UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE GUAYAQUIL

CARRERA: INGENIERÍA DE SISTEMAS

Proyecto Técnico previo a la obtención del título de: INGENIERO DE SISTEMAS

TEMA:
IMPLEMENTACIÓN DE HERRAMIENTAS DE SOFTWARE OPEN SOURCE PARA MONITOREAR LOS SISTEMAS DE COMUNICACIÓN DE VOZ Y DATOS DE LAS EMPRESAS TUVAL S.A., DIMULTI S.A., Y CASTEK S.A.

AUTOR:
DANNY ELÍAS OBANDO YUMBLA

DIRECTOR:
ING. DANNY BARONA VALENCIA

Guayaquil, enero de 2016

DECLARATORIA DE RESPONSABILIDAD Y AUTORIZACIÓN DE USO DE TRABAJO DE GRADO

Yo, Danny Elías Obando Yumbla autorizo a la Universidad Politécnica Salesiana la publicación total o parcial de este trabajo de grado y su reproducción sin fines de lucro.

Además declaro que los conceptos y análisis desarrollados y las conclusiones del presente trabajo son de exclusiva responsabilidad del autor.

Danny Elías Obando Yumbla
CC 0919662825

DEDICATORIA

Finalizando esta etapa de mi vida y teniendo sentimientos de alegría y nostalgia por los recuerdos de todos los momentos vividos durante mi estudio universitario, es mi deseo dedicar este título a todas y cada una de las personas que creyeron que era capaz de conseguir este logro tan importante en mi vida.

A mi madre Carmen, a mi madrina Janeth a mis hermanas Jéssica y Melany y a mi sobrina Natalia porque estoy convencido que están tan emocionados como yo por este triunfo en mi vida.

A mi esposa Maybelin por haber estado todos estos años junto a mí apoyándome y alentándome para que consiga este tan añorado título universitario.

Y finalmente a Dios por permitirme disfrutar con todos mi seres queridos de este maravilloso momento.

Danny Elías Obando Yumbla

AGRADECIMIENTO

A la Universidad Politécnica Salesiana sede Guayaquil por la enseñanza brindada que contribuyó a mi desarrollo académico y profesional.

A mis profesores de la carrera de ingeniería de sistemas que con su esfuerzo y dedicación fueron cimentando las bases del conocimiento que actualmente poseo.

A mis amigos que hice en la universidad, con los cuales compartimos muchos momentos de alegría, tensión y diversión.

A mi tutor el Ing. Danny Barona el cual me supo guiar de excelente manera para poder culminar el desarrollo del presente trabajo.

A mi madre y mi madrina que fueron piezas claves en mi educación como persona y que me inculcaron que el estudio es la base para ser una persona de bien.

A mi esposa que con su apoyo he conseguido lograr muchas metas y la culminación de este trabajo de titulación es parte de una de ellas.

Y por último pero no menos importante a Dios por ser mi compañía durante toda la vida y ser uno de los pilares fundamentales para que continúe avanzando día a día.

MUCHAS GRACIAS A TODOS

Danny Elías Obando Yumbla

Índice

a. Título 11
b. Resumen 11
c. Antecedentes 1
d. Justificación 16
e. Objetivos 19
e.1. General 19
e.2. Específicos 19
f. Cuerpo del proyecto 19
f.1. El Problema 19
f.2. Análisis del problema y la solución 20
f.3. Desarrollo e implementación 22
f.3.1. Cronograma de trabajo 22
f.3.2. Fase de análisis 25
f.3.3. Fase de pruebas 30
f.3.4. Fase de producción 36
f.4. Presupuesto 42
f.5. Pruebas y Métricas 43
g. Resultados 53
h. Conclusiones 53
i. Recomendaciones 54
j. Trabajos futuros 54
k. Referencias 55
l. Glosario 56
m. Anexos 58
m.1. Anexo A: Instalación de software de monitoreo 60
m.2. Anexo B: Manual para instalar agente Zabbix en clientes Linux y Windows 67
m.3. Anexo C: Creación de mapa de red 79
m.4. Anexo D: Modificación de trigger para adaptarlo a la necesidad de la empresa 91

Índice de gráficos

Gráfico 1: Ubicación de puntos de acceso inalámbrico en Tuval. 11
Gráfico 2: Ubicación de puntos de acceso inalámbrico en Dimulti. 12
Gráfico 3: Ubicación de puntos de acceso inalámbrico en bodega central (Inmaconsa). 12
Gráfico 4: Ubicación de puntos de acceso inalámbrico en Quito. 13
Gráfico 5: Ubicación de puntos de acceso inalámbrico en Cuenca. 13
Gráfico 6: Ubicación de puntos de acceso inalámbrico en Santo Domingo. 14
Gráfico 7: Ubicación de puntos de acceso inalámbrico en Manta. 14
Gráfico 8: Diagrama de red de infraestructura mixta MPLS – Punto a Punto del grupo de empresas Tuval S.A., Dimulti S.A. y Castek S.A. 17
Gráfico 9: Diagrama físico de red del grupo de empresas. 18

Índice de imágenes

Imagen 1: Ubicación satelital de las oficinas en Guayaquil. 1
Imagen 2: Ubicación satelital de la oficina en Manta. 2
Imagen 3: Ubicación satelital de la oficina en Cuenca. 2
Imagen 4: Ubicación satelital de oficina en Quito. 3
Imagen 5: Ubicación satelital de oficina en Santo Domingo. 3
Imagen 6: Ubicación satelital de oficinas a nivel nacional. 4
Imagen 7: Servidor de base de datos Dell Power Edge T610. 5
Imagen 8: Servidor de aplicaciones web Dell Power Edge 840. 5
Imagen 9: Servidor de antivirus Acer Aspire AXC-603G. 6
Imagen 10: Servidor proxy – firewall Dell Power Edge SC430. 6
Imagen 11: Servidor de correos Dell Power Edge T110 II. 7
Imagen 12: Servidor de respaldos de archivos Dell Power Edge 830. 7
Imagen 13: Servidor de telefonía IP Tuval. 8
Imagen 14: Servidor de telefonía IP bodega central (Inmaconsa). 9
Imagen 15: Servidor de telefonía IP Dimulti. 9
Imagen 16: Servidor de telefonía IP Quito. 10
Imagen 17: Servidor de telefonía IP Manta. 10
Imagen 18: Torre con antena en Tuval. 15
Imagen 19: Torre con antena en bodega central (Inmaconsa). 15
Imagen 20: Software Nagios: Pantalla de bienvenida 31
Imagen 21: Software Nagios: Pantalla de creación de host 31
Imagen 22: Software Nagios: Reporte de disponibilidad 32
Imagen 23: Software Nagios: Reporte de incidencias 32
Imagen 24: Software Zabbix: Pantalla de bienvenida 33
Imagen 25: Software Zabbix: Pantalla de creación de host 33
Imagen 26: Software Zabbix: Reporte de disponibilidad 34
Imagen 27: Software Zabbix: Reporte de incidencias 34
Imagen 28: Software Zabbix: Reporte de uso de CPU de un host 35
Imagen 29: Software Zabbix: Configuración de host 37
Imagen 30: Software Zabbix: Configuración de plantilla 37
Imagen 31: Software Zabbix: Configuración de host 38
Imagen 32: Software Zabbix: Selección de Plantilla 38
Imagen 33: Software Zabbix: Selección de comunidad SNMP 38
Imagen 34: Software Zabbix: Vista de hosts 39
Imagen 35: Software Zabbix: Vista de host por grupo 40
Imagen 36: Software Zabbix: Vista de triggers 40
Imagen 37: Software Zabbix: Creación de triggers 41
Imagen 38: Software Zabbix: Configuración de zabbix 41
Imagen 39: Pruebas: Estado normal del procesador. 44
Imagen 40: Pruebas: Incremento al 96% de uso del procesador 44
Imagen 41: Pruebas: Pantalla de alarma 45
Imagen 42: Pruebas: Recepción de correo electrónico 45

Imagen 43: Pruebas: Recepción de texto 46
Imagen 44: Pruebas: Mapa de red mostrando error en dispositivo 46
Imagen 45: Pruebas: Recepción de correo electrónico 47
Imagen 46: Pruebas: Recepción de mensaje de texto 47
Imagen 47: Pruebas: Gráfico de actividad de tarjeta de red sin tráfico 48
Imagen 48: Pruebas: Mapa de red sin errores 48
Imagen 49: Pruebas: Transferencia de archivo 49
Imagen 50: Pruebas: Gráfico de actividad de tarjeta de red con poco tráfico 49
Imagen 51: Pruebas: Gráfico de actividad de tarjeta de red con tráfico medio 50
Imagen 52: Pruebas: Gráfico de actividad de tarjeta de red con tráfico alto 50
Imagen 53: Pruebas: Mapa de red con error en dispositivo 51
Imagen 54: Pruebas: Gráfico de tarjeta de red con saturación 51
Imagen 55: Pruebas: Recepción de correo electrónico 52
Imagen 56: Pruebas: Recepción de mensaje de texto 52
Imagen 57: Anexo A: Pantalla de bienvenida de Zabbix 61
Imagen 58: Anexo A: Tabla de verificación de Pre-requisitos 61
Imagen 59: Anexo A: Parámetros de configuración de base de datos 62
Imagen 60: Anexo A: Parámetros de configuración del puerto a usar 62
Imagen 61: Anexo A: Revisión de parámetros de configuración ingresados 63
Imagen 62: Anexo A: Confirmación de instalación exitosa 63
Imagen 63: Anexo A: Pantalla de acceso al programa 64
Imagen 64: Anexo A: Pantalla principal de Zabbix 64
Imagen 65: Anexo C: Pantalla de ingreso 79
Imagen 66: Anexo C: Creación de mapa 79
Imagen 67: Anexo C: Pantalla de configuración de mapas 80
Imagen 68: Anexo C: Pantalla que muestra los mapas creados 80
Imagen 69: Anexo C: Mesa de trabajo 81
Imagen 70: Anexo C: Agregar nuevo elemento 81
Imagen 71: Anexo C: Editar elemento 82
Imagen 72: Anexo C: Seleccionar host 82
Imagen 73: Anexo C: Lista de host 83
Imagen 74: Anexo C: Elección de tipo de gráfico 83
Imagen 75: Anexo C: Vista de mapa 84
Imagen 76: Anexo C: Configuración de nuevo host 84
Imagen 77: Anexo C: Elección de tipo de gráfico 85
Imagen 78: Anexo C: Vista de mapa de red 86
Imagen 79: Anexo C: Lista de dispositivos inalámbricos 86
Imagen 80: Anexo C: Vista de dispositivo con link hacia otro 87
Imagen 81: Anexo C: Vista de mapa de red 87
Imagen 82: Anexo C: Mensaje de advertencia 88
Imagen 83: Anexo C: Botón de actualizar mapa 88
Imagen 84: Anexo C: Vista de mapa de red 89
Imagen 85: Anexo D: Vista de mapa de red 91
Imagen 86: Anexo D: Ventana de propiedades de host 91

Imagen 87: Anexo D: Opción de trigger 92
Imagen 88: Anexo D: Expresión de trigger 92
Imagen 89: Anexo D: Opción de habilitar/desabilitar trigger 93
Imagen 90: Anexo D: Botón para crear un trigger 93
Imagen 91: Anexo D: Creación de nuevo trigger 93
Imagen 92: Anexo D: Vista de mapa 94
Imagen 93: Anexo D: Recepción de correo electrónico 95
Imagen 94: Anexo D: Recepción de mensaje de texto 95

Índice de tablas

Tabla 1: Comparación de funciones entre software opensource 30
Tabla 2: Costo de hora/hombre..... 42
Tabla 3: Costo de materiales/equipos 43

a. Título

Implementación de herramientas de software open source para monitorear los sistemas de comunicación de voz y datos de las empresas TUVAL S.A., DIMULTI S.A., y CASTEK S.A.

b. Resumen

Dentro del organigrama del grupo de empresas Tuval S.A., Dimulti S.A. y Castek S.A. existe un departamento que se encarga de dar el soporte a los usuarios en el ámbito informático y también de velar por que las redes de comunicaciones siempre se encuentren operativas.

Una de las problemáticas que posee este departamento es que no cuenta con ninguna herramienta tecnológica que le permita identificar los motivos por los cuales en muchas ocasiones por ejemplo existe lentitud en el sistema transaccional de la compañía, o lentitud en el servicio de internet.

Si hablamos de un problema relacionado con las redes de computadora vemos que son varios los factores que pueden afectar el rendimiento de la misma, puede que en un determinado momento se trate de un problema muy puntual con un equipo que está mostrando lentitud, pero también puede ser que existan otros elementos dentro de la red que puedan estar ocasionando dicha lentitud.

También hay que tomar en cuenta que en ocasiones los problemas de lentitud no tienen nada que ver con las comunicaciones sino que por ejemplo se puede deber a problemas con los servidores que pudieran estar bajo de recursos para la demanda que actualmente está atendiendo.

Es necesario siempre evaluar cada una de las variables que intervienen desde que inicia hasta que termina una comunicación para poder sacar una conclusión que no solo resuelva un problema puntual sino que ayude a prevenir que vuelva a suceder el problema con el mismo equipo o cualquier otro.

Con la ejecución y puesta en marcha de este proyecto se pretende tener una herramienta tecnológica que alerte de posibles fallos en los diversos equipos de comunicación y servidores que están presentes dentro de la infraestructura de red.

En la actualidad existen herramientas que evalúan los estados de los dispositivos o equipos que intervienen dentro de la red, esto brinda la capacidad de con un solo software poder monitorear por ejemplo el tráfico que está circulando por un ruteador o analizar el consumo del procesador que está teniendo en este momento uno de los servidores.

Es precisamente este tipo de herramientas con las que el departamento de redes y soporte a usuarios no cuenta y por ende no existe un mecanismo que le permita dar una respuesta inmediata en caso de presentarse algún problema con un equipo de comunicación o servidor.

Para solucionar este problema se plantea seleccionar un software para luego instalarlo y configurarlo con lo que se logrará monitorear los equipos de comunicación y servidores existentes dentro del grupo de empresas.

Este software fue seleccionado analizado varios que existen en el mercado sin olvidar que se debió cumplir con la política de la empresa que es la de usar de preferencia herramientas open source.

Los parámetros que se analizaron para seleccionar el software fueron:

- Interfaz Web
- Sistema de Alarmas
- Gráficas
- Reportes
- Open source
- Monitorear varios sistemas operativos
- Fácil de usar
- Envío de notificaciones vía correo electrónico y mensajes de texto
- Escalable y robusto

Luego de analizado y seleccionado el software se procedió a realizar la instalación en un servidor y se fueron agregando cada uno de los elementos que intervienen dentro de la infraestructura de la red.

Adicional a la monitorización de los elementos ya agregados al software también se configuraron las siguientes alarmas para que envíen correos electrónicos y mensajes de texto en caso de que se presenten cualquiera de ellas en cualquiera de los dispositivos:

- Para los servidores:
  - Carga de CPU.
  - Carga de memoria RAM.
  - Tráfico en cada tarjeta de red.
  - Tiempo fuera de actividad.
- Para los dispositivos de acceso inalámbrico:
  - Tiempo de actividad.
  - Carga del dispositivo.
  - Tiempo fuera de actividad.
  - Tráfico en las tarjetas de red lan e inalámbrica.
- Para los enlaces de datos:
  - Tiempo de actividad.
  - Paquetes pedidos.
  - Tiempo fuera de actividad.
  - Tráfico en las tarjetas.
  - Umbral de ancho de banda en tarjeta de red.

Este proyecto resultó muy beneficioso porque incluso durante el desarrollo del mismo se pudieron sacar conclusiones como por ejemplo que en una de las agencias se necesitaba incrementar el ancho de banda para que ayudar en la velocidad del sistema transaccional de la empresa, otra conclusión fue la de hacer una segmentación del ancho de banda de internet para poder equilibrar el uso del mismo de forma homogénea para todas las agencias.

Una vez concluida su instalación y configuración permitió tener un monitoreo que envíe notificaciones en el instante que está sucediendo la incidencia o problema y con esto se pudo dar soluciones anticipándonos al hecho de que sea un usuario el que nos de aviso del error o problema.

c. Antecedentes

Las compañías TUVAL S.A., DIMULTI S.A. y CASTEK S.A. se dedican a la compra y venta de artículos de ferretería industrial, siendo el sector industrial el principal consumidor de los bienes y servicios que las compañías ofrecen.

Las tres compañías están bajo una misma directiva y cumplen las disposiciones que esta crea conveniente.

Al tratarse de un grupo de empresas manejadas por una misma directiva, todo el personal administrativo y de servicio trabaja para cumplir con los requerimientos que tengan cualquiera de ellas.

El área informática está dividida en dos grupos, el área de desarrollo y el área de soporte usuarios y redes.

Las compañías TUVAL S.A. y DIMULTI S.A. poseen una oficina en Guayaquil cada una, se encuentran ubicadas en el Km. 11/2 y Km 7/2 vía a Daule respectivamente.

La compañía CASTEK S.A. posee oficinas en Quito, Manta, Cuenca y Santo Domingo.

Las tres compañías comparten una bodega central ubicada en Guayaquil en el Km. 10/2 vía a Daule denominada "Centro de Distribución" la cual se encarga de abastecer de mercadería a cada una de ellas.

Imagen 1: Ubicación satelital de las oficinas en Guayaquil.
Fuente: Google, DigitalGlobe

Imagen 2: Ubicación satelital de la oficina en Manta.
Fuente: Google, DigitalGlobe

Imagen 3: Ubicación satelital de la oficina en Cuenca.
Fuente: Google, DigitalGlobe

Imagen 4: Ubicación satelital de oficina en Quito.
Fuente: Google, DigitalGlobe

Imagen 5: Ubicación satelital de oficina en Santo Domingo.
Fuente: Google, Landsat

Imagen 6: Ubicación satelital de oficinas a nivel nacional.
Fuente: Google, Landsat

A nivel de infraestructura informática las tres compañías comparten los recursos de los distintos servidores que desempeñan diversas funciones, en la siguiente lista se detallan los que se encuentran funcionando de forma centralizada en la oficina Tuval:

- ✓ 1 Servidor de Base de datos.
- ✓ 1 Servidor de Aplicaciones Web.
- ✓ 1 Servidor de Antivirus.
- ✓ 1 Servidor Proxy.
- ✓ 1 Servidor de Correo.
- ✓ 1 Servidor de Respaldo de archivos.

Imagen 7: Servidor de base de datos Dell Power Edge T610.
Fuente: El Autor

Imagen 8: Servidor de aplicaciones web Dell Power Edge 840.
Fuente: El Autor

Imagen 9: Servidor de antivirus Acer Aspire AXC-603G.
Fuente: El Autor

Imagen 10: Servidor proxy – firewall Dell Power Edge SC430.
Fuente: El Autor

Imagen 11: Servidor de correos Dell Power Edge T110 II.
Fuente: El Autor

Imagen 12: Servidor de respaldos de archivos Dell Power Edge 830.
Fuente: El Autor

Cada agencia tiene funcionando en sus oficinas un servidor de Telefonía IP, en total son 7 servidores distribuidos de la siguiente manera:

- 1 Tuval.
- 1 Bodega Central (Inmaconsa).
- 1 Dimulti.
- 1 Castek Quito.
- 1 Castek Manta.
- 1 Castek Cuenca.
- 1 Castek Santo Domingo.

Imagen 13: Servidor de telefonía IP Tuval.
Fuente: El Autor

Imagen 14: Servidor de telefonía IP bodega central (Inmaconsa).
Fuente: El Autor

Imagen 15: Servidor de telefonía IP Dimulti.
Fuente: El Autor

Imagen 16: Servidor de telefonía IP Quito.
Fuente: El Autor

Imagen 17: Servidor de telefonía IP Manta.
Fuente: El Autor

En total el grupo de empresas tiene funcionando 12 servidores, 6 centralizados en la oficina de Tuval y 6 distribuidos en cada una de las agencias.

La cantidad de puntos de acceso inalámbrico son variados en cada empresa pero en total suman 18 dispositivos y todos son de marca Ubiquiti.

Los dispositivos de acceso inalámbrico tienen como nombre la siguiente formulación:

- Las dos primeras letras corresponden al tipo de dispositivo: AP
- Las cinco siguientes corresponden al modelo del equipo: Unifi
- Las siguientes letras corresponden a las oficina donde está instalado:
    - Tuv = Tuval
    - Dim = Dimulti
    - Inma = Inmaconsa
    - UIO = Quito
    - CUE = Cuenca
    - StoDgo = Santo Domingo
    - MTA = Manta
- Los dos números finales corresponden a la secuencia incremental del dispositivo instalado en la oficina.

En los siguientes gráficos del 18 al 24 se mostrará un plano de planta de cada una de las agencias con la ubicación de instalación de los dispositivos de acceso inalámbrico, los dispositivos fueron instalados dependiendo de la necesidad de cada agencia.

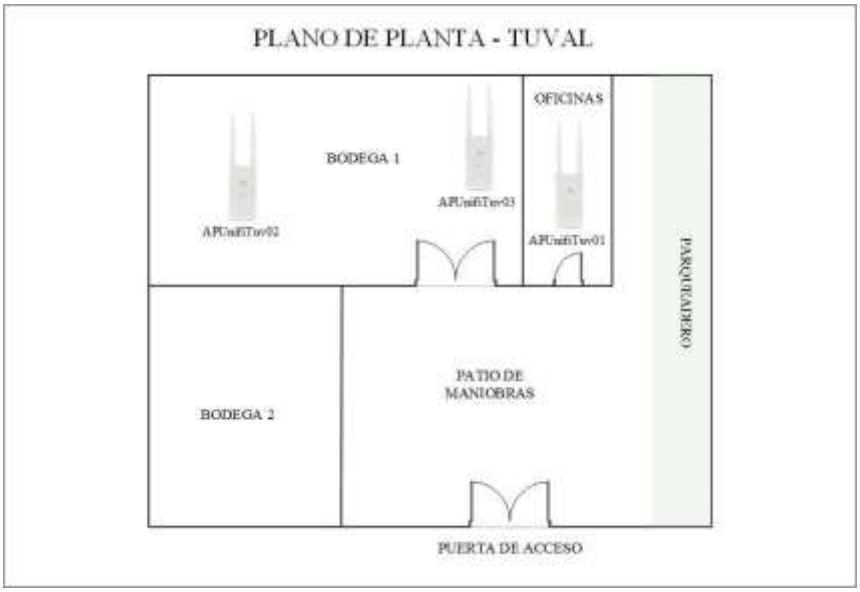


Gráfico 1: Ubicación de puntos de acceso inalámbrico en Tuval.
Fuente: El Autor

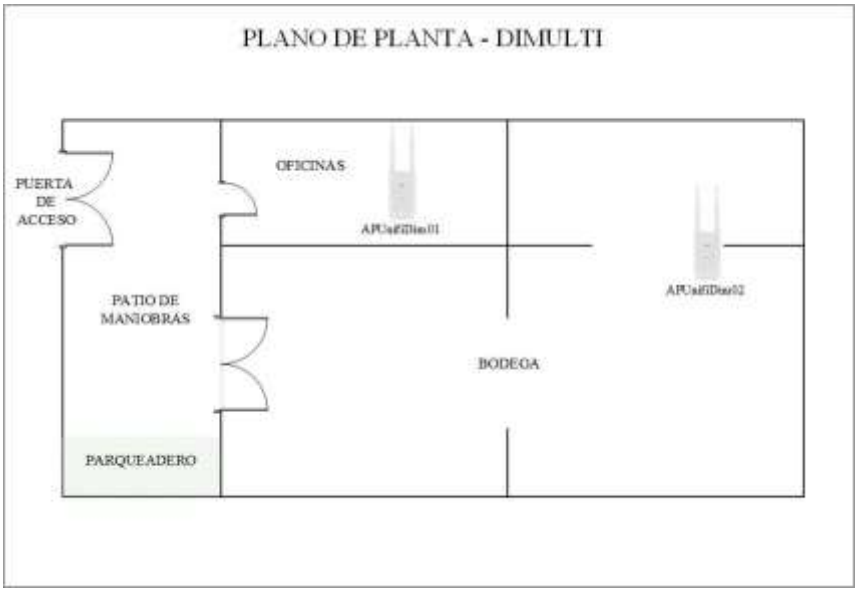


Gráfico 2: Ubicación de puntos de acceso inalámbrico en Dimulti.
Fuente: El Autor

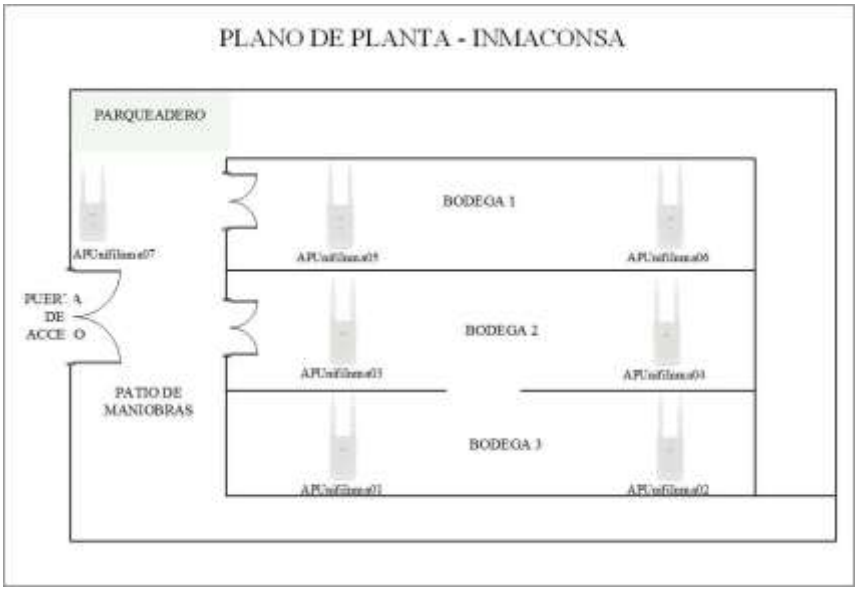


Gráfico 3: Ubicación de puntos de acceso inalámbrico en bodega central (Inmaconsa).
Fuente: El Autor

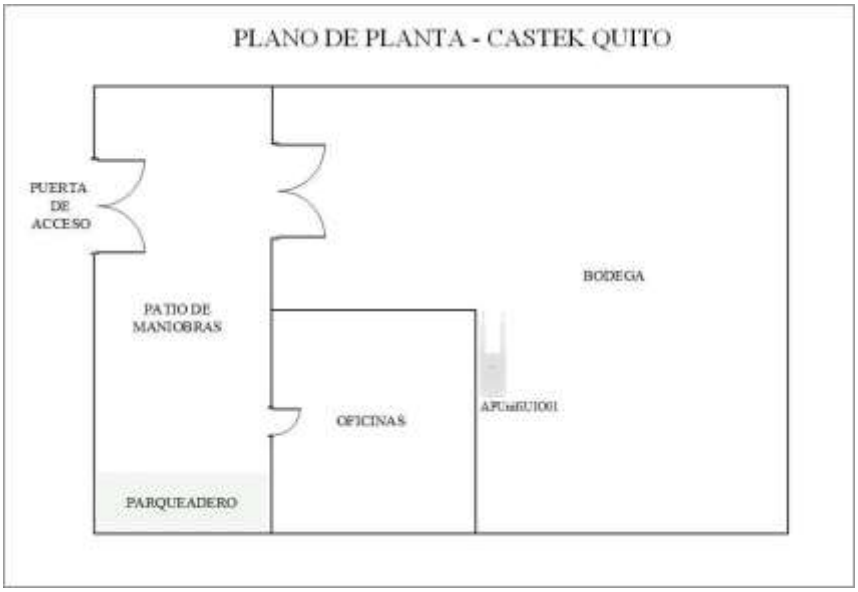


Gráfico 4: Ubicación de puntos de acceso inalámbrico en Quito.
Fuente: El Autor

Gráfico 5: Ubicación de puntos de acceso inalámbrico en Cuenca.
Fuente: El Autor

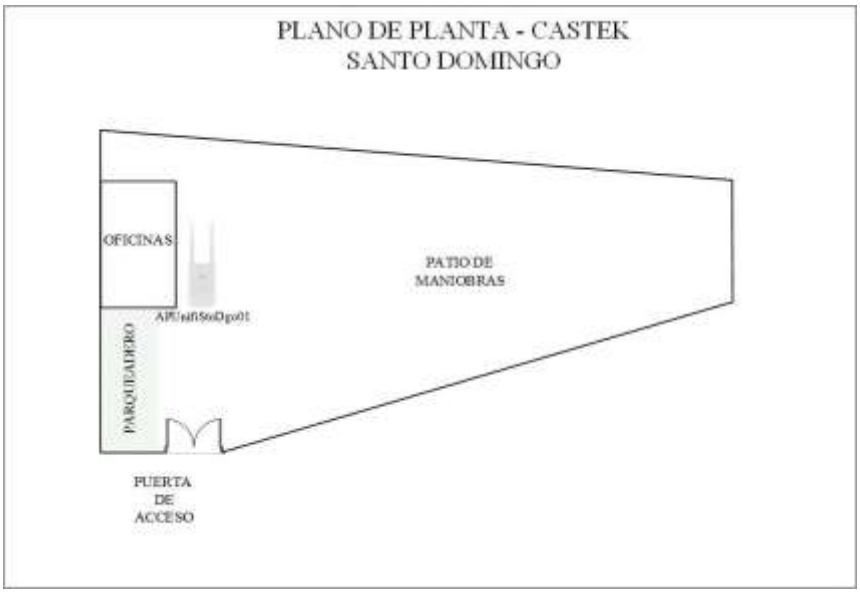


Gráfico 6: Ubicación de puntos de acceso inalámbrico en Santo Domingo.
Fuente: El Autor

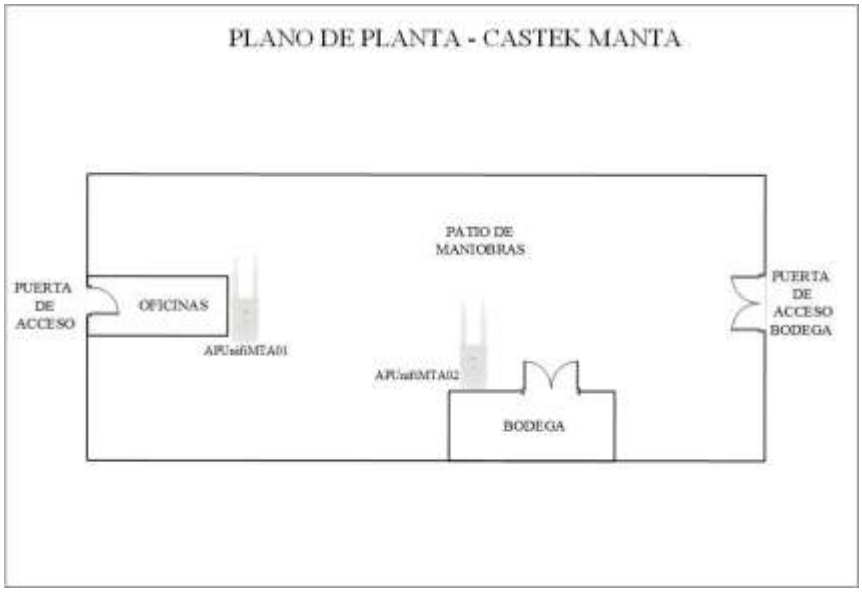


Gráfico 7: Ubicación de puntos de acceso inalámbrico en Manta.
Fuente: El Autor

Todas las empresas están conectadas mediante enlaces de datos brindados por la empresa Telconet S.A. y la oficina de TUVAL S.A. posee un enlace inalámbrico adicional hacia el "Centro de Distribución" denominado Inmaconsa.

Este enlace inalámbrico es parte inicial de un proyecto que en su etapa final pretende interconectar todas las agencias con enlaces propietarios, esta implementación se la realizó

instalando torres dentro de los terrenos de las oficinas y lo equipos de comunicación son de la marca Ubiquiti.

Imagen 18: Torre con antena en Tuval.
Fuente: El Autor

Imagen 19: Torre con antena en bodega central (Inmaconsa).
Fuente: El Autor

d. Justificación

Es importante para toda empresa el mantener siempre en funcionamiento los diversos servicios que permiten el normal desenvolvimiento de todos los empleados. En este grupo de servicios que son de vital importancia para las empresas se encuentran los servidores y las comunicaciones, siendo estos dos los responsables de los documentos electrónicos y de su correcta transmisión.

Tanto los servidores como las comunicaciones normalmente son componentes que para el común de los usuarios son imperceptibles y en algunos casos solo saben o se acuerdan que existen cuando sucede algún evento que no le permite empezar, continuar o terminar su tarea diaria.

Si lo vemos desde la perspectiva del usuario, la importancia que le da a los servidores o a las comunicaciones solo es cuando estos sufren un daño, pero para la directiva de una empresa; sea esta mediana o grande; estos dos elementos junto con el software transaccional o conjuntos de herramientas tecnológicas forman parte fundamental de los procesos de apoyo que tiene la cadena de valores en su organización.

Es por eso de la importancia de tener un departamento o persona que se haga responsable como administrador de la red de que todos los servidores y equipos de comunicación siempre estén funcionando de forma adecuada y que los enlaces se mantengan siempre operativos.

Y es que ante la multiplicación de servicios que existen en internet no es suficiente con solo mantener los equipos encendidos, sino de siempre estar monitoreando la actividad de los procesos, el tráfico que tengan los servidores y el tráfico de los datos que circulan por los enlaces de datos, todo esto con el fin de garantizar el correcto uso de los recursos y también poder establecer parámetros que permitan saber en qué momento se necesita de alguna renovación de hardware o un aumento del ancho de banda del canal de transmisión de datos.

La arquitectura que arme cada empresa para el ofrecimiento de los servicios a los usuarios es muy variada y siempre va a depender de las necesidades puntuales que tenga cada una, pero siempre va a ser necesario de una planificación inicial para establecer el lineamiento que se va a seguir y que en caso de un crecimiento no sea necesario realizar un cambio drástico de la arquitectura ya implementada.

En el caso particular de este grupo de empresas donde se va a plantear una solución de implementar herramientas de monitoreo hay que puntualizar que poseen una red de comunicación mixta que combina red tipo estrella internamente en cada oficina, MPLS para la comunicación entre ellas, una red inalámbrica punto a punto y posee servidores centralizados en la oficina de TUVAL S.A.

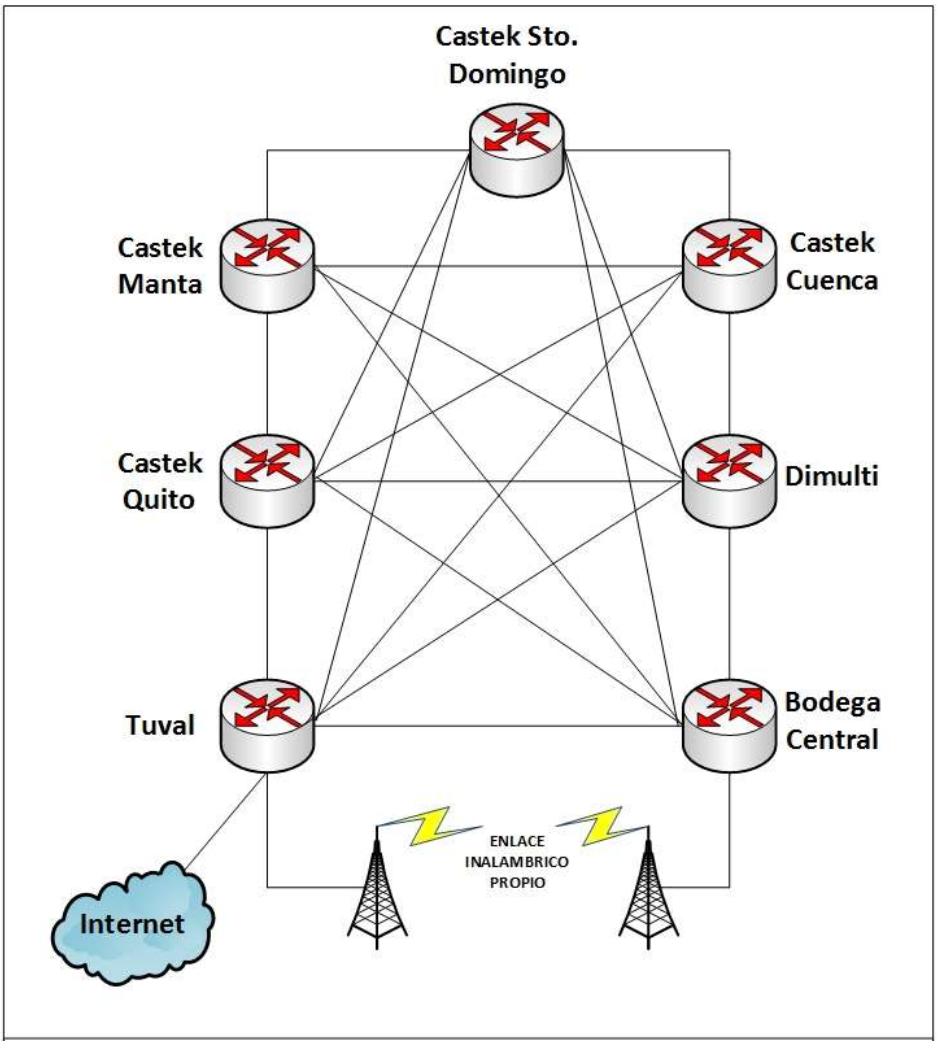


Gráfico 8: Diagrama de red de infraestructura mixta MPLS – Punto a Punto del grupo de empresas Tuval S.A., Dimulti S.A. y Castek S.A.
Fuente: El Autor

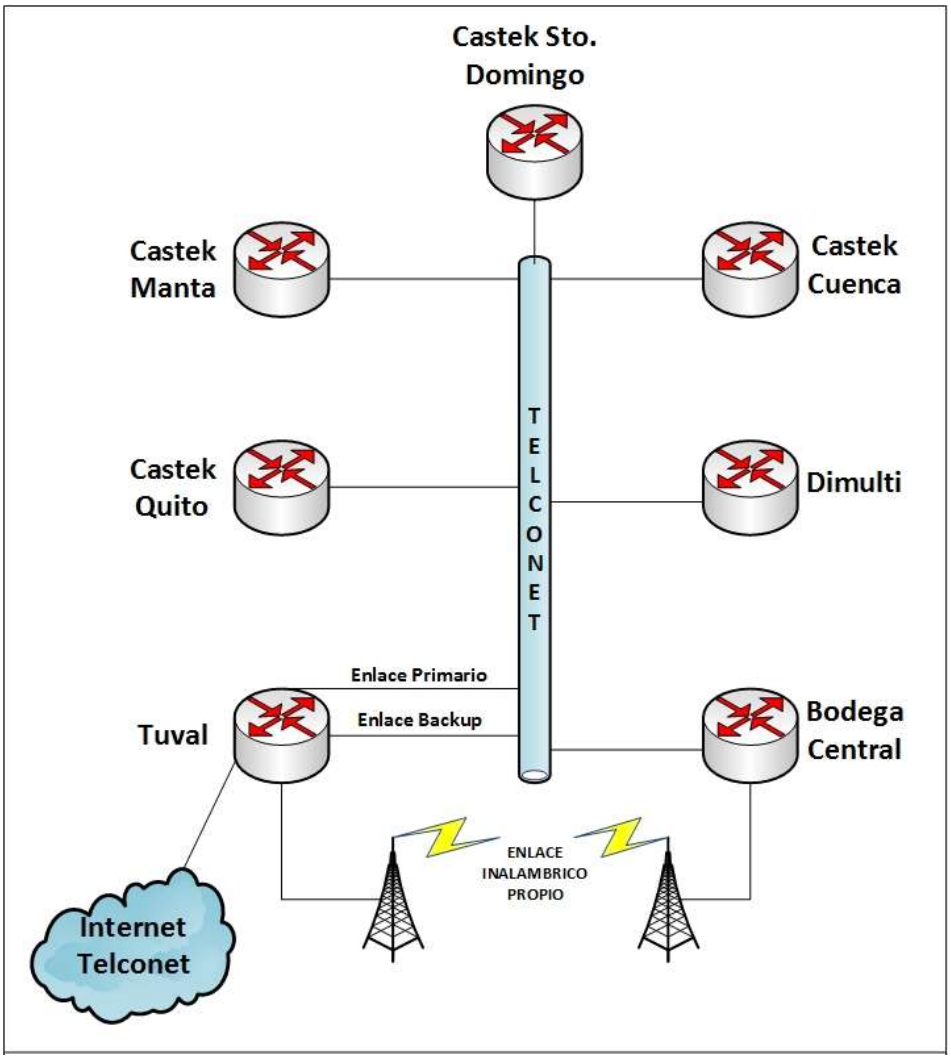


Gráfico 9: Diagrama físico de red del grupo de empresas.
Fuente: El Autor

El hecho de tener centralizados los servidores es el motivo por el cual es necesario que los enlaces de datos siempre estén operativos así como que los servidores siempre se encuentren activos para que las empresas puedan operar.

Uno de los servicios recientes que todas las empresas están obligadas a ir implementándolo poco a poco es el uso de documentos electrónicos autorizados por el Servicio de Rentas Internas del Ecuador organización que es la encargada del control y recolección de los impuestos del estado, por lo que para algunas empresas ya se volvió crítico el uso de internet, los enlaces de datos y de los servidores, puesto que en caso de que alguno de estos falle toda la operación de la o las empresas afectadas se detiene completamente.

e. Objetivos

e.1. General

Configurar un servidor utilizando herramientas open source que permitan visualizar el estado actual de todos los servidores, los enlaces de datos, puntos de accesos inalámbricos y salida hacia internet que poseen las tres compañías.

e.2. Específicos

- ✓ Analizar el software open source a usar.
- ✓ Implementar un laboratorio con las herramientas de software pre-seleccionadas.
- ✓ Realizar la instalación y configuración del servidor.

f. Cuerpo del proyecto

f.1. El Problema

El grupo de empresas ha ido creciendo paulatinamente con el transcurrir de los años a nivel empresarial, lo que equivale a mayor número de empleados, apertura de nuevas o ampliación de las agencias. Esto traducido en efectos reales para el departamento de redes y soporte a usuarios se había tornado en un desafío el poder brindar los servicios requeridos de forma óptima.

A medida que el grupo de empresas crecía se hacía absolutamente necesario potenciar los servidores que actualmente se tiene y en algunos casos reemplazar con nuevos y mejores, aumentar el canal de datos entre las agencias e incrementar el ancho de banda de salida hacia internet para poder cumplir con la demanda de recursos que poco a poco iban generando los usuarios.

Fue así como al día de hoy el grupo de empresas pasó a tener una infraestructura informática robusta que operada y administrada de forma correcta generaba una complacencia a la junta directiva y a todo el personal que labora para el grupo, pero para el área de soporte a usuarios y redes este incremento de la infraestructura informática poco a poco se fue convirtiendo en un dolor de cabeza por la administración de todos los equipos y enlaces que posee.

En la actualidad el grupo de empresas ya cuenta con 13 servidores, 18 puntos de acceso inalámbrico, 2 antenas para un enlace de radio, 7 ruteadores para los enlaces de datos para las seis agencias y 1 ruteador para la salida a internet.

Toda esta infraestructura informática no está deslindada a que en algún momento sufra un desperfecto ya sea que algún servidor falle o se corte la fibra de alguna de las agencias y

es ahí donde el área de soporte a usuarios y redes tiene que responder de forma ágil y oportuna en la resolución del problema.

Solo cuando algún componente de la infraestructura informática falla es cuando se dan cuenta de los problemas que trae consigo, por ejemplo al tener los servidores del sistema transaccional centralizados en las oficinas de Tuval siempre se va a estar expuesto a que con cualquier corte de servicio en alguna de las agencias se quede sin servicio y esto implica el que tengan que paralizar completamente la operación ya sean estas ventas, despachos o cobros hasta que el problema sea resuelto.

Este tipo de eventos donde se queden sin servicio o exista lentitud de los servicios informáticos en una o todas las agencias del grupo de empresas son las que pueden desencadenar en pérdidas económicas leves o muy graves.

Si vemos estos eventos desde la perspectiva del cliente podremos notar claramente que esto le causa una mala imagen y malestar trayendo como consecuencia que el cliente no compre o que comience a ver otras opciones de proveedores donde no solo tome en consideración el mejor precio sino agilidad en la compra y despacho.

Dependerá de que tan grave considere la junta directiva este tipo de acontecimientos para que se tomen medidas de carácter urgente para tratar en lo posible de minimizar cualquier tipo de incidencia y así que todos los departamentos de la organización pueden trabajar de forma armónica.

f.2. Análisis del problema y la solución

De forma ideal u optimista siempre se quiere que toda la infraestructura informática trabaje de forma normal, pero en efectos prácticos la realidad es que siempre hay equipos o enlaces que fallan y es ahí donde el departamento de soporte a usuario y redes tiene una falencia puesto que los tiempos de respuesta que toma el identificar y luego resolver el problema son elevados.

Los problemas que genera el fallo de un equipo de comunicación o de un servidor siempre van a depender del servicio que esté brindando, algunos fallos son considerados como críticos como por ejemplo el desperfecto del servidor de base de datos u otros considerados leves como por ejemplo el apagado de uno de los puntos de acceso inalámbrico, pero lo cierto es que ya sean estos críticos o leves siempre van a causar malestar en los usuarios.

Ningún equipo informático está exento de sufrir un desperfecto pero también hay situaciones que no necesariamente tienen que ver con un fallo pero que provocan lentitud o inhibición del equipo, por ejemplo puede darse el caso de que todos los equipos estén correctamente encendidos pero una de las agencias llame a reportar que no tiene sistema o que está lento, estos eventos también son necesarios considerar para que la solución a implementar sea de forma integral.

Tomando en cuenta que no es suficiente solo con comprobar que los servidores y equipos de comunicación se encuentren encendidos sino, que existen diversos tipos de mediciones que se pueden realizar para garantizar el correcto funcionamiento y prevenir de posibles problemas inmediatos o futuros en alguno de estos componentes es necesario tomar en cuenta otros parámetros en la implementación a realizar.

Entre los diferentes parámetros que nos pueden indicar una posible falla por ejemplo se encuentra el de temperatura de un servidor, este parámetro nos puede indicar una posible falla por sobre calentamiento que puede llegar hasta quemar la placa de base y traer graves problemas, claro está que siempre se va a depender del grado de profundidad que se le quiera dar al monitoreo y de que si el hardware de los equipos brinda la información necesaria para poder realizarla.

Como una solución que permita identificar posibles problemas en los servidores, enlaces de comunicación y puntos de acceso inalámbrico se decide realizar la instalación de un software de monitoreo donde se incluyan los equipos o servidores de la organización considerados como críticos reporten su estatus y genere alertas vía correo y mensajes de texto para que el personal del departamento de soporte a usuarios y comunicaciones tenga un reporte inmediato de la incidencia generada.

Los equipos o servidores de la organización considerados como críticos son:

- ✓ Servidores
  - 1 Servidor de Base de datos.
  - 1 Servidor de Aplicaciones Web.
  - 1 Servidor de Antivirus.
  - 1 Servidor Proxy.
  - 1 Servidor de Correo.
  - 1 Servidor de Respaldo de archivos.
  - 7 Servidores de telefonía IP:
    - 1 Tuval.
    - 1 Bodega Central (Inmaconsa).
    - 1 Dimulti.
    - 1 Castek Quito.
    - 1 Castek Manta.
    - 1 Castek Cuenca.
    - 1 Castek Santo Domingo.
- ✓ Equipos de acceso inalámbrico
  - 3 puntos de acceso inalámbrico en Tuval.
  - 7 puntos de acceso inalámbrico en Bodega Central (Inmaconsa)
  - 2 puntos de acceso inalámbrico en Dimulti.
  - 1 punto de acceso inalámbrico en Castek Quito.
  - 1 punto de acceso inalámbrico en Castek Manta.
  - 3 puntos de acceso inalámbrico en Castek Cuenca.
  - 1 punto de acceso inalámbrico en Castek Santo Domingo.

- 2 antenas de transmisión inalámbrica entre Tuval y Bodega Central (Inmaconsa).

Las mediciones que se van a tomar en cuenta en esta implementación son:

- Para los servidores:
  - Carga de CPU mayor al 50%.
  - Carga de memoria RAM mayor al 50%.
  - Saturación del tráfico en cada tarjeta de red.
  - Desconexión del equipo.
- Para los dispositivos de acceso inalámbrico:
  - Desconexión del equipo.
  - Carga del dispositivo mayor al 50%.
  - Saturación del tráfico en las tarjetas de red lan e inalámbrica.
- Para los enlaces de datos (ruteadores del proveedor):
  - Desconexión del equipo.
  - Paquetes perdidos superiores a 10.
  - Umbral de ancho de banda en tarjeta de red.

f.3. Desarrollo e implementación

El proyecto va a desarrollarse en tres fases:

- Fase de análisis
- Fase de pruebas
- Fase de producción

f.3.1.Cronograma de trabajo

La ejecución de este proyecto se realizó en base al siguiente horario:

CALENDARIO BASE: Día	Calendario Proyecto Horas
lunes	10:00 - 13:00, 14:00 - 17:30
martes	10:00 - 13:00, 14:00 - 17:30
miércoles	10:00 - 13:00, 14:00 - 17:30
jueves	10:00 - 13:00, 14:00 - 17:30
viernes	10:00 - 13:00, 14:00 - 17:30
sábado	9:00 - 12:30
domingo	No laborable
Excepciones:	Ninguna

Se usaron 5 horas diarias de lunes a viernes y los días sábados se usarán 3 horas y medias adicionales por lo que semanalmente sumaron 28 horas y medias.

Para la culminación del proyecto se usaron 64 horas para las sesiones con el tutor en horarios y fechas que se coordinaron y de 336 horas con las que se lograron completar las 4 fases contempladas en este proyecto.

Calendario Proyecto

desde lun 30/11/15

Fechas			
Comienzo:	vie 17/07/15	Fin:	mar 03/11/15
Comienzo línea	NOD	Fin línea de base:	NOD
Comienzo real:	NOD	Fin real:	NOD
Variación de co	0 días	Variación de fin:	0 días

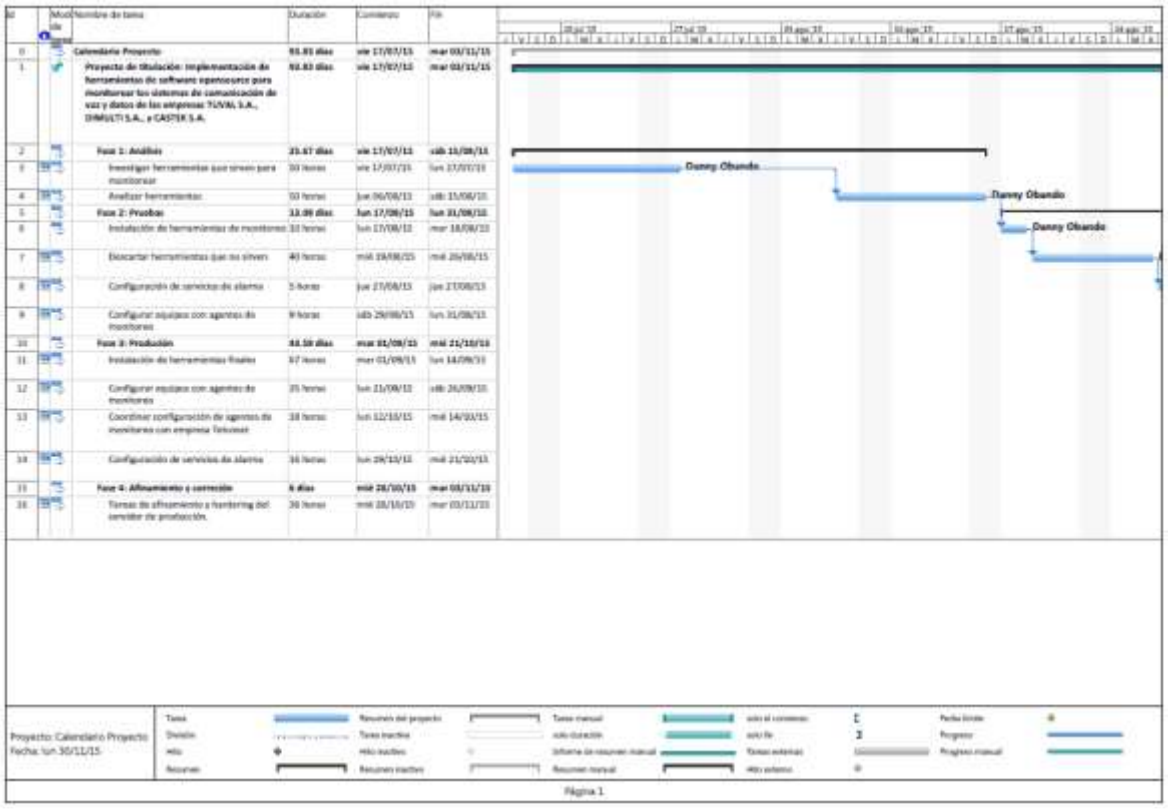
Duración			
Programada:	93.83 días	Restante:	93.83 días
Prevista:	0 días	Real:	0 días
Variación:	93.83 días	Porcentaje completado:	0%

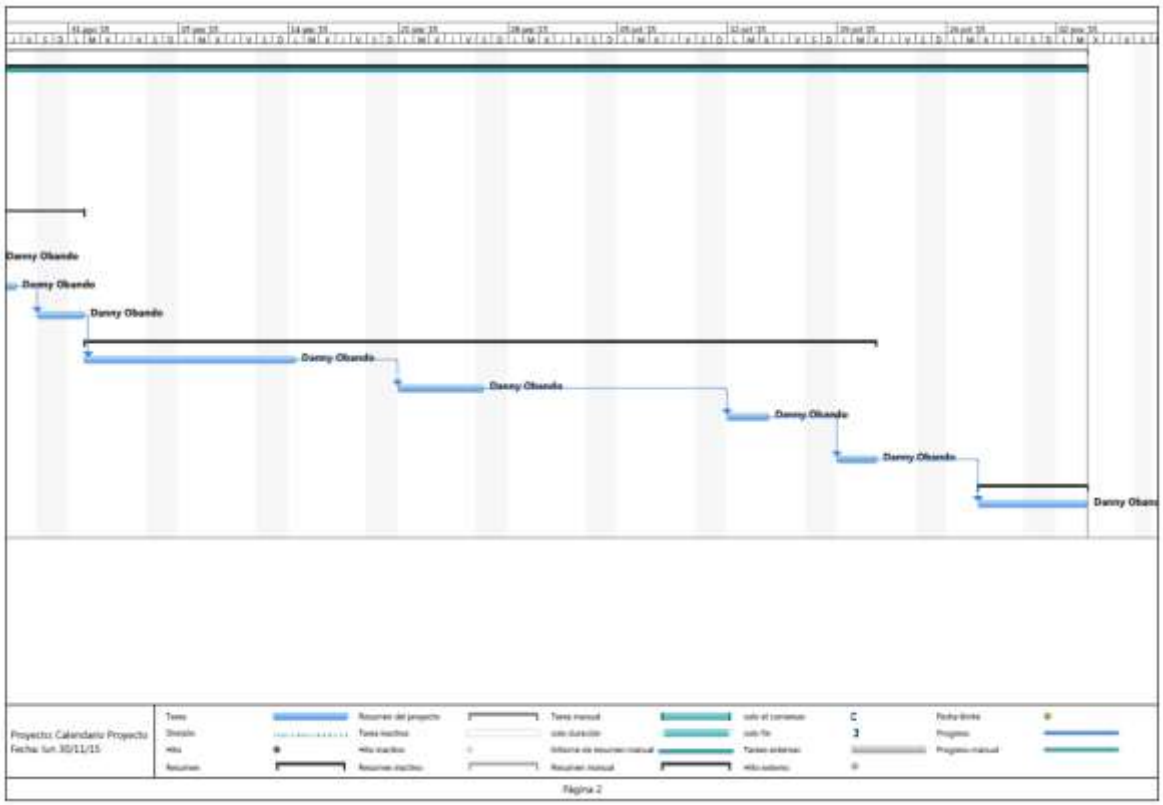
Trabajo			
Programado:	336 horas	Restante:	336 horas
línea de base:	0 horas	Real:	0 horas
Variación:	336 horas	Porcentaje completado:	0%

Costos			
Programados:	$ 8,400.00	Restantes:	$ 8,400.00
línea de bases:	$ 0.00	Reales:	$ 0.00
Variación:	$ 8,400.00		

Estado de las tareas		Estado de los recursos	
Tareas aún no comenzadas:	16	Recursos de trabajo:	1
Tareas en curso:	0	Recursos de trabajo sobreasigna	0
Tareas finalizadas:	0	Recursos materiales:	0
Total de tareas:	16	Total de recursos:	1

El cronograma de actividades del uso de las 336 horas en el horario especificado se representará en el siguiente diagrama de Gantt.


Id
Modo de tarea
Nombre de tarea
Duración
Comienzo
Fin
0 Calendario Proyecto 93.83 días vie 17/07/15 mar 03/11/15
1 Proyecto de titulación: Implementación de herramientas de software opensource para monitorear los sistemas de comunicación de voz y datos de las empresas TUVAL S.A., UNILIT! S.A., y CASTER S.A. 93.83 días vie 17/07/15 mar 03/11/15
2 Fase 1: Análisis 23.67 días vie 17/07/15 sáb 15/08/15
3 Investigar herramientas que sirven para monitorear 10 horas vie 17/07/15 lun 17/07/15
4 Analizar herramientas 10 horas jue 06/08/15 sáb 15/08/15
5 Fase 2: Pruebas 12.08 días lun 17/08/15 lun 31/08/15
6 Instalación de herramientas de monitoreo 10 horas lun 17/08/15 mar 18/08/15
7 Descartar herramientas que no sirven 40 horas mié 19/08/15 mié 26/08/15
8 Configuración de servicios de alarma 5 horas jue 27/08/15 jue 27/08/15
9 Configurar equipos con agentes de monitoreo 9 horas sáb 29/08/15 lun 31/08/15
10 Fase 3: Producción 44.58 días mar 01/09/15 mié 21/10/15
11 Instalación de herramientas finales 67 horas mar 01/09/15 lun 14/09/15
12 Configurar equipos con agentes de monitoreo 35 horas lun 21/09/15 sáb 26/09/15
13 Coordinar configuración de agentes de monitoreo con empresa Telcosat 18 horas lun 12/10/15 mié 14/10/15
14 Configuración de servicios de alarma 16 horas lun 19/10/15 mié 21/10/15
15 Fase 4: Afinamiento y corrección 6 días mié 28/10/15 mar 03/11/15
16 Tareas de afinamiento y hardening del servidor de producción 30 horas mié 28/10/15 mar 03/11/15
Danny Obando
Danny Obando
Danny Obando
Danny Obando
Proyecto: Calendario Proyecto
Fecha: lun 30/11/15
Página 1


Danny Obando
Danny Obando
Danny Obando
Danny Obando
Danny Obando
Danny Obando
Danny Obando
Danny Obando
Proyecto: Calendario Proyecto
Fecha: lun 30/11/15
Página 2

f.3.2.Fase de análisis

La junta directiva de las empresas Tuval S.A., Dimulti S.A. y Castek S.A. tiene como uno de sus ejes en inversión tecnológica el uso de herramientas open source por lo que uno de los factores a analizar del software a instalar es que sea un producto open source.

Dentro de la búsqueda que se realizó en distintos foros de monitoreo se encontraron que las opciones de software open source a analizar son las siguientes:

- Cacti
- Nagios
- Munin
- Zenoss
- Zabbix

A continuación se pone una breve descripción sacada de la web oficial de los desarrolladores de cada una de las herramientas a analizar.

Cacti

Es una interfaz completa de RRDTool, almacena toda la información necesaria para crear gráficos y rellenar con los datos una base de datos MySQL. La interfaz está manejada por PHP. Además de ser capaz de manejar los gráficos, fuentes de datos, y archivos Round Robin en una base de datos, Cacti se encarga de la recogida de datos. También hay soporte SNMP para la creación de gráficos de tráfico con MRTG. (The Cacti Group, Inc, 2004-2012)

Fuentes de datos

Para manejar la recolección de datos, se puede alimentar Cacti vía cualquier script / comando externo junto con los datos que el usuario tendrá que "rellenar", Cacti entonces recopila estos datos en un tarea programada y rellena una base de datos MySQL o los archivos round robin. (The Cacti Group, Inc, 2004-2012)

Las fuentes de datos también se pueden crear, que corresponden a los datos reales en el gráfico. Por ejemplo, si un usuario quisiera graficar los tiempos de ping a un host, puede crear una fuente de datos utilizando un script que hace ping un host y devuelve su valor en milisegundos. Después de definir las opciones de RRDTool como la forma de almacenar los datos que usted será capaz de definir cualquier información adicional

que la fuente de entrada de datos requiere, como un anfitrión para hacer ping en este caso. Una vez que se crea una fuente de datos, que se mantiene de forma automática en intervalos de 5 minutos. (The Cacti Group, Inc, 2004-2012)

Gráficos

Una vez que una o más fuentes de datos se definen, un gráfico de RRDTool se puede crear con los datos. Cacti le permite crear casi cualquier gráfico RRDTool imaginables utilizando todos los tipos estándar de gráfico RRDTool y funciones de consolidación. Un área de selección de color y la función automática de relleno de texto también ayudan en la creación de gráficos para hacer el proceso más fácil. (The Cacti Group, Inc, 2004-2012)

No sólo se puede crear gráficos basados RRDTool en Cacti, pero hay muchas formas de mostrar ellos. Junto con una "vista de lista" estándar y un "modo de vista previa", que se asemeja a la interfaz RRDtool, hay una "vista de árbol", lo que le permite poner gráficos en un árbol jerárquico para los propósitos de la organización. (The Cacti Group, Inc, 2004-2012)

Gestión de usuarios

Debido a las muchas funciones de Cacti, una herramienta de gestión basada en el usuario está construido en lo que puede añadir usuarios y darles derechos a ciertas áreas de Cacti. Esto permitiría a alguien crear algunos usuarios que pueden cambiar los parámetros del gráfico, mientras que otros sólo pueden visualizar las gráficas. Cada usuario también mantiene su propia configuración cuando se trata de gráficos de visualización. (The Cacti Group, Inc, 2004-2012)

Plantillas

Por último, Cacti es capaz de escalar a un gran número de fuentes de datos y gráficos mediante el uso de plantillas. Esto permite la creación de una plantilla de gráfico o fuente de datos únicos que define cualquier fuente gráfico o los datos asociados con él. Plantillas de host permiten definir las capacidades de un host para Cacti pueden sondear para información sobre la adición de un nuevo huésped. (The Cacti Group, Inc, 2004-2012)

Nagios

Lanzado por primera vez en 1999, Nagios ha crecido hasta incluir a miles de proyectos desarrollados por la comunidad Nagios en todo el mundo. Nagios es patrocinado oficialmente por Nagios Enterprises, que apoya a la comunidad en un número de diferentes maneras a través de las ventas de sus productos y servicios comerciales. (Nagios Entreprises, 2009-2016)

Nagios controla toda su infraestructura de TI para asegurar que los sistemas, aplicaciones, servicios y procesos de negocio están funcionando correctamente. En el caso de una falla, Nagios puede alertar al personal técnico del problema, lo que les permite comenzar los procesos de remediación antes que los cortes afecten a los procesos de negocio, usuarios finales o clientes. Con Nagios usted nunca dejará de tener que explicar por qué un corte de la infraestructura no se ve herido la rentabilidad de su organización. (Nagios Entreprises, 2009-2016)

¿**Qué provee Nagios?**

Diseñado con la escalabilidad y flexibilidad en mente, Nagios le da la tranquilidad de saber que viene de conocer los procesos de negocio de su organización no se verá afectada por los cortes de desconocidos. (Nagios Entreprises, 2009-2016)

Nagios es una poderosa herramienta que le proporciona la conciencia inmediata de la infraestructura de TI de misión crítica de su organización. Nagios le permite detectar y reparar problemas y mitigar futuras ediciones antes de que afecten a los usuarios finales y clientes. (Nagios Entreprises, 2009-2016)

(Nagios Entreprises, 2009-2016) Mediante el uso de Nagios, puede:

- Planee para las mejoras de infraestructura antes que los sistemas obsoletos causan fallas
- Responder a las cuestiones a la primera señal de un problema
- Reparar automáticamente los problemas cuando se detectan
- Coordinar las respuestas del equipo técnico
- Asegurarse de que las interrupciones de infraestructura tienen un efecto mínimo en la rentabilidad de su organización
- Supervisar toda su infraestructura y procesos empresariales

Munin

Munin presenta toda la información en gráficos a través de una interfaz web. Su énfasis está en la capacidad de ser Plug and Play. Después de completar una instalación de un gran número de plugins de monitoreo estará jugando sin más esfuerzo. (Edgewall Software, 2003-2013)

Usando Munin se puede controlar fácilmente el rendimiento de sus ordenadores, redes, redes SAN, aplicaciones, mediciones meteorológicas y todo lo que viene a la mente. Esto hace que sea fácil de determinar "lo que es diferente hoy" cuando un problema de rendimiento surge. Esto hace que sea fácil de ver cómo lo está haciendo capacidad sabio en cualquier recurso. (Edgewall Software, 2003-2013)

Munin utiliza la excelente RRDTool (escrito por Tobi Oetiker) y el marco está escrito en Perl, mientras que los plugins pueden ser escritos en cualquier idioma. Munin tiene una Arquitectura nodo principal en el que el maestro se conecta a todos los nodos a intervalos regulares y les pide datos. A continuación, almacena los datos en ficheros RRD, y (si es necesario) actualiza los gráficos. Uno de los objetivos principales ha sido la facilidad de crear nuevos plugins (gráficos). (Edgewall Software, 2003-2013)

Zenoss

Zenoss Core es un software de monitoreo IT Open Source galardonado que ofrece visibilidad de toda la infraestructura de IT, desde los dispositivos de red hasta las aplicaciones. Las características incluyen la detección automática, monitoreo de la disponibilidad, gráficos de rendimiento, alerta sofisticada, un portal web fácil de usar y mucho más. (Zenoss, Inc., 2005-2015)

Zabbix

"Es un software de nivel empresarial diseñado para monitoreo de alta disponibilidad y rendimiento de toda la infraestructura informática. Zabbix es open source y no tiene costo." (Zabbix LLC., 2001-2016)

Con Zabbix es posible reunir virtualmente ilimitadamente información de la red. Alto rendimiento de monitoreo en tiempo real de miles de servidores, máquinas virtuales y dispositivos de red pueden ser monitoreados simultáneamente. Junto con el almacenamiento de datos, están disponibles características de visualización (mapas, gráficos, etc.) así como manera muy flexibles de analizar los datos con el fin de alertar. (Zabbix LLC., 2001-2016)

Zabbix ofrece un gran rendimiento para la recopilación de datos y se puede escalar en ambientes muy grandes. Opciones de monitorización distribuidos están disponibles con el uso de proxies Zabbix. Viene con una interfaz basada en la web, autenticación de usuario segura y un esquema de permisos de usuarios muy flexible. El sondeo y captura se admite con agentes de alto rendimiento nativo que recolecta datos desde prácticamente cualquier de los sistemas operativos más populares; otros métodos de monitoreo sin agentes también están disponibles. (Zabbix LLC., 2001-2016)

Monitoreo web, así como la supervisión de máquinas virtuales de VMware es posible con Zabbix. Puede descubrir automáticamente servidores y dispositivos de la red, así como realizar el descubrimiento a bajo nivel con los métodos de asignación automática de controles de rendimiento y disponibilidad a las entidades descubiertas. (Zabbix LLC., 2001-2016)

¿Por qué elegir Zabbix?

(Zabbix LLC., 2001-2016) Hay muchas razones para elegir Zabbix sobre sus competidoras. La mejor manera de asegurarse de que es la opción número 1 para su organización es dándole una oportunidad. Antes de empezar sin embargo debe de considerar los siguientes beneficios del uso de Zabbix:

- Zabbix ofrece la libertad de utilizar esta solución opensource sin dependencia de un proveedor y el código fuente es de libre acceso.
- La instalación y configuración de Zabbix es muy fácil, por lo tanto posee una baja curva de aprendizaje.
- Los agentes Zabbix son altamente eficientes para las plataformas basadas en UNIX y Windows (x32, x64, Itanium) por lo que proporcionan capacidades de supervisión más amplias y a mayor velocidad.

- Un sistema de monitoreo centralizado permite almacenar toda la información (datos de configuración y rendimiento) en una base de datos relacional para el procesamiento más fácil y re-usando los datos.
- Rica capacidad de visualización permiten trabajar con sus datos más rápido e inteligentemente.
- Construido bajo procedimientos que permiten mantener sus datos bien organizados.

Característica	Cacti	Nagios	Munin	Zenoss	Zabbix
Interfaz Web	X	X	X	X	X
Alarmas	X	X	X	X	X
Gráficas	X	X	X	X	X
Reportes		X		X	X
Open Source	X		X	X	X
Distintos Sistemas Operativos		X			X
Fácil de usar		X			X
Envía notificaciones email, mensajes de texto		X			X
Escalable y robusto		X			X

Tabla 1: Comparación de funciones entre software opensource
Fuente: El Autor

Las dos mejores opciones para realizar la fase de pruebas son el software Nagios y Zabbix, ambos tienen versiones pagadas pero en la siguiente fase se analizará si la versión open source brinda las opciones requeridas.

f.3.3.Fase de pruebas

Una vez obtenidas y clasificadas las herramientas pre-seleccionadas se armó un laboratorio donde se instalaron de una forma lógica y ordenada todo ese software.

Capturas de pantallas de software Nagios

Imagen 20: Software Nagios: Pantalla de bienvenida
Fuente: El Autor

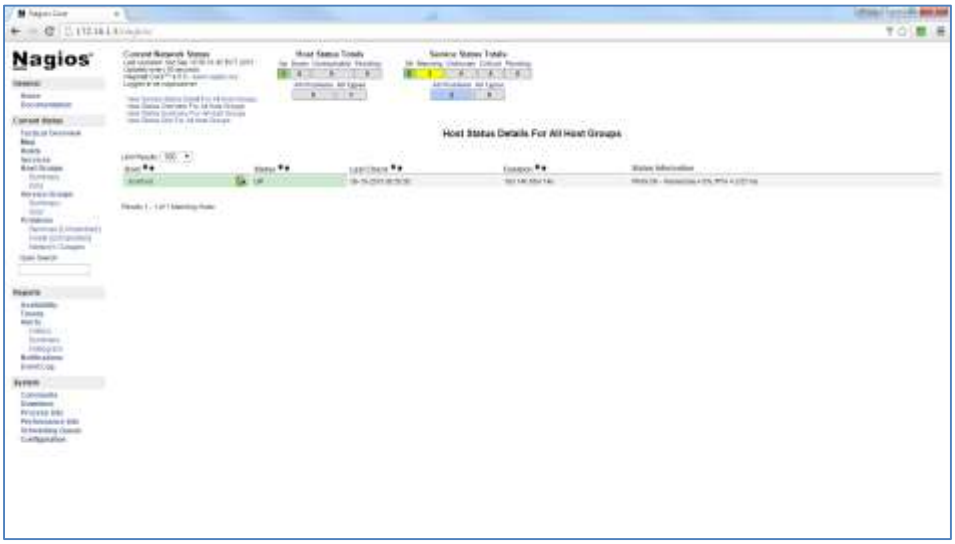


Imagen 21: Software Nagios: Pantalla de creación de host
Fuente: El Autor

Imagen 22: Software Nagios: Reporte de disponibilidad
Fuente: El Autor

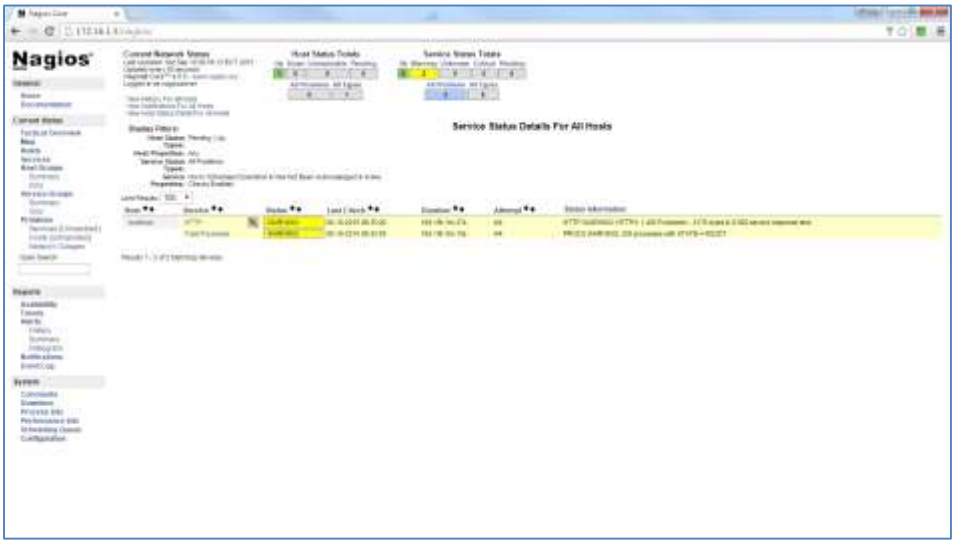


Imagen 23: Software Nagios: Reporte de incidencias
Fuente: El Autor

Pros:

- Fácil de instalar.

Contras:

- Creación de host mediante línea de comandos.
- Pobre interfaz web.
- Reportes básicos.
- Prácticamente todo se configura en línea de comandos.

Capturas de pantallas de software Zabbix

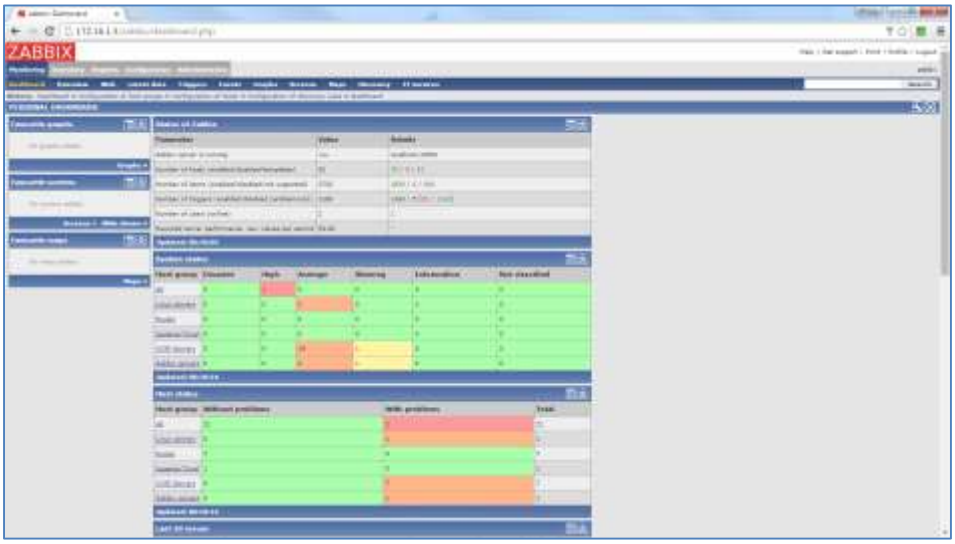


Imagen 24: Software Zabbix: Pantalla de bienvenida
Fuente: El Autor

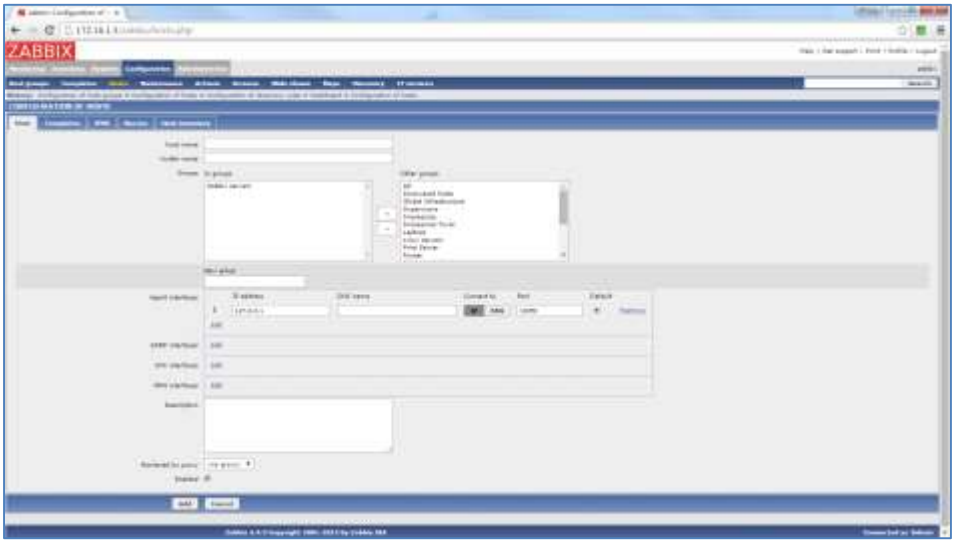


Imagen 25: Software Zabbix: Pantalla de creación de host
Fuente: El Autor

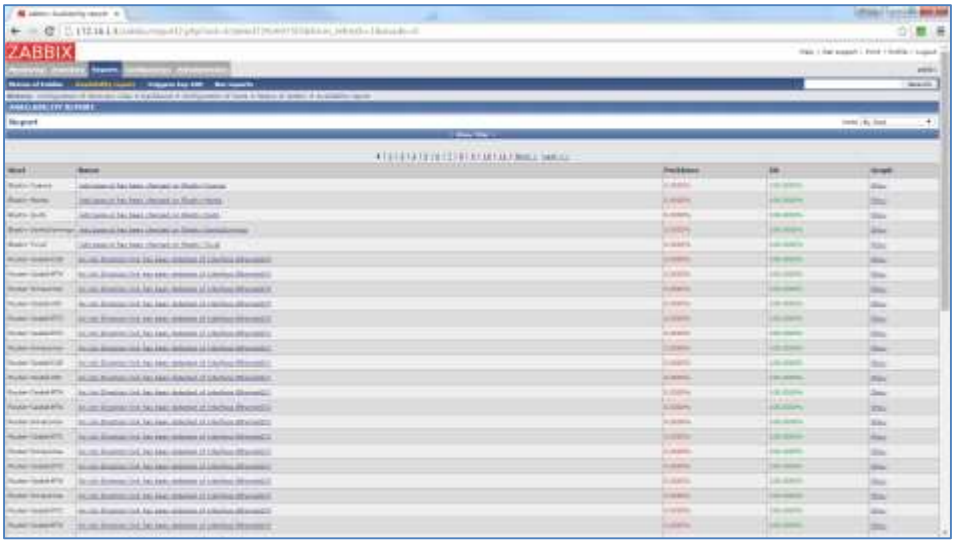


Imagen 26: Software Zabbix: Reporte de disponibilidad
Fuente: El Autor

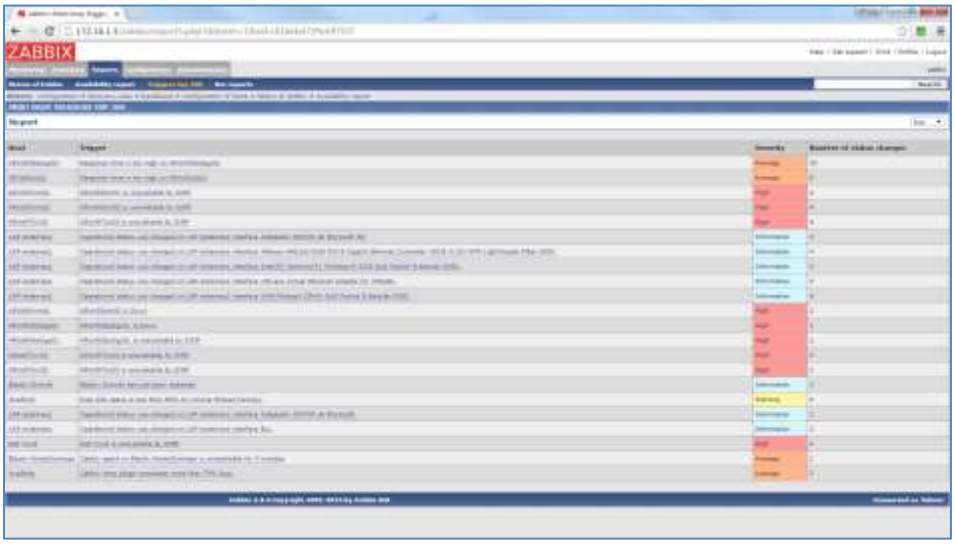


Imagen 27: Software Zabbix: Reporte de incidencias
Fuente: El Autor

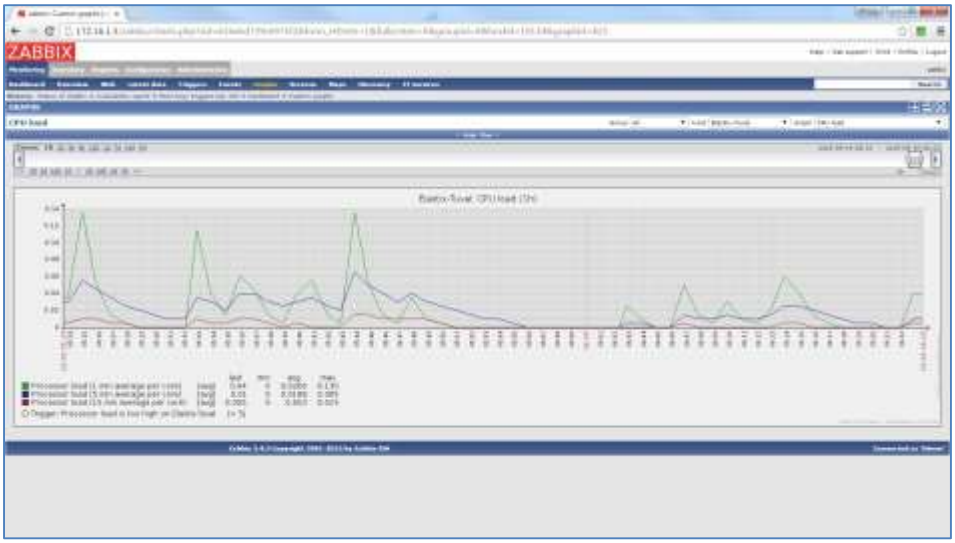


Imagen 28: Software Zabbix: Reporte de uso de CPU de un host
Fuente: El Autor

Pros:

- Buena interfaz gráfica.
- Toda la configuración se la realiza vía web.
- Reportes variada.
- Emisión de alertas vía correo electrónico.

Contras:

- No es sencilla la configuración.

Dentro de las pruebas que se desarrollaron se consideró que la herramienta de monitoreo sea capaz de emitir alarmas basadas en los siguientes parámetros:

- Para los servidores:
  - Carga de CPU.
  - Carga de memoria RAM.
  - Tráfico en cada tarjeta de red.
  - Tiempo fuera de actividad.
- Para los dispositivos de acceso inalámbrico:
  - Tiempo de actividad.
  - Carga del dispositivo.
  - Tiempo fuera de actividad.
  - Tráfico en las tarjetas de red lan e inalámbrica.
- Para los enlaces de datos:
  - Tiempo de actividad.
  - Paquetes pedidos.
  - Tiempo fuera de actividad.

    - Tráfico en las tarjetas.
    - Umbral de ancho de banda en tarjeta de red.
- Reporte de incidencias.
- Histórico de incidencias.

La emisión de mensajes de texto y de correos electrónicos deberá de ser capaz de enviar información relacionada específicamente con la incidencia ocurrida, con esto la persona que lo reciba puede tomar acciones inmediatas sabiendo a detalle del problema que está sucediendo.

Al finalizar las pruebas en ambos se decide que la mejor opción es la implementación del software Zabbix para poner en producción por los pros mencionados.

f.3.4.Fase de producción

Se procedió a realizar la instalación del servidor Zabbix como se muestra en el Anexo A.

En Zabbix existen los Templates que son archivos XML donde se están especificados todos los parámetros del host como por ejemplo los MIB, reportes, triggers (alertas/disparadores).

Todos los fabricantes publican los MIB para cada uno de sus productos, normalmente estos MIB son los mismos independientemente del fabricante pero si suele pasar que cambian uno que otro parámetro.

Dentro del foro de la comunidad Zabbix existen personas que han creado sus propias plantillas con opciones específicas para cada servicio o equipo, con esto se logra que el software muestre la información detalla y concreta del producto y no de forma general, por ejemplo si uso una plantilla para ruteadores me mostrará una lista de 20 interfaces de red, en cambio sí logro encontrar la plantilla de router cisco modelo 1811 me mostrará solo las 4 interfaces que posee.

Creación de host con agente de monitoreo Zabbix

La creación del host comprende de dos partes, una consiste en instalar el agente de monitoreo en cada una de los equipos a monitorear (Ver Anexo B) y la otra de crearlo en el servidor.

Para crearlo en el servidor nos dirigimos a:

Configuration → Host → New host
Es necesario llenar los siguientes campos:

- ***Host name***: Nombre del host.
- ***Visible name***: El nombre que aparece en los reportes.
- ***Groups***: Se puede crear uno nuevo o asignarlo a alguno existente.

- ***Agent interfaces***: Si hemos instalado el agente de Zabbix en el equipo remoto es necesario llenar este campo con la dirección IP y el puerto de comunicación.
- ***SNMP Interfaces***: Este parámetro normalmente es usado en los equipos como ruteadores o dispositivos de acceso inalámbrico, si lo queremos usar debemos de escribir la dirección IP y el puerto de comunicación.
- ***Enabled***: Con esto podemos habilitar o deshabilitar el host creado.

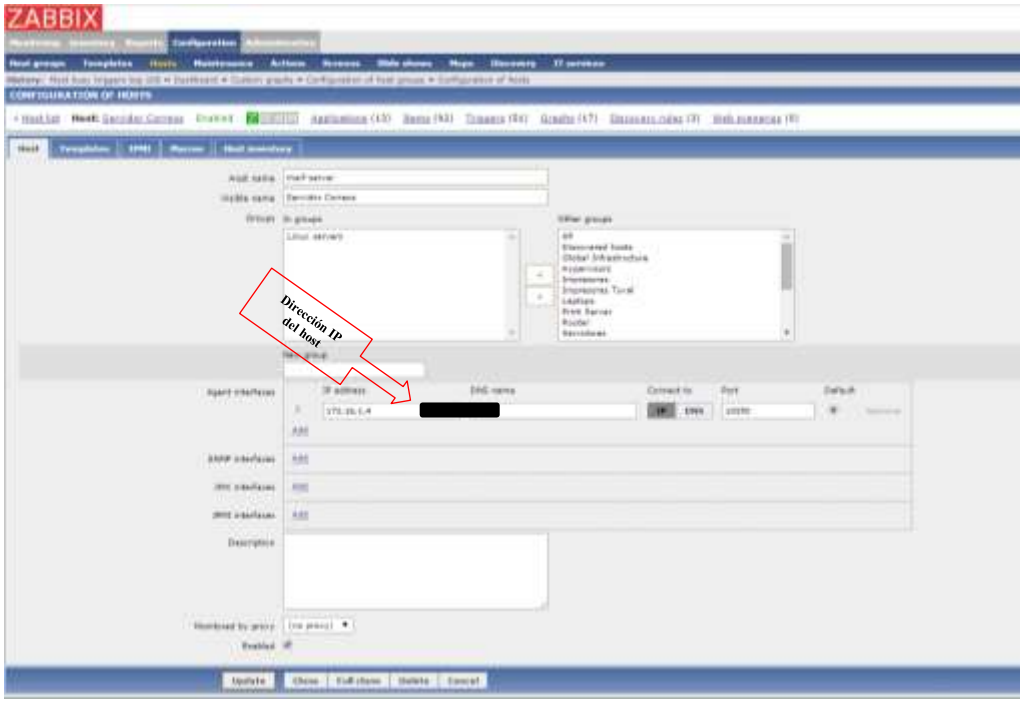


Imagen 29: Software Zabbix: Configuración de host
Fuente: El Autor

- Selección de la plantilla.

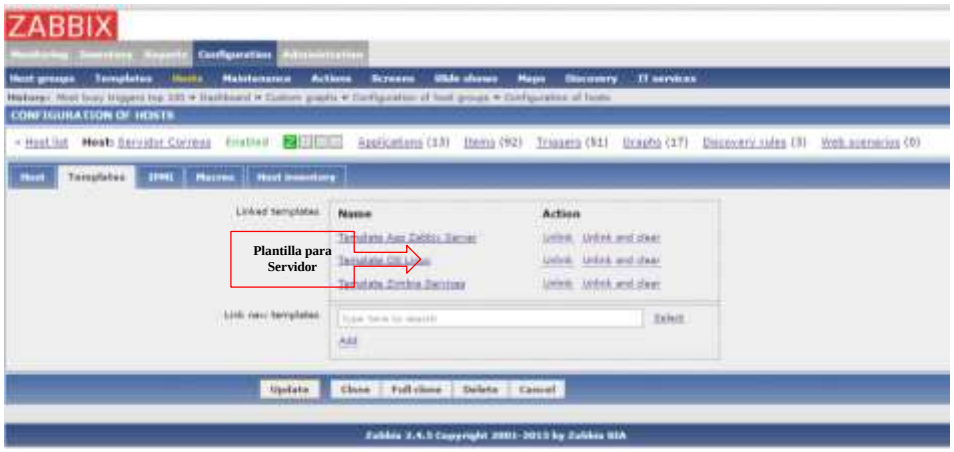


Imagen 30: Software Zabbix: Configuración de plantilla
Fuente: El Autor

Se procedió a solicitar a la empresa Telconet la configuración de la comunidad SNMP en los equipos de comunicación que están instalados en cada una de las oficinas del grupo de empresas.

- Creación de host con agente de monitoreo SNMP.

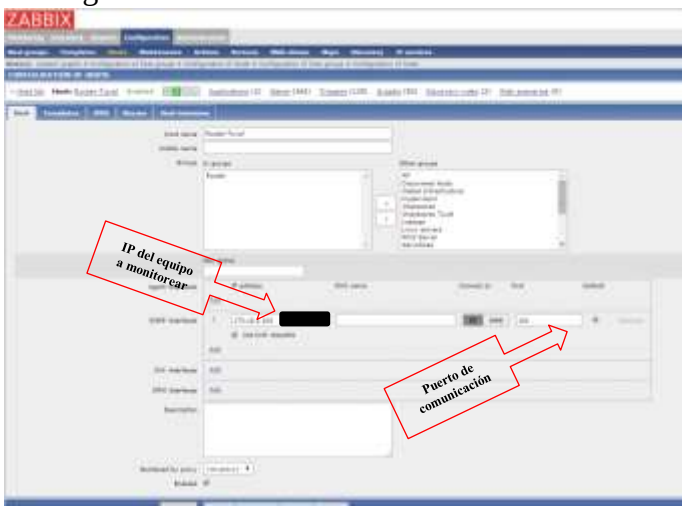


Imagen 31: Software Zabbix: Configuración de host
Fuente: El Autor

- Selección de plantilla.

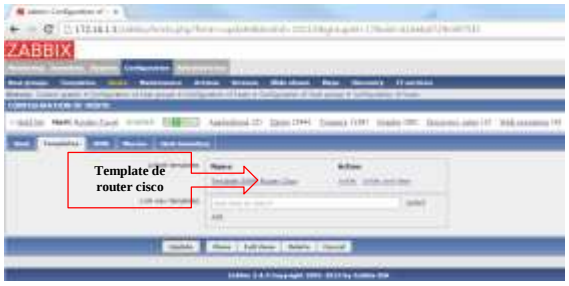


Imagen 32: Software Zabbix: Selección de Plantilla
Fuente: El Autor

- Selección de la comunidad SNMP.

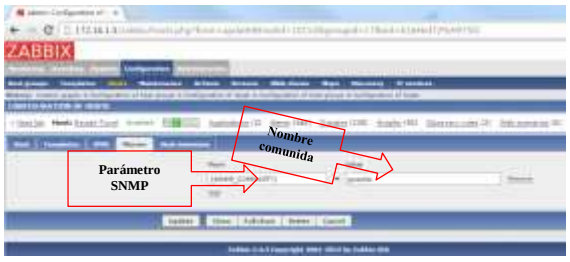


Imagen 33: Software Zabbix: Selección de comunidad SNMP
Fuente: El Autor

También se deberán de configurar los agentes de monitoreo en los servidores, equipos de comunicación propios y los puntos de acceso inalámbricos del grupo de empresas.

La herramienta zabbix nos permite crear en base a nuestras necesidades condiciones específicas para que al cumplirse una condición determinada realice la acción configurada, a este elemento zabbix lo llama trigger.

Existen trigger que vienen por defecto configurados en la plantilla que se haya seleccionado, pero estos poseen parámetros muy generales por lo que va a depender que tanto se desee profundizar en el monitoreo para modificarlos o dejarlos como vienen pre-configurados.

Creación de trigger para medición de ancho de banda de una interfaz de red

- Ir a la opción Configuration → Hosts

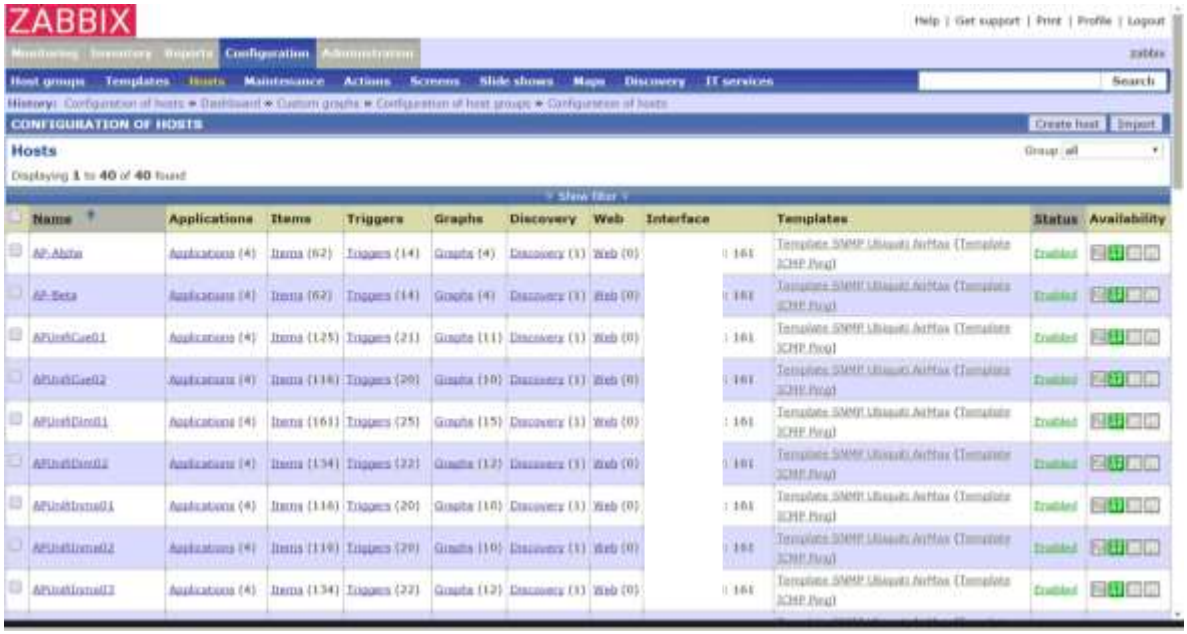


Imagen 34: Software Zabbix: Vista de hosts
Fuente: El Autor

- Si se ha asignado grupos a los equipos al momento de la creación, seleccionamos el grupo de los ruteadores.

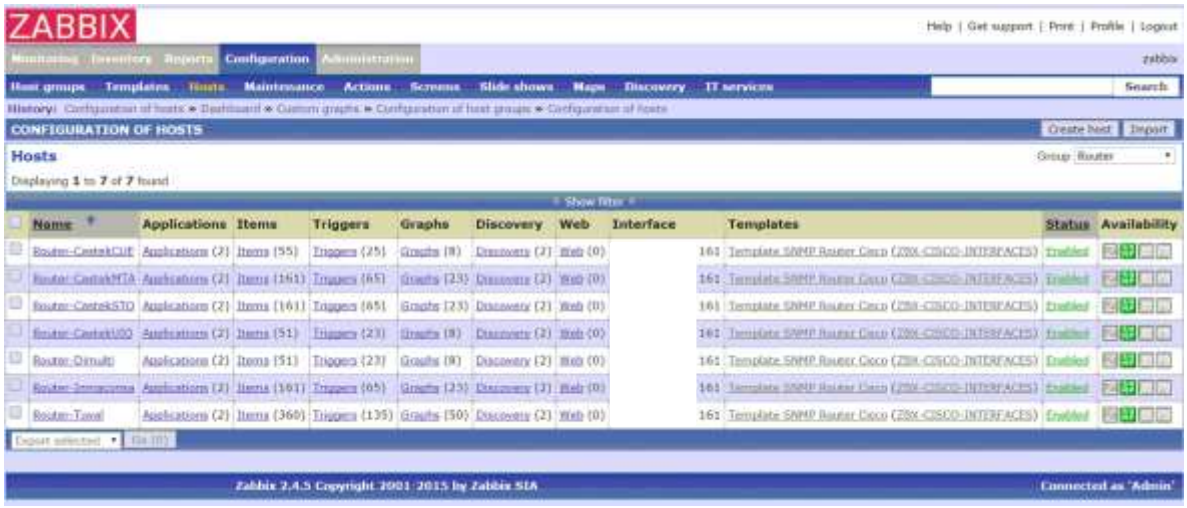


Imagen 35: Software Zabbix: Vista de host por grupo
Fuente: El Autor

- Dar un clic sobre la palabra Triggers correspondiente al equipo que se va a configurar.

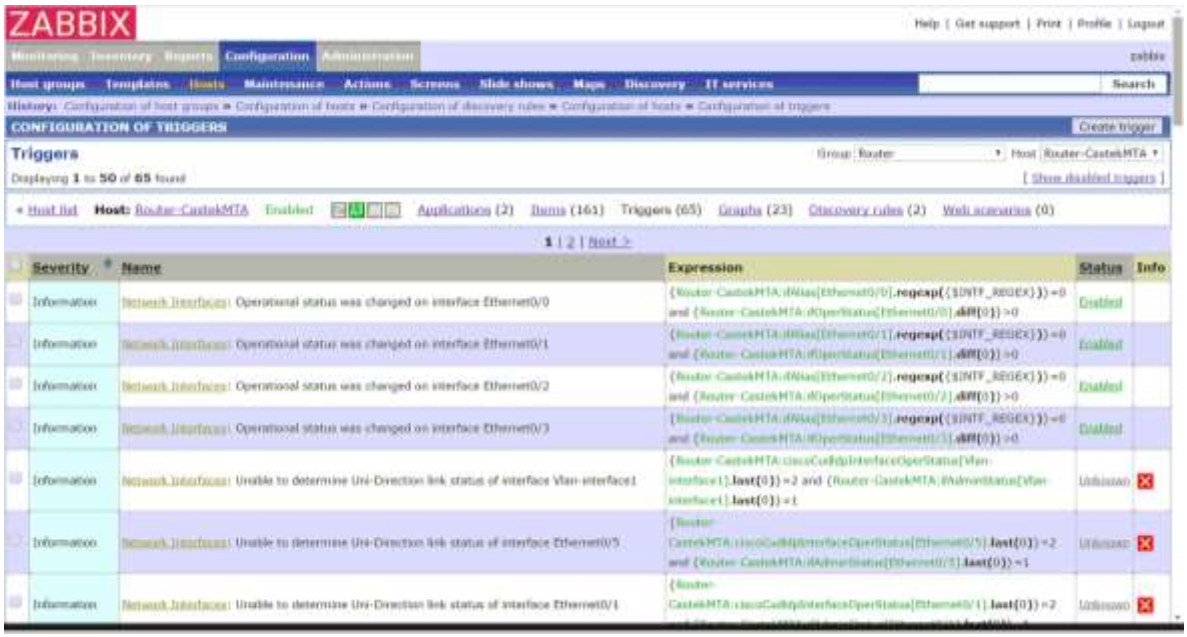


Imagen 36: Software Zabbix: Vista de triggers
Fuente: El Autor

- Se visualizan los Triggers pre-configurados, se procede a crear el Trigger dando clic en créate trigger.

Imagen 37: Software Zabbix: Creación de triggers
Fuente: El Autor

- Esta agencia posee 1 Mb de conexión de datos, por lo que se va a crear un trigger para que nos muestre una alerta cuando sobrepase los 800 Kbps por más de 5 minutos.

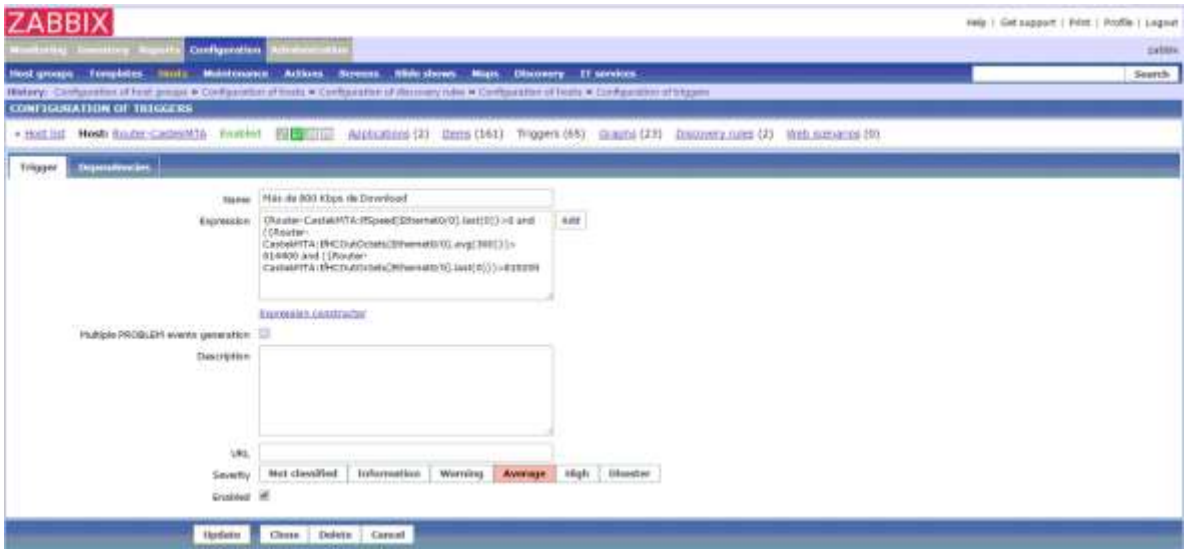


Imagen 38: Software Zabbix: Configuración de zabbix
Fuente: El Autor

- Se explica a que corresponde cada parámetro:
  Name: Es una descripción breve de lo que mide el trigger.
  Expression: Se pone la condición que se desee.
  Severity: Se especifica el nivel de gravedad que posee este trigger.
  Enabled: Indica si está habilitado o no el trigger.

- El parámetro más importante del trigger es el de expression por lo que se detalla:
  Se explica cada uno de las variables que contiene la expresión.
  - *Router-CastekMTA* es el nombre del host al que se le está creando el trigger.
  - *:ifSpeed* función de zabbix que permite capturar la velocidad de conexión de la interfaz, por ejemplo 10, 100, 1000 Mbits.
  - *[Ethernet0/0]* es la interfaz de la que se va a analizar.
  - *:IfHCOutOctets* es una función de zabbix que permite capturar el tráfico de datos que está pasando por la interfaz.

- *.avg(300)* es una función de zabbix que permite sacar un promedio de los datos de la función anterior por un periodo de tiempo que se ubica en números dentro de los paréntesis, el tiempo está dado en segundos.
- *.last(0)* es una función de zabbix que obtiene el último dato de la función que antecede a esta.
- Los valores *614400* y *819200* están dados en bits por Segundo.
- {Router-CastekMTA:ifSpeed[Ethernet0/0].last(0)}>0 and ({Router-CastekMTA:IfHCOutOctets[Ethernet0/0].avg(300)})> 614400 and ({Router-CastekMTA:IfHCOutOctets[Ethernet0/0].last(0)})>819200
- La expression traduciendola a lenguaje común se lee de la siguiente forma: Si el Ruteador de CastekMTA está conectado y durante los últimos 5 minutos el tráfico que está pasando por la interfaz es mayor a 600 Kbps y en este momento el tráfico que pasa por la interfaz es de 800 Kbps entonces activar la alarma.

f.4. Presupuesto

El proyecto actual requiere de uso hora/hombre así como de un servidor donde se va a instalar el servidor Zabbix.

El servidor que se va a usar es uno que ya posee el grupo de empresas por lo que ese rubro va a ser $ 0.

Se tiene previsto el uso de 336 horas para la culminación de todo el proyecto y conociendo que el costo hora/hombre para trabajos como este es de $ 25 el total es $8,400.00

Sumando el costo del servidor más él hora/hombre el total es de: $8,400.00

Costo de Hora / Hombre			
Mes	**Horas**	**Costo/hora**	**Subtotal**
Julio	100	$ 25.00	$ 2,500.00
Agosto	80	$ 25.00	$ 2,000.00
Septiembre	20	$ 25.00	$ 500.00
Octubre	85	$ 25.00	$ 2,125.00
Noviembre	51	$ 25.00	$ 1,275.00
		Total A:	$ 8,400.00

Tabla 2: Costo de hora/hombre
Fuente: El Autor

Materiales / Equipos			
Cantidad	**Descripción**	**Costo**	**Subtotal**
1	Servidor	$ -	$ -
		Total B:	$ -

Tabla 3: Costo de materiales/equipos
Fuente: El Autor

Presupuesto Total (A + B): **$ 8,400.00**

f.5. Pruebas y Métricas

Existen algunas pruebas que se tienen que realizar para que el software de monitoreo cumpla con todas las condiciones planteadas.

Las pruebas a realizar se basan en las siguientes métricas:

- Para los servidores:
  - Carga de CPU mayor al 50%.
  - Carga de memoria RAM mayor al 50%.
  - Saturación del tráfico en cada tarjeta de red.
  - Desconexión del equipo.
- Para los dispositivos de acceso inalámbrico:
  - Desconexión del equipo.
  - Carga del dispositivo mayor al 50%.
  - Saturación del tráfico en las tarjetas de red lan e inalámbrica.
- Para los enlaces de datos (ruteadores del proveedor):
  - Desconexión del equipo.
  - Paquetes perdidos superiores a 10.
  - Umbral de ancho de banda en tarjeta de red.

Pruebas en los servidores

Carga de cpu mayor al 75%

Para esta prueba se procede a saturar al servidor mediante el comando ***stress*** de Linux el uso de más del 75% del procesador.

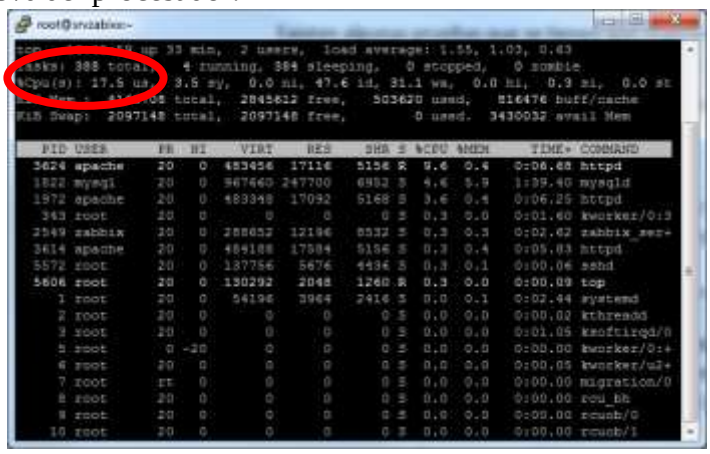


Imagen 39: Pruebas: Estado normal del procesador.
Fuente: El Autor

Se ejecutó el siguiente comando en el servidor donde se va a realizar la prueba:
stress -c 2 -i 1 --m 1 –vm-bytes 2048M -t 900s

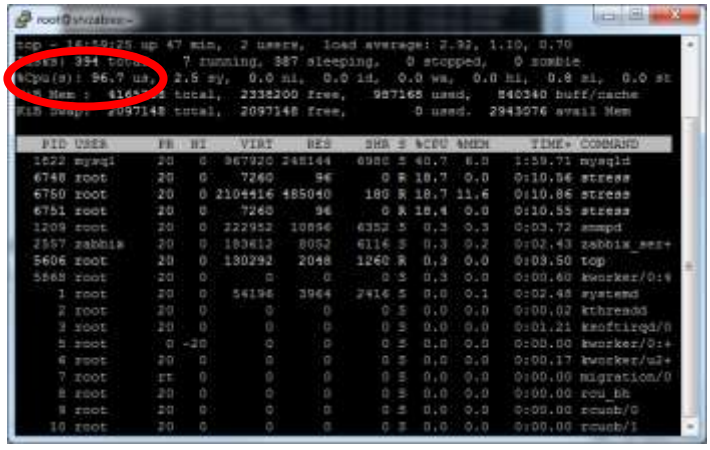


Imagen 40: Pruebas: Incremento al 96% de uso del procesador
Fuente: El Autor

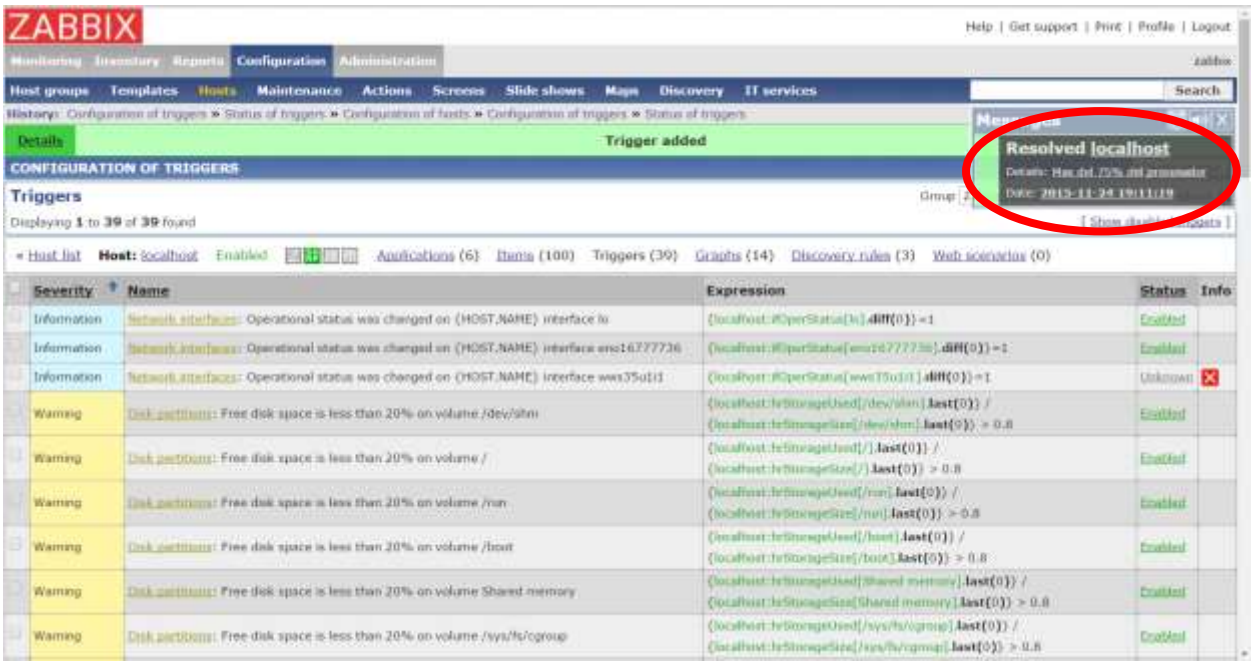


Imagen 41: Pruebas: Pantalla de alarma
Fuente: El Autor

El software automáticamente envió la alerta visual, el correo electrónico y el mensaje de texto con el detalle del problema.

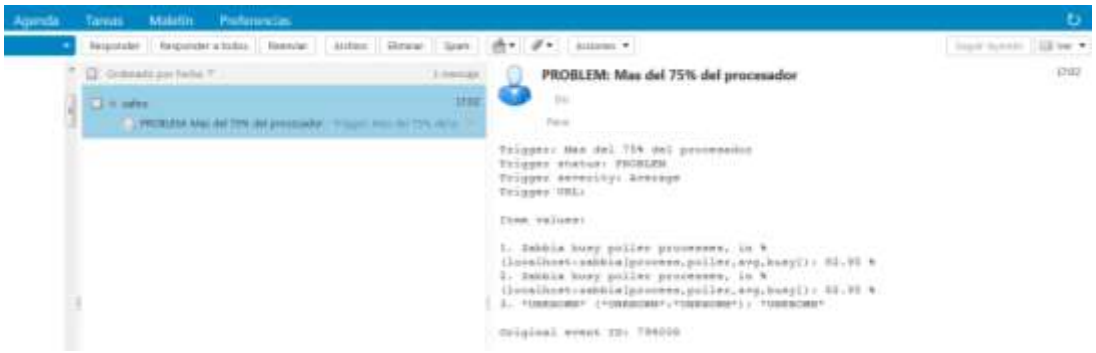


Imagen 42: Pruebas: Recepción de correo electrónico
Fuente: El Autor

Imagen 43: Pruebas: Recepción de texto
Fuente: El Autor

Pruebas en los dispositivos de acceso inalámbrico

Desconexión del equipo

Se procedió a desconectar de la energía eléctrica a un dispositivo inalámbrico.

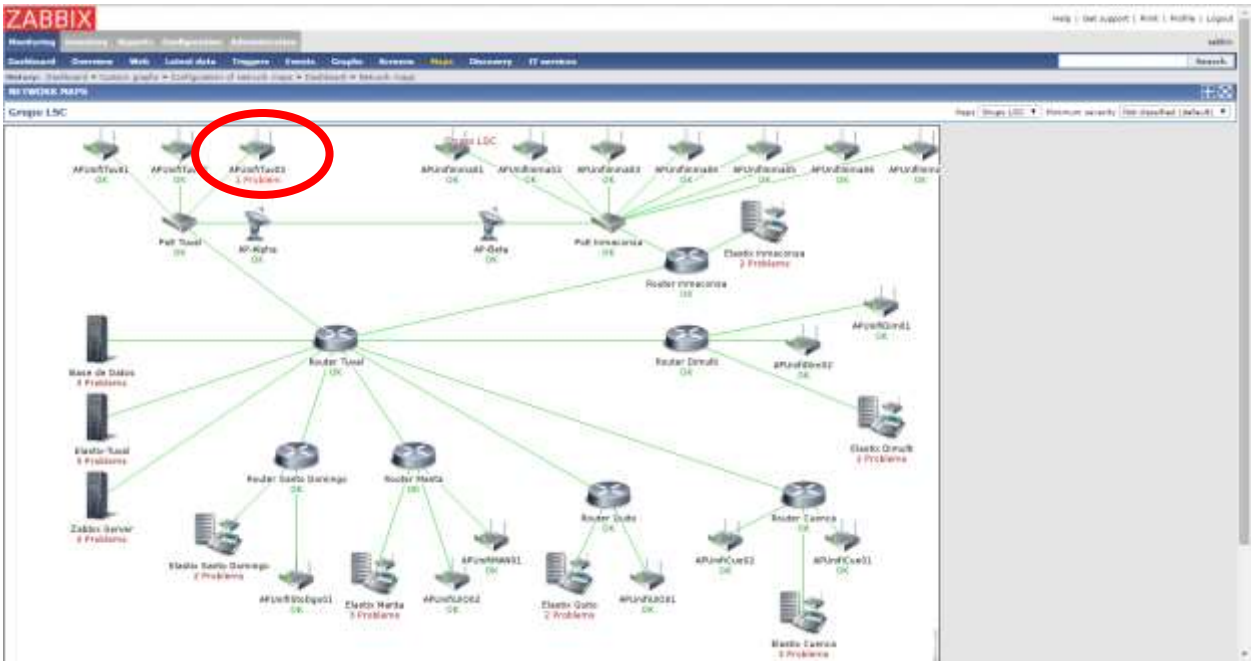


Imagen 44: Pruebas: Mapa de red mostrando error en dispositivo
Fuente: El Autor

El software automáticamente envió la alerta visual, el correo electrónico y el mensaje de texto con el detalle del problema.

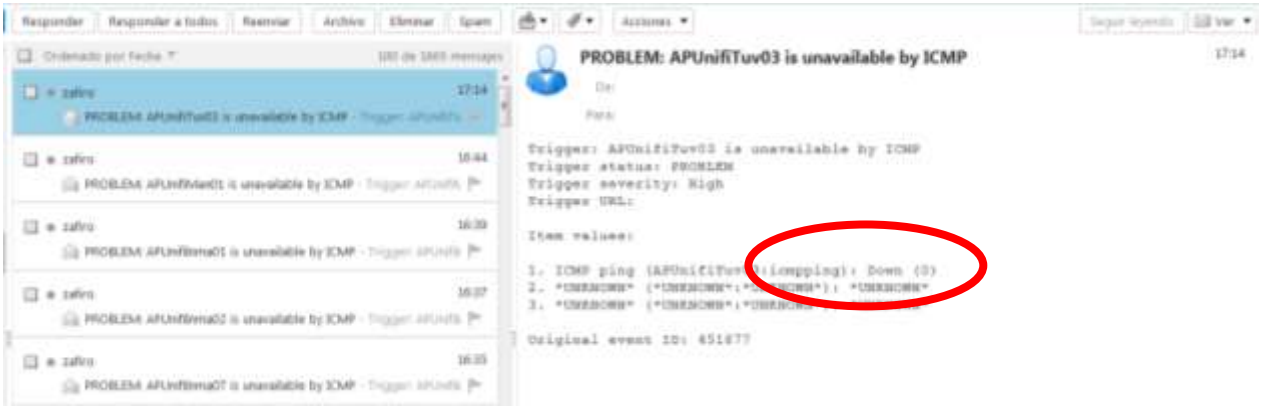


Imagen 45: Pruebas: Recepción de correo electrónico
Fuente: El Autor

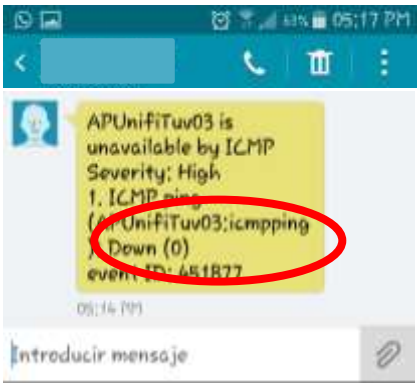


Imagen 46: Pruebas: Recepción de mensaje de texto
Fuente: El Autor

Pruebas en los enlaces de datos

Umbral de ancho de banda en una tarjeta de red

Se procede a generar saturación del ancho de banda en uno de los ruteadores de la compañía para probar la alarma.

El siguiente gráfico de la interfaz muestra la interfaz de red sin tráfico.

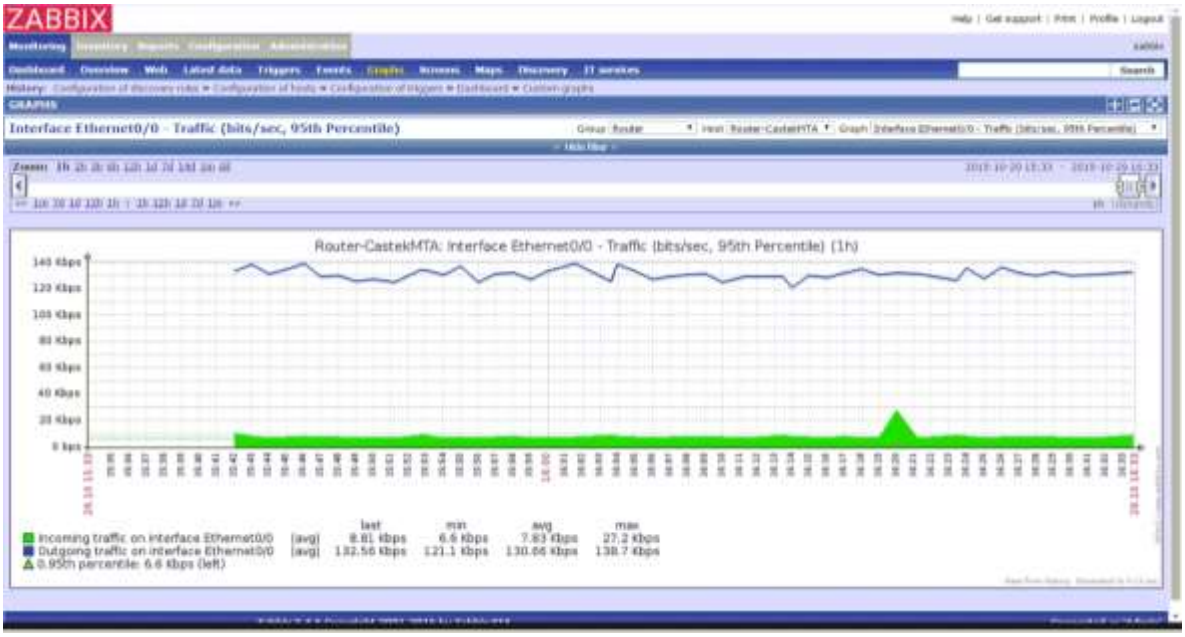


Imagen 47: Pruebas: Gráfico de actividad de tarjeta de red sin tráfico
Fuente: El Autor

En el mapa general de la red se aprecia que no tiene ninguna advertencia el ruteador.

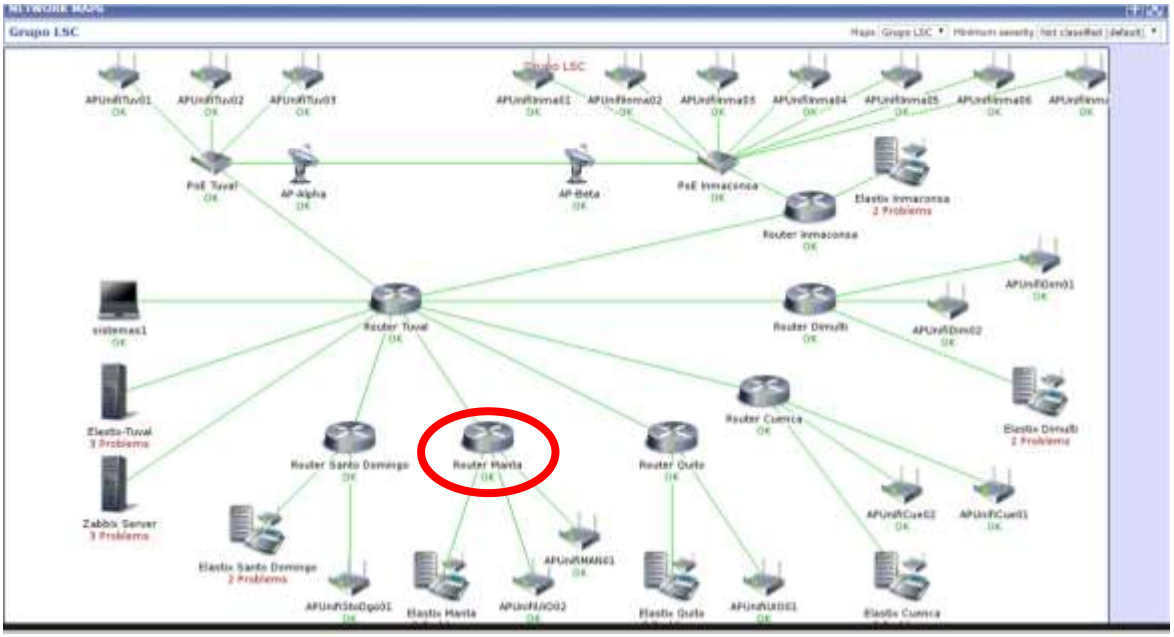


Imagen 48: Pruebas: Mapa de red sin errores
Fuente: El Autor

Se procede a generar tráfico pasándole un archivo muy pesado a cualquiera de las computadoras dentro de la red de esa agencia.

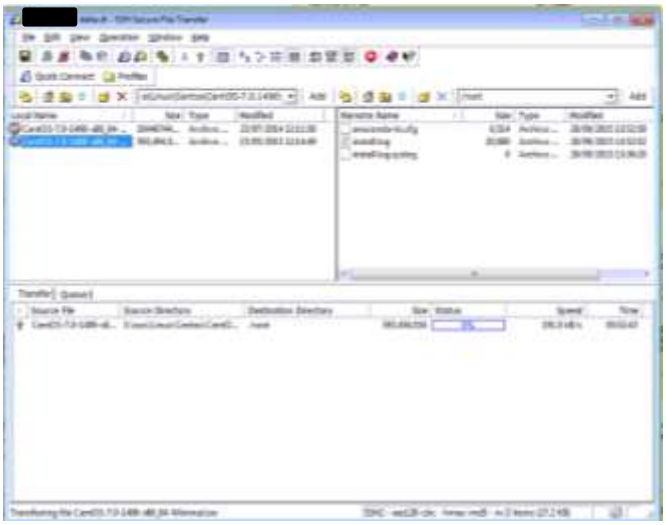


Imagen 49: Pruebas: Transferencia de archivo
Fuente: El Autor

Al pasar unos minutos se puede apreciar cómo va cambiando el gráfico de la interfaz.

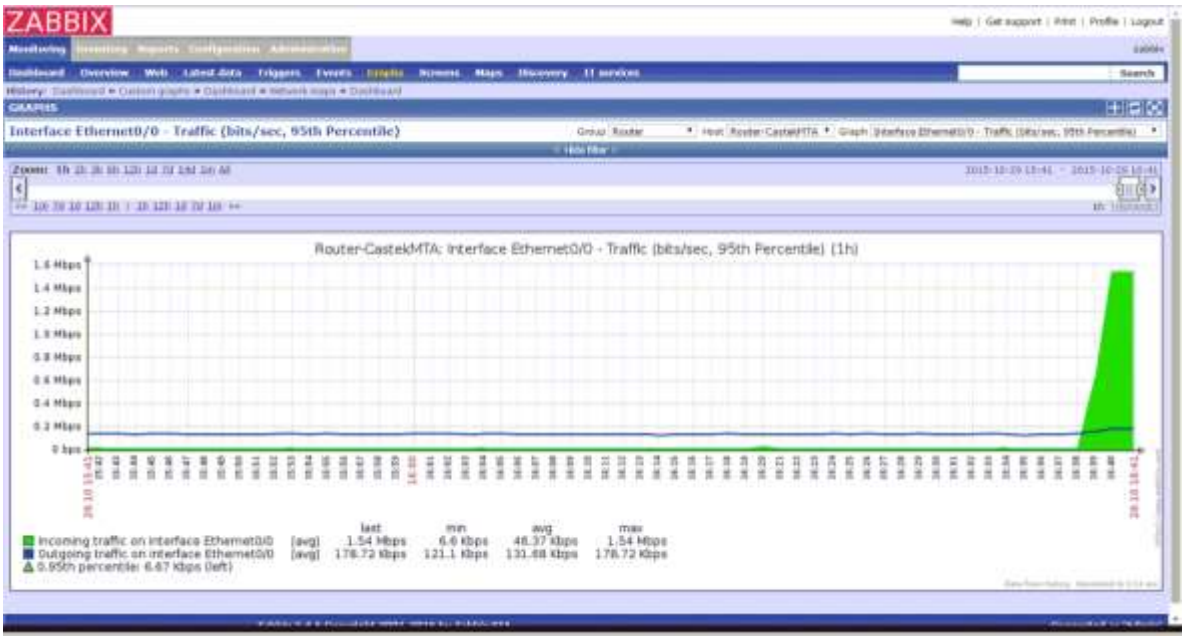


Imagen 50: Pruebas: Gráfico de actividad de tarjeta de red con poco tráfico
Fuente: El Autor

Es importante recordar que el trigger está creado para que cuando el promedio después de 5 minutos sea superior a 600 Kbps ***CastekMTA:IfHCOutOctets[Ethernet0/0].avg(300)})>***

614400 y la última velocidad sea mayor a 800 Kbps ***({Router-CastekMTA:IfHCOutOctets[Ethernet0/0].last(0)})>819200*** se encienda la alarma.

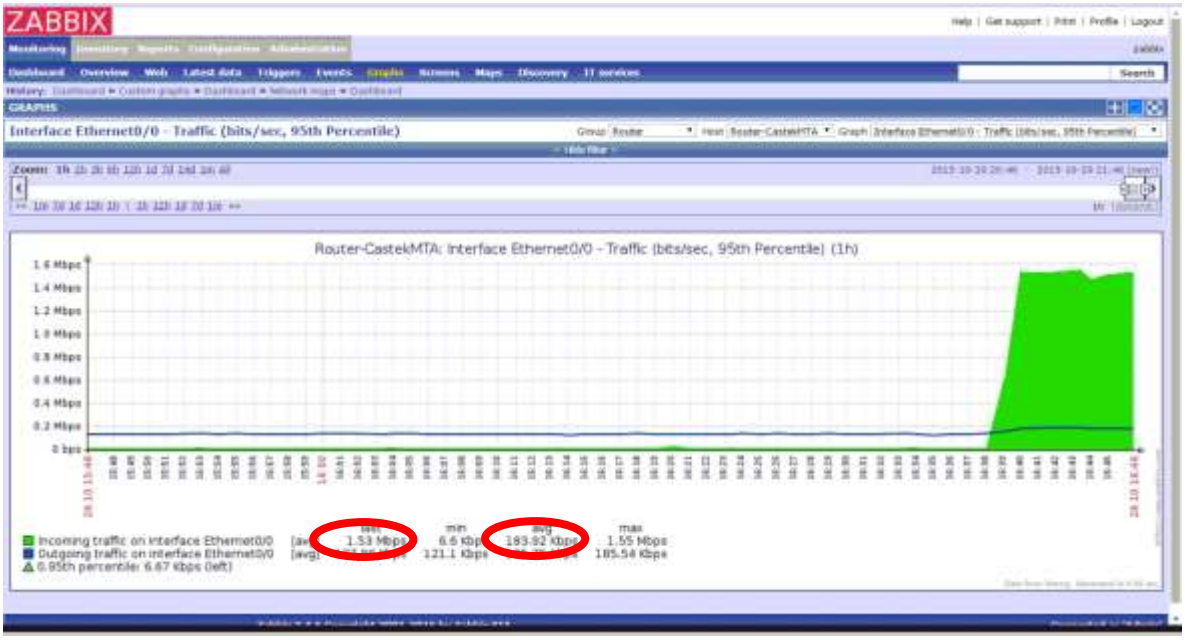


Imagen 51: Pruebas: Gráfico de actividad de tarjeta de red con tráfico medio
Fuente: El Autor

En la imagen anterior se observa que a pesar de que han pasado 5 minutos aún no se activa la alarma, esto es porque en las condiciones del trigger indica que cuando sea mayor a 600 Kbps durante los últimos 5 minutos y no desde el momento que se empezó la prueba.

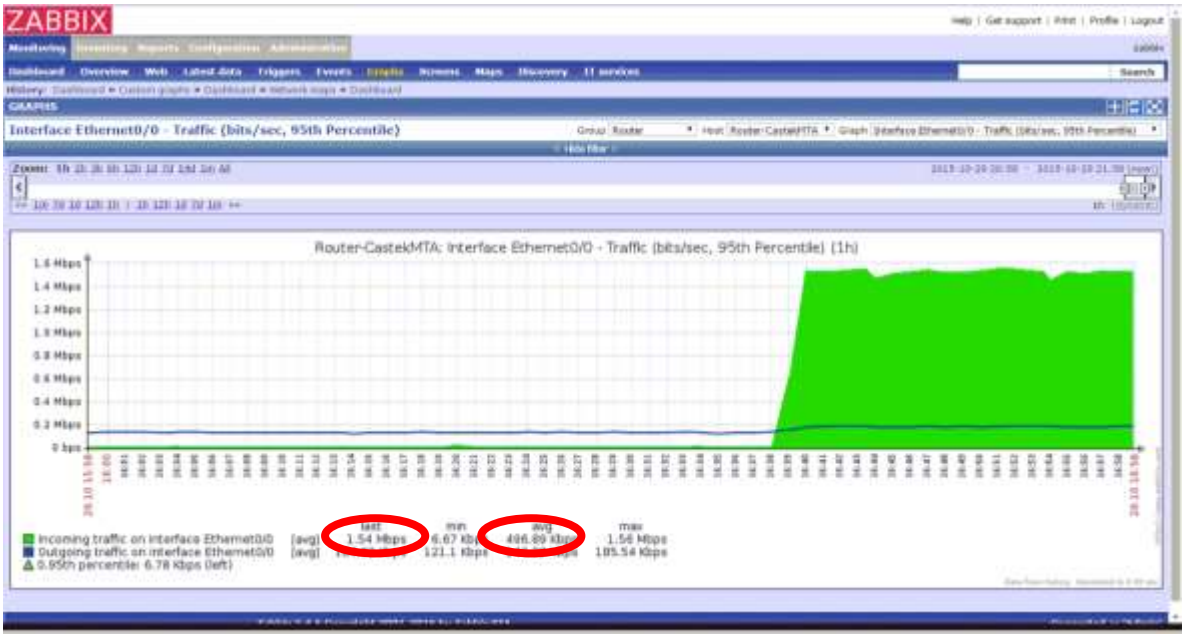


Imagen 52: Pruebas: Gráfico de actividad de tarjeta de red con tráfico alto
Fuente: El Autor

Luego de que han pasado 5 minutos con un promedio superior a los 600 kbps y el tráfico es mayor a 800 kbps el software zabbix muestra la alerta.

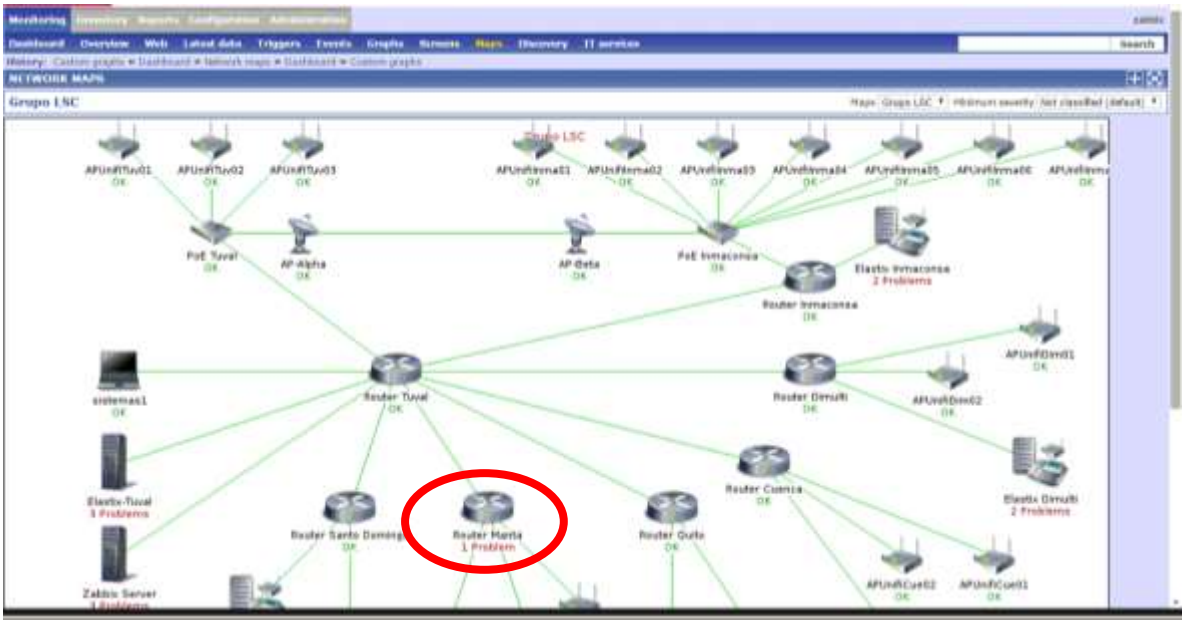


Imagen 53: Pruebas: Mapa de red con error en dispositivo
Fuente: El Autor

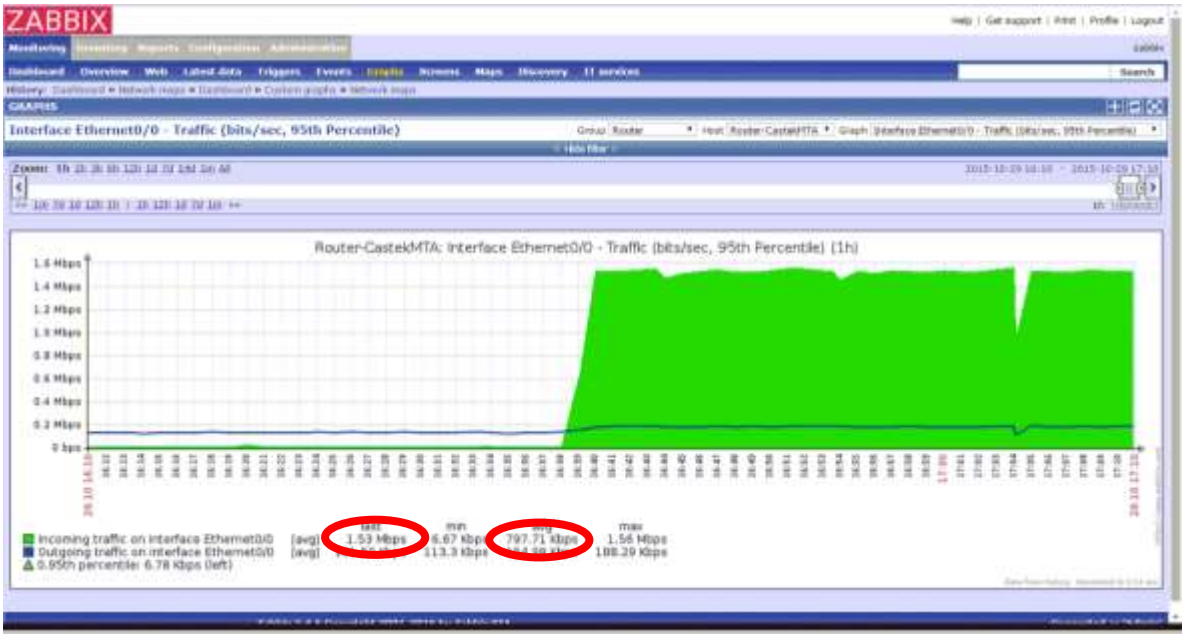


Imagen 54: Pruebas: Gráfico de tarjeta de red con saturación
Fuente: El Autor

El software automáticamente envió la alerta visual, el correo electrónico y el mensaje de texto con el detalle del problema.

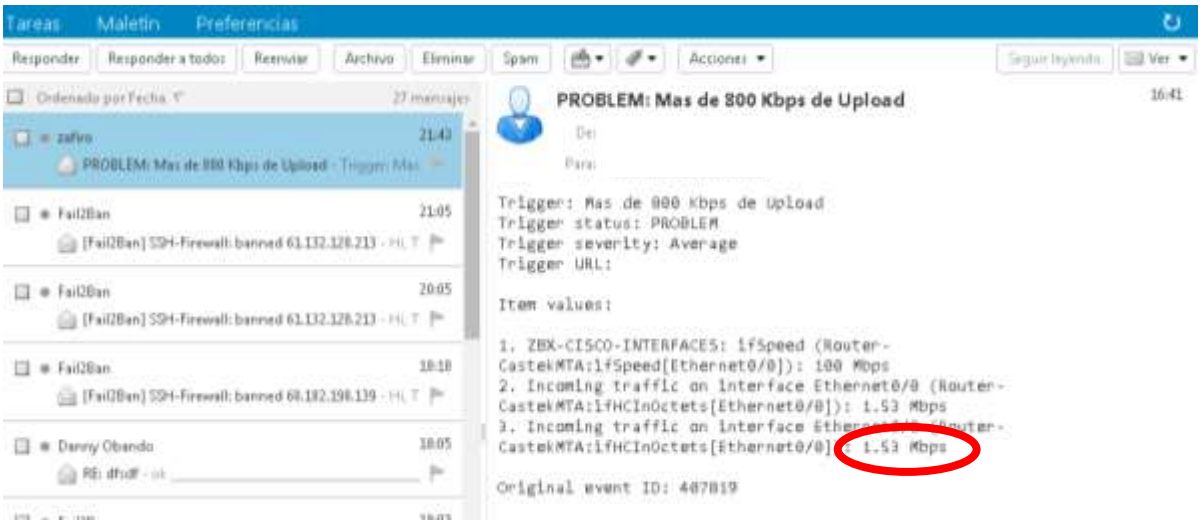


Imagen 55: Pruebas: Recepción de correo electrónico
Fuente: El Autor

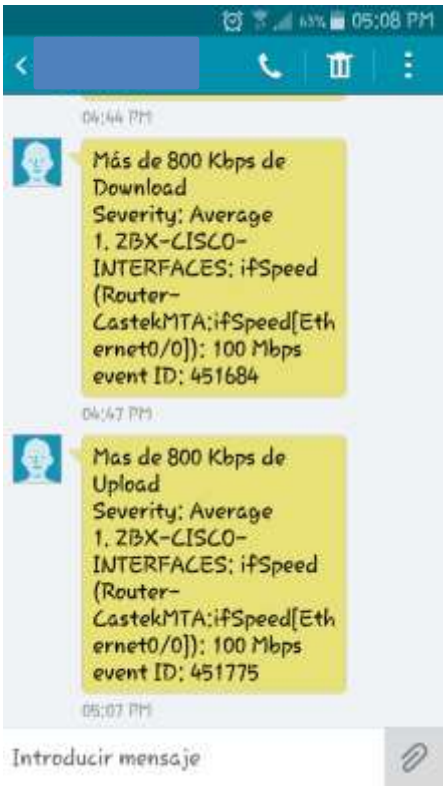


Imagen 56: Pruebas: Recepción de mensaje de texto
Fuente: El Autor

g. Resultados

Con la implementación del software de monitoreo opensource Zabbix el departamento de soporte a usuarios y redes fue capaz de identificar y en algunos casos prevenir los problemas que se han ido presentando en el transcurrir de los días.

Un ejemplo de lo útil que resultó la implementación de esta herramienta fue el poder identificar en que agencia se necesitaba incrementar el ancho de banda de datos para que se solucionen los problemas de lentitud en el sistema transaccional de le empresa.

Al tener este tipo de herramientas tecnológicas que permitan una correcta administración, la junta directiva y los usuarios han podido ver una disminución considerable en el tiempo de respuesta en caso de presentarse alguna eventualidad en la infraestructura informática.

Así también el personal que labora en el departamento de soporte a usuarios y redes ha podido liberarse de carga de trabajo y ahora puede enfocarse en otras tareas o en la implementación de futuros proyectos.

h. Conclusiones

La implementación de herramientas de monitoreo open source permitirá la identificación de errores, prevención de incidencias, monitoreo de alarmas de la Red de los sistemas de comunicación de voz y datos de las empresas TUVAL S.A., DIMULTI S.A., y CASTEK S.A.

Utilizar herramientas open source permite optimizar recursos económicos y financieros a la organización, los mismos que podrían ser utilizados en inversiones que coadyuven al mejoramiento de infraestructura tecnológica de la empresa.

La obtención de datos que brinda el software de monitoreo permitió mejorar la administración de los recursos informáticos con lo que se logró mayor eficiencia en todos los elementos que intervienen en la comunicación del grupo de empresas.

Se logró asegurar la conectividad entre las agencias al permitir diagnosticar problemas que podían ser causantes de interrupciones en el servicio.

Al tener un software de monitoreo constante sobre los equipos de comunicación y servidores se pudo tener mayor eficiencia en los recursos al poder redistribuirlos o reasignarlos al equipo o servidor que más lo demande.

i. Recomendaciones

Hacer responsable al administrador de la red o persona de sistemas a cargo sobre el correcto uso del software de monitoreo a fin de que exista alguien al que le lleguen las notificaciones del sistema de monitoreo.

Analizar la infraestructura de red que posea la empresa e identificar los equipos de comunicaciones y/o servidores que se desean monitorear.

Consultar con el departamento de presupuestos o con la gerencia de cada empresa sobre la posibilidad de invertir en software de monitoreo licenciado para poder realizar la comparación con los open source y así tener un mayor panorama antes de tomar la decisión sobre que software instalar.

Comprobar periódicamente que el software de monitoreo esté funcionando correctamente realizando pruebas que simulen saturaciones o desconexiones para garantizar el correcto funcionamiento del mismo.

Categorizar los dispositivos o equipos que se agreguen al software de monitoreo para tener mayor facilidad de búsqueda en la interfaz gráfica de administración.

Añadir nuevos dispositivos o servidores que adquiera la compañía para que el software esté con la información completa de los elementos de la red.

Modificar según crea conveniente los triggers que vienen predeterminados con las plantillas para adaptarlos a la realidad de cada empresa.

j. Trabajos futuros

Como un trabajo complementario se pueden agregar todos los equipos de computación de los usuarios e impresoras que no son considerados como críticos al software Zabbix, estos equipos que no son de relativa importancia puesto que no afectan a toda la red sino de forma aislada a uno u otro usuario deben ser considerados para una segunda etapa porque si influyen en el normal desenvolvimiento de las tareas diarias de los usuarios.

A nivel del departamento de soporte a usuarios y redes del grupo de empresas el siguiente proyecto a implementar es continuar con la integración de las agencias con los enlaces inalámbricos propietarios por lo que los siguientes puntos a integrar son la agencia Dimulti S.A. con Tuval S.A.

Otro proyecto pensado pero sin fecha determinada es la implementación de un software de mesa de ayuda con la asignación de ticket por incidencias.

k. Referencias

CISCO. (s.f.). Obtenido de http://www.cisco.com/web/ES/administracion-publica/centro-de-datos/cisco-san.html

Dueñas, J. B. (03 de 06 de 2014). Obtenido de www.alcancelibre.org: http://www.alcancelibre.org/staticpages/index.php/como-linux-snmp

Edgewall Software. (2003-2013). *Munin*. Obtenido de http://munin-monitoring.org/

Fundación Wikimedia, Inc. (31 de 03 de 2014). *Enlace de datos.* Obtenido de https://es.wikipedia.org/wiki/Enlace_de_datos

Fundación Wikimedia, Inc. (16 de 03 de 2016). *Host*. Obtenido de https://es.wikipedia.org/wiki/Host

Fundación Wikimedia, Inc. (28 de 03 de 2016). *Monitoreo de red*. Obtenido de https://es.wikipedia.org/wiki/Monitoreo_de_red

Fundación Wikimedia, Inc. (3 de 04 de 2016). *Ping*. Obtenido de https://es.wikipedia.org/wiki/Ping

Microsoft. (01 de 2005). *Protocolo de mensajes de control de Internet*. Obtenido de https://msdn.microsoft.com/es-es/library/cc758065%28v=ws.10%29.aspx

Ministerio de Educación, Cultura y Deporte de España. (s.f.). *Proxy Squid | Redes Linux.* Obtenido de http://www.ite.educacion.es/formacion/materiales/85/cd/linux/m6/proxy_squid.html

Nagios Entreprises. (2009-2016). *About Nagios*. Obtenido de https://www.nagios.org/about/

Oetiker, T. (13 de 01 de 2012). *MRTG - What's is*. Obtenido de http://oss.oetiker.ch/mrtg/doc/mrtg.en.html

OETIKER+PARTNER AG. (30 de 09 de 2015). *About RRDtool*. Obtenido de http://oss.oetiker.ch/rrdtool/

Opensource.org. (22 de 03 de 2007). *The Open Source Definition.* Obtenido de https://opensource.org/osd

Oracle Corporation . (s.f.). *MySQL*. Obtenido de https://www.mysql.com/products/

PHP Documentation Group. (1997-2016). *PHP: Conceptos básicos*. Obtenido de http://php.net/manual/es/preface.php

Siemens. (28 de 05 de 2003). Obtenido de www.siemens.com: https://support.industry.siemens.com/cs/document/15177711/-mib-%28management-information-base%29-en-el-snmp-?dti=0&lc=es-WW

The Cacti Group, Inc. (2004-2012). *Cacti*. Obtenido de http://www.cacti.net/what_is_cacti.php

Zabbix LLC. (2001-2016). Retrieved from http://www.zabbix.com/product.php

Zabbix SIA. (2001-2015). *www.zabbix.com.* Obtenido de https://www.zabbix.com/documentation/2.4/manual/config/triggers

Zenoss, Inc. (2005-2015). *Zenoss Open Source Core.* Obtenido de http://pages.zenoss.com/WF-Core-Download-Req.html

l. Glosario

Open Source: El código abierto no sólo significa el acceso al código fuente. Los términos de distribución de software de código abierto deben cumplir con algunos criterios. (Opensource.org, 2007)

Monitoreo de red: El término Monitoreo de red describe el uso de 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 correo electrónico, pager u otras alarmas. Es un subconjunto de funciones de la administración de redes. (Fundación Wikimedia, Inc., 2016)

Enlaces de datos: En telecomunicaciones, un enlace de datos (en inglés: data link) es el medio de conexión entre dos lugares con el propósito de transmitir y recibir información. Puede hacer referencia a un conjunto de componentes electrónicos, que consisten en un transmisor y un receptor (dos piezas de un equipo terminal de datos) y el circuito de telecomunicación de datos de interconexión. Esto se rige por un protocolo de enlace que permite que los datos digitales puedan ser transferidos desde una fuente de datos a un receptor de datos. (Fundación Wikimedia, Inc, 2014)

Proxy: Un proxy de conexión a Internet es un servidor que hace de intermediario entre los PCs de la red y el router de conexión a Internet, de forma que cuando un usuario quiere acceder a Internet, su PC realiza la petición al servidor Proxy y es el Proxy quien realmente accede a Internet. Posteriormente, el Proxy enviará los datos al PC del usuario para que los muestre en su pantalla. El PC del usuario no tendrá conexión directa con el router, sino que accederá a Internet por medio del proxy. (Ministerio de Educación, Cultura y Deporte de España)

Redes SAN: "SAN, una red especializada para almacenamiento, es una arquitectura que auna diversos dispositivos como si fuesen uno solo y en ella los sistemas están disponibles para todos los servidores." (CISCO, s.f.)

RRDtool: RRDtool es el estándar de la industria de código abierto, el registro de datos de alto rendimiento y un sistema de representación gráfica de los datos de series de tiempo. RRDtool se puede integrar fácilmente en los scripts de shell, Perl, Python, Ruby, lua o aplicaciones TCL. (OETIKER+PARTNER AG, 2015)

MYSQL: “MySQL es la base de datos de código abierto más popular del mundo.” (Oracle Corporation , s.f.)

PHP: PHP, acrónimo de "PHP: Hypertext Preprocessor", es un lenguaje de 'scripting' de propósito general y de código abierto que está especialmente pensado para el desarrollo web y que puede ser embebido en páginas HTML. Su sintaxis recurre a C, Java y Perl, siendo así sencillo de aprender. El objetivo principal de este lenguaje es permitir a los desarrolladores web escribir dinámica y rápidamente páginas web generadas; aunque se puede hacer mucho más con PHP. (PHP Documentation Group, 1997-2016)

SNMP: “(Simple Network Management Protocol o Protocolo Simple de administración de red) es uno protocolos del conjunto definido por la Fuerza de Trabajo en Ingeniería de Internet (IETF o Internet Engineering Task Force), clasificada en el nivel de aplicación del modelo TCP/IP y que está diseñado para facilitar el intercambio de información entre dispositivos de red y es ampliamente utilizado en la administración de redes para supervisar el desempeño, la salud y el bienestar de una red, equipo de cómputo y otros dispositivos.” (Dueñas, 2014)

MRTG: “Es una herramienta para monitorizar la carga de tráfico en los enlaces de red. MRTG genera páginas HTML que contienen imágenes PNG que proporcionan una representación visual en vivo de este tráfico.” (Oetiker, 2012)

Ping: Como programa, ping es una utilidad diagnóstica en redes de computadoras que comprueba el estado de la comunicación del host local con uno o varios equipos remotos de una red IP por medio del envío de paquetes ICMP de solicitud (ICMP Echo Request) y de respuesta (ICMP Echo Reply). Mediante esta utilidad puede diagnosticarse el estado, velocidad y calidad de una red determinada. (Fundación Wikimedia, Inc., 2016)

Host: “El término host ("anfitrión", en español) es usado en informática para referirse a las computadoras conectadas a una red, que proveen y utilizan servicios de ella.” (Fundación Wikimedia, Inc., 2016)

MIB: “Un MIB (Management Information Base – Base de información de gestión) es una base de datos estándar formada por diferentes variables SNMP, las cuales se definen en un idioma independiente del sistema destino.” (Siemens, 2003)

Trigger: “Son expresiones lógicas que evalúan los datos recogidos por los ítems y que representan el estado actual del sistema” (Zabbix SIA., 2001-2015)

ICMP: El Protocolo de mensajes de control de Internet (ICMP) es un estándar TCP/IP necesario definido en RFC 792, "Internet Control Message Protocol (ICMP)". Con ICMP, los hosts y los enrutadores que utilizan la comunicación IP pueden informar de errores e intercambiar información de control y estado limitada. (Microsoft, 2005)

m. Anexos

- Anexo A: Instalación de servidor de Monitoreo.
- Anexo B: Manual para instalar Agente Zabbix en clientes Linux y Windows.
- Anexo C: Creación de mapa de red.
- Anexo D: Modificación de trigger para adaptarlo a la necesidad de la empresa.

ANEXO A

m.1. Anexo A: Instalación de software de monitoreo

Este documento se creó a partir del manual de instalación publicado en la página oficial de Zimbra. URL de consulta:

https://www.zabbix.com/documentation/2.4/manual/installation/install_from_packages

Como pre-requisito se debe de tener instalar la base de datos mysql. URL de consulta: http://dbahire.com/como-instalar-mysql-5-6-en-centos-7/

Requisitos mínimos de hardware y software del servidor:

- Procesador Intel Pentium 4 o superior
- Memoria RAM de 2 Gb o superior
- Disco duro de 80 Gb o superior
- Sistema Operativo Centos 7 instalado en forma minimalista

Pasos necesarios para la instalación

1. Ingresar por consola al sistema operativo.

2. Instalar el repositorio de configuración de zabbix.
```
# rpm -ivh http://repo.zabbix.com/zabbix/2.4/rhel/7/x86_64/zabbix-release-2.4-1.el7.noarch.rpm
```

3. Instalar los paquetes necesarios para el correcto funcionamiento del zabbix.
```
# yum install zabbix-server-mysql zabbix-web-mysql
```

4. Crear la base de datos zabbix en MySQL.
```
# cd /usr/share/doc/zabbix-server-mysql-2.4.0/create
# mysql -uroot zabbix < schema.sql
# mysql -uroot zabbix < images.sql
# mysql -uroot zabbix < data.sql
```

5. Establecer la base de datos en el archivo de configuración de zabbix.
```
# vi /etc/zabbix/zabbix_server.conf
DBHost=localhost
DBName=zabbix
DBUser=zabbix
DBPassword=zabbix
```

6. Iniciar el servicio zabbix.
```
# service zabbix-server start
```

Configuración de Zabbix

1. Para configurar zabbix es necesario abrir el browser e ingresar la siguiente URL: http://IP-servidor/zabbix/

Imagen 57: Anexo A: Pantalla de bienvenida de Zabbix
Fuente: El Autor

2. Proceder dando clic en Next.

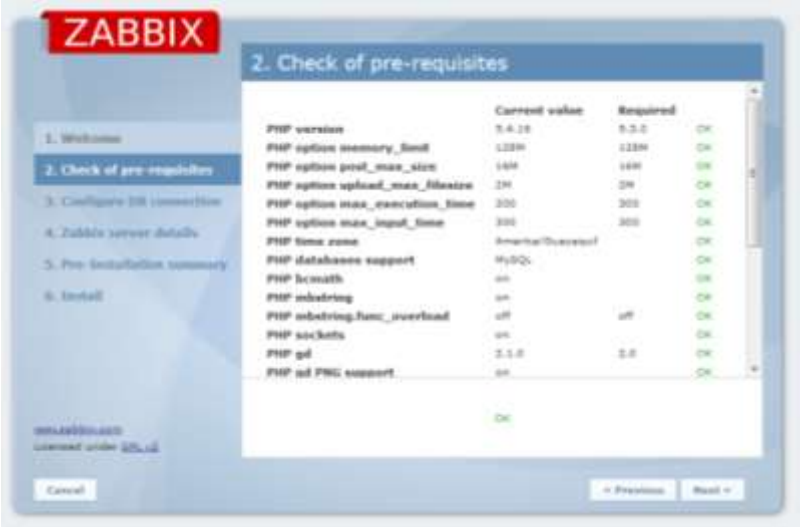


Imagen 58: Anexo A: Tabla de verificación de Pre-requisitos
Fuente: El Autor

3. Llenar los campos con respecto a la base de datos del zabbix y dar clic en Next.

Imagen 59: Anexo A: Parámetros de configuración de base de datos
Fuente: El Autor

4. Se debe de indica el puerto con el que va a trabajar el servidor y opcional se puede poner un nombre, continuar dando clic en Next.

Imagen 60: Anexo A: Parámetros de configuración del puerto a usar
Fuente: El Autor

5. Muestra el resumen de la instalación, si luego de confirmar que todos los parámetros estén correctamente ingresados se procede a dar clic en Next.

Imagen 61: Anexo A: Revisión de parámetros de configuración ingresados
Fuente: El Autor

6. Si no existe ningún problema el instalador indica que escribió el archivo de configuración, para finalizar se da clic en Finish.

Imagen 62: Anexo A: Confirmación de instalación exitosa
Fuente: El Autor

7. Terminado el proceso de configuración automáticamente será redirigido a la pantalla del login del zabbix.

Imagen 63: Anexo A: Pantalla de acceso al programa
Fuente: El Autor

El usuario por defecto es: Admin y la clave por defecto es: Zabbix

Imagen 64: Anexo A: Pantalla principal de Zabbix.
Fuente: El Autor

Recomendaciones:

- Hay que deshabilitar el SELINUX.
- Subir el servicio del httpd y habilitarlo para que se inicie con el SO.

```
# systemctl enable httpd.service
# systemctl start httpd.service
```

Problemas y soluciones:

- Problema de pre-requisitos:
    a. Si en el paso 2 del presente manual muestra un error del php en referencia a la zona horaria se debe ingresar via consola y realizar lo siguiente:
    ```
    # vi /etc/httpd/conf.d/zabbix.conf
    ```

    b. Dentro de ese archivo se debe descomentar la línea de la zona horaria y ubicar la la correcta dependiendo de la región que se encuentren, para el caso de este manual la línea debe de quedar de la siguiente forma:
    ```
    php_value date.timezone America/Guayaquil
    ```

- Problema al iniciar el zabbix
    a. Si da problemas al iniciar el zabbix con este error:
    zabbix_server_m[13777]: segfault at 18 ip 00007fe6639a8fe0 sp 00007fffbb66e498 error 4 in libpthread-2.18 - crash in "main" process

    b. La solución es realizar un downgrade del paquete gnutls.x86_64 0:3.3.8-12.el7 en sus versiones 3.3.8* hay que instalar la versión gnutls.x86_64 0:**3.1.18**-8.el7 que viene en el cd de instalación. El comando a usar es el siguiente:
    ```
    # yum downgrade gnutls*
    ```

ANEXO B

m.2. Anexo B: Manual para instalar agente Zabbix en clientes Linux y Windows

El agente Zabbix es necesario instalar en todos los sistemas operativos remotos que se desee monitorear a través del servidor Zabbix. El agente Zabbix recoge los datos de la utilización de recursos, datos de las aplicaciones del sistema para luego proporcionárselos al servidor Zabbix.

Instalar Agente Zabbix en Centos

1. Añadir el repositorio de Zabbix. Elegir dependiendo de la versión de la distribución.
   CentOS/RHEL 7:

```
# rpm -Uvh http://repo.zabbix.com/zabbix/2.4/rhel/7/x86_64/zabbix-release-2.4-1.el7.noarch.rpm
```

   CentOS/RHEL 6:

```
# rpm -Uvh http://repo.zabbix.com/zabbix/2.4/rhel/6/x86_64/zabbix-release-2.4-1.el6.noarch.rpm
```

   CentOS/RHEL 5:

```
# rpm -Uvh http://repo.zabbix.com/zabbix/2.4/rhel/5/x86_64/zabbix-release-2.4-1.el5.noarch.rpm
```

2. Instalar agente Zabbix.

```
# yum -y install zabbix zabbix-agent
```

3. Modificar el archivo de configuración de agente Zabbix.
   - Ingresar al directorio de configuración:

     ```
     # cd /etc/zabbix/
     ```

   - Modificar el archivo de configuración:

     ```
     # vi zabbix_agentd.conf
     ```

   - Cambiar los siguientes parámetros:

     ```
     Server=192.168.1.3
     Hostname=Nombre-del-Equipo
     ```

4. Habilitar el servicio zabbix para que inicie con el Sistema Operativo e iniciarlo.

```
# chkconfig zabbix-agent on
# /etc/init.d/zabbix-agent start
```

Instalar agente Zabbix en servidor de correos

Para el servidor de correos Zimbra en su versión 8.6 existe una plantilla publicada por la página https://github.com con la cual permite conocer el status de cada uno de los servicios internos que ejecuta el servidor Zimbra.

Para lograr conocer el status de los servicios internos aplica una de las funcionalidades que ofrece el servidor Zabbix la cual permite ejecutar comandos en el host monitoreado, con esto se logra no solo conocer los procesos básicos de sistema sino el status completo del sistema operativo y la aplicación que se ejecuta en dicho servidor.

A continuación se detallan los pasos a seguir del lado del host cliente:

1. Instalar el agente Zabbix en Centos.
2. Crear el script de nombre ***sudo_zbx-zimbra.conf*** dentro del directorio ***/etc/sudoers.d/*** con el siguiente contenido:

```
# Don't log every invocation of zmcontrol
Cmnd_Alias ZIMBRA_BIN_ZABBIX = /opt/zimbra/bin/zmcontrol
Defaults!ZIMBRA_BIN_ZABBIX !syslog
zabbix ALL=(zimbra) NOPASSWD: ZIMBRA_BIN_ZABBIX
```

3. Crear el script de nombre ***yo-zimbra.conf*** dentro del directorio ***/etc/zabbix/zabbix_agent.conf.d/*** con el siguiente contenido:

```
UserParameter=zimbra.status[*],/etc/zabbix/scripts/zbx_zimbra.sh "$1"
UserParameter=zimbra.version,/etc/zabbix/scripts/zbx_zimbra.sh version
UserParameter=zimbra.discovery,/etc/zabbix/scripts/zbx_zimbra.sh discover
# zmcontrol takes some time...
Timeout=15
```

4. Crear la carpeta llamada ***scripts*** dentro de ***/etc/zabbix/***
5. Crear el archivo ***zbx_zimbra.sh*** dentro de la carpeta ***/etc/zabbix/scripts/*** con el siguiente contenido:

```
#!/bin/sh

# Zabbix script to check Zimbra services and perform service discovery.
# Supports Zimbra 8.6 and "two-worded" service names
# Author: Lorenzo Milesi <maxxer@yetopen.it>
# Copytight: YetOpen S.r.l. 2015
# License: GPLv3
# uncomment for debug
```

```
#set -x
COMMAND="sudo -u zimbra /opt/zimbra/bin/zmcontrol"
case "$1" in
   version)
   # Return zimbra version
   VERS=$($COMMAND -v)
   if [ $? -eq 0 ] ; then
      echo $VERS
      exit 0;
   fi
   # error
   exit 1;
   ;;
   discover)
   # Return a list of running services in JSON
     echo "{"
     echo -e "\t\"data\":[\n"
     SRVCS=$($COMMAND status | grep Running | awk '{$(NF--)=""; print}' | sed
's/^/\t{ \"{#ZIMBRASERVICE}\":\"/' | sed 's/\ $/\" },/')
     # Remove last comma from the sting, to make a good JSON
     echo $(echo $SRVCS | sed 's/,\+$//')
     echo -e "\n\t]\n"
     echo "}"
   exit 0;
   ;;
   *)
   # move on...
     check=$1

     if [ "$check" = "" ]; then
       echo "No Zimbra service specified..."
       exit 1
     fi

     maxage=120
     file='/var/run/zabbix/zimbra_status'

     # Very basic concurrency check
     x=0
     while [ -f "$file.tmp" ]; do
               sleep 5;
               x=$((x+1))
               # don't wait too long anyway, remove an eventually stale lock. Anyway
we have 15s zabbix agent timeout
```

```
                if [ $x -ge 3 ]; then
                        rm "$file.tmp";
                fi
        done
        #check if cached status file size > 0
        if [ -s ${file} ]; then
          OLD=`stat -c %Z $file`
          NOW=`date +%s`
          # if older then maxage, update file
          if [ `expr $NOW - $OLD` -gt $maxage ]; then
            $COMMAND status > $file.tmp
            mv $file.tmp $file
          fi
        else
            rm -f ${file}
            $COMMAND status > $file.tmp
            mv $file.tmp $file
        fi
        STATUS="$(cat $file | grep "$check" | awk '{print $NF}')"
        if [ "$STATUS" != "Running" ]; then
          echo 0
        else
          echo 1
        fi
      ;;
esac
exit 0;
```

6. Crear el archivo ***yo_zimbra_template.xml*** e importarla en el servidor con el siguiente contenido:

```
<?xml version="1.0" encoding="UTF-8"?>
<zabbix_export>
    <version>2.0</version>
    <date>2014-12-29T13:55:05Z</date>
    <groups>
        <group>
            <name>Templates</name>
        </group>
    </groups>
    <templates>
        <template>
            <template>Template Zimbra Services</template>
```

```
<name>Template Zimbra Services</name>
<groups>
   <group>
      <name>Templates</name>
   </group>
</groups>
<applications>
   <application>
      <name>Zimbra</name>
   </application>
   <application>
      <name>Zimbra service</name>
   </application>
</applications>
<items>
   <item>
      <name>Zimbra version</name>
      <type>0</type>
      <snmp_community/>
      <multiplier>0</multiplier>
      <snmp_oid/>
      <key>zimbra.version</key>
      <delay>43200</delay>
      <history>7</history>
      <trends>365</trends>
      <status>0</status>
      <value_type>1</value_type>
      <allowed_hosts/>
      <units/>
      <delta>0</delta>
      <snmpv3_contextname/>
      <snmpv3_securityname/>
      <snmpv3_securitylevel>0</snmpv3_securitylevel>
      <snmpv3_authprotocol>0</snmpv3_authprotocol>
      <snmpv3_authpassphrase/>
      <snmpv3_privprotocol>0</snmpv3_privprotocol>
      <snmpv3_privpassphrase/>
      <formula>1</formula>
      <delay_flex/>
      <params/>
      <ipmi_sensor/>
      <data_type>0</data_type>
      <authtype>0</authtype>
      <username/>
```

```
            <password/>
            <publickey/>
            <privatekey/>
            <port/>
            <description/>
            <inventory_link>0</inventory_link>
            <applications>
               <application>
                  <name>Zimbra</name>
               </application>
            </applications>
            <valuemap/>
            <logtimefmt/>
         </item>
      </items>
      <discovery_rules>
         <discovery_rule>
            <name>Zimbra services discovery</name>
            <type>0</type>
            <snmp_community/>
            <snmp_oid/>
            <key>zimbra.discovery</key>
            <delay>86400</delay>
            <status>0</status>
            <allowed_hosts/>
            <snmpv3_contextname/>
            <snmpv3_securityname/>
            <snmpv3_securitylevel>0</snmpv3_securitylevel>
            <snmpv3_authprotocol>0</snmpv3_authprotocol>
            <snmpv3_authpassphrase/>
            <snmpv3_privprotocol>0</snmpv3_privprotocol>
            <snmpv3_privpassphrase/>
            <delay_flex/>
            <params/>
            <ipmi_sensor/>
            <authtype>0</authtype>
            <username/>
            <password/>
            <publickey/>
            <privatekey/>
            <port/>
            <filter>:</filter>
            <lifetime>30</lifetime>
            <description/>
```

```
<item_prototypes>
   <item_prototype>
      <name>Zimbra service &amp;quot;$1&amp;quot;</name>
      <type>0</type>
      <snmp_community/>
      <multiplier>0</multiplier>
      <snmp_oid/>
      <key>zimbra.status[{#ZIMBRASERVICE}]</key>
      <delay>120</delay>
      <history>7</history>
      <trends>365</trends>
      <status>0</status>
      <value_type>3</value_type>
      <allowed_hosts/>
      <units/>
      <delta>0</delta>
      <snmpv3_contextname/>
      <snmpv3_securityname/>
      <snmpv3_securitylevel>0</snmpv3_securitylevel>
      <snmpv3_authprotocol>0</snmpv3_authprotocol>
      <snmpv3_authpassphrase/>
      <snmpv3_privprotocol>0</snmpv3_privprotocol>
      <snmpv3_privpassphrase/>
      <formula>1</formula>
      <delay_flex/>
      <params/>
      <ipmi_sensor/>
      <data_type>0</data_type>
      <authtype>0</authtype>
      <username/>
      <password/>
      <publickey/>
      <privatekey/>
      <port/>
      <description/>
      <inventory_link>0</inventory_link>
      <applications>
         <application>

            <name>Zimbra service</name>
         </application>
      </applications>
      <valuemap>
         <name>Service state</name>
```

```
                    </valuemap>
                    <logtimefmt/>
                  </item_prototype>
                </item_prototypes>
                <trigger_prototypes>
                  <trigger_prototype>
                    <expression>{Template Zimbra
Services:zimbra.status[{#ZIMBRASERVICE}].last()}#1</expression>
                    <name>Zimbra service &amp;quot;{#ZIMBRASERVICE}&amp;quot; not
running on {HOST.NAME}</name>
                    <url/>
                    <status>0</status>
                    <priority>2</priority>
                    <description/>
                    <type>0</type>
                  </trigger_prototype>
                </trigger_prototypes>
                <graph_prototypes/>
                <host_prototypes/>
              </discovery_rule>
            </discovery_rules>
            <macros/>
            <templates/>
            <screens/>
          </template>
        </templates>
</zabbix_export>
```

Instalar Agente Zabbix en OpenSuse

1. Añadir el repositorio de Zabbix. Elegir dependiendo de la versión de la distribución.

   OpenSuse 12.3:

```
# zypper addrepo
http://download.opensuse.org/repositories/server:/monitoring/openSUSE_12.3
server_monitoring
```

   OpenSuse 13.2:

```
# zypper addrepo
http://download.opensuse.org/repositories/server:/monitoring/openSUSE_13.2
server_monitoring
```

   OpenSuse 42.1:

```
# zypper addrepo http:/
/download.opensuse.org/repositories/server:/monitoring/openSUSE_Leap_42.1
server_monitoring
```

2. Actualizar los repositorios del sistema.

```
# zypper update
```

3. Inslar el agente zabbix.

```
# zypper install zabbix-agent
```

4. Cambiar el archivo de configuración de agente Zabbix.
   a. Ingresar al directorio de configuración:
      `# cd /etc/zabbix/`
   b. Modificar el archivo de configuración:
      `# vi zabbix_agentd.conf`
   c. Cambiar los siguientes parámetros:

```
Server=192.168.1.3
Hostname=Nombre-del-Equipo
```

5. Habilitar el servicio del agente Zabbix.

```
# systemctl enable zabbix-agentd.service
```

6. Iniciar el servicio del agente Zabbix.

```
# systemctl start zabbix-agentd.service
```

Instalar Agente Zabbix en Debian

1. Añadir el repositorio de Zabbix. Elegir dependiendo de la versión de la distribución.

   Zabbix 2.0 para Debian 6:

   ```
   # wget http://repo.zabbix.com/zabbix/2.0/debian/pool/main/z/zabbix-release/zabbix-release_2.0- 1squeeze_all.deb
   ```

   Zabbix 2.0 para Debian 7:

   ```
   # wget http://repo.zabbix.com/zabbix/2.0/debian/pool/main/z/zabbix-release/zabbix-release_2.0-1wheezy_all.deb
   ```

2. Instalar agente Zabbix.

   ```
   # apt-get install zabbix-agent
   ```

3. Cambiar el archivo de configuración de agente Zabbix.
   a. Ingresar al directorio de configuración:
      ```
      # cd /etc/zabbix/
      ```
   b. Modificar el archivo de configuración:
      ```
      # vi zabbix_agentd.conf
      ```
   c. Cambiar los siguientes parámetros:
      ```
      Server=192.168.1.3
      Hostname=Nombre-del-Equipo
      ```

4. Habilitar el servicio del agente Zabbix.

   ```
   # systemctl enable zabbix-agentd.service
   ```

5. Iniciar el servicio del agente Zabbix.

   ```
   # systemctl start zabbix-agentd.service
   ```

Instalar Agente Zabbix en Windows

1. Descargar el agente desde la URL: http://www.zabbix.com/download.php
2. Extraer la carpeta en: C:\Archivos de Programas\zabbix
    a. Se extraerán dos carpetas: bin y conf
3. Entrar a la carpeta conf
    a. Modificar con el wordpad el archivo: zabbix_agentd.win.conf
    b. Abrir el wordpad como administrador.
    c. En el parámetro Server poner la IP del servidor: Server=172.16.1.3
    d. En el parámetro Hostname poner el nombre del equipo.
4. Copiar el archivo de configuración dentro de la carpeta bin y luego en la carpeta que indique correctamente el tipo de sistema operativo.
5. Abrir el cmd como administrador
    a. Ingresar a la ruta: cd C:\Archivos de Programas\zabbix\bin\win32\
    b. Ejecutar el comando: zabbix_agent.exe -c zabbix_agentd.win.conf --install
    c. Ejecutar el comando: zabbix_agent.exe –start
6. Para desinstalar: zabbix_agent.exe -c zabbix_agentd.win.conf –uninstall
7. Agregar en el firewall de Windows o del antivirus para que el ejecutable zabbix_agent.exe tenga permiso de entrada y de salida.

ANEXO C

m.3. Anexo C: Creación de mapa de red

Una de los componentes que trae consigo el software Zabbix es la de poder crear un mapa con todos los host configurados, en este manual procederemos a indicar como lo creamos paso a paso.

Como requisito para poder crear el mapa necesitamos haber agregado los host que queremos aparezcan en el gráfico.

Ingresar a la página de configuración de software vía web. URL: http://IP-Servidor

Imagen 65: Anexo C: Pantalla de ingreso
Fuente: El Autor

Ingresar el usuario y la clave.

1. Dirigirse a: Configuration → Maps → Create map

Imagen 66: Anexo C: Creación de mapa
Fuente: El Autor

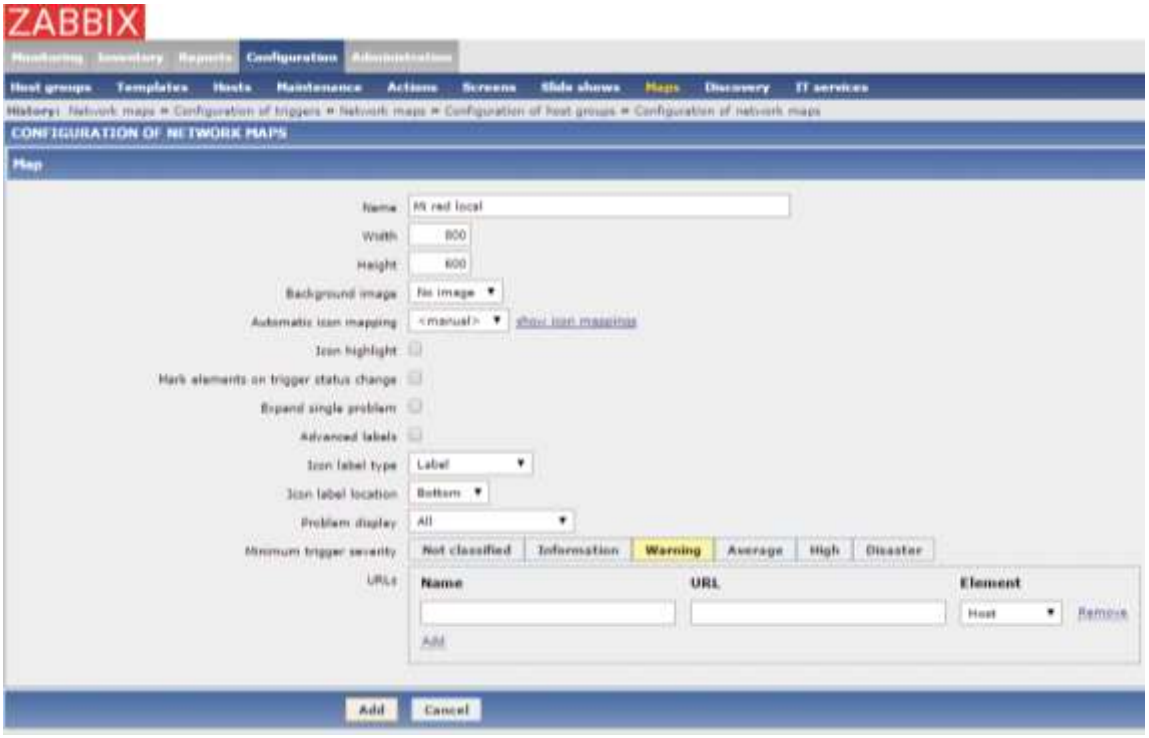


Imagen 67: Anexo C: Pantalla de configuración de mapas
Fuente: El Autor

Los datos necesarios de llenar son:

- Name: Poner un nombre de identificación.
- Width y Height: Ingresar el ancho y alto que se quiera a la "mesa de dibujo".
- Minimun trigger severity: Especificar desde que tipo de incidencias queremos se muestre.

Dar clic en Add.

2. Se regresa a la pantalla anterior y dar clic sobre el nombre del gráfico creado.

Imagen 68: Anexo C: Pantalla que muestra los mapas creados
Fuente: El Autor

Esto enviará a la mesa de dibujo donde se debe ir agregando los hosts.

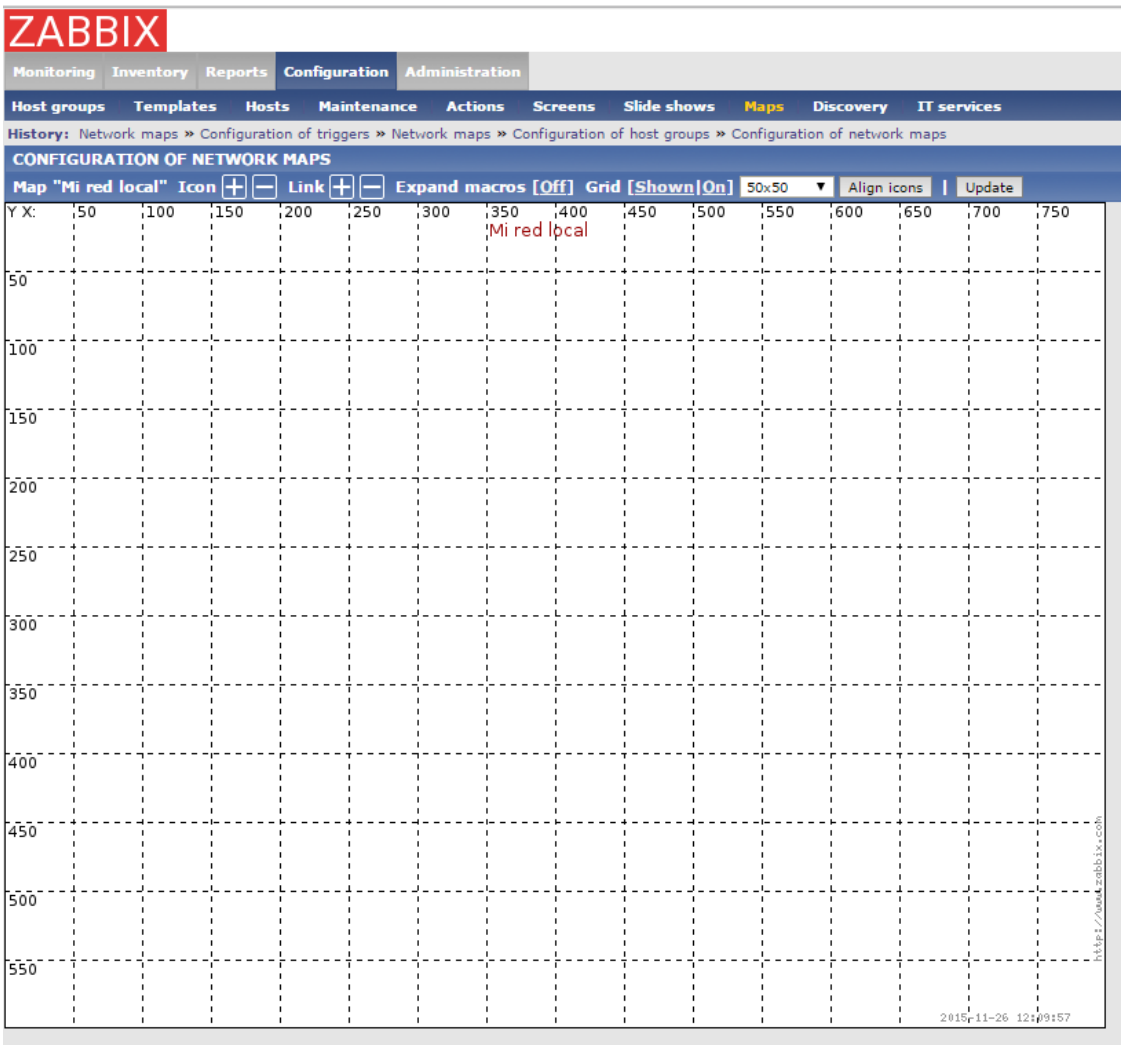


Imagen 69: Anexo C: Mesa de trabajo
Fuente: El Autor

3. Dar un clic sobre el símbolo + de Icon e inmediatamente aparecerá un nuevo elemento.

Imagen 70: Anexo C: Agregar nuevo elemento
Fuente: El Autor

4. Dar un clic sobre el nuevo elemento y se abre una pequeña ventana.

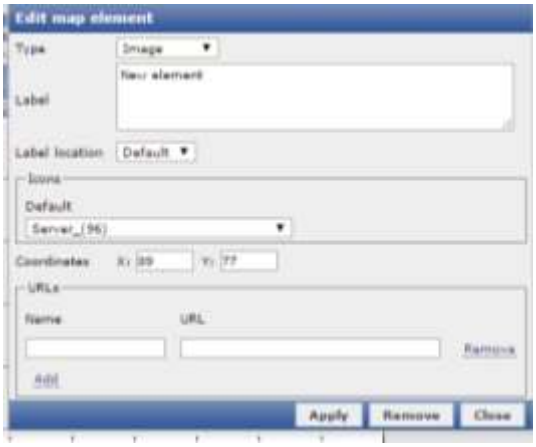


Imagen 71: Anexo C: Editar elemento
Fuente: El Autor

5. En el casillero Type especificar que es host y dar clic en Select.

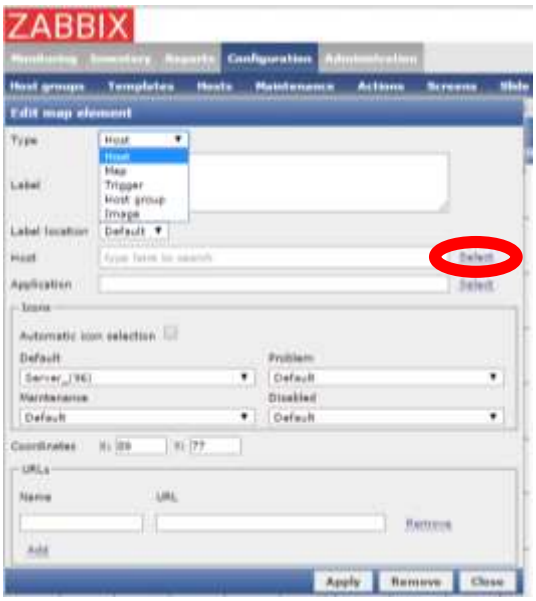


Imagen 72: Anexo C: Seleccionar host
Fuente: El Autor

Este proceso abre una nueva ventana donde muestra la lista de hosts disponibles.

En la parte superior elegir el grupo y en la parte inferior aparecen los hosts asignados a ese grupo.

Imagen 73: Anexo C: Lista de host
Fuente: El Autor

6. Seleccionar cualquiera de la lista y regresa a la pantalla anterior.
7. Zabbix trae varios tipos de gráficos para cada elemento, en este caso se seleccionará el que dice que es un servidor.

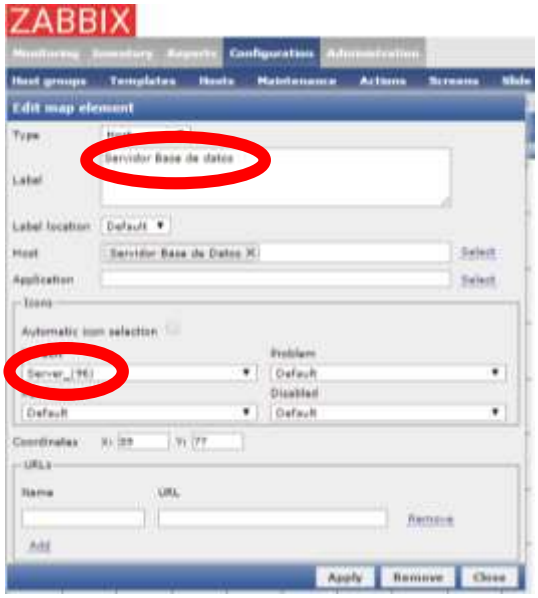


Imagen 74: Anexo C: Elección de tipo de gráfico
Fuente: El Autor

8. En el casillero Label dar un nombre con el que va a aparecer en el gráfico

9. Dar clic en Apply y luego Close. Con esto procedimiento se ha agregado un host.

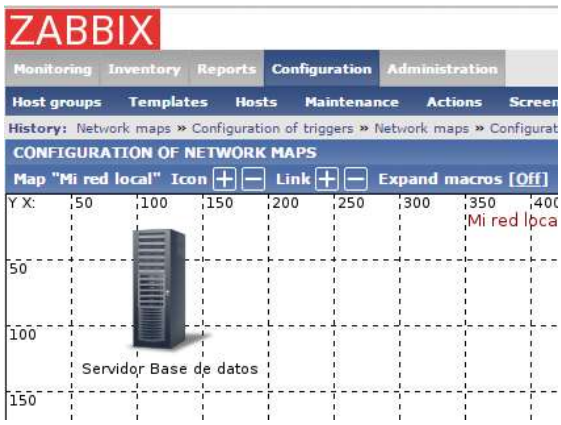


Imagen 75: Anexo C: Vista de mapa
Fuente: El Autor

Ahora se va a proceder a agregar otro host pero que va a ser de tipo Acces Point, repetir los pasos del 3 al 6.

En el paso 7 elegir tipo Router, el número que está en paréntesis es el tamaño del ícono por lo que puede elegir uno más grande o más pequeño.

Imagen 76: Anexo C: Configuración de nuevo host
Fuente: El Autor

Luego de haber elegido continuar con los pasos 8 y 9.

Agregando los host se puede notar que se muestran de una forma “indenpendiente” que no muestra la realidad de la conexión, para eso se puede añadir elementos tipo imagen como un switch para unirlos.

Repetimos los pasos 3 y 4, en el número 5 elegimos Type: Image y saltarse al paso 7 donde se especifica que es un Switch.

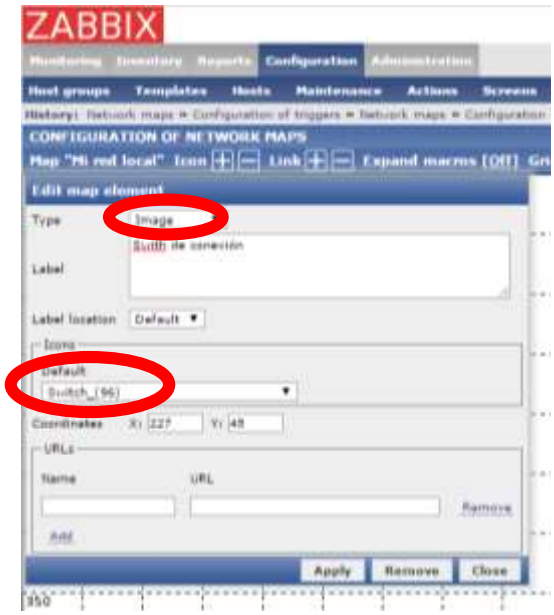


Imagen 77: Anexo C: Elección de tipo de gráfico
Fuente: El Autor

Luego de haberlo seleccionado se debe de proseguir con los pasos 8 y 9.

El gráfico deberá de verse de la siguiente manera:

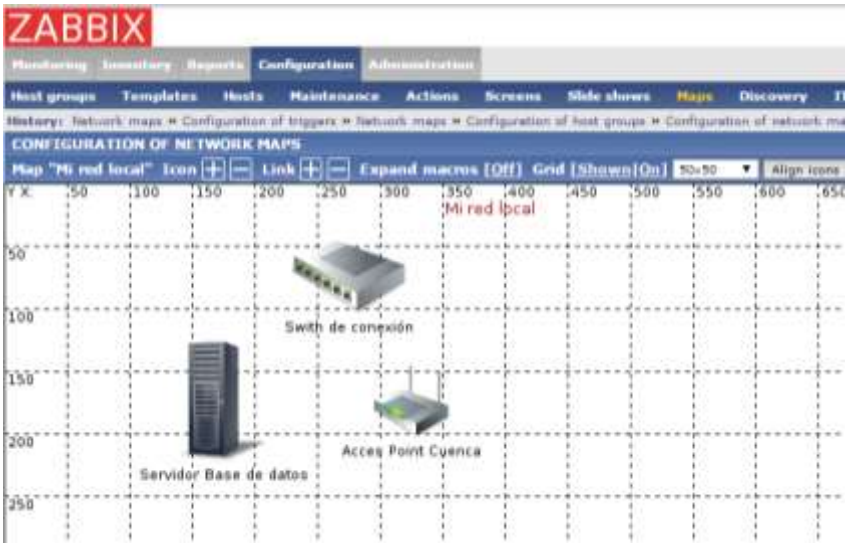


Imagen 78: Anexo C: Vista de mapa de red
Fuente: El Autor

Ahora se deben de unir los elementos.

Al seleccionar dos elementos con el mouse e inmediatamente se abre una pantalla.

Imagen 79: Anexo C: Lista de dispositivos inalámbricos
Fuente: El Autor

Con esa venta abierta dar un clic en el + que está al lado derecho de la palabra Link.

Imagen 80: Anexo C: Vista de dispositivo con link hacia otro
Fuente: El Autor

Con eso se ve en la parte inferior del gráfico anterior que automáticamente se agrega una relación entre los dos hosts.

Dar clic en Apply y Close.

Ahora se debe de ver en nuestro mapa una línea verde que une los dos elementos.

Imagen 81: Anexo C: Vista de mapa de red
Fuente: El Autor

Repetir estos pasos para todos los elementos se quieran unir.

Hay que seleccionar bien con el mouse solo los dos elementos que se deseen unir porque si seleccionamos más de dos, el programa va a mostrar una advertencia donde indica que solo se pueden unir dos elementos.

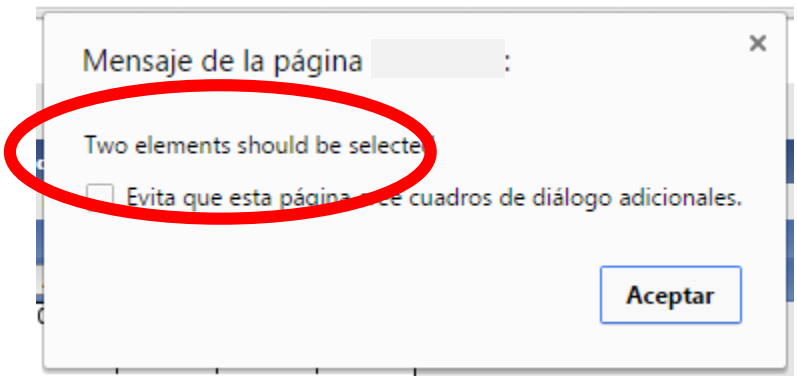


Imagen 82: Anexo C: Mensaje de advertencia
Fuente: El Autor

Es importante que cada vez que se haga un cambio dar un clic en el botón Update, caso contrario NO se guardarán los cambios.

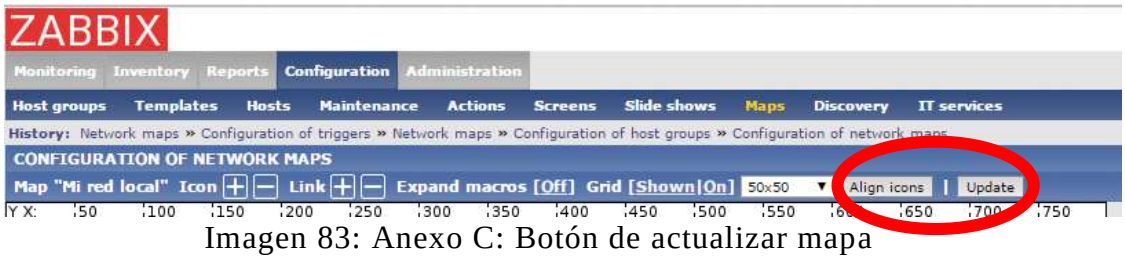


Imagen 83: Anexo C: Botón de actualizar mapa
Fuente: El Autor

Una vez unidos agregados y hechas las relaciones entre los dispositivos se tendrá un gráfico como el siguiente.

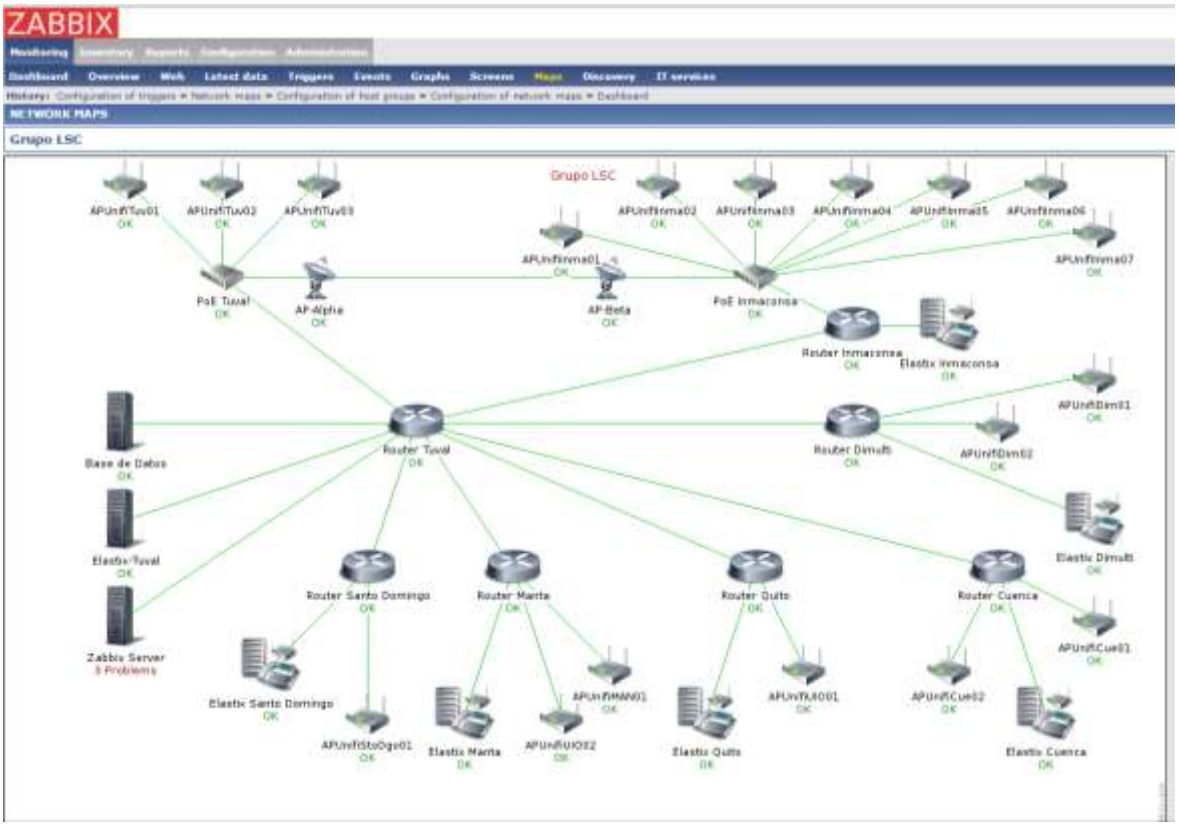


Imagen 84: Anexo C: Vista de mapa de red
Fuente: El Autor

ANEXO D

m.4. Anexo D: Modificación de trigger para adaptarlo a la necesidad de la empresa

Los trigger por defecto traen una configuración estándar para que se adapten a muchas empresas por lo que es necesario modificarlo para que aplique a la realidad de cada cual.

En el siguiente gráfico vamos a ver que el software nos muestra una alerta provocada por que existen muchos procesos en ejecución.

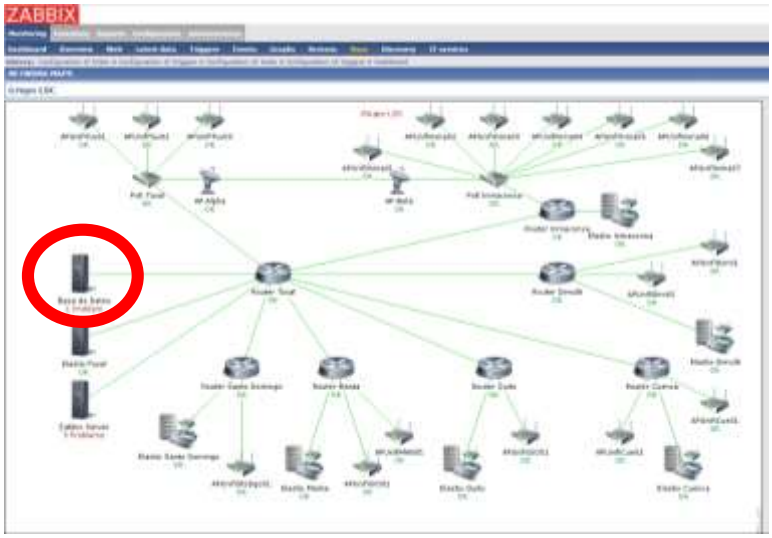


Imagen 85: Anexo D: Vista de mapa de red
Fuente: El Autor

Dar un clic sobre el gráfico e ir a la opción Triggers.

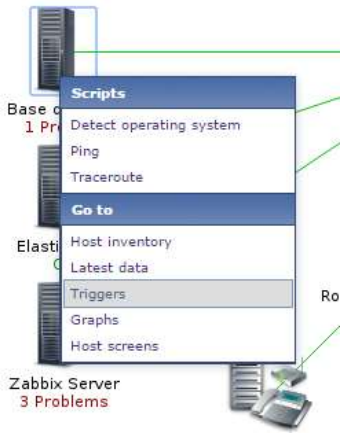


Imagen 86: Anexo D: Ventana de propiedades de host
Fuente: El Autor

Dar un clic sobre el nombre del Trigger e ir a la opción Configuration.

Imagen 87: Anexo D: Opción de trigger
Fuente: El Autor

En el siguiente gráfico se puede ver la Expression que se está utilizando.

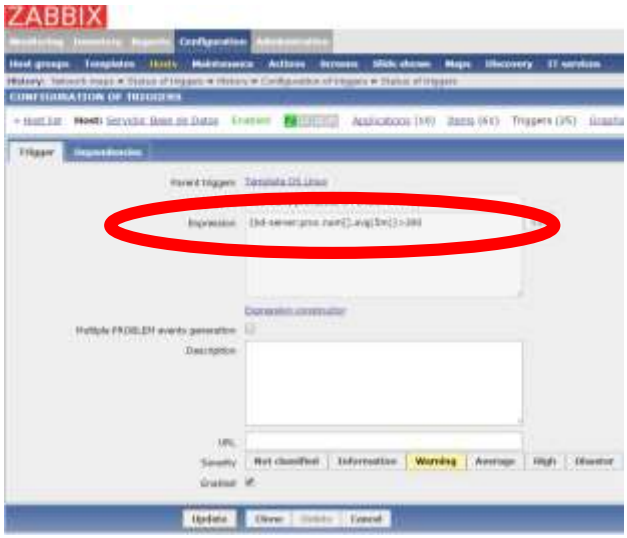


Imagen 88: Anexo D: Expresión de trigger
Fuente: El Autor

La expresión indica que cuando existan por más de 5 minutos más de 300 procesos muestre la advertencia, para la realidad de la empresa en la que se está desarrollando este proyecto el hecho de que el servidor de base de datos tenga 300 procesos en ejecución es poco y no justifica la activación de la advertencia.

Este trigger como viene heredado de la plantilla de servidores Linux (Template OS Linux) no puede ser modificada por lo que se procede a deshabilitarla y a crear otra modificando la cantidad de procesos.

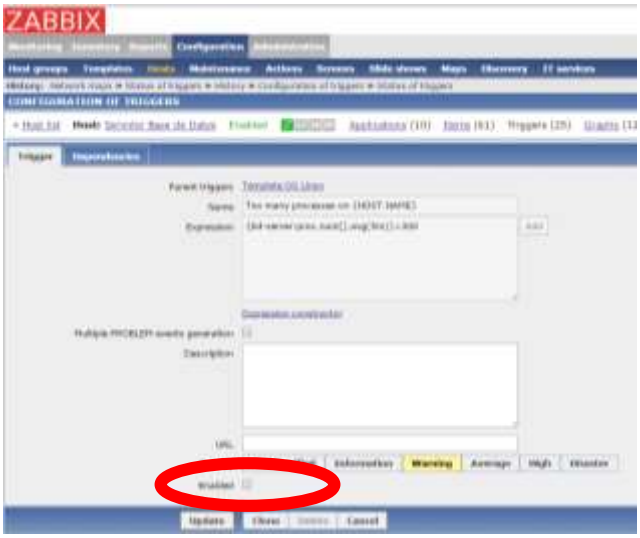


Imagen 89: Anexo D: Opción de habilitar/desabilitar trigger
Fuente: El Autor

Dar clic en Update.

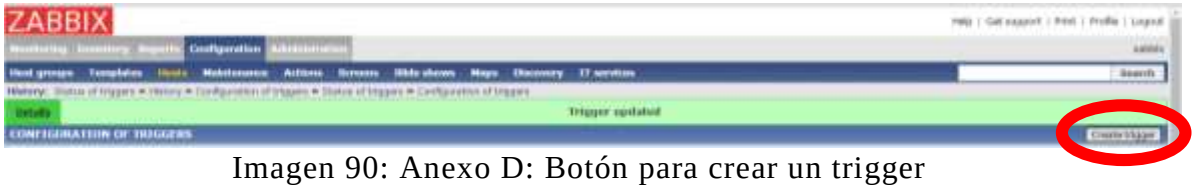


Imagen 90: Anexo D: Botón para crear un trigger
Fuente: El Autor

Dar clic en Create trigger.

Imagen 91: Anexo D: Creación de nuevo trigger
Fuente: El Autor

Se procede a llenar los campos necesarios. Se procede a explicar cada uno.

- Name: Un nombre que para poder indentificar la incidencia.
- Expression: La expresión a evaluar:
- Severity: Que categoría le vamos a dar a la incidencia.
- Enabled: Para habilitar el trigger.

La expresión indica: {bd-server:proc.num[].avg(5m)}>400

- bd-server: Es el nombre con el que fue añadido el host.
- proc.num[]: Función que pregunta la cantida de procesos presentes en el sistema operativo.
- avg(5m): Va a evaluar en un promedio de 5 minutos.
- >400: Cuando sea mayor a 400 procesos se activa el trigger.

Con esto se ha modificado el trigger y se peude ver en el gráfico que ya no muestra el problema.

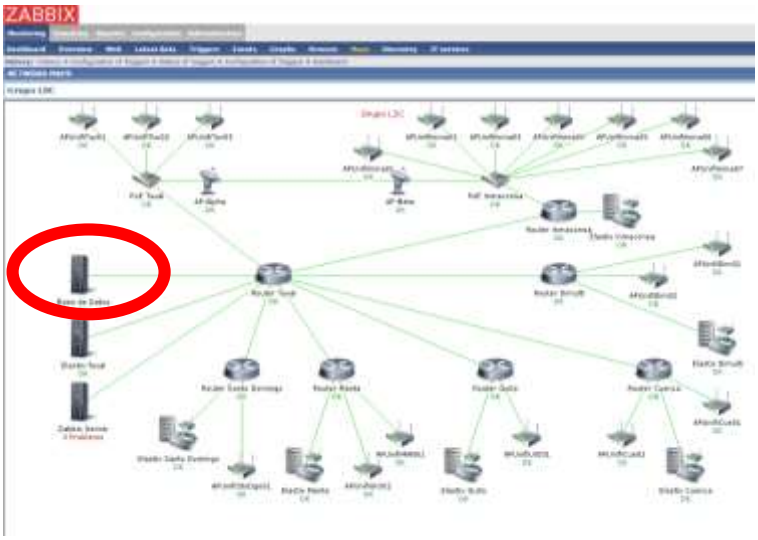


Imagen 92: Anexo D: Vista de mapa
Fuente: El Autor

Si se desea comprobar el correcto funcionamiento del trigger podemos crear procesos de prueba con el comando stress para que se incrementen y nos muestre la advertencia.

Imagen 93: Anexo D: Recepción de correo electrónico
Fuente: El Autor

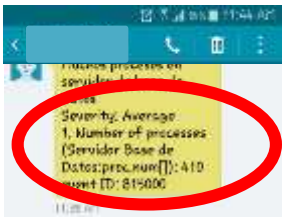


Imagen 94: Anexo D: Recepción de mensaje de texto
Fuente: El Autor

Recepción de correo electrónico y mensaje de texto notificando la incidencia e indicando la cantidad de procesos encontrados.