UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

FACULTAD DE INGENIERÍA DE SISTEMAS Y
ADMINISTRACIÓN DE EMPRESAS

CARRERA PROFESIONAL DE INGENIERÍA DE SISTEMAS

USO DE UN SISTEMA DE GESTIÓN DE MONITOREO PARA LA MEJORA DE LA ADMINISTRACIÓN DE SERVIDORES DE CLIENTES HOSTING EN GMD

TEMA DE INVESTIGACIÓN PARA OPTAR EL TÍTULO DE INGENIERA DE SISTEMAS

PRESENTADO POR LA BACHILLER:

LIZETH ELVIRA CAJAHUARINGA QUISPE

VILLA EL SALVADOR
2015

DEDICATORIA

Dedicado a Dios, a mi familia y amigos. En especial a mis amados padres que han estado a mi lado en cada momento de mi vida.

AGRADECIMIENTO

Agradezco a todos los profesores que en cada ciclo compartieron sus conocimientos y experiencias para enriquecer las nuestras. A los catedráticos del curso de titulación, porque hicieron que este tiempo de regresar a las aulas universitarias fuera la experiencia más grata de mi vida adulta. También agradezco a todas las autoridades, que gracias a ellos es posible todo lo logrado hasta ahora. De manera muy especial agradezco a mi asesor, el Dr. Ing. Frank Edmundo Escobedo Bailón por su apoyo y paciencia.

ÍNDICE

CAPITULO III:
DESARROLLO DE LA METODOLOGÍA

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

El presente trabajo de investigación lleva por título “USO DE UN SISTEMA DE GESTIÓN DE MONITOREO PARA LA MEJORA DE LA ADMINISTRACIÓN DE SERVIDORES DE CLIENTES HOSTING EN GMD” para optar el título de “Ingeniera de Sistemas”, presentado por la bachiller Lizeth Cajahuaringa Quispe.

Actualmente, cada vez más organizaciones han visto la necesidad de utilizar soluciones de monitoreo para tener un control de sus servidores. Inicialmente este tipo de herramientas sólo eran utilizadas por grandes empresas, ya que resulta bastante costoso acceder a este tipo de herramientas.

Al ser GMD una empresa de servicios del rubro de TI, ha visto la necesidad de implementar un sistema de gestión de monitoreo para la detención de fallas, inicialmente, en el servicio hosting que ofrecen a sus clientes.

En el mundo de la monitorización de servicios de red encontramos distintas aplicaciones. Las más utilizadas son las de código abierto o licenciado bajo licenciado bajo la GNU.

En este caso, GMD ha elegido la aplicación distribuida por la empresa altamente reconocida CA Technologies. Los nombre las aplicaciones son CA Spectrum y CA eHealth.

La estructura que hemos seguido en este proyecto se compone de 3 capítulos. El primer capítulo comprende el planteamiento del problema, el segundo capítulo el desarrollo del marco teórico y el tercer capítulo corresponde al desarrollo del proyecto.

CAPITULO I:
PLANTEAMIENTO DEL PROBLEMA

1.1. DESCRIPCIÓN DE LA REALIDAD PROBLEMÁTICA

Las soluciones de tecnología de GMD optimizan la estabilidad, confiabilidad y rendimiento de la infraestructura de sus clientes. Asimismo, le dan la flexibilidad que se requiere para integrar nuevas tecnologías con el fin de satisfacer las cambiantes necesidades de los usuarios.

Parte del servicio que ofrece GMD en la modalidad hosting a sus clientes es garantizar una administración de calidad a la TI del cliente. Para ello la empresa mediante el área de Operaciones Tecnológicas (COT), ofrece el servicio de gestión de monitoreo. El COT trabaja directamente con el área de Servicios Administrados, como su nombre hace suponer, en dicha área encontramos a los administradores de sistema operativo.

La gestión de monitoreo del COT consiste en notificar las fallas en el sistema del cliente a los administradores de sistemas para que puedan atender y solucionar las incidencias. Es preciso aclarar que bajo el servicio de monitoreo, el COT tiene como única función notificar incidencias al área Servicios Administrados. Sin embargo desde hace un tiempo se ha estado presentando una mayor cantidad de incidencias, así como también se observa que en tiempo de atención ante una situación crítica ha aumentado.

Actualmente se realiza el servicio de monitoreo en servidores mediante la aplicación de nombre SMonitor. Este software de monitoreo de red permite verificar la conectividad de red de hosts TCP / IP en Internet y a nivel de una red LAN. El programa realiza periódicamente pings de puertos TCP y UDP en los equipos clientes. Si el host de destino no responde a un ping; la aplicación realiza la notificación mediante alarmas audibles, notificaciones visibles, o mensajes de correo electrónico en forma continua. Es decir que cuando se presenta una falla en el sistema de algún cliente, la aplicación procede a realizar el envío de correos en forma continua y repetitiva a todos los operadores de sistemas del COT hasta que la incidencia haya sido atendida.

Puesto que actualmente se tienen 21 computadoras de escritorio con la aplicación SMonitor y en cada PC se registran distintas incidencias causa que los operadores de sistemas obvien alertas y nunca lleguen a ser reportadas, generando la degradación del servicio. En el mejor de los casos tardan mucho tiempo en reportar una situación crítica.

Otro gran problema es el tiempo de atención a un incidente. Ya que realizar el diagnóstico del problema consume mucho tiempo, esto genera que el tiempo de indisponibilidad de servicio sea mayor.

En vista de la gran cantidad de servidores que se tienen y requieren el servicio de monitoreo, se tiene la necesidad de contar con un registro de incidencias presentadas en los servidores al que podamos acceder de forma ágil y práctica. Asimismo, que sea capaz de concentrar todas las alertas en una sola consola.

También se debe automatizar la gestión de incidencias, por ello se necesita una solución de software que aparte de monitorear la conectividad a través del protocolo ICMP y otros protocolos en los equipos, permita conocer la utilización de recursos de un servidor en tiempo real. Es decir, se necesita una herramienta más completa, que nos permita tener una visión más amplia de los servidores. Para que en un caso de urgencia, el administrador pueda realizar descartes de forma rápida y oportuna, ya que actualmente la gestión de un

administrador inicia con un incidente en el servidor. Es decir se trabaja de forma reactiva.

De igual forma se carece de un sistema de reportes de comportamiento de un equipo que sea capaz de mostrar la utilización de recursos en un periodo de tiempo.

1.2. JUSTIFICACIÓN DE LA INVESTIGACIÓN

GMD es una empresa que va en ascenso. Por ello debe contar con tecnología que le permita hacer frente a la competencia y asegurar un servicio de calidad a sus clientes.

Esta investigación presentará un sistema de gestión de monitoreo que, de acuerdo al prestigio del fabricante de la aplicación, asegurará la continuidad del servicio para los clientes hosting.

Una herramienta de monitoreo de servidores es fundamental para asegurar el funcionamiento de los sistemas informáticos. La monitorización de equipos también ayuda a optimizar el servicio, ya que facilita información detallada sobre el uso de recursos.

Los resultados obtenidos de esta investigación contribuirán en la comprensión de una nueva ola de soluciones tecnológicas revolucionarias para empresas. Un sistema de gestión de monitoreo ha dejado de ser considerado un complemento del servicio hosting y ha pasado a convertirse en una línea de negocio para las empresas de TI.

En conclusión, la solución de monitoreo que se propondrá cubre diferentes funcionalidades y permite tener una vista integral de la infraestructura de TI.

1.3. DELIMITACIÓN DE LA INVESTIGACIÓN

1.3.1 Conceptual

Servicio Hosting

El servicio hosting es una modalidad de alojamiento destinado principalmente a grandes empresas. Consiste básicamente en vender o alquilar un espacio físico de un centro de datos para que el cliente coloque ahí su propio ordenador. La empresa le da la provee a los equipos de energía eléctrica y la conexión a Internet, pero el servidor lo elige completamente el cliente, incluso el hardware.

Ya sea que se requiera reducir costos, aumentar la disponibilidad, incrementar la seguridad, integrar nuevas tecnologías u optimizar sus sistemas actuales.

Sistema de gestión de monitoreo para servidores

Una herramienta de monitoreo es fundamental para asegurar el funcionamiento de los sistemas informáticos y para evitar fallos en los sistemas. La monitorización también nos ayuda a optimizar la administración, ya que nos facilita información detallada en tiempo real sobre el uso de recursos del servidor.

Una solución de monitorización de servidores provee tranquilidad, confidencia y comodidad para el negocio.

Administración de servidores

Referida a la operación y mantenimiento de un servidor y/o un sistema de TI.

Generalmente, los administradores de servidores son responsables de la instalación, soporte y mantenimiento de un sistema o servidor informático.

Los servidores centralizados son fuentes de datos para una empresa y asegurarse de que funcionen sin problemas es fundamental. Evitar el tiempo de inactividad del servidor a través de un mantenimiento

programado, garantizando la seguridad del servidor y ayudar al personal en la conexión con el servidor son todas las tareas importantes de un administrador de servidores. Hacer una copia de seguridad de los datos del servidor es también un deber del personal de administración de servicios.

1.3.2 Espacial

La investigación se desarrollará en la Empresa GMD SA – Grupo Graña y Montero.

1.3.2 Temporal

Inicio: 20 de marzo del 2014

Término: 29 de setiembre del 2014.

1.4. FORMULACIÓN DEL PROBLEMA

¿De qué manera el uso de un sistema de gestión de monitoreo mejorará la administración de servidores de clientes hosting de GMD?

1.5. OBJETIVOS

1.5.1 Objetivo General

Establecer de qué manera la implementación y utilización de un sistema de gestión de monitoreo mejora la administración de servidores de los clientes hosting en GMD.

1.5.2 Objetivos Específicos

- Identificar los requerimientos del Centro de Operaciones Tecnológicas (COT).
- Implementar un sistema de gestión de monitoreo para servidores en GMD de acuerdo a los requerimientos del COT.
- Comprobar que la implementación de un sistema de gestión de monitoreo para servidores mejore la gestión de incidencias en GMD.

CAPITULO II:
MARCO TEÓRICO

2.1. ANTECEDENTES

Fausto Lamiña Lugmaña, Ana Ramos Tapia y Marco Yugsi Casa en su tesis “Análisis e implementación de un sistema de monitorización para la infraestructura tecnológica del edificio matriz del Instituto Nacional de Contratación Pública utilizando software de libre distribución” menciona cuán importante es una herramienta que permita controlar los recursos tecnológicos de una organización. También describe que un sistema de monitorización es un medio para alcanzar un fin y no un fin en sí mismo.

El enfoque de este proyecto consiste en tener control sobre los activos, la idea es tratar de fomentar la eficiencia en el manejo de las operaciones de la organización. Además de procurar que exista un control interno para mantener a la administración informada sobre el manejo operativo y financiero. También se considera dar visibilidad confiable de los recursos tecnológicos, para así, permitir a la gerencia tomar decisiones adecuados a la situación real que está atravesando la empresa.

En conclusión se puede decir, que el control interno está adquiriendo importancia en los últimos tiempos, a causa de numerosos problemas producidos por la ineficiencia en la utilización de recursos que conlleva a descuidar la continuidad de los servicios. (Ecuador, 2012).

Héctor Julián Selley Rojas en su tesis “Monitoreo del comportamiento de servidores de aplicaciones” destaca que la calidad del servicio se basa en el desempeño de los servidores de aplicaciones.

La calidad del servicio se mide a través de métricas o factores que pueden ocasionar problemas de desempeño en un servidor. Dichas métricas vienen a ser parámetros que reflejan el comportamiento o performance de un equipo.

Encontramos información teórica que sustenta bajo qué juicio se eligieron los parámetros para la medición de desempeño que realiza el software.

Además encontramos una metodología eficaz para la medición del desempeño de aplicaciones. Se puede observar que la herramienta desarrollada realiza un monitoreo permanente sobre un conjunto de métricas selectas y justificadas. Tal monitoreo devuelve valores, que son datos suficientes para que el usuario pueda observarlos y concluir en el desempeño que experimenta el servidor en ese momento. (México D.F., 2008).

Raúl Tapia Jardinez y David Sánchez Ruiz en su tesis “Propuesta de un sistema de monitoreo para la red de ESIME ZACATENCO utilizando el protocolo SNMP y software libre” muestran una alternativa de monitorización de red basada en software libre. Se muestra a detalle la implementación del software Nagios. Desde los requerimientos a nivel de arquitectura de la solución hasta la definición de objetos a ingresarse en la aplicación. Pasando por la descripción detallada de la configuración del software. Nagios es un sistema de supervisión de red y aplicación. Permite observar hosts y servicios que nosotros especifiquemos, además de alertar cuando sucesos inesperados ocurren en los Host y cuando estos están en buen estado. La gestión de Nagios se complementa con el MRTG (Multi Router Traffic Grapher) es una herramienta para supervisar principalmente la carga de tráfico en los enlaces de la red. MRTG genera páginas HTML que contienen imágenes PNG que ofrecen una representación visual de este tráfico en tiempo real. (México D.F., 2009).

José Luis Pinto Martinez en su tesis “Monitoreo centralizado de servidores de movilnet con herramientas de software libre” muestra una comparación entre un software libre y uno propietario. El mayor aporte encontrado son las consideraciones que se deben tomaren cuenta antes de la elección de una herramienta de monitoreo que finalmente prestará servicios a varios clientes. Si bien es cierto en esta investigación se concluye que Nagios, el software libre, permite mejores funcionalidades en el servicio; también es necesario evaluar la parte comercial a la hora de la elección. Es decir, en el trabajo se llega a demostrar la amplia ventaja del software libre a nivel de costos. Pero también se debe considerar que una empresa de servicios necesita soporte de las soluciones con las que trabaja.

Al contar con varios clientes nos exponemos a varias situaciones, para ello se necesita contar con el apoyo de especialistas que sean capaces de brindar una rápida solución a los problemas que se puedan generar.

También es necesario dejar en claro que las empresas dedicadas a la tecnología de la información deben estar a la vanguardia y contar con soluciones reconocidas para mayor tranquilidad de sus clientes. (Caracas, 2011).

Wilman Darío Sánchez Pico en su tesis **“**Propuesta de monitoreo de la infraestructura tecnológica de los servidores del ministerio de finanzas, basado en el modelo ITIL v3 y en la herramienta HP Sitescope” muestra una propuesta de monitoreo ha sido realizada siguiendo las recomendaciones de los procesos de ITIL V3 (Biblioteca de Infraestructura de Tecnologías de la Información) porque su metodología de trabajo ayudará a mantener la disponibilidad de los servicios.

En esta investigación de determinaron los procesos de Gestión de Disponibilidad de Eventos son los que se adaptan al monitoreo de infraestructura y a la vez ayudan a incrementar la satisfacción de los administradores quienes son responsables de optimizar y monitorizar los servicios para que funcionen ininterrumpidamente y de manera fiable, cumpliendo los niveles de servicios establecidos. (Quito, 2014).

2.2. BASES TEÓRICAS

2.2.1 Sistema de Gestión de Monitoreo y su evolución

Definición de un sistema de gestión de monitoreo

Un sistema de gestión de monitoreo es aquel que mediante una aplicación gestiona y centraliza la visualización del comportamiento de equipos en tiempo real.

Actualmente tenemos mercados dinámicos y competitivos que revelan la necesidad de contar con infraestructura tecnológica confiable y segura para agregar valor al negocio. Sin embargo, la administración de esta es cada vez más compleja y costosa, pues debe integrar un conjunto de servidores, sistemas operativos, aplicaciones, redes y almacenamiento de diversos proveedores de hardware y software.

Bajo esta situación, las empresas necesitan expandir sus capacidades, mejorar sus servicios y bajar sus riesgos y costos, lo que se consigue haciendo uso de un sistema de monitoreo.

Las herramientas de monitoreo facilitan la vida a los administradores de tecnología de la información. Directamente permiten conocer el uso de los recursos en el tiempo, el estado de las aplicaciones o servicios, ver el estado actual de hardware y software entre otros. Indirectamente permite proyectar la adquisición de nuevos equipos o partes, prevenir futuros problemas, incluso solucionar problemas actuales.

Las herramientas de monitoreo cumplen objetivos generales como:

- Alertar sobre problemas inminentes o actuales.
- Tener una visión centralizada de los equipos, servicios, software, hardware, versiones.
- Tener datos históricos de uso de recursos.

- Mostrar gráficos, reportes, resúmenes que ayudan a sintetizar la información.

Estos objetivos permiten a los administradores de TI realizar tareas como:

- Prevenir posible problemas futuros relacionados con falta de recursos por aumento de carga o uso.
- Resolver problemas inminentes con avisos y alertas pertinentes antes que el problema sea alertado por los usuarios finales.
- Estimar presupuestos para adquisiciones de software/hardware brindando datos históricos para sustentar la inversión.
- Realizar mejoras y optimizaciones en el uso de los recursos.
- Prevenir fallas de seguridad.
- Reforzar los puntos débiles de la infraestructura, ya sea hardware, software o servicios.

Evolución de las herramientas de monitoreo de redes

Entre los retos que por años han tenido que enfrentar los ejecutivos de TI está el presentar la información de su operación de manera tal que los ejecutivos de la organización; que tradicionalmente no son de origen tecnócrata; dispongan de elementos suficientes para reconocer y fomentar la importancia de la tecnología como un componente habilitador del negocio.

Han sido muchos los esfuerzos para hacer que la industria acuerde un estándar universal, primeramente a través de protocolos como la propuesta del ITU (Unión Internacional de Telecomunicaciones[1]): CMIP (Protocolo de administración de información común[2]), o las del IETF SNMP (Grupo de Tareas de Ingeniería de Internet)[3] (Protocolo Simple de Administración de Red)[4] y

[1] (ITU, s.f.)
[2] (ntmoduloredes, s.f.)
[3] (DICCIONARIO DE INFORMÁTICA Y TECNOLOGÍA, s.f.)
[4] (Huidobro, s.f.)

RMON (Monitoreo remoto de redes)[5], o bien a través de plataformas donde converge la información de todos los recursos de TI, como las aplicaciones de monitoreo HP Openview, IBM Tivoli, Sun Solstice o CA Infrastructure Management, por mencionar algunos.

La evolución de las herramientas de monitoreo también se ha ido alimentando mediante la llegada de protocolos más avanzados de visualización de tráfico como NetFlow, Jflow, Cflow, sflow, IPFIX o Netstream; el propósito hoy es tener una perspectiva global del "todo" para categorizar adecuadamente los eventos que afectan el desempeño de un servicio o del proceso de negocio involucrado.

Este arduo camino ha atravesado diferentes etapas como parte de su evolución y podríamos enumerarlas de la siguiente forma:

1ª Generación – Aplicaciones propietarias para monitorear dispositivos activos o inactivos

La industria ha desarrollado un sinfín de herramientas para tratar de presentar los recursos de una forma amable y en tiempo real. "Ahí, donde está la caja en rojo, eso quiere decir que el ruteador está fuera de servicio, por eso no hay conexión a la planta", esto es lo que dice el operador de la consola de monitoreo al contralor que ha solicitado previamente un reporte al momento de mermas en las líneas de producción para un artículo que está por lanzarse al mercado.

Las herramientas de monitoreo mostraban los elementos a través de un código universal de colores:

- En verde: todo está funcionando bien;
- En amarillo: se detectó que hay algún problema temporal que no afecta la disponibilidad, sin embargo, se deben realizar ajustes para no perder la comunicación;

[5] (eia.udg.es, s.f.)

- En naranja: el problema se ha hecho persistente y requiere pronta atención para evitar afectaciones a la disponibilidad;
- En rojo: el dispositivo se encuentra fuera de servicio en este momento y requiere acciones inmediatas para su restablecimiento.

Parece muy sencillo comprender esta convención de colores pero usualmente el nivel de detalle es insuficiente como se puede observar en la Figura N°1 ¿Qué pasa si el dispositivo que está en rojo sí está en funcionamiento y aun así no está realizando su función habitual?

Figura N°1
Sistema de Gestión de Monitoreo de 1ª Generación

Fuente: magazcitum.com

2ª Generación – Aplicaciones de análisis de parámetros de operación a profundidad

La siguiente generación de herramientas hace lo que se llama "*drill down*" o "análisis a profundidad"[6] con el fin de evaluar el estado de los componentes dentro del dispositivo (CPU, memoria, espacio de almacenamiento, paquetes enviados y recibidos, *broadcast*, *multicast*, etc.) de manera que se puedan buscar los parámetros de ajuste y que, de la misma forma en que se aprieta una tuerca en un engranaje de una máquina, los valores que se modifiquen permitan elevar los niveles de servicio del dispositivo como se puede observar en la Figura N°2.

Figura N°2 Sistema de Gestión de Monitoreo de 2ª Generación

Fuente: magazcitum.com

[6] (stefymichel.blogspot.com, s.f.)

Este tipo de aplicaciones se apoyan en analizadores de protocolos o "*sniffers*" y en elementos físicos distribuidos conocidos como "*probes"*, cuya función es exclusivamente la de colectar estadísticas del tráfico y que son controlados típicamente desde una consola central[7].

Si volvemos al mismo escenario del operador con estas nuevas posibilidades, éste sería un ejemplo de su argumento para explicar por qué no se genera el reporte: "Las estadísticas de transmisión de paquetes nos indican que la interfaz WAN 3 del ruteador está transmitiendo con altos niveles de *broadcast*, lo que está provocando que haya malos tiempos de respuesta y que, en consecuencia, se produzcan retransmisiones de paquetes".

Tenemos considerablemente mayor información pero aún no hemos podido llevarla de una manera tangible a un ejecutivo del negocio para valorar conjuntamente el nivel de afectación que se esté dando.

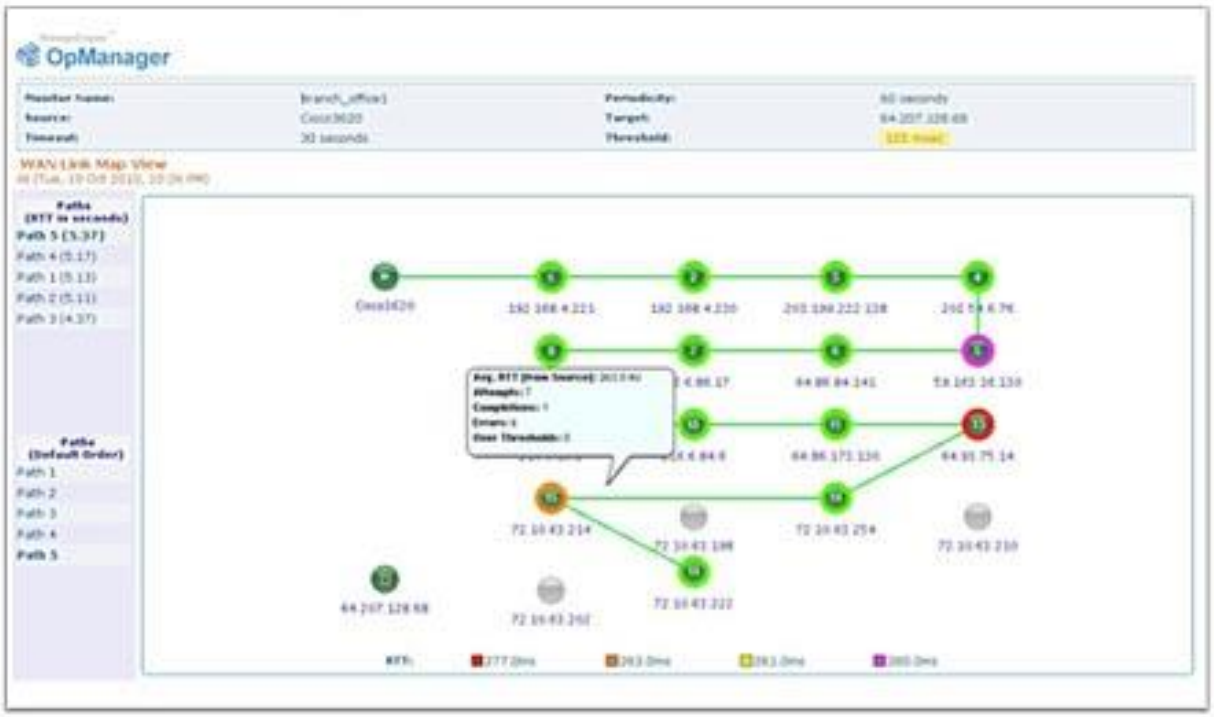
3ª Generación – Aplicaciones de análisis punta a punta con enfoque a servicio

Con mayores niveles de información sobre los dispositivos tenemos elementos adicionales de análisis, pero aún no existen suficientes parámetros para tomar decisiones. Ahora un problema es provocado por la conjunción de varios dispositivos que participan dentro de un mismo servicio; la visión debe ser más integral y en la medida de lo posible correlacionar el comportamiento de elementos tan autónomos y dispersos como una base de datos, un servidor, un switch y hasta un enlace de comunicaciones, pero al mismo tiempo mantenerlos interdependientes porque todos participan en un mismo servicio. Como ejemplo se podría tomar una consulta de inventarios o la colocación de un pedido.

[7] (www.ca.com, s.f.)

Esta generación de aplicaciones con enfoque transaccional captura ahora “flujos” de tráfico e identifica cuellos de botella y latencias; lapso necesario para que un paquete de información se transfiera[8]; a lo largo de las conexiones que existen entre los componentes de un servicio, y entrega información acerca de la salud del mismo.

Figura N°3 Sistema de Gestión de Monitoreo de 3ª Generación



Fuente: magazcitum.com

Haciendo el símil con un eventual caso de la vida real, se tendría una explicación más o menos como la siguiente: “…….los niveles de uso de CPU en el servidor de base de datos están en picos que van por arriba de 80%, esto aumenta los tiempos de respuesta de la aplicación Web y entonces se genera un alto número de retransmisiones que saturan el actual ancho de banda que

[8] (www.alegsa.com.ar, s.f.)

tenemos; esta serie de factores se reflejan en que el Servicio de Consulta de Créditos en línea sea uno de los primeros afectados…."

Esta vez hemos logrado construir un puente entre los elementos de tecnología y los servicios que están disponibles para cualquier usuario de la organización. Ahora podríamos decir que todas las partes hablan el mismo lenguaje y que las decisiones podrán ser tomadas con un enfoque de la repercusión que generan en el negocio como se puede observar en la Figura N°3.

4ta. Generación – Personalización de indicadores de desempeño de los procesos de negocio.

Llevando el crecimiento de las soluciones tecnológicas a los requerimientos de las organizaciones de hoy, llegamos a las vistas de "dashboard"[9] que son indicadores que el cliente puede crear y personalizar de acuerdo a sus necesidades como se observa en la Figura N°4, además de poder seleccionar las variables que requiere correlacionar para mostrar de una manera gráfica a los tomadores de decisiones qué nivel de cumplimiento se está entregando en los procesos de negocio.

Dentro de esta generación de soluciones están aquellas que monitorean el Desempeño de Aplicaciones (APM, por sus siglas en inglés), donde convergen elementos de tecnología ("Backend") con los sistemas de los que forman parte, y éstos con las aplicaciones que integran para llevar a cabo las transacciones que impulsan los procesos de negocio ("Frontend"). Esto, en otras palabras, es el análisis de punta a punta.[10]

[9] (www.sixtinagroup.com, s.f.)
[10] (www.alegsa.com.ar, s.f.)

Figura N°4 Sistema de Gestión de Monitoreo de 4ª Generación

Fuente: magazcitum.com

2.2.2 Administración De Servidores

La administración de servidores es una tarea con conocimientos científicos, humanísticos, técnicos, lógicos y sistémicos que lo capacitan para formular, diseñar, implementar y auditar políticas, estrategias, planes y programas en el campo de los sistemas de información utilizados en las distintas organizaciones.

“ En la pequeña, mediana y gran organización se necesita control; control concerniente a quién tiene permitido el acceso a los recursos de información de la organización, cómo se verifica la identidad de alguien, qué se le permite

hacer, cómo hacer un efectivo control y cómo almacenar los incidentes para una auditoria e incrementar la eficiencia de la infraestructura de red.

El software de sistema operativo proporciona a los profesionales de TI más control sobre sus servidores e infraestructura de red y les permite centrarse en las necesidades críticas del negocio. Capacidades mejoradas en secuencias de comandos y automatización de tareas, como las que ofrece Windows PowerShell, ayudan a los profesionales de TI a automatizar tareas comunes de TI.

Las funcionalidades del sistema operativo facilitan la tarea de administrar y proteger las múltiples funciones de servidor en una empresa. También proporciona un único origen para administrar la configuración del servidor y la información del sistema. Existen asistentes que automatizan muchas de las tareas de implementación de sistemas que tardan más tiempo. De igual manera encontramos herramientas mejoradas de administración del sistema, como el monitor de rendimiento y confiabilidad, ofrecen información sobre sistemas y alertan al personal de TI sobre problemas potenciales antes de que sucedan."[11]

Por consiguiente, un administrador de sistemas operativos debe ser un conocedor crítico de las innovaciones, cambios, tendencias y desafíos tecnológicos relacionados con el desarrollo informático, a fin de que pueda garantizar el eficiente funcionamiento y administración de los recursos informáticos que posee la empresa, además de estar en capacidad de crear y dirigir empresas que aporten soluciones a las necesidades informáticas del entorno, contribuyendo al desarrollo de la sociedad en general. Dentro de los roles que desempeña encontramos los siguientes:

- Realizar copias de seguridad de datos.
- Aplicar actualizaciones del sistema operativo, y los cambios de configuración.
- Instalación y configuración de nuevo hardware / software.

[11] (SENATI, Manual de Practicante - Administración de Redes, 2008)

- Añadir / borrar / modificar información de cuenta de usuario, restablecer contraseñas, etc.
- Respuesta a consultas de carácter técnico.
- Responsable de la seguridad.
- Documentar la configuración del sistema.
- Afinar el rendimiento de los sistemas.
- Mantener la red funcionando.
- Crear nuevos usuarios.
- La restauración de contraseñas de usuario.
- Bloqueo / desbloqueo de cuentas de usuario.
- Monitor de la seguridad del servidor
- Monitor de servicios especiales, etc.
- Administración de usuarios (instalación y mantenimiento de cuentas)
- El mantenimiento de sistema.
- Comprobar que los periféricos funcionan correctamente
- En caso de fallo de hardware, el designa los horarios de reparación
- Monitor de rendimiento del sistema
- Crear sistemas de ficheros
- Crear la política de copias de seguridad y recuperación
- Monitor de la comunicación de red
- Actualizar los sistemas según sean accesibles nuevas versiones de SO y software aplicativo
- Aplicar las políticas para el uso del sistema informático y de red
- Configuración de las políticas de seguridad para los usuarios (Un administrador de sistemas debe contar con una sólida comprensión de la seguridad informática por ejemplo, cortafuegos y sistemas de detección de intrusos).

Todas las actividades nombradas inicialmente se realizan para prevenir incidentes en el equipo que tienen bajo su administración. Parte muy importante las labores de la administración de sistemas es atender las

situaciones en que el servidor corre peligro, es decir cuando se produce un incidente.

2.2.3 CA Spectrum Infrastructure Manager

CA Spectrum es un sistema de servicios y gestión de la infraestructura que monitorea el estado de elementos, incluyendo la gestión de dispositivos, aplicaciones, sistemas host y conexiones.
La información de estado, como fallos y rendimiento de datos a partir de estos elementos se recogen y almacenan. CA Spectrum analiza constantemente esta información para realizar un seguimiento de las condiciones dentro de la infraestructura informática. Si se detecta una condición anormal, se aísla y se notifica. También indica las posibles causas y soluciones al problema.

El diseño de CA Spectrum se basa en el modelo cliente / servidor. Su servidor principal, el SpectroSERVER, es responsable de recolección, almacenamiento y procesamiento de datos.

El SpectroSERVER utiliza Inductive Modeling Technology (IMT) para realizar estas funciones. IMT combina una base de datos orientada a objetos con la inteligencia de los controladores de inferencia. La base de datos orientada a objetos contiene los tipos de modelos que definen cómo se representa un elemento administrado, y los modelos que representan elementos administrados específicos. La base de datos orientada a objetos también contiene las relaciones que definen las posibles asociaciones entre los tipos de modelo. Los controladores de inferencia aportar funciones adicionales a este sistema por reacción a los eventos producidos por CA Spectrum o elementos gestionados.

SpectroSERVER almacena data en la base de conocimientos en la que se definen los tipos, modelos y relaciones. El SpectroSERVER también sondea los elementos gestionados y recibe información de alerta de la infraestructura

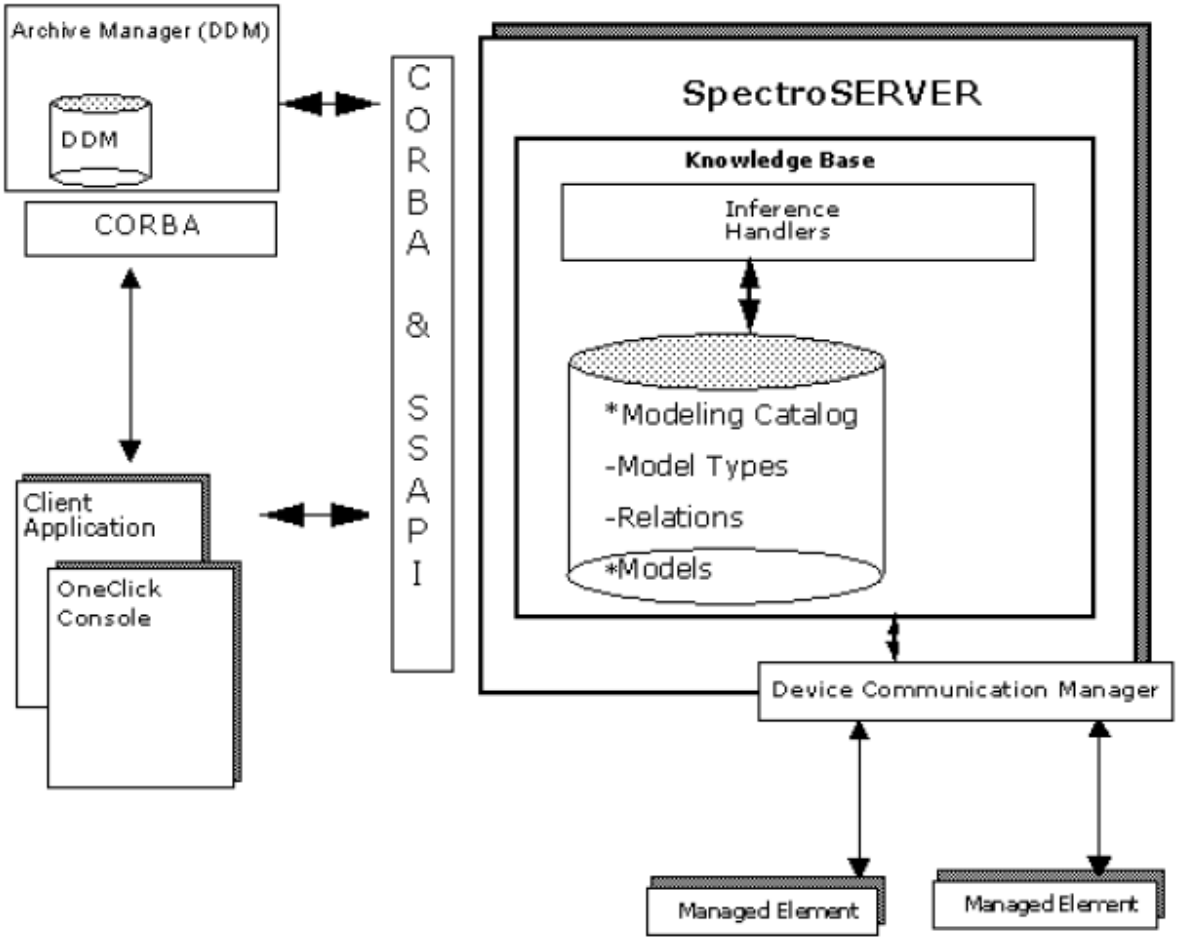
informática. También analiza y almacena esta información en la base de conocimientos, y da acceso a la información de las aplicaciones del cliente.

CA Spectrum incluye una serie de aplicaciones para el cliente. Su aplicación principal es OneClick, que proporciona la interfaz gráfica de usuario que se utiliza para controlar la red y lanzar otras aplicaciones. Las vistas proporcionadas en la Consola de OneClick contienen iconos, tablas y gráficos que representan los diferentes elementos de la red. Estos componentes gráficos proporcionan información de estado actual y proporcionan acceso para la gestión específica de facilities. Toda la información presentada por las aplicaciones es a partir del SpectroSERVER.

SpectroSERVER

El SpectroSERVER es el servidor principal de CA Spectrum. Funciona como un servidor de base de datos, motor de modelado, y el administrador de dispositivos. Además procesa eventos, genera alarmas y seguimiento de las estadísticas relativas a los elementos gestionados. Toda esta información está disponible para aplicaciones de cliente y se puede solicitar a través de la interfaz de programación de aplicaciones SpectroSERVER (SSAPI) y la interfaz de CA Spectrum CORBA, ver la Figura N°1.

Figura N°5 Componentes de la SpectroSERVER



Fuente: CA Spectrum® Infrastructure Manager - Concepts Guide r9.2

El SpectroSERVER también se conoce como el VMN[12] o Máquina Virtual Network. Específicamente, el término VNM se refiere a la porción de la SpectroSERVER que es responsable para el modelado de elementos gestionados.

CA Spectrum Bases de datos

CA Spectrum incluye las siguientes bases de datos:

- Base de datos SpectroSERVER, requeridos por el SpectroSERVER.

[12] (Ministerio de Educación, 2007)

- Distributed Data Manager (DDM) de base de datos, requerido por el Administrador de Archivos.
- Herramientas de base de datos MIB, requeridos por la utilidad Herramientas MIB.
- Base de datos de informes, requerido por el Administrador de informes y el Administrador de servicios.
- Base de datos de integración eHealth, requerido por la integración CA Spectrum y eHealth.

Base de Conocimiento

Uno de los principales componentes de SpectroSERVER es la base de conocimientos. La base de conocimientos está compuesta tanto por los datos como la información sobre los procedimientos necesarios para gestionar una infraestructura de computación.

La base de conocimientos tiene un componente que almacena los tipos de modelos, relaciones y eventos y la información estadística. Utiliza un sofisticado sistema de modelos y relaciones entre modelos para representar y almacenar información sobre los elementos de la infraestructura informática. En esencia, este sistema de modelos y las relaciones entre ellos, cuando se ve como una sola entidad lógica, describe la topología física y lógica de la infraestructura informática de CA Spectrum que construye sus capacidades de análisis de causa raíz de esta base.

Todos los modelos de la base de conocimientos se basan en plantillas conocidas como tipos de modelos. Los tipos de modelo definen las propiedades que conforman un modelo instanciado y se almacenan en el catálogo de modelos de la base de conocimientos.

La base de conocimientos también contiene procesos que proporcionan inteligencia a los tipos de modelo. Estos procesos incluyen controladores y

acciones de inferencia. Los datos generados o utilizados para apoyar estos procesos se almacenan en la memoria mientras el SpectroSERVER está en marcha y es también parte de la base de conocimientos. Además de los modelos y tipos de modelo, la base de conocimientos utiliza el Administrador de Archivos y el Administrador de datos distribuidos (DDM) para almacenar el evento histórico y la información estadística sobre modelos específicos. Esta información se acumula con el tiempo, dejando CA Spectrum obtener un amplio conocimiento acerca de la infraestructura informática se está gestionando.

Catálogo de Modelado

El catálogo de modelos es meta-datos de la base de conocimientos. Los objetos del catálogo de modelos son cargados con CA Spectrum y son relativamente estáticos. Sin embargo, se puede manipular algunos aspectos del catálogo para fines de ajuste, o personalizarlo para que CA Spectrum pueda estar al tanto de las nuevas tecnologías de red o nuevos tipos de elementos gestionados introducidas en la infraestructura informática.

Tipos de modelos

Tipos de modelo corresponden principalmente a diferentes familias de elementos gestionados y son las plantillas utilizadas para construir modelos. Los tipos de modelo contienen la información o atributos necesarios para gestionar un tipo específico de elemento. También poseen la inteligencia que le dice a Spectrum CA cómo el elemento gestionado representado por el tipo de modelo se comporta y cómo reacciona a los eventos que ocurren en el elemento gestionado o en otras partes de la red.

Por ejemplo, el catálogo de modelado CA Spectrum contiene un tipo de modelo NokiaFW. Este tipo de modelo representa ciertos tipos de Nokia Firewalls como IP330, IP440, IP650, IP740 e. CA Spectrum los utiliza para crear un modelo que representa un Nokia Firewall específico en una red. Cada tipo de modelo se identifica de forma única en el catálogo de modelos

utilizando un número que referencia un tipo de modelo, por lo general representado en formato hexadecimal.

Tipo Modelo Atributos

Cada tipo de modelo tiene atributos que definen la mayor parte del conocimiento declarativo que define las características y propiedades del elemento gestionado que representa el tipo de modelo. Estos atributos pueden ser internos o externos. Atributos internos reflejan información que es específica para la gestión del espectro CA de un elemento particular. Atributos externos reflejan los objetos de los MIB soportados por el elemento gestionado. Todos los atributos tienen valores predeterminados asociados con el tipo de modelo.

Reporting database o Base de datos de informes

El administrador de informes se incluye en la instalación OneClick. Es utilizado para almacenar datos de la gestión del servicio, datos de activos, acontecimiento histórico y datos de alarma para los informes.

El SpectroSERVER e Hilos

El SpectroSERVER debe manejar las peticiones de muchas aplicaciones de cliente y al mismo tiempo de acceso del disco y red.

Por eficiencia, la SpectroSERVER funciona con una arquitectura multi-hilo pues tiene menos sobrecarga que ejecutando procesos por separado. El SpectroSERVER crea algunos hilos en el arranque que terminan únicamente cuando el SpectroSERVER termina. También crea otros hilos de forma dinámica y los termina cuando ya no son necesarios. Por ejemplo, cada vez que un cliente se conecta al SpectroSERVER o hace una solicitud a través de una API, se inicia un nuevo hilo. Normalmente, no es necesario preocuparse por este mecanismo; sin embargo, este concepto puede llegar a ser importante

en un sistema muy cargado cuando se requiere la sintonización avanzada para maximizar el rendimiento del sistema.

Elementos Gestionados

El SpectroSERVER utiliza modelos para representar elementos gestionados, y dichos modelos se encuentran definidos en el catálogo de modelado. En algunos tipos de modelos se pueden crear instancias para representar un dispositivo, una aplicación o un host que opera en la infraestructura informática.

SpectroSERVER puede comunicarse directamente con estos elementos gestionados utilizando SNMP.

Gestión de comunicación en dispositivo (DCM)

Es la interfaz entre el SpectroSERVER y los elementos gestionados. El DCM incluye varias interfaces de protocolo que se comunican con elementos gestionados utilizando un protocolo específico. Hay una interfaz para cada uno de los dos protocolos soportados, SNMP e ICMP. Cuando el SpectroSERVER comunica con el elemento gestionado, la solicitud se envía a la interfaz de protocolo adecuado en el DCM. El DCM, a su vez, pasa la petición al elemento gestionado.

Polling

El SpectroSERVER actualiza constantemente su conocimiento de las condiciones de red que utilizan los servicios de poll y registro. El DCM se encarga de la comunicación con el elemento gestionado siendo sondeado. Cuando se definen atributos para un tipo de modelo, que puede ser externa (que se obtiene a partir del elemento gestionado) o interna (almacenado en memoria o la base de datos). La frecuencia de sondeo se basa en el valor del atributo polling_interval que se define para el modelo. Los valores de los atributos externos que no tienen establecido el indicador de votación se obtienen a partir del elemento que gestione cuando una aplicación cliente o controlador de inferencia pide al valor.

El acortamiento de los intervalos de sondeo puede limitar la capacidad de respuesta de la SpectroSERVER y generar una cantidad inaceptable de tráfico.

Alertas, Eventos y Alarmas

CA Spectrum es un sistema de gestión de los servicios y la infraestructura diseñada para que le notifique si hay un fallo en un elemento gestionado particular en el entorno informático. Una manera en que CA Spectrum logra esto es mediante la recepción de alertas (generalmente traps SNMP) de las áreas problemáticas en la infraestructura informática, y convertir esas alertas en eventos y alarmas que se muestran en las aplicaciones de CA Spectrum.

Además utiliza una serie de archivos de soporte llamados archivos de configuración de eventos para indicar cómo se procesan las alertas, eventos y alarmas.

Alertas

Una alerta es un mensaje no solicitado enviado desde un elemento logrado CA Spectrum. El protocolo de gestión de primaria que CA Spectrum utiliza para comunicarse con los elementos gestionados es SNMP. Una alerta enviada por un elemento gestionado compatible con SNMP recibe el nombre de trampa o trap. Los elementos gestionados con trampas SNMP activadas se pueden configurar para dirigir dichas trampas al SpectroSERVER.

El SpectroSERVER utiliza la dirección IP de origen de la trampa para identificar el modelo asociado con ese elemento gestionado. Una vez que se conoce el modelo, la trampa se procesa como se indica por el archivo AlertMap que está asociado con ese tipo de modelo. Existe un archivo AlertMap para la mayoría de los tipos de modelo de dispositivo dentro de CA Spectrum. El

AlertMap es un archivo ASCII que se utiliza para asignar las capturas SNMP en eventos de CA Spectrum.

Eventos

Un evento es un objeto que representa un suceso instantáneo dentro de CA Spectrum. Los eventos generalmente indican que algo significativo se ha producido en relación con el modelo u otro componente. La mayoría de los tipos de modelo del dispositivo tiene un archivo de configuración de eventos EventDisp asociado con ellos. Un archivo EventDisp es un archivo ASCII que indica cómo se procesa un evento. Después de un archivo AlertMap convierte una captura de SNMP en un evento, el archivo EventDisp dice CA Spectrum cómo manejar este evento para este modelo en particular. El procesamiento de un evento puede incluir el registro del evento y la generación de una alarma.

Alarmas

Una alarma es un objeto que indica que existe una condición anormal en el entorno administrado. Por lo general, se genera una alarma cuando se produce un evento y el archivo EventDisp especifica que una alarma se debe generar. Una alarma también puede ser generada como resultado de un reloj configurado, o porque CA Spectrum detecta una situación anormal no se basa en un evento. Cuando la condición anormal que causó la alarma termina, la alarma correspondiente se puede borrar automáticamente por otro evento, o puede desactivarla. Las notificaciones de alarma pueden ser enviadas a las aplicaciones y controladores de inferencia que necesitan esta información. CA Spectrum puede examinar los eventos de red innumerables, analizarlos y producir una pequeña cantidad de avisos importantes.

Información general Aplicaciones cliente

La principal aplicación de CA Spectrum cliente es OneClick, pero también hay algunas otras aplicaciones cliente que le permiten interactuar con la información almacenada y procesada en el SpectroSERVER.

Las aplicaciones cliente que pueden ser necesarios cuando se personaliza CA Spectrum o la integración con CA Spectrum se incluyen las siguientes:

- AlarmNotifier: Esta aplicación se utiliza para reenviar datos de alarma a los scripts definidos por el usuario o aplicaciones de terceros.
- SANM: Esta aplicación se utiliza con el AlarmNotifier para especificar políticas que los datos de alarma filtro envían a los scripts definidos por el usuario o aplicaciones de terceros.

OneClick Consola

La Consola de OneClick muestra información de la SpectroSERVER utilizando iconos y puntos de vista. Los iconos son ilustraciones de los modelos definidos para representar elementos gestionados de la infraestructura informática. Las vistas son las diversas formas en que los datos de la SpectroSERVER están organizados para su visualización.

OneClick Iconos de la consola

Los iconos son representaciones gráficas de los modelos instanciados en base a los tipos de modelo del catálogo de modelado CA Spectrum. Hay muchos tipos diferentes de iconos de CA Spectrum. Los iconos pueden representar elementos gestionados individuales, grupos de elementos gestionados, ubicaciones geográficas, los usuarios, los paisajes, las conexiones entre los modelos, y así sucesivamente. Las tuberías son un tipo

especial de icono utilizado para representar la conectividad entre los elementos gestionados.

Información general acerca de un modelo, como el nombre del modelo y el nombre del tipo de modelo, es visible en el icono. La información detallada sobre un modelo se encuentra dentro de varias subvistas icono que se accede haciendo doble clic en el icono. Algunos iconos utilizan el color para indicar el estado de los elementos gestionados que representan.

Vistas jerárquicas

Una vista en CA Spectrum es una forma de organizar los datos para que pueda ser mostrado o manipulado. Vistas jerárquicas representan formas de estructurar los datos de la red. Al estructurar sus datos de red en el archivo XML, puede elegir a partir de elementos que representan cada una de las vistas jerárquicas. Hay dos tipos de vistas jerárquicas: Topología y Ubicación.

Vista de topología

La vista de topología es realmente una abstracción de los componentes de red. Cuando se trabaja con este punto de vista, usted representa los componentes físicos o lógicos de la red y el grupo de estos componentes con conectividad lógica en mente. También puede elegir para representar gráficamente las conexiones, utilizando tubos que muestran cómo los dispositivos se conectan a nivel de puerto o dispositivo. En la consola de OneClick, este punto de vista aparece como la topología Universo.

Vistas de Ubicación

La vista Ubicación organiza sus datos de la red por ubicación física. El uso de este punto de vista se puede representar de la red en términos de geografía.

Puede comenzar con sus oficinas en el mundo e ir directamente a la sala de cableado en cada planta de cada edificio en cada región donde se encuentran

sus oficinas. En la consola de OneClick, este punto de vista aparece como la topología Mundial.

2.2.4 CA EHEALTH

Ayuda a gestionar el rendimiento de extremo a extremo y la disponibilidad de su tecnología de la información (TI), la suite de eHealth ofrece soluciones para las siguientes áreas:

- Gestión de redes
- Sistema de gestión y aplicación
- La gestión del rendimiento de aplicaciones
- Gestión de la infraestructura de extremo a extremo
- Cada solución se integra componentes relevantes de la suite de eHealth para dar una respuesta integral a sus necesidades de TI.

Gestión de Red

Administra y mantiene una red, hace un seguimiento de todos los routers, conmutadores y otros componentes de red. También supervisa el rendimiento de la red para determinar el porcentaje de tiempo de disponibilidad de los componentes de red, si el ancho de banda actual de la red es suficiente, y si el tráfico de red aumenta con el tiempo.

eHealth ofrece un sistema integrado y proactivo ante fallas, rendimiento y gestión de la disponibilidad a través de entornos heterogéneos de TI complejas.

Con eHealth, puede hacer lo siguiente:

- Gestión de múltiples plataformas y arquitecturas.
- Administrar servicios de red críticos.
- Logra la integración por defecto y la gestión del rendimiento.
- Realizar la planificación inteligente de capacidades.

- Administrar y documentar los niveles de servicio.

eHealth recoge una amplia variedad de datos de la infraestructura de red para generar alarmas e informes.

Sistemas y Gestión de Aplicaciones

Además de los componentes de red de monitoreo, es necesario asegurar que los sistemas y aplicaciones que forman la estructura subyacente de la infraestructura en la que pueden apoyar su negocio. Si los sistemas críticos de las aplicaciones no están disponibles, (como el correo electrónico, los servidores web y sistemas de gestión de bases de datos) o tienen un mal desempeño, la productividad disminuye.

eHealth provee la visualización del rendimiento y la disponibilidad a través de la gestión de sistemas complejos, heterogéneos y entornos de aplicaciones. Mediante la detección automática, aísla y corrige problemas, eHealth ayuda a mejorar la disponibilidad y el rendimiento de los sistemas y aplicaciones, lo que mejora la productividad del usuario.

Con eHealth, puede hacer lo siguiente:

- Administrar los sistemas multi-plataforma.
- Administrar aplicaciones de infraestructura.
- Administrar aplicaciones desarrolladas internamente.
- Recibir notificación inmediata de las interrupciones del servicio.
- Reducción de costos en TI debido a la administración por excepción.
- Mapa de TI para el negocio.
- Viabilidad de activos hardware y software.

Los sistemas y aplicaciones que se pueden controlar y gestionar el uso de la sanidad electrónica son las siguientes:

- Servidores
- Computadoras de escritorio

- Los servidores Web
- E-mail
- Aplicaciones de bases de datos
- Se puede supervisar umbrales, eventos NT, archivos de registro y realizar el muestreo de la historia.

Gestión de rendimiento de aplicaciones

Cuando las aplicaciones de negocios se llevan a cabo lentamente, disminuye la productividad del usuario y las empresas se ven afectadas. Para garantizar un rendimiento óptimo, se debe ser capaz de controlar los tiempos de respuesta de las aplicaciones y la disponibilidad que terminan experiencia de los usuarios.

eHealth le permite medir y controlar el tiempo real de respuesta de las aplicaciones de usuario final para aplicaciones comerciales o personalizadas de Windows o Web que están basada en TCP / IP. También ayuda a entender la disponibilidad de aplicaciones a través de un enfoque sintético (de prueba) desde cualquier parte del mundo. Con esta información, usted puede ayudar a garantizar que las aplicaciones críticas de negocio están disponibles y funcionando bien por lo que los usuarios y sus clientes funcionen eficazmente.

Con eHealth, puede hacer lo siguiente:

- Controlar y gestionar los tiempos de respuesta de las aplicaciones críticas para el negocio y las transacciones individuales.
- Recibir alarmas basadas en umbrales personalizados para el desempeño de respuesta del usuario final y disponibilidad de las aplicaciones.
- Mejorar la resolución de problemas mediante la profundización de las alarmas en tiempo real a los informes históricos de rendimiento de aplicaciones.
- Proporcionar informes para la planificación de la capacidad y la documentación de nivel de servicio.

Gestión de Infraestructuras de extremo a extremo

La salud y el bienestar de toda la infraestructura de TI depende del rendimiento de todos los recursos de la empresa: aplicaciones, sistemas y redes.

eHealth ofrece la integración y proactividad por defecto, el rendimiento y la disponibilidad a través de la gestión de aplicaciones, sistemas y redes. Aumenta su calidad de servicio al reducir el tiempo medio de reparación (MTTR), reduce el costo de propiedad, y proporciona una gestión automatizada del nivel de servicio.

eHealth ofrece lo siguiente:

- Gestión de redes
- Gestión de respuesta de las aplicaciones
- Sistemas de gestión multi-plataforma
- Gestión de fallos y rendimiento integrado
- Notificación inmediata de las interrupciones del servicio
- Planificación de la capacidad y el nivel de servicio de gestión
- Gestión de aplicaciones de infraestructura

eHealth puede proporcionar una visión única e integrada de la salud de toda su infraestructura de TI, incluyendo redes, sistemas y aplicaciones. Permite lo siguiente:

- Identificar los puntos conflictivos de vistas personalizadas del negocio.
- Dispositivos de red monitor, sistemas y caminos de respuesta.
- Ofrecer evaluación automática de impacto por los clientes, regiones y tecnologías.

Generación de informes

eHealth ofrece un completo conjunto de informes para proporcionar la información necesaria para administrar la infraestructura de TI. Se puede utilizar cualquier tipo de informe de varias maneras para mostrar distintos tipos

de información, en función de los criterios de filtro con que se ejecute el informe. Además permite ejecutar informes a petición o programarlos para que se ejecuten regularmente.

2.2.5 Integración entre Ehealth y Spectrum

La integración de CA Spectrum y CA eHealth ayuda a mantener los niveles de servicio críticos a través de entornos de red complejos mediante la combinación de la disponibilidad automática y la gestión del rendimiento con el servicio de red de CA Spectrum y la plataforma de análisis de CA eHealth.

CA Spectrum administra las redes y corrige problemas. Emite alertas de los cambios en la red o el estado del dispositivo. El sistema crea un modelo de cada entidad de la red, incluidos los cables, los dispositivos de red, servidores y aplicaciones. Además proporciona una vista perfecta de la red de la empresa.

CA eHealth proporciona datos históricos a través de reportes de comportamiento de los equipos. Automatizan las tareas de cálculo de tendencias a largo plazo, proporcionando una línea de base para los recursos de red. También proporciona informes sobre la ejecución de los componentes críticos de la red, tales como los clústeres de servidores y enlaces de Internet. También ofrece características de solución de problemas y la planificación de la capacidad proactiva.

La integración de CA Spectrum y CA eHealth le da tiempo significativo y beneficios de productividad. La integración le permite:

- Utilizar CA eHealth para descubrir automáticamente los dispositivos gestionados por CA Spectrum, lo que elimina la necesidad de volver a introducir manualmente y actualizar continuamente los datos de configuración.
- Acceso a los informes de CA eHealth, como At-a-Glance y Trend, directamente de la topología de CA Spectrum OneClick, que le da una

visión rápida del estado del dispositivo y la información en profundidad histórica.

- Administrar alarmas generadas en la consola Live Exception de CA eHealth desde la consola de CA Spectrum OneClick. Gracias a la integración podemos ver el detalle una alarma que permite reducir el tiempo medio de reparación para los problemas de la red.
- CA eHealth informa de las alarmas de CA Spectrum, esta relación permite tener un contexto histórico para que la solución de problemas sea más eficaz.
- Utilización de CA eHealth para la planificación de la capacidad, la solución de problemas proactiva, la optimización del rendimiento y la gestión de nivel de servicio de los componentes de red gestionados por CA Spectrum.
- En CA eHealth permite alta disponibilidad y recuperación ante fallos. En escenarios de desastres, un servidor secundario se hace cargo de un servidor primario cuando sea necesario.

  CA Spectrum mediante la consola OneClick proporciona la ubicación de un equipo dentro una red.

2.3. Marco Conceptual

- Arquitectura multi-hilo

  SpectroServer tiene unidades centrales de procesamiento con capacidad multi-hilo. Es decir tiene soporte en hardware para ejecutar eficientemente múltiples solicitudes de ejecución.

- Backend y Frontend

  La idea general es que el front-end es responsable de recoger entradas de los usuarios, y ser procesadas de tal manera que cumplan las especificaciones para que el back-end pueda usarlas. La conexión entre front-end y el back-end es un tipo de interfaz.

- CMIP

  (Common Management Information Protocol: Protocolo de Administración Común de Información). Protocolo estándar para administración de redes a través de objetos manejados que provee seguridad avanzada y reporteo de condiciones inusuales de la red. El protocolo CMIP fue creado para simplificar y mejorar las deficiencias y capacidades de administración del protocolo SNMP.

- Dashboard

  Utilizan una metodología centrada en el usuario1 que integra datos de acuerdo con los problemas, funciones principales o procesos comerciales críticos de la empresa. Los Dashboards están diseñados frecuentemente para tratar un único problema de forma aislada y desarrollar desde simples informes en línea hasta una compleja representación visual de mediciones clave.

- Hosting

  Conjunto de servicios que se puede contratar para gestionar servidores. Típicamente se encuentra:

✓ Alquiler de servidores dedicados
✓ Administración de aplicaciones
✓ Copias de seguridad
✓ Monitorización del rendimiento de los servidores

- Tecnología de información TI

  Se conoce como tecnología de información a la utilización de tecnología. Específicamente computadoras y ordenadores electrónicos para el manejo y procesamiento de información. Referida a la captura, transformación, almacenamiento, protección, y recuperación de datos e información.

- IETF

  (Internet Engineering Task Force - Grupo de Tareas de Ingeniería de Internet). Organización de técnicos que administran tareas de ingeniería de telecomunicaciones, principalmente de Internet (ej: mejora de protocolos o darlos de baja, etc.)

- ITU

  La UIT (Unión Internacional de Telecomunicaciones) es el organismo especializado de las Naciones Unidas para las tecnologías de la información y la comunicación.

- Latencia

  Es el tiempo o lapso necesario para que un paquete de información se transfiera de un lugar a otro. La latencia, junto con el ancho de banda, son determinantes para la velocidad de una red.

- Probes

  Los probes o sondas dentro de un sistema de gestión de monitoreo accesan y monitorean recursos locales específicos o eventos y envían alarmas o mensajes a la consola central de administración.

- RMON

  Protocolo para la monitorización remota de redes. Es un estándar que define objetos actuales e históricos de control, permitiendo que usted capture la información en tiempo real a través de la red entera. El estándar de RMON es una definición para Ethernet, además de formar parte del protocolo TCP/IP.

- SNMP

  (Simple Network Management Protocol), en sus distintas versiones, es un conjunto de aplicaciones de gestión de red que emplea los servicios ofrecidos por TCP/IP, protocolo del mundo UNIX, y que ha llegado a convertirse en un estándar. Surge a raíz del interés mostrado por la IAB

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

CAPITULO III:
DESARROLLO DE LA METODOLOGÍA

3.1 ANÁLISIS DEL MODELO/HERRAMIENTA/SISTEMA

En este capítulo se mostrará el resultado de la implementación de un sistema de gestión de monitoreo y se explicarán los componentes en que se basan las funcionalidades y demás elementos que garantizan el servicio de monitorización.

3.1.1 Diagnostico estratégico

1. Análisis de la organización FODA

Fortalezas

- GMD forma parte del grupo de Ingeniería #1 del Perú.
- Graña y Montero, y cuenta con 29 años de experiencia desarrollando e implementando exitosamente soluciones que generan valor a los procesos de negocios de sus clientes.
- La empresa cuenta con un staff de más de 1600 profesionales y certificaciones internacionales como ISO 9001, ISO 27001, NTP 392-030 y metodologías de clase mundial CMMI-3, ITIL y PMI, que le han permitido consolidar su operación.
- GMD cuenta con la mejor infraestructura, la Fábrica de Software más grande del país.

- GMD tiene el 2°Data Center de Clase Mundial Tier III, 2° Call Center y más de 9,900 m2 de oficinas, todo lo cual le permite proveer un servicio de calidad y ayudar a sus clientes a alcanzar un alto rendimiento
- Empresa de TI con mayor confiabilidad y experiencia del Perú.
- Certificación CMMI, ISO 27001, ISO 9001.Fábrica de Software más grande del país.

Oportunidades

- GMD es la empresa de Outsourcing de Procesos de Negocios y Outsourcing de Tecnología de la Información (TI) con mayor confiabilidad y experiencia del Perú.
- La empresa ofrece distintos servicios a sus clientes, que van desde el hosting hasta la administración de aplicaciones.
- GMD provee una amplia gama de soluciones de negocios innovadoras, flexibles y escalables para los sectores: Industria y Comercio, Banca y Finanzas, Gobierno y Servicios Públicos.
- Las soluciones van desde la provisión de equipos de cómputo y comunicaciones, pasando por la integración de sistemas y soluciones de negocios, hasta la completa externalización de procesos y formación de sociedades comerciales.
- Nuevas propuestas de servicios de acuerdo a las necesidades del cliente.

Debilidades

- Al ser una empresa de servicio esta contantemente adaptándose a las necesidades del cliente.
- La empresa tiene gran cantidad de colaboradores, por ello debe prestar especial atención en la gestión de recursos humanos.
- El mundo de TI se encuentra en constante cambio, por ellos la empresa debe invertir en capacitar a sus colaboradores periódicamente.

- Graña y Montero es reconocida como una corporación dedicada a la industria constructora. La mayoría de personas ignora que dentro del grupo de empresas de dirige la corporación encontramos a GMD.

Amenazas

- GMD es competidor directo de empresas trasnacionales.

2. Visión

Proveer soluciones de outsourcing de procesos de negocio y de tecnología de la información, que favorezcan el logro de los objetivos empresariales de nuestros clientes.

3. Misión

Ser la empresa de soluciones de Outsourcing de Procesos de Negocio y de Tecnología de la Información más confiable de América Latina.

4. Valores

Valores En GMD tenemos muy claro que hemos superado estos 27 años gracias al respeto por nuestros cuatro valores fundamentales corporativos que son:

- Cumplimiento
- Seriedad
- Eficiencia
- Calidad

Y para responder al exigente negocio de la tecnología de la información, ponemos en práctica nuestros valores organizacionales:

Calidad

Es trabajar con estándares internacionales de calidad de servicio, respeto al medio ambiente y prevención de riesgos, actuando con responsabilidad social y generando valor en nuestros servicios, a fin de lograr la confianza y satisfacción de nuestros clientes y el desarrollo de nuestros colaboradores.

Innovación

Consiste en usar nuestro conocimiento, creatividad, tecnología e investigación para el cambio y la mejora de nuestros procesos, desarrollando soluciones innovadoras que generen valor en la realización de nuestras actividades diarias y a nuestros clientes, sin perder el foco de nuestros objetivos y metas trazadas.

Eficiencia

Se refiere a nuestro esfuerzo por aumentar la productividad en todas las áreas de la empresa, evitando los retrabajos, a través de la incorporación de metodologías, procesos de gestión y tecnología.

Equidad

Consiste en fomentar y velar por la creación de relaciones transparentes y justas con nuestros compañeros, clientes y proveedores, estableciendo reglas claras que generen valor para todos.

Seriedad

Es la ética y profesionalismo que demostramos en nuestra labor diaria, cumpliendo nuestros compromisos con responsabilidad y manteniendo el principio de honestidad en nuestras prácticas comerciales y organizacionales, bajo los lineamientos de la "Carta de Ética y Código de Conducta" del Grupo Graña y Montero.

Cumplimiento

Es realizar, con calidad, los compromisos que asumimos con los clientes, nuestro equipo y terceros, antes del plazo establecido, logrando así desarrollar una cultura de compromiso en cada una de nuestras actividades.

5. Objetivos estratégicos

- Promover las mejores prácticas en los servicios que brindan a sus clientes.
- Promover el trabajo en equipo y la creación de un buen clima laboral.
- Mejorar continuamente la eficacia del sistema de Gestión de la Calidad.

6. Situación Actual

Notificación y escalamiento de incidentes

El Centro de Operaciones tecnológicas (COT) es el área encargada de prestar el servicio de respaldo y monitorización de todos los clientes que tiene GMD. Para ello cuenta con un jefe de operaciones, una línea de supervisores y administradores. Además de operadores de sistemas que prestan servicios en el horario de 24x7. Todo el año y todos los días del año.

Entre las funciones que cumplen los operadores de sistemas se encuentran velar por el respaldo de la información del cliente y el monitoreo de los servicios.

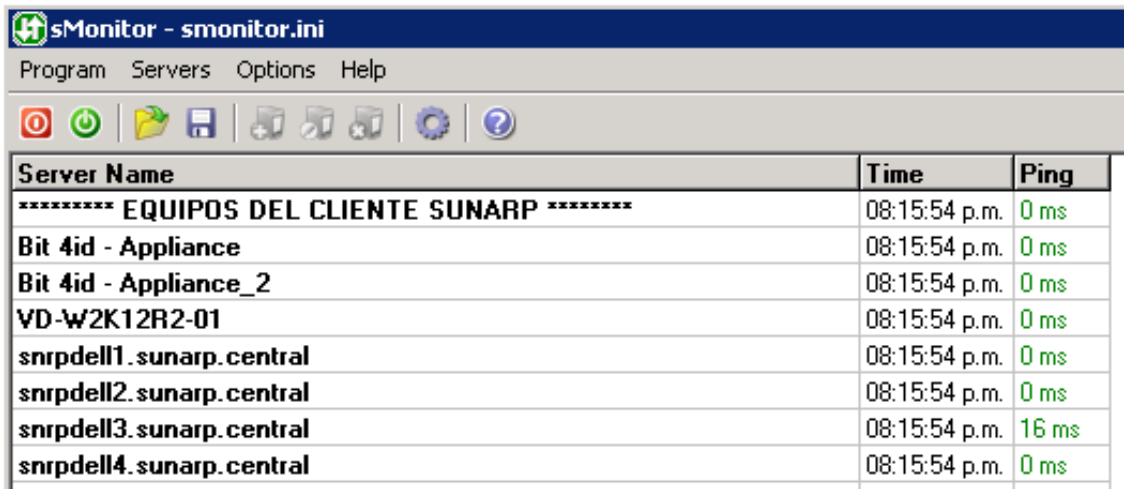
Esta última actividad consiste en la notificación y escalamiento de incidencias sobre los sistemas del cliente al administrador designado. Para ello el COT cuenta con la aplicación de nombre SMonitor. Ver Figura N° 2 SMonitor 4.2.

sMonitor es un software de monitoreo de red que le permite verificar la conectividad de red de hosts TCP / IP en Internet y LAN. El programa

periódicamente realiza pings y verificación de conectividad de puertos TCP y UDP en los equipos especificados por el usuario u otros dispositivos de red.

Si el host de destino no responde a un ping, solicitud de conexión, o datagramas de usuario, sMonitor avisa mediante alarmas audibles, notificaciones visibles, mensajes de correo electrónico, software de terceros, de módem y las conexiones Telnet. Además, el programa genera archivos de registro, archivos de formato CSV, y crea los archivos subidos por FTP el archivo HTML, lo que refleja una situación actual. Con base en los resultados de pruebas, el programa puede operar sistemas remotos (administración de energía, reinicio, presentación de informes de alarma) por módem y telnet utilizando scripts personalizados. sMonitor puede ejecutarse como aplicación estándar de Windows o el servicio NT.Diagrama de red de smonitor.

Figura N° 6 SMonitor 4.2



Fuente: COT - GMD

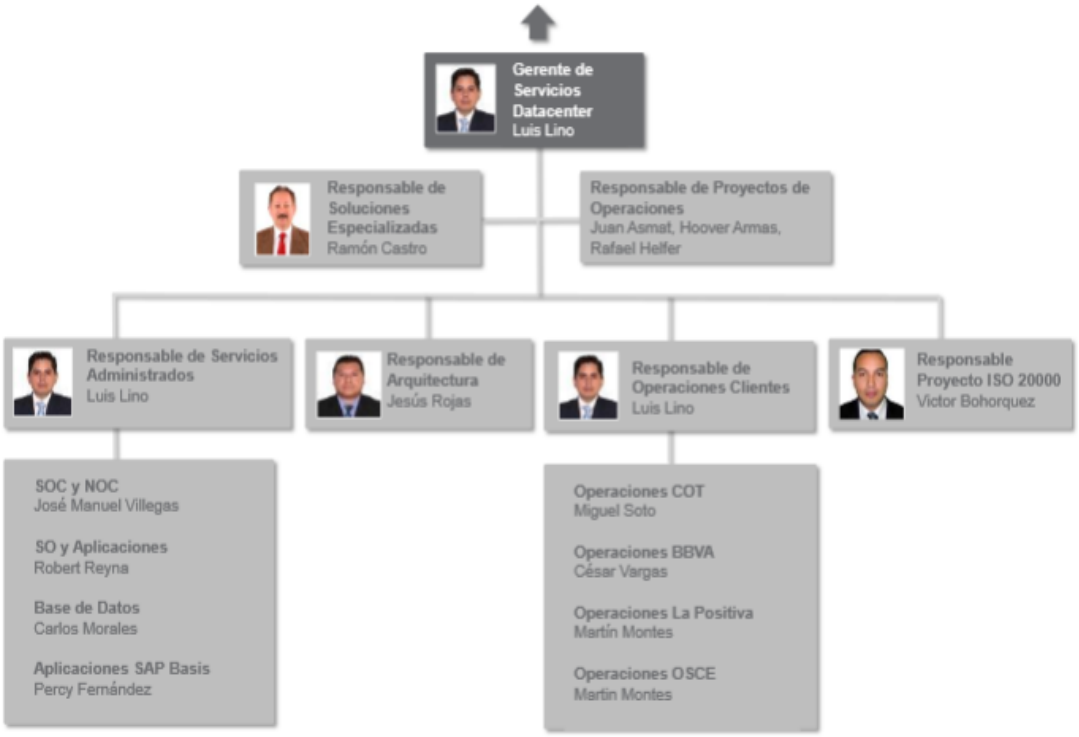
El procedimiento que realizaban los operadores ante un incidente era el siguiente:

1. Ingresar a las PC de monitoreo del COT y verificar conectividad hacia los servidores. Informar a los administradores que corresponda ante cualquier eventualidad.
2. Adicionalmente, se procede a notificar la incidencia haciendo el envío de un correo electrónico. Entonces el operador procede a reenviar la notificación que envió la aplicación de manera automática a los administradores para que puedan revisar y solucionar el incidente.

7. Organigrama

El área que se benefició con la implementación del sistema de gestión del monitoreo es el Centro de Operaciones Tecnológicas y el área de servicios administrados, que ubicamos con el nombre de SO y Aplicaciones dentro de la Figura N°7.

Figura N°7 Organigrama de Servicios Datacenter



Fuente: GMD

3.1.2 Análisis de requerimientos

Al iniciar el proyecto se definieron ciertas características que el software de monitoreo debía tener. A continuación se describen cada una de ellas. Al ser un centro de operaciones que brinda servicios a distintos clientes y poseer una cantidad importante de servidores en distintas plataformas se han considerado lo siguiente:

1. Requerimientos funcionales

- Criticidad de la alerta.

  Se deberá clasificar las alertas de acuerdo a su importancia y a la urgencia. La aplicación deberá tener estados que permitan identificar la gravedad de un incidente.

- Tiempo configurable para censar los recursos.

  Referente al tiempo en que la aplicación realiza consultas a los equipos que monitorea para revisar su comportamiento e indicar una alerta fuera necesaria.

- Campo para indicar el número de ticket asignado al incidente.

  Cada vez que se presenta un incidente, los operadores de sistemas deben crear un ticket de atención y notificar a los administradores asignados a determinado cliente.

- Modelo que permita fácil administración.

  Se necesita un sistema ágil. La empresa posee una gran cantidad de equipos que deberán tener servicio de monitorización. Por ello la necesidad de un sistema que permita iniciar el servicio rápidamente.

- Desactivación de alertas sobre determinado equipo.

  Los servidores están sujetos a cambios físicos y lógicos de acuerdo a los requerimientos del cliente. Por ello se necesita desactivar las alertas que puedan generarse cuando un servidor se encuentra involucrado en trabajos de mantenimiento o actualización.

- Herramienta de monitoreo de tenencia múltiple.

  La empresa presta servicio a varios clientes. Por tal motivo la aplicación de monitorización deberá permitir la visualización de servidores por grupos de clientes. Además la configuración realizada sobre un grupo deberá ser independiente a los demás grupos.

- Configuración de cuentas de usuario con vistas independientes.

  Parte del servicio del servicio de monitorización consiste en darle al cliente visibilidad se sus equipos. Es decir, que puedan observar el

comportamiento de sus servidores en tiempo real. Por ello cada cliente tendrá una vista construida especialmente.

- Visualización y modelado de la topología de red.

  Referente a la visualización de la topología lógica y/o física del cliente.

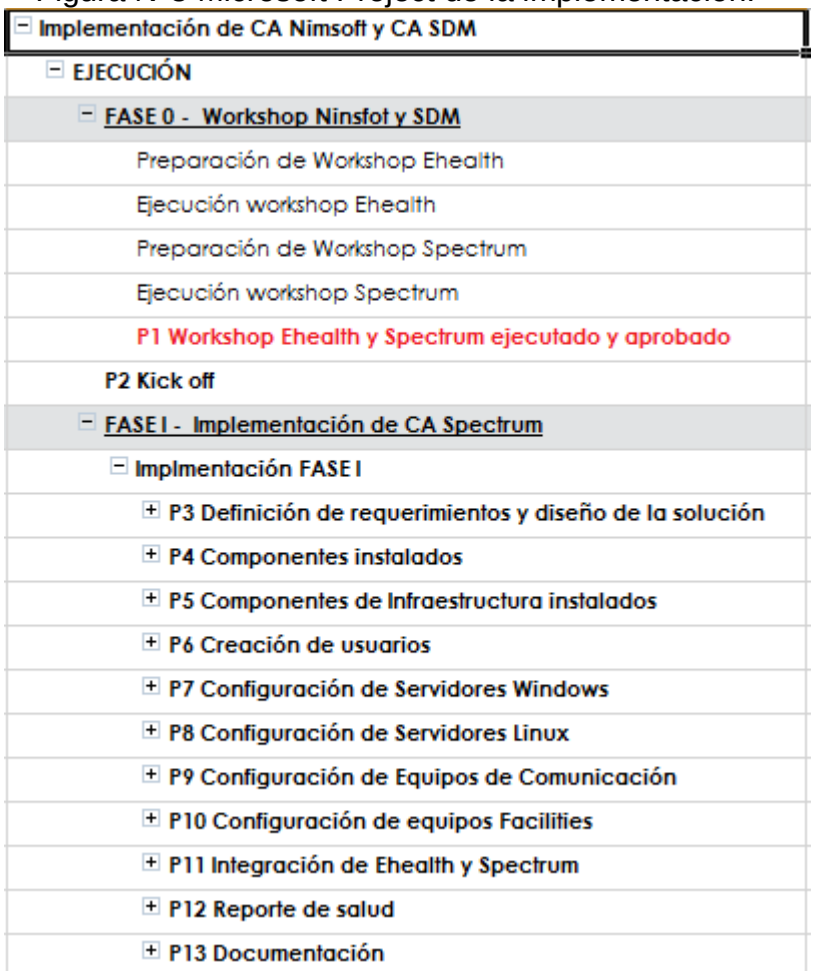
2. Requerimientos no funcionales

- Los Campos de Spectrum. La consola principal de la aplicación deberá mostrar campos como el grupo al que los operadores deban notificar una incidencia, el número de ticket asignado al evento.
- Colores que diferencien y resalten la gravedad de una incidencia. Con el fin de que los operadores de sistemas puedan reconocer y notificar rápidamente la incidencia presentada en un servidor.

3.2 CONSTRUCCIÓN/DISEÑO O SIMULACIÓN DE LA HERRAMIENTA/MODELO/SISTEMA

3.2.1 Cronograma del proyecto

Figura N°8 Microsoft Project de la implementación.



Fuente: GMD

3.2.2 Resultados que se han considerado

El sistema de Gestión de monitoreo permite el registro de incidencias de todos clientes en una sola consola. Visión del estado del performance de los servidores en tiempo real sin tener la necesidad de ingresar al servidor.

La solución implementada está basada en el uso de dos aplicaciones. La integración de las funcionalidades de Ehealth y Spectrum permitirá obtener el modelo esperado. El sistema propuesto se basa en el protocolo SNMP.

CONFIGURACIÓN DEL PROTOCOLO SNMP

El primer paso para iniciar el servicio de monitorización es asegurar la conectividad entre el servidor cliente y los servidores de monitoreo.

El segundo paso es verificar que el protocolo SNMP se encuentre instalado en el servidor cliente. Por lo general se instala por defecto.

Luego se procede a realizar las tareas de configuración del protocolo SNMP en el sistema operativo del servidor.

El tercer paso es configurar los parámetros de monitoreo bajo los que se generará una alerta. Es decir, bajo qué valores de consumo o performance se considera que el servidor se encuentra en peligro de sufrir un incidente. De esta manera se definen que indicadores a nivel de sistema operativo se deberán tomar en cuenta en el comportamiento de un servidor para prevenir un contratiempo.

3.2.3 Arquitectura propuesta

1. Arquitectura de Red de GMD

A continuación se muestra la arquitectura de monitoreo de GMD.

Se pueden distinguir claramente varios segmentos de red:

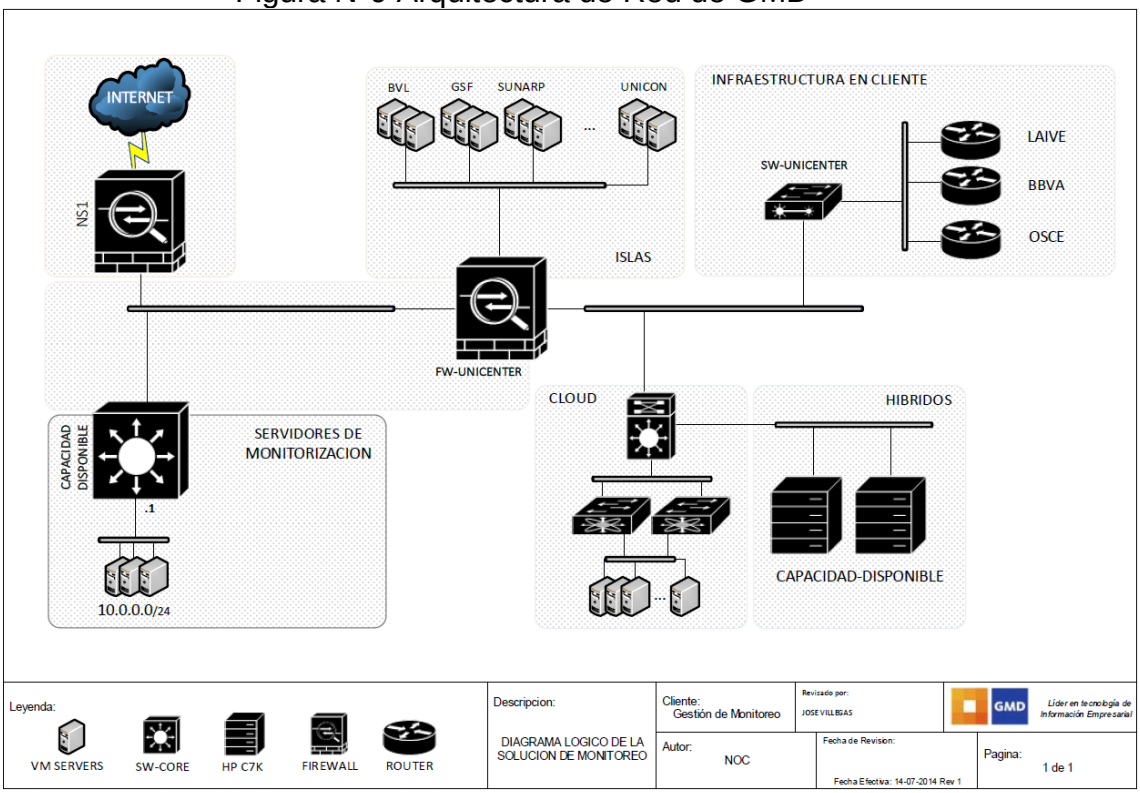
- Red de Monitorización.- es el segmento de red donde estarán ubicados los servidores principales de la solución. Esta red está en el segmento 10.0.0.0 /24.
- Infraestructura en Cliente.- conformada por los enlaces hacia las sedes de los clientes de GMD en donde residen los servidores de los clientes.

En total, son 3 clientes que conforman esta red externa en donde GMD monitorea sus respectivos servidores. Estos clientes son: BBVA, LAIVE y OSCE.

- Red Cloud.- conformada por varios segmentos de red. Cada uno perteneciente a un cliente diferente de GMD como por ejemplo: OSCE, MARATHON, EUROMOTORS, LAIVE, etc.
- Red Híbridos.- conformada por diferentes segmentos de red, cada uno de ellos perteneciente a un cliente diferente.
- Red Islas.- conformada por diferentes segmentos de red (BVL, GSF, SUNARP, UNICON, etc.) cada uno de ellos perteneciente a un cliente diferente.

Nota.- para llegar a cualquiera de los servidores, desde la red de monitorización, ubicados en la Red Híbridos, Red Cloud, Red Infraestructura en Cliente, o red Islas, es necesario pasar por un servidor Firewall (FW-UNICENTER) por el lado de GMD y en el caso de los clientes remotos (Infraestructura en cliente) cada cliente cuenta con su propio firewall por lo que la apertura de puertos a realizar también debe ser realizada en estos firewalls de clientes.

Figura N°9 Arquitectura de Red de GMD



Fuente: Documento de diseño de la solución.

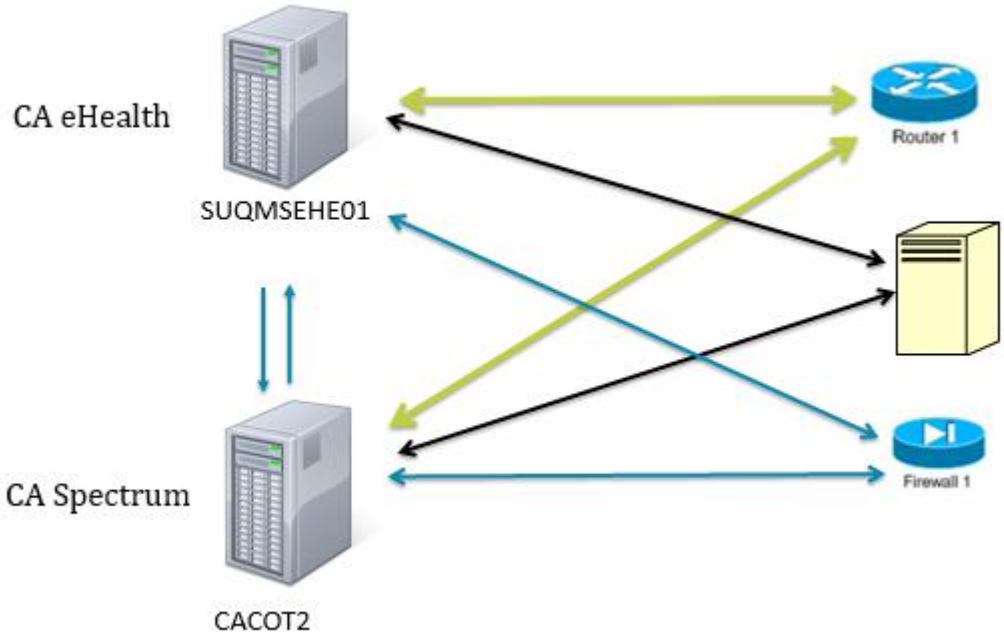
2. Arquitectura de Red de las aplicaciones

A continuación se muestra la arquitectura lógica del modelo desarrollado.

Cada servidor que sea monitoreado por la solución propuesta recibirá y contestará las consultas enviadas por las dos aplicaciones Ehealth y Spectrum.

Toda la comunicación realizada es a través del puerto 161 UDP, que deberá estar habilitado en cada servidor que forme parte del sistema de monitoreo.

Figura N°10 Arquitectura de Red de la solución



Fuente: Documento de diseño de la solución.

3. Detalle de la Arquitectura Propuesta

La arquitectura propuesta consta de dos servidores para la solución:

- **1 Servidor de CA Spectrum,** en este servidor se realizó la instalación del SpectroServer es el servidor principal de Spectrum. Funciona como un servidor de base de datos, motor de modelado, y el administrador de dispositivos. SpectroServer contiene todas las funcionalidades de la aplicación. En este servidor también se instaló OneClick Server que proporciona la interfaz gráfica de usuario que se utiliza para la administración del sistema de gestión de monitoreo.

- **1 servidor de CA Ehealth,** en este servidor se encuentra la el OneCLick Server de Ehealth, así como también la base la datos de la aplicación.

4. Requisitos de hardware para la arquitectura propuesta

- Hardware requerido para la instalación de CA Spectrum.

Tabla N°1 Requerimientos de hardware Ca Spectrum

Nombre / Funcion / Componentes CA	Hardware			Software		
	Procesador	RAM	Particiones	SO	BD	Dependencias
Servidor CA Spectrum	**Dos procesadores de cuatro núcleos Clase XEON de 64 bits, 2.67 GHz**	**20 GB**	**C: 40 Gb E: 150 Gb**	**Windows 2008 R2 (32 bit)**		

Fuente: Documento de diseño de la solución.

- Hardware requerido para la instalación de CA eHealth.

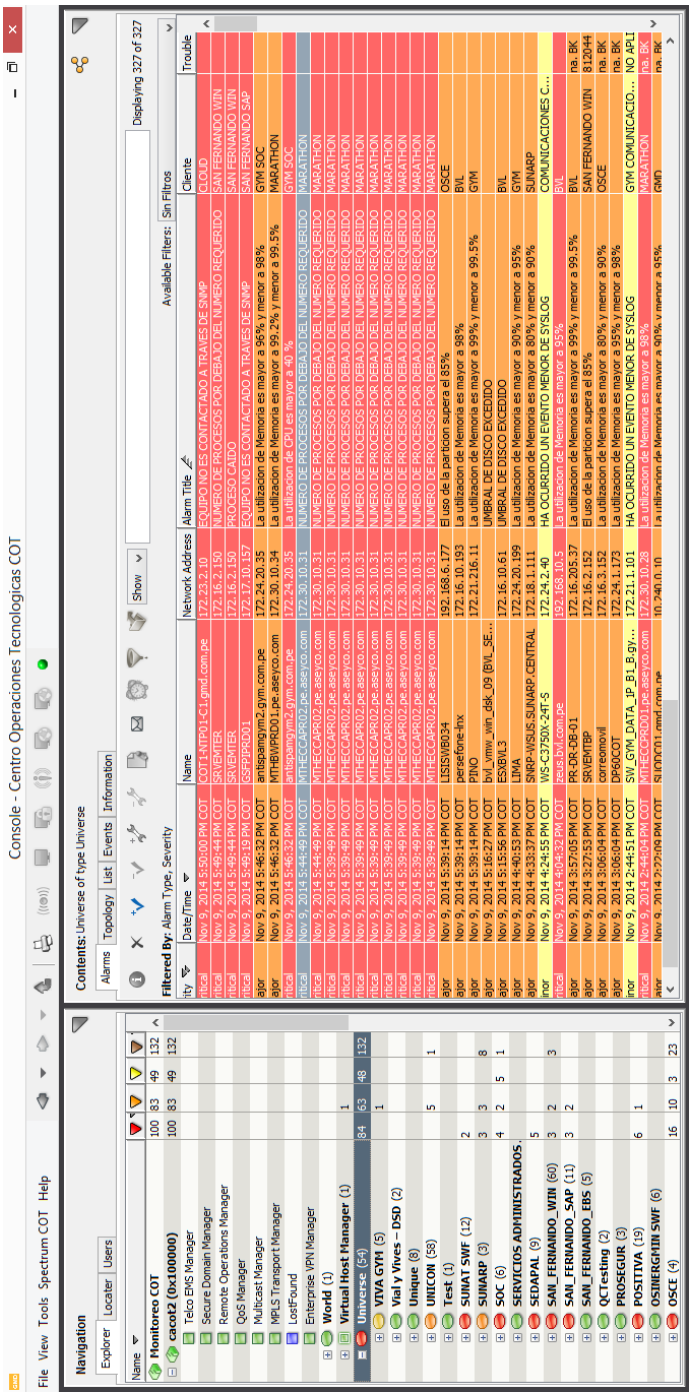
Tabla N°2 Requerimientos de hardware Ca eHealth

Nombre / Funcion / Componentes CA	Hardware			Software		
	Procesador	RAM	Particiones	SO	BD	Dependencias
Servidor CA eHealth	**Dos procesadores de cuatro núcleos Clase XEON de 64 bits, 2.67 GHz**	**8 GB**	**C: 100 Gb D: 100 Gb E: 100 Gb**	**Windows 2008 R2 (64 bit)**		

Fuente: Documento de diseño de la solución

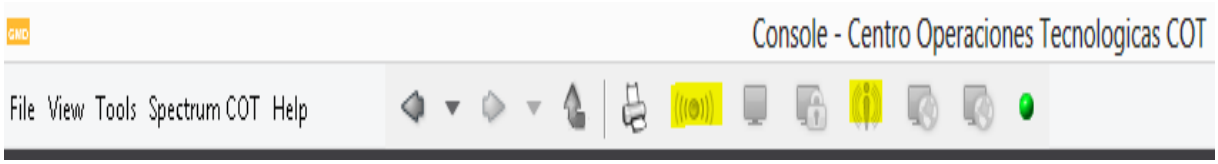
3.2.4 Esbozo del modelo

Figura N°11 Consola OneClick de Spectrum



Fuente: GMD

Figura N°12 Barra de menú de la consola OneClick de Spectrum



Fuente: GMD

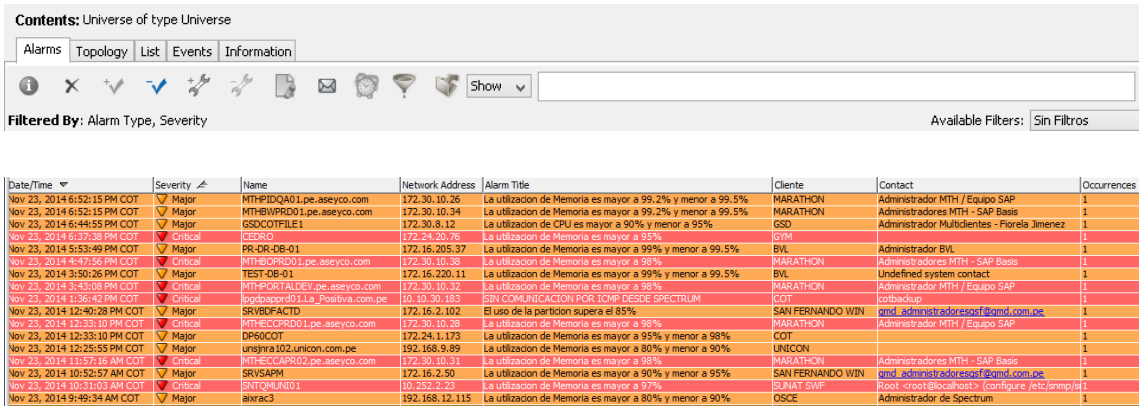
Se puede realizar la validación de conectividad y operatividad del servicio SNMP de la aplicación hacia cualquier servidor.

El modelo propuesto concentra todas las alertas en la consola OneClick de Spectrum. Podemos encontrar distinta información dentro de las 3 sub-ventanas.

La ventana de navegación encontramos los contenedores, que albergan un grupo de servidores. Cada contenedor representa un cliente. Además los colores obedecen a las alertas registradas en los servidores que contienen.

La ventana de contenido muestra una línea de pestañas que nos permiten acceder a información sobre el servidor o contenedor seleccionado.

Figura N°13 Pestaña Alarm de la ventana de contenido - Consola OneClick de Spectrum

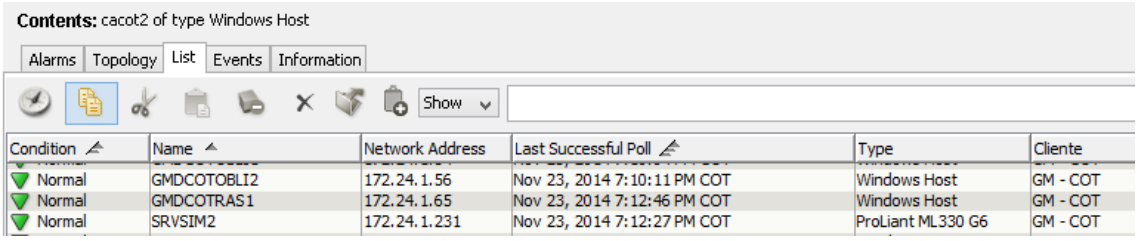


Date/Time	Severity	Name	Network Address	Alarm Title	Cliente	Contact	Occurrences
Nov 23, 2014 6:52:15 PM COT	Major	MTHPIDQA01.pe.aseyco.com	172.30.10.26	La utilizacion de Memoria es mayor a 99.2% y menor a 99.5%	MARATHON	Administrador MTH / Equipo SAP	1
Nov 23, 2014 6:52:15 PM COT	Major	MTHBWPRD01.pe.aseyco.com	172.30.10.34	La utilizacion de Memoria es mayor a 99.2% y menor a 99.5%	MARATHON	Administradores MTH - SAP Basis	1
Nov 23, 2014 6:44:55 PM COT	Major	GSDCOTFILE1	172.30.8.12	La utilizacion de CPU es mayor a 90% y menor a 95%	GSD	Administrador Multiclientes - Fiorela Jimenez	1
Nov 23, 2014 6:37:33 PM COT	Critical	[illegible]	172.24.20.76	La utilizacion de Memoria es mayor a 95%	GYM		1
Nov 23, 2014 5:53:49 PM COT	Major	PR-DR-DB-01	172.16.205.37	La utilizacion de Memoria es mayor a 99% y menor a 99.5%	BVL	Administrador BVL	1
Nov 23, 2014 4:47:56 PM COT	Critical	MTHBOPRD01.pe.aseyco.com	172.30.10.38	La utilizacion de Memoria es mayor a 98%	MARATHON	Administradores MTH - SAP Basis	1
Nov 23, 2014 3:50:26 PM COT	Major	TEST-DB-01	172.16.220.11	La utilizacion de Memoria es mayor a 99% y menor a 99.5%	BVL	Undefined system contact	1
Nov 23, 2014 3:43:08 PM COT	Critical	MTHPORTALDEV.pe.aseyco.com	172.30.10.32	La utilizacion de Memoria es mayor a 98%	MARATHON	Administrador MTH / Equipo SAP	1
Nov 23, 2014 1:36:42 PM COT	Critical	ipgdpapprd01.La_Positiva.com.pe	10.10.30.183	SIN COMUNICACION POR ICMP DESDE SPECTRUM	COT	cotbackup	1
Nov 23, 2014 12:40:28 PM COT	Major	SRVBDFACTD	172.16.2.102	El uso de la particion supera el 85%	SAN FERNANDO WIN	gmd_administradoresgsf@gmd.com.pe	1
Nov 23, 2014 12:33:10 PM COT	Critical	MTHECCPRD01.pe.aseyco.com	172.30.10.28	La utilizacion de Memoria es mayor a 98%	MARATHON	Administrador MTH / Equipo SAP	1
Nov 23, 2014 12:33:10 PM COT	Major	DP60COT	172.24.1.173	La utilizacion de Memoria es mayor a 95% y menor a 98%	COT		1
Nov 23, 2014 12:25:55 PM COT	Major	unsjnra102.unicon.com.pe	192.168.9.89	La utilizacion de Memoria es mayor a 80% y menor a 90%	UNICON		1
Nov 23, 2014 11:57:15 AM COT	Critical	MTHECCMPR02.pe.aseyco.com	172.30.10.31	La utilizacion de Memoria es mayor a 98%	MARATHON	Administradores MTH - SAP Basis	1
Nov 23, 2014 10:52:57 AM COT	Major	SRVSAPM	172.16.2.50	La utilizacion de Memoria es mayor a 90% y menor a 95%	SAN FERNANDO WIN	gmd_administradoresgsf@gmd.com.pe	1
Nov 23, 2014 10:31:03 AM COT	Critical	SNTQMUN101	10.252.2.23	La utilizacion de Memoria es mayor a 97%	SUNAT SWF	Root <root@localhost> (configure /etc/snmp/sn	1
Nov 23, 2014 9:49:34 AM COT	Major	aixrac3	192.168.12.115	La utilizacion de Memoria es mayor a 80% y menor a 90%	OSCE	Administrador de Spectrum	1

Fuente: GMD

- ✓ **Alarms**, visualización de alertas. Dentro de esta pestaña podemos observar campos como:
- Date/Time: Tiempo en que se generó la alerta.
- Severity: Tipo de alerta. Podria ser Minor, Mayor o Critical.
- Name: Nombre del servidor donde se presenta la alerta
- Network Address: IP del servidor alertado.
- Alarm Title: Causa de que el servidor esté alertado.
- Cliente: Cliente al que pertenece el servidor alertado.
- Contact: Grupo de administradores que deberá atender la alerta.
- Ocurrences: Número de alertas generadas en el servidor por la misma causa.
- ✓ **Topología**, visualización de los diagramas de red y la relación entre los equipos.
- ✓ **List**, muestra una vista rápida del estado de los servidores que se encuentran dentro de un contenedor.

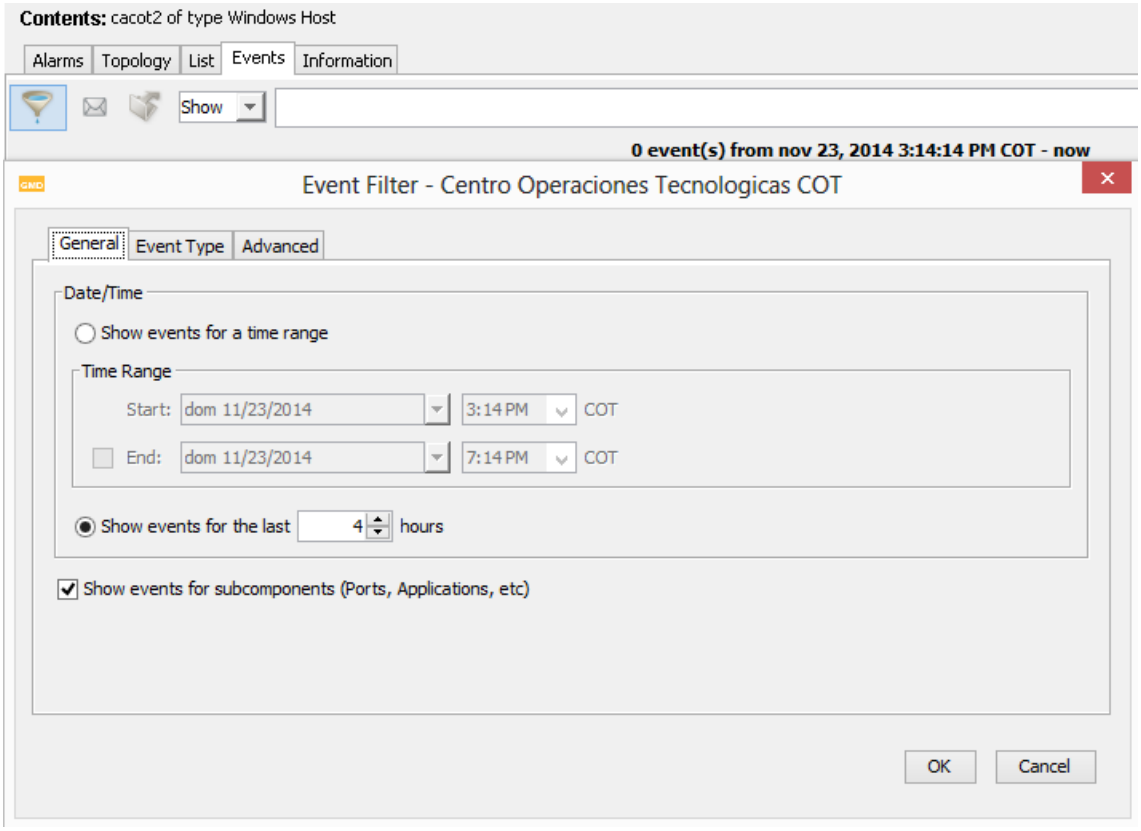
Figura N°14 Pestaña List de la ventana de contenido - Consola OneClick de Spectrum



Fuente: GMD

- ✓ **Events,** podemos a visualizar las alertas ocurridas con anterioridad sobre un servidor. El tiempo máximo de antigüedad es para la observación de alertas es de 45 días.

Figura N°15 Pestaña Events de la ventana de contenido - Consola OneClick de Spectrum



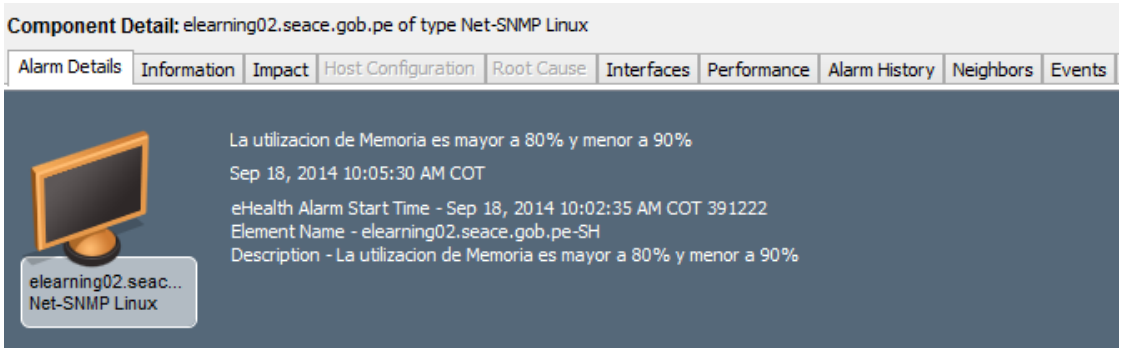
Fuente: GMD

- ✓ **Information** Muestra una descripción detallada sobre el servidor o contenedor seleccionado**.**

La ventana de detalle de componente contiene varias pestañas. Cada una de ellas nos permite obtener distinta información sobre el servidor. Así tenemos:

- ✓ **Alarm Details**

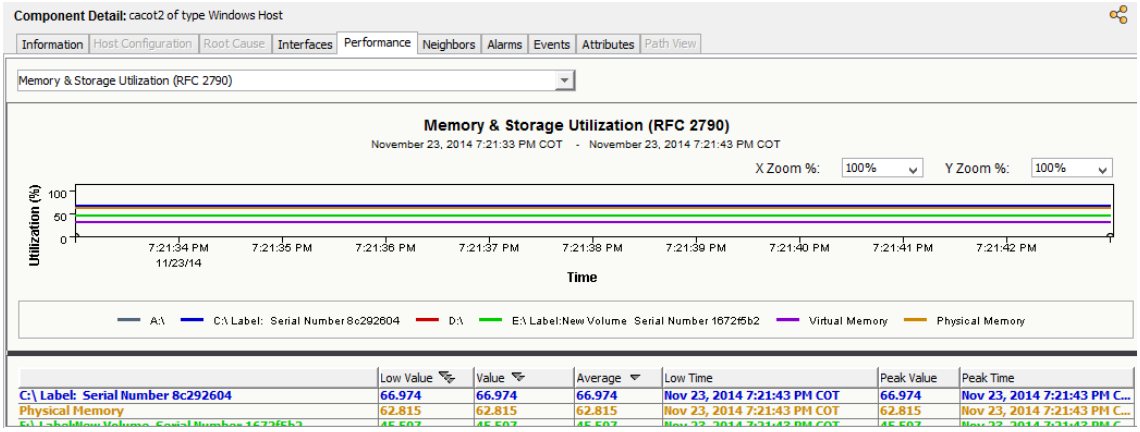
Figura N°16 Pestaña Alarm Details de la ventana detalle de contenido - Consola OneClick de Spectrum



Fuente: GMD

- ✓ **Information,** muestra una descripción detallada sobre el servidor o contenedor seleccionado**.**
- ✓ **Interfaces,** muestra información sobre la configuración de red der servidor.
- ✓ **Performance,** podemos observar el comportamiento del servidor en tiempo real.

Figura N°17 Pestaña Performance de la ventana detalle de contenido - Consola OneClick de Spectrum



Fuente: GMD

3.2.5 Integración de las aplicaciones

El sistema de gestión de monitoreo se compone de dos aplicaciones, Ehealth y Spectrum. Estas aplicaciones trabajan juntas, es decir, están integradas. Si bien es cierto, Ehealth se define como una aplicación utilizada para obtener reportes. Con el fin de tener una administración sencilla y ágil, se han configurado grupos en Ehealth. Estos grupos permiten albergar elementos de los servidores. De igual manera se pueden asignar perfiles en los grupos.

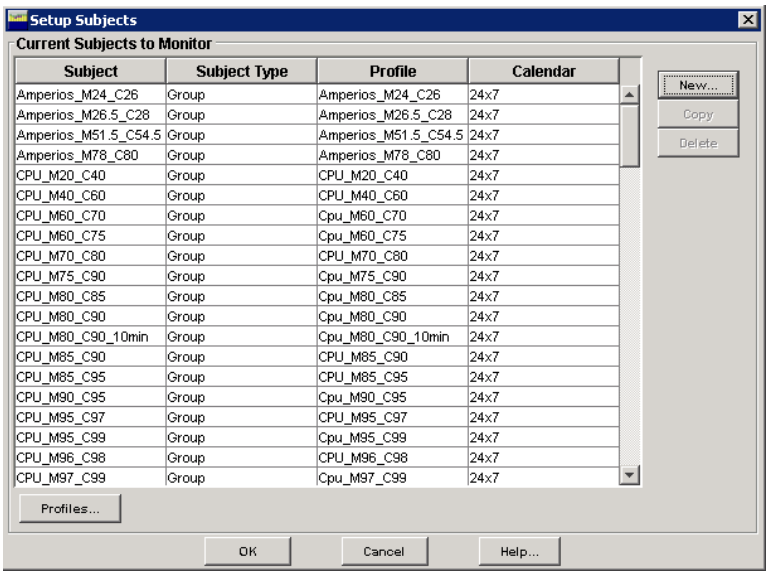
Figura N°18 Grupos creados en Ehealth

Group Name
CPU_M20_C30
CPU_M20_C40
CPU_M20_C60
CPU_M40_C60
CPU_M50_C70
CPU_M55_C65
CPU_M60_C70
CPU_M60_C75
CPU_M65_C75

Fuente: GMD

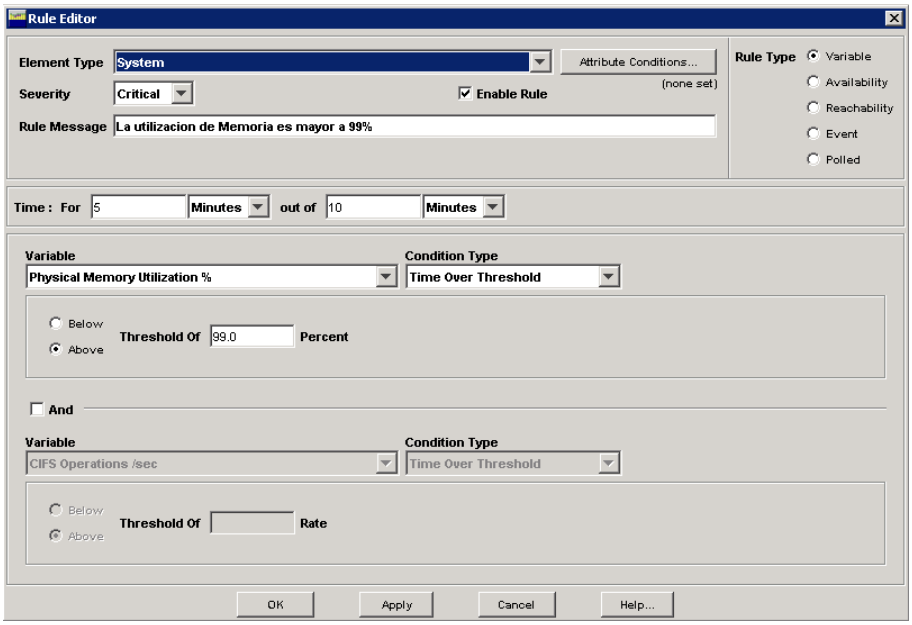
Ahora bien, los perfiles están compuestos por reglas donde se realizó la configuración de umbrales de consumo de recursos. Entre los perfiles que se han configurado se encuentran perfiles de consumo de CPU, Memoria física, partición en disco y memoria virtual.

Figura N°19 Ventana de asociación de perfiles y grupos.



Fuente: GMD

Figura N°20 Ventana de configuración de una regla.



Fuente: GMD

La creación de grupos, asignación de perfiles y creación de reglas dan como resultado las alertas registradas en la ventana “eHealth Live Exceptions”.

En dicha ventana se observan las alertas generadas en los servidores. Dentro de los campos que se encuentran tenemos:

Severidad: Tipo de alerta, podría ser Minor, Mayor o Critical.

Start: la hora en que se registró la alerta,

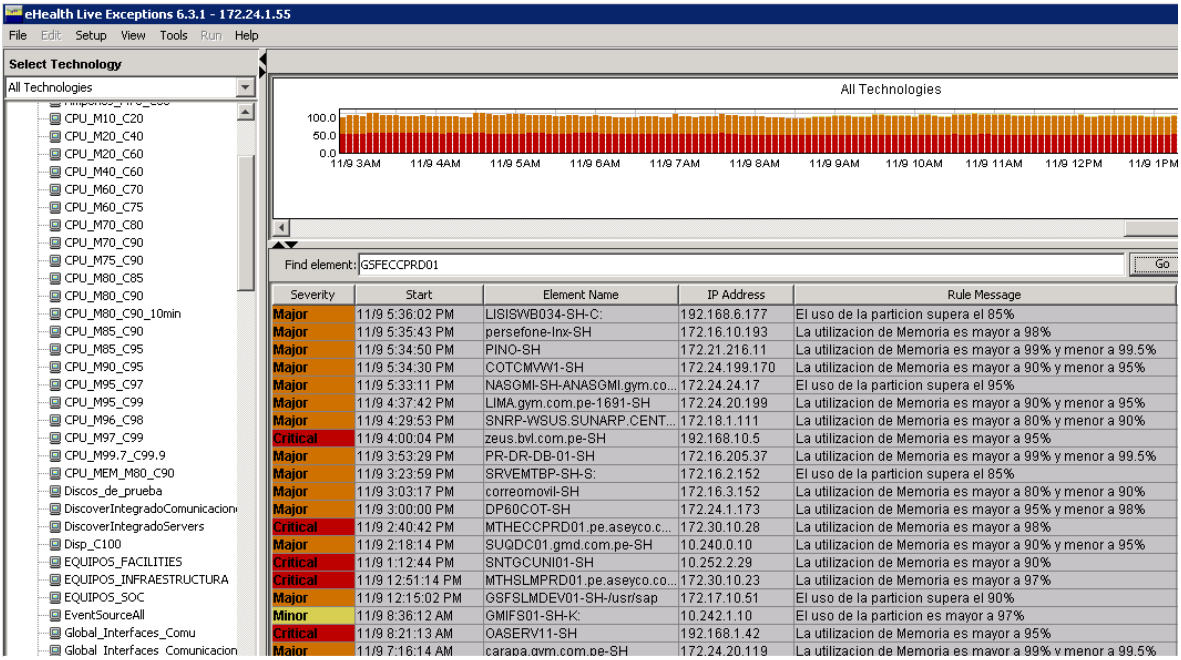
Element tipe: nombre del servidor donde se registra la alerta,

IP Address: IP del servidor.

Rule Message: Motivo por el cual se ha generado la alerta. Mensaje que se incluyó en la regla del perfil asignado al grupo.

End: Hora en que la alerta deja de presentarse en el servidor.

Figura N°21 Consola Live Exceptions

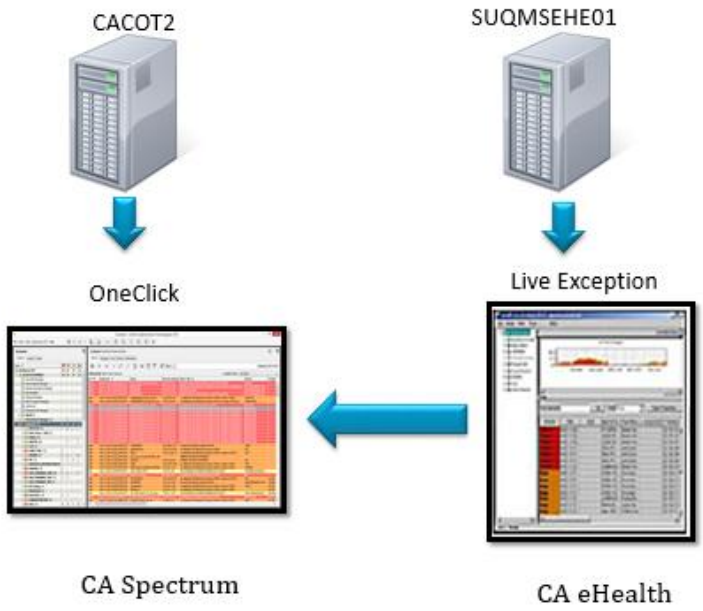


Fuente: GMD

En el modelo todas las alertas que se muestran en la consola Live Exceptions de Ehealth pasan a la consola OneClick de Spectrum.

La integración entre estas dos aplicaciones permite tener una sola consola, que consolide todas las alertas. El tiempo máximo para que las alertas se muestren en la consola de Spectrum es de 3 minutos.

Figura N°22 Flujo de Alarmas enviadas desde Ehealth



Fuente: GMD

3.3 REVISIÓN Y CONSOLIDACIÓN DE RESULTADO

3.3.1 Comparación de hallazgos

Para la presente investigación se procedió a aplicar 2 encuestas a los administradores de sistemas en distintas etapas del proyecto. Pues ellos son los encargados de tomar acciones sobre las incidencias que reciben del Centro de Operaciones Tecnológicas en los servidores.

La población está compuesta por los administradores de sistemas operativo en su totalidad. Dentro de este grupo encontramos a los administradores de todas las plataformas, como son Windows, Linux y AIX.

Cabe mencionar que de acuerdo al modelo organizacional de la empresa, cada administrador es asignado a uno o a un grupo de clientes.

La muestra está compuesta por una selección aleatoria. Teniendo en cuenta que todos los clientes se encuentren representados por al menos un administrador.

La primera encuesta se aplicó antes de la implementación. Es decir, bajo la situación que se describió en la realidad problemática del Capítulo 1. Cuando la empresa no tenía un sistema de monitorización y sólo contaba con un software de monitoreo de red, que únicamente le permitía censar la conectividad de los servidores.

La segunda encuesta fue aplicada luego de que el proyecto fue puesto en producción. Incluso se consideró un periodo de cinco semanas en que se realizó la capacitación sobre la utilización de las herramientas de monitoreo y la estabilización de la misma en el servicio. Pues la intención era reflejar en qué grado se ha beneficiado el servicio y cómo perciben la utilización del sistema de gestión de monitoreo.

Las encuestas se desarrollaron de la manera antes explicada para poder reflejar la opinión de los administradores de sistemas antes y después de la implementación del sistema de gestión de monitoreo (SGM).

3.3.2 Resultados de la encuesta e interpretación

En líneas generales, los resultados de la encuesta indican que el sistema de gestión de monitoreo implementado ha reducido el tiempo de atención de las incidencias. Así como también el número de incidentes, ya que al tener una visión del performance de los servidores se pueden prever problemas.

A continuación procederemos a analizar los resultados obtenidos en ambas encuestas.

Ítem 1 ¿Cuántas alertas le reportan en 1 día?

Como se puede observar en la Tabla N°4 (Pregunta 1 - Encuesta Final) notamos que luego de la implementación se incrementó el número de

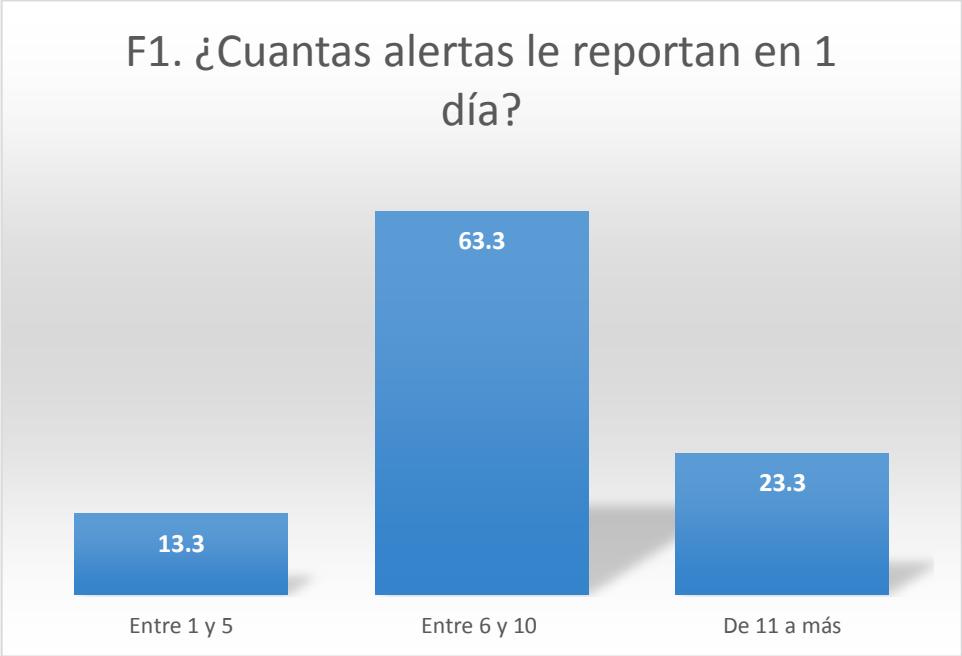
incidentes notificados a los administradores de sistemas en comparación a lo encontrado en la situación inicial.

Tabla N°3 Pregunta 1 - Encuesta inicial

Fuente: Propia

Esto sugiere que existe un gran número de incidentes que no estaba siendo captado por el software que se tenía en la situación inicial.

Tabla N°4 Pregunta 1 - Encuesta Final

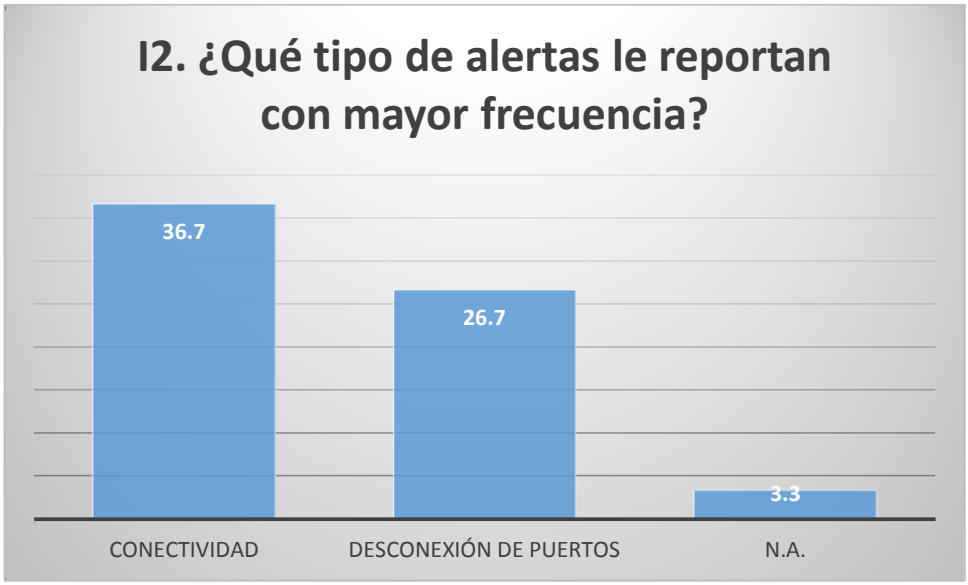


Fuente: Propia

Ítem 2 ¿Qué tipo de alertas le reportan con mayor frecuencia?

Como se observa en la Tabla N°6 (Pregunta 2 - Encuesta Final) gran parte de los incidentes son producto de un consumo elevado de recursos en el servidor. Es decir, que un servidor tenga como comportamiento habitual un gran consumo de sus recursos de performance como son la utilización de la memoria física, CPU y discos genera una abrupta caída del sistema operativo.

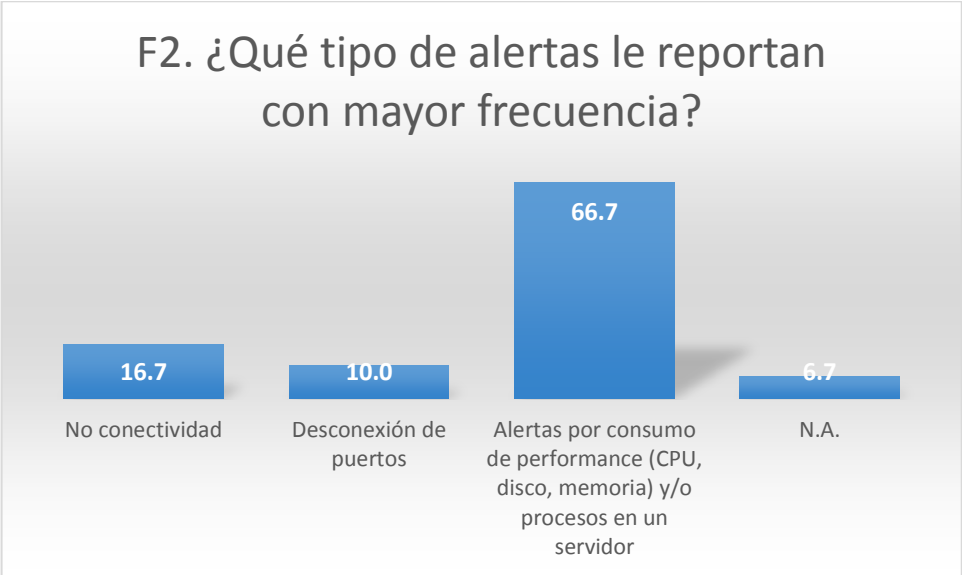
Tabla N°5 Pregunta 2 - Encuesta Inicial



Fuente: Propia

Luego de la implementación del sistema de gestión de monitoreo se redujeron los incidentes relacionados con caídas del sistema operativo y aumentó el número de alertas relacionadas con la utilización de recursos ver Tabla N°6 (Pregunta 2 - Encuesta Final).

Tabla N°6 Pregunta 2 - Encuesta Final



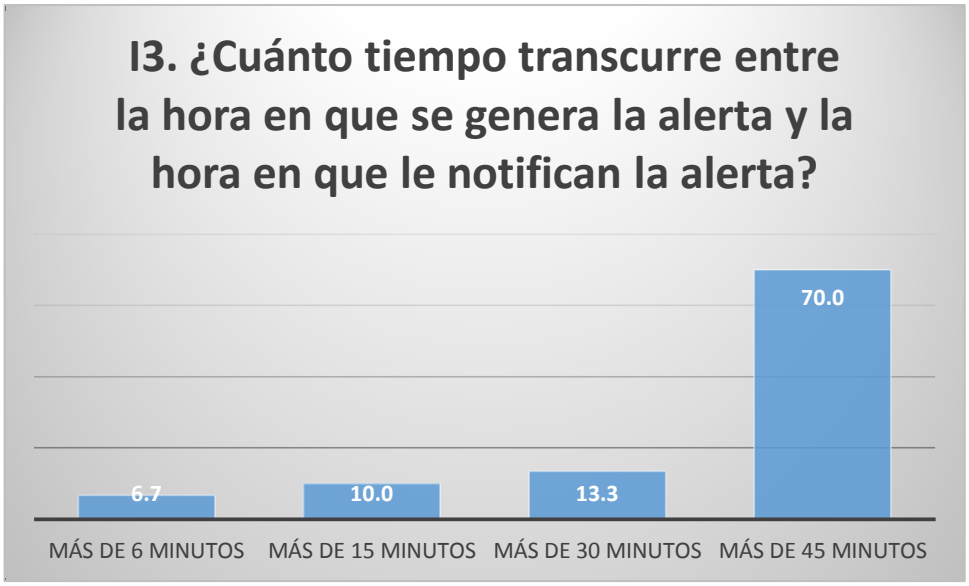
Fuente: Propia

Esto demuestra que nuestro SGM gracias a la detención temprana de incidentes evita la interrupción del servicio.

Ítem 3 ¿Cuánto tiempo transcurre entre la hora en que se genera la alerta y la hora en que le notifican la alerta?

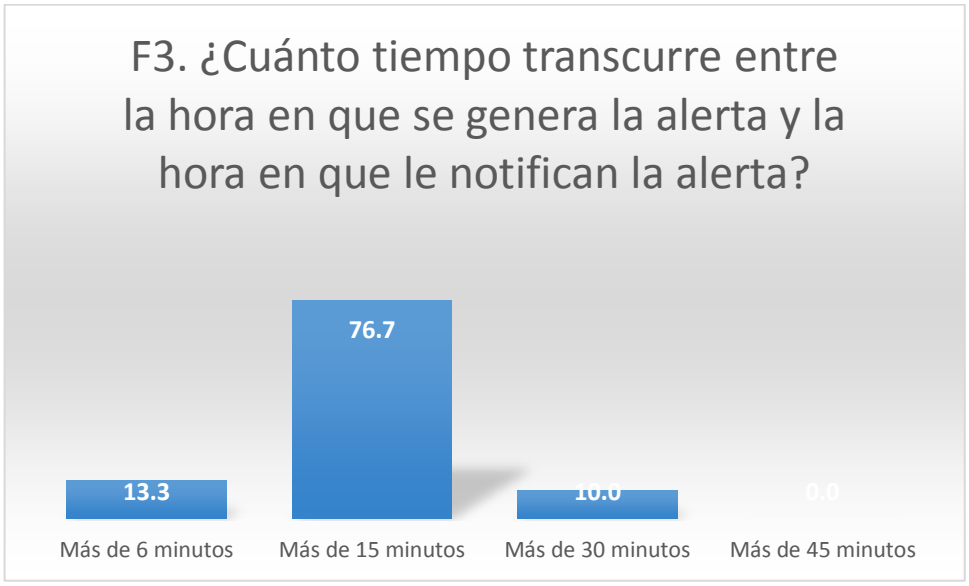
Se comprueba que el SGM reduce el tiempo en que una alerta es notificada por el COT (Tabla N°8 Pregunta 3 - Encuesta Final). La consola central de monitorización les da visibilidad de todas las incidencias a los operadores de sistemas. Permite distinguir la criticidad de un incidente e identificar de forma rápida a qué grupo de administradores deberá notificar el incidente. Por consiguiente el escalamiento de una situación crítica se realiza rápidamente.

Tabla N°7 Pregunta 3 - Encuesta Inicial



Fuente: Propia

Tabla N°8 Pregunta 3 - Encuesta Final

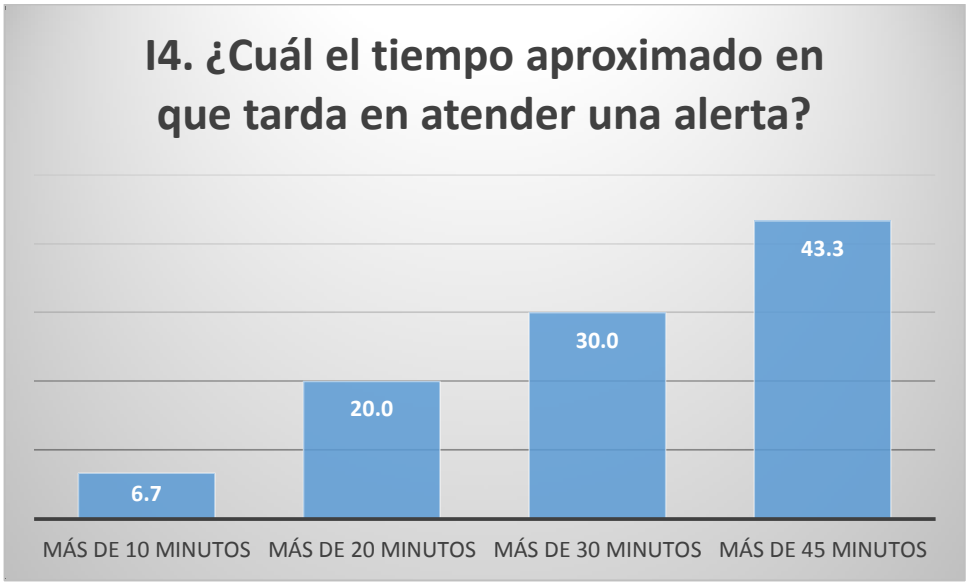


Fuente: Propia

Ítem 4 ¿Cuál el tiempo aproximado en que tarda en atender una alerta?

Se observa que el tiempo de atención en una situación crítica ha reducido notablemente. El tener un SGM que permita registrar todos los incidentes y guardar un historial de los mismos (Tabla N°10 Pregunta 4 - Encuesta Final).

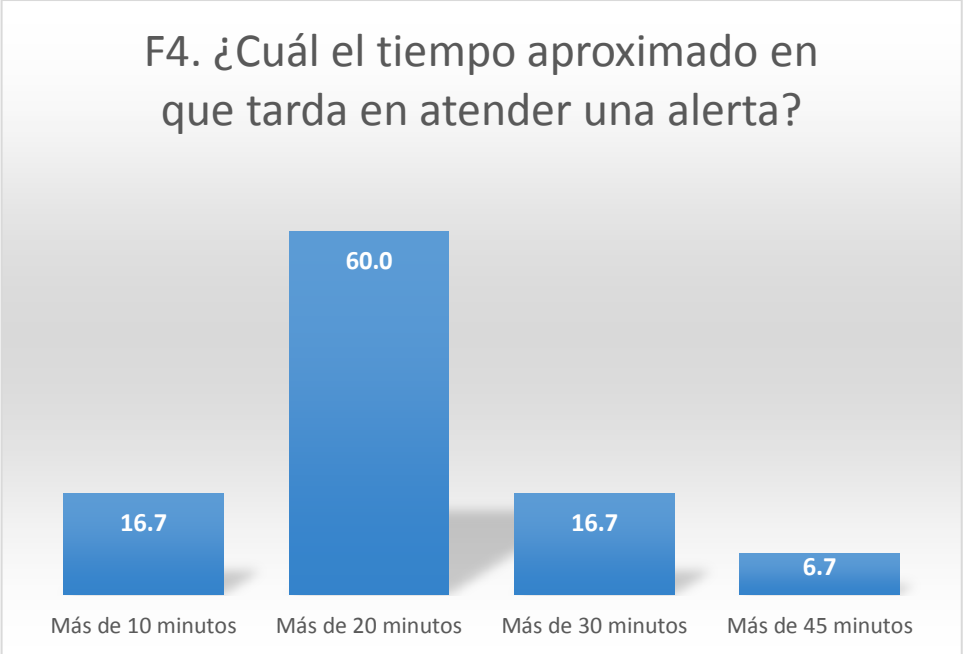
Tabla N°9 Pregunta 4 - Encuesta Inicial



Fuente: Propia

Esto nos da visibilidad acerca de los problemas más comunes y repetitivos en un equipo. Prácticamente es como un historial médico. Además de la rápida notificación del incidente que también un factor que nos permite reducir el tiempo de atención.

Tabla N°10 Pregunta 4 - Encuesta Final

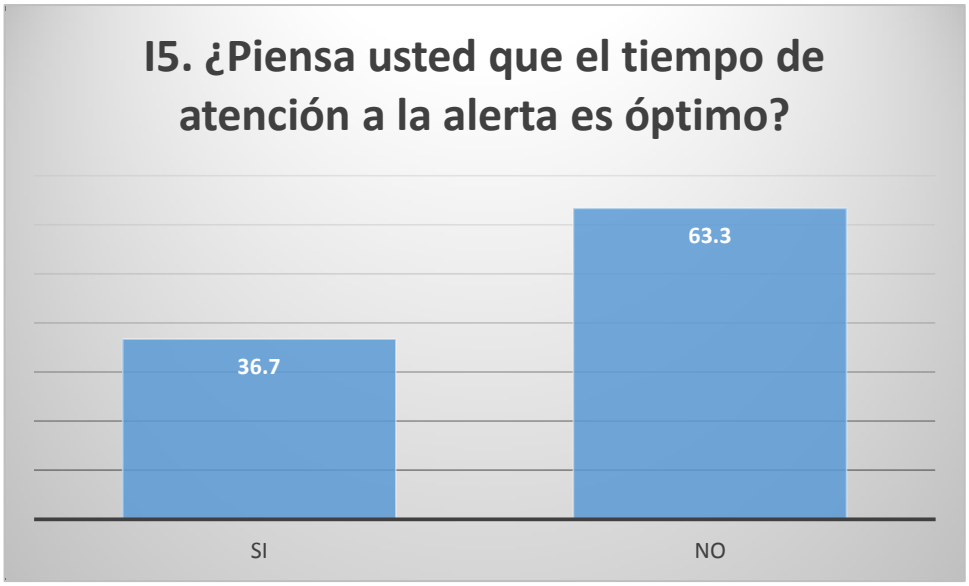


Fuente: Propia

Ítem 5 ¿Piensa usted que el tiempo de atención a la alerta es óptimo?

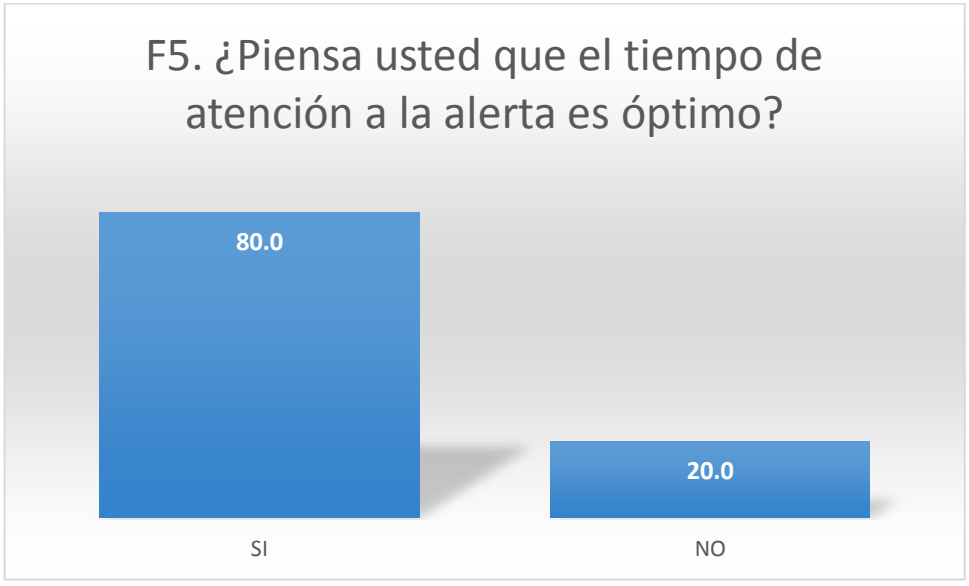
La opinión de los propios administradores de sistemas sobre el servicio ha cambiado. Cerca al 17% de la muestra ha cambiado de opinión con respecto a la encuesta inicial y considera que luego de la implementación de un SGM los tiempos de atención del servicio han mejorado. Es decir que se puede atender una incidencia en un mejor tiempo, generando eficiencia en el servicio (Tabla N°12 Pregunta 5 - Encuesta Final).

Tabla N°11 Pregunta 5 - Encuesta Incial



Fuente: Propia

Tabla N°12 Pregunta 5 - Encuesta Final

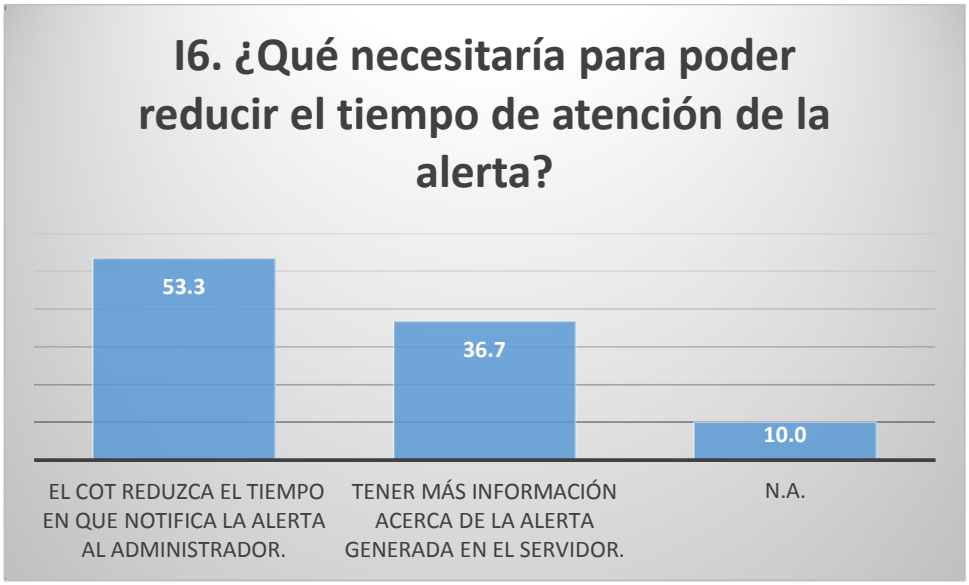


Fuente: Propia

Ítem 6 ¿Qué necesitaría para poder reducir el tiempo de atención de la alerta?

En este ítem vemos nuevamente que la opinión de los administradores de sistemas ha cambiado. Si bien inicialmente (Tabla N°12 Pregunta 6 - Encuesta Inicial) declaraban que el mayor obstáculo en la atención de una incidencia era que la notificación de la misma tardaba mucho en llegar a ellos, finalmente (Tabla N°13 Pregunta 6 - Encuesta Final) tenemos que lo que se necesita es obtener más información sobre la alerta.

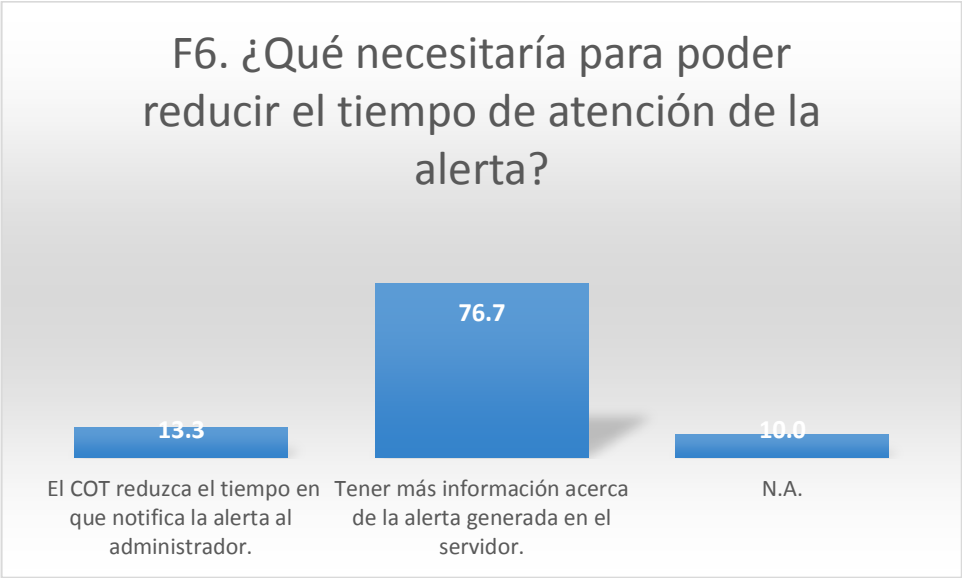
Tabla N°13 Pregunta 6 - Encuesta Inicial



Fuente: Propia

Habiendo dejado claro que los tiempos de notificación han mejorado, aún se mantiene un indicio que nos podría llevar a pensar que a pesar que se necesita más del SGM.

Tabla N°14 Pregunta 6 - Encuesta Final

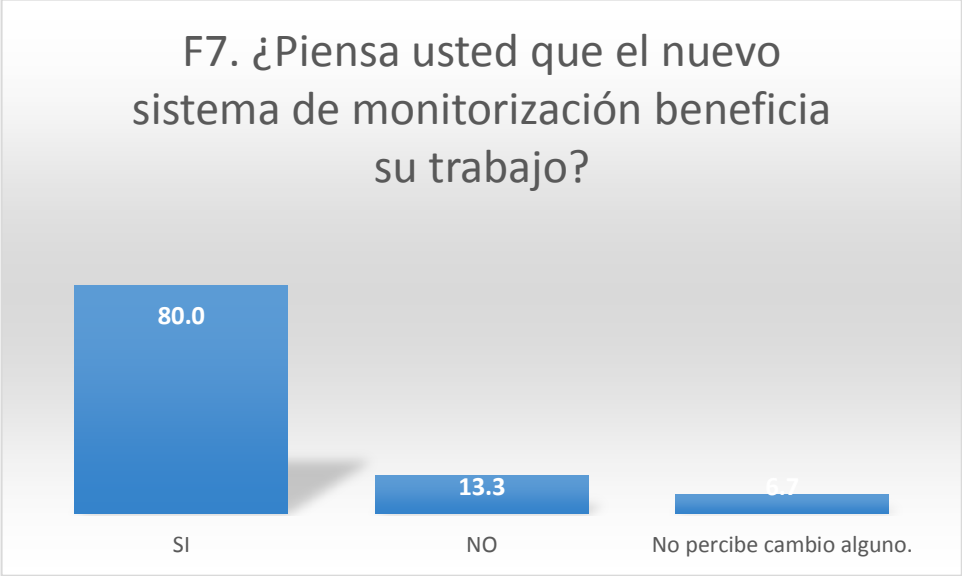


Fuente: Propia

Ítem 7 ¿Piensa usted que el nuevo sistema de monitorización beneficia su trabajo?

Este ítem sólo fue considerado en la segunda encuesta (Tabla N°14 Pregunta 7 - Encuesta Final). Básicamente se deseaba conocer cuál era la impresión que tenían los administradores de sistemas del SGM con que se cuenta.

Tabla N°15 Pregunta 7 - Encuesta Final



Fuente: Propia

Como se puede observar, la gran mayoría se siente beneficiado.

CONCLUSIONES

1. Luego de la implementación del SGM se han registrado un mayor número de incidentes. Lo que revela que ahora tenemos una visión más amplia del estado de los servidores.
   Es decir, se tiene una base de datos de incidentes que permite indagar sobre la causa raíz que desencadena una situación crítica, lo que nos permite solucionar rápidamente un incidente. Incluso prever incidentes, tener un comportamiento proactivo.

2. Se encontró que un gran grupo de servidores presentaba gran consumo de sus recursos, lo que generaba la caída de servicios. Gracias a la obtención de reportes se realizó el diagnóstico y la gestión para incrementar espacio en disco y capacidad de procesamiento. Se demuestra de esta manera que un sistema de gestión de monitoreo de servidores influye en la disponibilidad del servicio. Además influye en la toma de decisiones, como fue el aprovisionamiento de recursos.

3. Se ha reducido el tiempo de escalamiento de alertas que realizar los operadores del Centro de Operaciones Tecnológicas hacia los administradores de sistemas casi en media hora en la mayoría de los casos.

4. El tiempo de resolución de incidentes se redujo notablemente gracias a la base de datos de incidencias. Ya que se tiene visibilidad de los problemas más comunes y repetitivos en un servidor, lo que permite tomar una rápida acción al administrador y normalizar las situaciones críticas.

RECOMENDACIONES

1. Cuando se realiza la implementación de una aplicación que prestará servicios y en todos los casos en general, es muy importante realizar un redimensionamiento de la solución. Es decir, debemos asegurarnos de que la aplicación será capaz de prestar servicio a un determinado número de equipos. También se debe tomar en cuenta la escalabilidad del producto a implementar.
2. Debemos asegurarnos de contar con una versión estable del producto a implementar.
3. Es muy importante contar con el soporte del fabricante. Ya que en la primera etapa de los proyectos de implementación casi todas las situaciones son nuevas para el grupo de administradores responsables.

BIBLIOGRÁFIA

- SENATI. Manual de Practicante - Administración de Redes. Lima: SENATI - Programa Nacional de Informática, 2008

- San Román Esteban. Evolución y tendencias de las herramientas de monitoreo de redes. [Monografía de Internet]. México, D.F.: Magazcitum; 2011 [acceso 25 de Setiembre de 2014]. Disponible en: http://www.magazcitum.com.mx/?p=1157
- Lamiña FP, Ramos AK, Yugsi MV. Análisis e implementación de un sistema de monitorización para la infraestructura tecnológica del edificio matriz del Instituto Nacional de Contratación Pública utilizando software de libre distribución. [Monografía de Internet]. Ecuador, Quito: Universidad Central del Ecuador; 2012 [acceso 21 de julio de 2014]. Disponible en: http://www.dspace.uce.edu.ec/handle/25000/148

- Selley Rojas Héctor Julián. Monitoreo del comportamiento de servidores de aplicaciones. [Monografía de Internet]. México, D.F.: Instituto Politécnico Nacional; 2008 [acceso 25 de julio de 2014]. Disponible en: http://www.saber.cic.ipn.mx/cake/SABERsvn/trunk/Repositorios/webVerArchivo/305/1

- Tapia R, Sánchez DS. Propuesta de un sistema de monitoreo para la red de ESIME ZACATENCO utilizando el protocolo SNMP y software libre. [Monografía de Internet]. México, D.F.: Instituto Politécnico Nacional Escuela Superior De Ingeniería Mecánica Y Eléctrica Unidad Profesional “Adolfo López Mateos”; 2009 [acceso 27 de julio de 2014]. Disponible en: http://itzamna.bnct.ipn.mx/dspace/bitstream/123456789/5456/1/PROPUESTASISTEMA.pdf

- Pinto Martinez José Luis. Monitoreo centralizado de servidores de Movilnet con herramientas de software libre. [Monografía de Internet].

Venezuela, Caracas: Universidad Simón Bolívar; 2011 [acceso 30 de julio de 2014]. Disponible en: http://159.90.80.55/tesis/000151305.pdf

- Sánchez Pico Wilman Darío. Propuesta de monitoreo de la infraestructura tecnológica de los servidores del ministerio de finanzas, basado en el modelo ITIL v3 y en la herramienta HP Sitescope. [Monografía de Internet]. Ecuador, Quito: Universidad Politécnica Salesiana; 2014 [acceso 4 de agosto de 2014]. Disponible en: http://dspace.ups.edu.ec/bitstream/123456789/6822/1/UPS-ST001101.pdf

- UIT. Acerca de UIT [Sede Web]. México: UIT; 2015 [acceso 30 de julio de 2014]. Extraído de: http://www.itu.int/es/ITU-D/Pages/Regional-Presence.aspx
- Alegsa. IETF [Sede Web]. Argentina: Alegsa; 2013 [acceso 10 de agosto de 2014]. Extraído de: http://www.alegsa.com.ar/Dic/ietf.php
- Huidobro J. Manuel. SNMP Un protocolo simple de gestión [Sede Web]. Madrid: IIES; 2008 [acceso 15 de agosto de 2014]. Extraído de: http://www.coit.es/publicac/publbit/bit102/quees.htm
- EIA. RMON [Sede Web]. Argentina: EIA; 2010 [acceso 16 de agosto de 2014]. Extraído de: http://eia.udg.es/~cmantill/admonxarxes/rmon.pdf
- Alegsa. Latencia [Sede Web]. Argentina: Alegsa; 2011 [acceso 19 de agosto de 2014]. Extraído de: http://www.alegsa.com.ar/Dic/latencia.php
- Marcelo French. Dashboard y Scorecards [Sede Web]. Argentina: Sixtina; 2011 [acceso 20 de agosto de 2014]. Extraído de: http://www.sixtinagroup.com/db-bsc-diferencia/
- Alegsa. Backend y Frontend [Sede Web]. Argentina: Alegsa; 2011 [acceso 23 de agosto de 2014]. Extraído de: http://www.alegsa.com.ar/Dic/back-end.php

ANEXOS

ANEXOS 1

PRESENTACIÓN DE LA ENCUESTA N°1

1. ¿Cuantas alertas le reportan en 1 día?
    a) Entre 1 y 5
    b) Entre 6 y 10
    c) De 11 a más
2. ¿Qué tipo de alertas le reportan con mayor frecuencia?
    a) No conectividad
    b) Desconexión de puertos
    c) N.A.
3. ¿Cuánto tiempo transcurre entre la hora en que se genera la alerta y la hora en que le notifican la alerta?
    a) Más de 6 minutos
    b) Más de 15 minutos
    c) Más de 30 minutos
    d) Más de 45 minutos
4. ¿Cuál el tiempo aproximado en que tarda en atender una alerta?
    a) Más de 10 minutos
    b) Más de 20 minutos
    c) Más de 30 minutos
    d) Más de 45 minutos
5. ¿Piensa usted que el tiempo de atención a la alerta es óptimo?
    a) Sí
    b) No
6. ¿Qué necesitaría para poder reducir el tiempo de atención de la alerta? De ser necesarios marcar más de una opción.

a) El COT reduzca el tiempo en que notifica la alerta al administrador.
b) Tener más información acerca de la alerta generada en el servidor.
c) N.A.

ANEXOS 2

PRESENTACIÓN DE LA ENCUESTA N°2

1. ¿Cuantas alertas le reportan en 1 día?
    d) Entre 1 y 5
    e) Entre 6 y 10
    f) De 11 a más
2. ¿Qué tipo de alertas le reportan con mayor frecuencia?
    d) No conectividad
    e) Desconexión de puertos
    f) N.A.
3. ¿Cuánto tiempo transcurre entre la hora en que se genera la alerta y la hora en que le notifican la alerta?
    e) Más de 6 minutos
    f) Más de 15 minutos
    g) Más de 30 minutos
    h) Más de 45 minutos
4. ¿Cuál el tiempo aproximado en que tarda en atender una alerta?
    e) Más de 10 minutos
    f) Más de 20 minutos
    g) Más de 30 minutos
    h) Más de 45 minutos
5. ¿Piensa usted que el tiempo de atención a la alerta es óptimo?
    c) Sí
    d) No
    e) N.A.

6. ¿Qué necesitaría para poder reducir el tiempo de atención de la alerta? De ser necesarios marcar más de una opción.
   a) El COT reduzca el tiempo en que notifica la alerta al administrador.
   b) Tener más información acerca de la alerta generada en el servidor.
   c) N.A.

7. ¿Piensa usted que el nuevo sistema de monitorización beneficia su trabajo?
   a) SI
   b) NO
   c) No percibe cambio alguno.