primer año de egreso, que son aproximadamente $580.000 para la mantención mensual.



Fuente: mifuturo.cl

Figura 3-7: Ingresos brutos mensuales de un Técnico en Telecomunicaciones.

3.4 SUMARIO DE COSTOS

La tabla 3-12, muestra la cantidad y el total que se debería pagar en costos elementos y mano de obra para el estudio de un monitoreo de red eficaz, que dé como resultado una correcta implementación en el laboratorio. *Valor UF octubre 2019 = $CLP 28.050.

Tabla 3-12: Precio total de componentes.

Elemento	**Precio unitario en $CLP**	**Cantidad**	**Precio total**
Router 2901	$1.872.570	3	$5.617.710
Switch 2960	$1.284.035	3	$3.852.105
Router WLAN	$84.990	1	$84.990
Teléfono IP	$138.195	3	$414.585
PBX IP	$587.790	1	$587.790
Cámara IP	$76.989	1	$76.989
Computadora	$426.970	3	$1.280.910
Cable UTP+RJ45	$1.490	10	$14.900
SO Windows 10	$126.090	3	$378.270
Investigación	$580.000	-	$580.000
Escrito	$20.000	-	$20.000
Instalación	$15.000	3	$45.000
Pruebas	$145.000	-	$145.000
		Suma:	$13.098.249
		Imprevistos (5%):	$654.912
		Total:	$13.753.161
		Total en dólares:	18540,3
		Total en UF:	$490,3

Fuente: Elaboración propia

CONCLUSIONES Y RECOMENDACIONES

La elección de centrarse en monitorear redes fue tomada principalmente para ampliar los conocimientos en una de las áreas que más gustamos de la carrera, las redes, además de ver la necesidad que presenta el laboratorio objetivo, permitiendo así medir el rendimiento de sus componentes y contabilizar el uso de la red, tomando en cuenta el ancho de banda.

Al momento de monitorear, son muy importantes los Triggers con sus alarmas y los informes generados por cada uno de ellos, para que, al momento de cualquier percance, el administrador pueda detectar tempranamente el error y solucionarlo de inmediato, de esta manera se garantiza un buen funcionamiento de los dispositivos de red.

Es necesario una correcta selección de las herramientas y dispositivos a emplear dentro de la red, en función de optimizar los recursos y la propia infraestructura. Para ello hay que investigar cada una de las posibles herramientas, analizando sus características, ventajas, desventajas, costos, como también el lugar al cual se le quiere implementar el monitoreo. En este caso el lugar seleccionado fue el laboratorio de redes M-207, para el que se seleccionó la herramienta Zabbix, elegida principalmente por ser un software de carácter libre y de interfaz intuitiva que permite realizar gráficas en tiempo real de cada uno de los dispositivos, que van desde un router hasta una cámara IP.

También hay que entender lo que podría pasar si no existe un monitoreo constante en la red y los elementos que la conforman. En el caso de un servidor, si este presenta una falla y uno no se da cuenta de este percance, cuando el servidor colapse por completo, si este está asociado a una empresa proveedora de servicios, no solo se tendría que reponer el servidor que fallo si no también se tendrían problemas con los clientes asociados a él, en el caso del laboratorio de redes USM M-207, si uno de los componentes vitales de la sala falla, se podría interrumpir el proceso educativo.

El nivel de conformidad sobre este trabajo es alto, sobre todo porque se sabe que posiblemente ayude al mejoramiento del laboratorio y a las siguientes generaciones de estudiantes, a los cuales les puede servir como una experiencia más de redes.

BIGLOGRAFÍA

LISTA DE SITIOS WEB

Fecha de consulta	Sitio Web
03/2019	https://es.wikipedia.org/wiki/Anexo:Comparaci%C3%B3n_de_sistemas_de_monitorizaci%C3%B3n_de_redes https://www.itsitio.com/mx/por-que-es-importante-el-monitoreo-de-redes/ https://blog.pandorafms.org/es/monitorizacion-de-sistemas/ http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1684-18592018000100009 https://searchitoperations.techtarget.com/definition/Nagios https://searchitoperations.techtarget.com/definition/Nagios https://blog.pandorafms.org/es/metricas-ti/ https://fp.uoc.fje.edu/blog/la-importancia-del-monitoreo-de-red-en-las-empresas/ http://www.auben.net/index.php/tecnologias/monitoreo-y-gestion-de-red https://www.interbel.es/la-importancia-de-tener-un-buen-sistema-de-monitorizacion/ https://smarterworkspaces.kyocera.es/blog/5-razones-las-las-empresas-deben-monitorizar-la-red/ https://www.universidadviu.es/monitorizar-red-consejos-herramientas-hacerlo-la-perfeccion
05/2019	https://bit.ly/2Ie2ZRT https://es.wikipedia.org/wiki/Monitoreo_de_red https://www.quasarbi.com/ZABBIX.html https://www.zabbix.com/documentation/2.0/manual/config/visualisation/maps/map https://techexpert.tips/category/zabbix/
07/2019	https://www.mifuturo.cl/buscador-de-estadisticas-por-carrera/

ANEXOS

ANEXO A: COTIZACIONES

Clickbox

Inicio › Técnicos

Cisco Ip-pbx 2-bri-isdn 4-fxs 8-poe 1-rptnc-2dbi Co Clickbox

$ 587.890

---

cintegral 25 JUNTO A US$ Buscar en la tienda...

PC Y PORTÁTILES | IMPRESIÓN E IMAGEN | SUMINISTROS

CAMARA D-LINK DCS-942L CLOUD ...

Precio:
$76.989

PC FACTORY
Tu partner tecnológico

Inicio | Arma tu PC | Productos 2da Selección | Tiendas | Contáctenos

Todas las Categorías | Buscar: Buscar por palabra(s) clave o código | Carro de Compras Contiene 1 item(s) | Cotización Online Contiene 0 item(s)

32738

Intel ® CPU Core i5-9400F 4.10 GHz 9MB (1151-v2)

Precio Unitario Efectivo
$ 151.990

1

SubTotal
$ 151.990

32917

MSI ® M/B Intel H310M PRO-VDH PLUS (1151-v2)

Precio Unitario Efectivo
$ 55.990

1

SubTotal
$ 55.990

34620

Kingston ® DDR4 8GB 2400MHz Value RAM

Precio Unitario Efectivo
$ 36.990

1

SubTotal
$ 36.990

20010

DLink ® Tarjeta de Red Interna PCI-E RJ45 10/100/1000 DGE-560T

Precio Unitario Efectivo
$ 14.190

1

SubTotal
$ 14.190

20751

Microsoft ® Windows 10 Profesional OEM 64 bits

Precio Unitario Efectivo
$ 126.090

1

SubTotal
$ 126.090