ISSN: 2594 - 2905

NOTIFICACIÓN DE ALERTAS PARA SU GESTIÓN EN DISPOSITIVOS DE LA RED MULTICLIENTES POR MEDIO DE NAGIOS

NOTIFICATION OF ALERTS FOR MANAGEMENT ON MULTI-CLIENT NETWORK DEVICES VIA NAGIOS

Martínez Ramírez Violeta[1], Luciano Machorro Teresa[2], Osorio Ramírez Efrén Armando[3], García Sierra Margarita Raquel[4], Guarneros Rojas Aymée[5]

[1].Doctorado en Educación. Tecnológico Nacional de México, Campus Instituto Tecnológico de Puebla. Departamento de Sistemas y Computación. Dirección: violeta.martinez@puebla.tecnm.mx, Av. Tecnológico 420 Col. Maravillas, C.P. 72220. Puebla, Puebla, México.
[2]Maestría en Ingeniería. Tecnológico Nacional de México, Campus Instituto Tecnológico de Puebla. Dirección: teresa.luciano@puebla.tecnm.mx, Av. Tecnológico 420 Col. Maravillas, C.P. 72220. Puebla, Puebla, México.
[3]Doctorado en Ciencias en Planificación de Empresas y Desarrollo Regional. Tecnológico Nacional de México, Campus Instituto Tecnológico de Puebla. efren.osorio@puebla.tecnm.mx, Av. Tecnológico 420 Col. Maravillas, C.P. 72220. Puebla, Puebla, México.
[4]Maestría en Ingeniería Administrativa. Tecnológico Nacional de México, Campus Instituto Tecnológico de Puebla. Departamento de Ciencias Básicas. Dirección: margaritaraquel.garcia@puebla.tecnm.mx, Av. Tecnológico 420 Col. Maravillas, C.P. 72220. Puebla, Puebla, México.
[5].Estudiante del 9° semestre de la carrera en Ingeniería en Tecnologías de la Información y Comunicaciones. Tecnológico Nacional México, Campus Instituto Tecnológico de Puebla. Dirección. i17221555.19@puebla.tecnm.mx, Av. Tecnológico 420 Col. Maravillas, C.P. 72220. Puebla, Puebla, México

Resumen – El presente desarrollo consiste en gestionar correctamente la notificación de alertas en dispositivos de la red multiclientes en el área Network Operation Center (NOC) de la empresa dedicada a ofrecer servicios digitales líder en la región, por medio del software NAGIOS con el fin de mejorar la calidad del servicio de monitorización y administración de incidencias para disminuir costos y eliminar tiempos de inactividad.
El área donde se implementa responsabiliza del tratamiento de eventos y alarmas que aparecen en las consolas de monitorización. El NOC actúa como el sistema nervioso para administrar y optimizar las tareas críticas para el negocio, como la solución de problemas de red, la distribución y actualización de software, la administración de nombres de dominio y routers, la supervisión del rendimiento y la coordinación con redes afiliadas.
Palabras Clave: alertas, multiclientes, notificación, NAGIOS, red.

Abstract -- The present development consists of correctly managing the notification of alerts in multi-client network devices in the Network Operation Center (NOC) area of the company dedicated to offering leading digital services in the region, through the NAGIOS software in order to improve the quality of incident monitoring and management service to reduce costs and eliminate downtime.
The area where it is implemented is responsible for the treatment of events and alarms that appear on the monitoring consoles. The NOC acts as the nervous system for managing and optimizing business-critical tasks such as network troubleshooting, software distribution and upgrades, domain name and router management, performance monitoring, and coordination with affiliate networks.
Key words – alerts, multi-tenants, notification, NAGIOS, network.

INTRODUCCIÓN

La situación actual, surge por la necesidad de solucionar diversas problemáticas que generan alarmas a partir de diferentes situaciones causadas por los enlaces de datos sobrecargados o conexiones de red, así como la supervisión de los routers, switches y más, por mencionar las más comunes.
Los incidentes antes mencionados se resuelven con los alcances divididos en tres plazos; a corto plazo, la detección de las alarmas reveladas por monitorización, así como el reconocimiento de dichos eventos para buscar una posible solución; a mediano plazo, se revisa la existencia de instrucciones especiales y posteriormente se hará el registro de las acciones realizadas en la herramienta de ticketing; y a largo plazo, se gestionará constantemente el tratamiento de las alarmas derivadas de dichas incidencias alertadas en dispositivos de red multiclientes.

Estado del Arte

Existen publicados proyectos que han implementado en sistemas informáticos de Hispanoamérica para minimizar tiempos de inactividad de los servicios y equipos de comunicación generando beneficios para las empresas.
Uno de ellos es Perú, donde a una institución financiera que favoreció el desempeño de la red exitosamente a costo bajo por ser una herramienta Open Source [1].
En España la presencia de NAGIOS en un software que ahorre tiempos en gestionar alertas de caída o criticidad de los sistemas Implantación de un sistema de monitorización para infraestructuras de telecomunicaciones, basado en Nagios, con alarma temprana exitosa ante incidencias, considerando las

siguientes áreas: - Equipos informáticos. - Equipos de comunicaciones. - Centro de datos [2].

En el mismo país, la publicación de una implementación con NAGIOS sobre la instalación y configuración de un sistema de gestión de Red (NMS) en una Red que incluye diferentes subredes, routers, servidores y servicios. El despliegue del sistema de gestión se llevó a cabo sobre una Red virtualizada exitosamente [3].

Dentro del sector de alimentos se implementa el sistema de monitoreo que controla el total de la red, actividades de los servicios y servidores. Además, registra equipos, alerta al administrador de fallos que presenta la red; facilitando la búsqueda de soluciones eficazmente y logrando que hosts o servicios estén registrados para llevar un análisis de monitoreo preciso, por lo tanto, se tiene un mejor seguimiento en conjunto con los alertamientos sobre los comportamientos de los equipos de hardware y servicios de software, brindará a usuarios el mayor grado de rendimiento de los dispositivos [4].

El siguiente desarrollo implementado en el campus universitario en España demostró las ventajas de usar una herramienta de monitorización basado en NAGIOS, aportando usabilidad, disponibilidad, continuidad, rendimiento y normalidad, integrando open source en una red donde dispone de información instantánea de problemas en dispositivos, servidores y servicios que tienen un nivel crítico alto, siendo éstos muy importantes para facilitar un servicio a usuario y clientes, y posteriormente medir la satisfacción de los usuarios que acceden a ellos [5].

Justificación

En el área de NOC de la empresa líder en servicios digitales se realizará a fin de monitorear dispositivos de red multiclientes que ahorre dinero y eliminar el tiempo de inactividad.

Cuando se trata de herramientas de monitorización de red de código abierto, las organizaciones más grandes del mundo recurren a NAGIOS. NAGIOS supervisa la red para los problemas causados por los enlaces de datos sobrecargados o conexiones de red, así como la supervisión de los routers, switches y más. Fácilmente capaz de supervisar la disponibilidad, el tiempo de actividad y el tiempo de respuesta de cada nodo de la red, NAGIOS entrega los resultados en una variedad de representaciones visuales e informes.

Por lo antes expuesto, se justifica la implementación de la herramienta NAGIOS en el sistema de alertas que gestione el monitoreo de la red mulicliente.

Objetivo general

Notificación de alertas para su gestión en dispositivos de la red multiclientes por medio de NAGIOS.

Objetivos específicos

- Detectar el evento o alarma revelado por monitorización.
- Reconocer el evento o alarma detectado por monitorización.
- Revisar existencia de instrucciones especiales para el evento o alarma detectado.
- Registrar las acciones realizadas en la herramienta de ticketing.
- Monitorear el tratamiento de alarmas derivadas de incidencias alertadas en dispositivos de red multiclientes.

Alcances y Límites

- Adecuar funciones semejantes a otras áreas de soporte de hardware y software.
- Cobertura 24/7 de los servicios de monitoreo.
- Dirigido a la gestión de notificaciones por alertas en los protocolos de red.
- Desarrollado para el área NOC de a empresa líder en servicios digitales para multiclientes.

Enunciado de investigación

NAGIOS favorece la gestión de alertas se servicios en una red multiclientes.

NAGIOS

El monitoreo de red de NAGIOS: según su portal, esta herramienta de monitoreo de red se define de código abierto, El monitoreo del servidor se facilita en Nagios debido a la flexibilidad se seguimiento a servidores con monitoreo basado en agente y sin agente. Con más de 5000 complementos diferentes disponibles.

Además, proporciona herramientas para monitorear las aplicaciones y su estado, incluidas en los sistemas operativos de Windows, Linux, UNIX y las aplicaciones web.

Los componentes de infraestructura de misión crítica, incluidas servicios, sistemas operativos, protocolos de red, métricas de sistemas e infraestructura de red también pueden ser monitoreados. [6]

Junto a Meraki CISCO [7], ofrece soluciones de TI completas, escalables e intuitivas para la gestión en la nube. Meraki es una de las carteras de negocios de más rápido crecimiento de Cisco y es el líder del mercado en redes administradas en la nube con más de:

o 250.000 clientes en todo el mundo.
o 1.5 millones de redes de Meraki conectadas

Cuya habilidad favorece al proyecto descrito en este trabajo donde soporta entornos multi-cliente gracias a puntos de acceso que optimizan el rendimiento en función del perfil

DESARROLLO

Según los tipos de redes [8], la topología en cuestión [9] y la forma de interconexión [10] de cada elemento que integra la red [11] en cada negocio, el monitoreo ayuda significativamente a un servidor de este tipo [12] que coordine eficientemente los protocolos [13] de comunicación digital dentro de la intranet [14].

Detección y tratamiento del evento o alarma

La primera actividad consta de identificar los eventos o alarmas que se despliegan a través de la herramienta de monitorización NAGIOS, mencionada y detallada en párrafos anteriores.

A través de NAGIOS se observan las diversas problemáticas que generan la aparición de alarmas, tales como enlaces de datos sobrecargados o conexiones de red, errores en puertos, conectividad de VPN, así como la supervisión y gestión de los diversos dispositivos de red multiclientes, como servidores, routers, switches, gateways de voz y de más.

Las alarmas se clasifican en 4 categorías, (CRIT) critical son los eventos que deben tratarse con mayor prioridad, ya que su fallo representa una afectación significativa en el servicio del cliente; (MAJOR) major son eventos que pueden o no representar una afectación significativa en el servicio del cliente, por lo tanto, la criticidad con la que trata es media;(WARN) warning tal como su nombre lo dice, son alarmas de advertencia, al igual que las major estás pueden o no representar una afectación significativa en los servicios, así que son tratadas con prioridad media o baja, dependiendo el caso; y finalmente los eventos (OK) que son las notificaciones o alarmas que nos indican que el estado de los equipos ha vuelto a la normalidad y se encuentran trabajando correctamente.
En la siguiente figura 1, se visualizan las alarmas detectadas en la herramienta de monitorización NAGIOS, las cuales indican que el tratamiento de dichos dispositivos debe ser tratado con una criticidad alta.

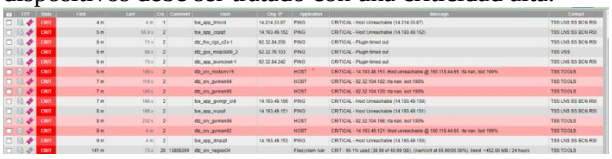


Figura 1. Alarmas críticas desplegadas en NAGIOS

Las alarmas de criticidad media (major), se muestran en la figura 2.

Figura 2. Alarmas major desplegadas en NAGIOS

Los eventos o alarmas warning cuya criticidad es media o baja, se muestran en la siguiente figura 3.

Figura 31. Alarmas warning desplegadas en NAGIOS.

Finalmente, una figura de cómo se muestran los eventos en OK. Ver. Figura 4.

Figura 4. Alarmas OK desplegadas en NAGIOS.

Revisar existencia de instrucciones especiales para el evento o alarma
Algunos equipos que se gestionan y monitorizan desde el NOC cuentan con instrucciones especiales para el tratamiento y gestión de sus incidencias, estas instrucciones se muestran desde la herramienta NAGIOS. Para visualizar si un equipo tiene instrucciones especiales, es necesario ver la información almacenada en el inventario (PISA), desde el icono ubicado al inicio de la alarma desplegada. Ver figura 4.

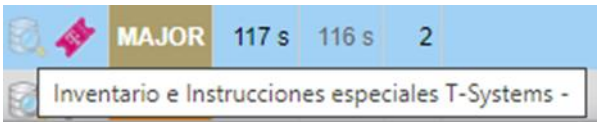


Figura 4. Visualización de inventarios e instrucciones especiales.

Donde se despliega la ventana con la información más importante del dispositivo para poder identificarlo en la base de datos de interés, y también la instrucción especial con la que debe ser tratada y gestionada la incidencia.
Si la alarma no cuenta con instrucciones especiales, debe ser trata con el procedimiento estándar de monitorización y gestión de incidencias (véase figura 5).

Figura 5. Alarma sin instrucciones especiales.

Diagnóstico del evento o alarma

Para determinar cuáles son las posibles causas que provocaron la aparición del evento, se realiza el troubleshooting correspondiente al tipo de alarma detectada, y en caso de ser necesario se solicita ayuda de personal on-site para determinar el origen del problema.
Con la ayuda del aplicativo Meraki, mencionado y detallado en párrafos anteriores, es posible validar el estado en el que se encuentran los dispositivos. Ver figura 6.

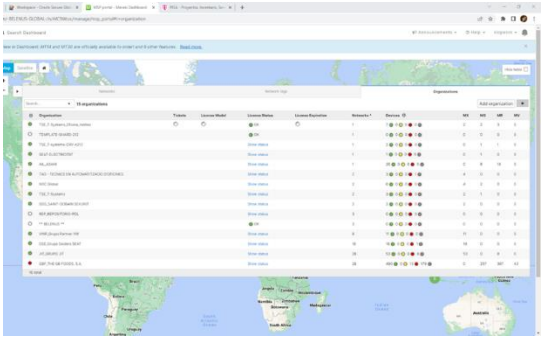


Figura 6. Dashboard principal de CISCO Meraki.

Desde el Dashboard de Meraki, se visualizan los diversos clientes, las diversas redes o sitios en las que se divide el cliente y los respectivos equipos de cada sede, que son

gestionados y monitorizados desde Network Operation Center (NOC).

El dashboard permite visualizar la topología completa de los sitios gestionados en la nube. Ver figura 7.

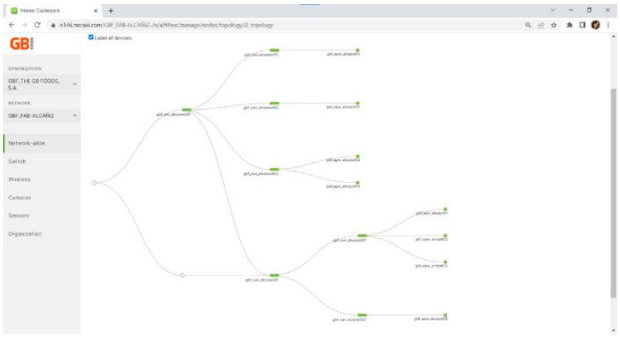


Figura 7. Topología vista desde CISCO Meraki.

En la figura 8 se observa información y estadísticas para conocer el estado en el que encuentran los dispositivos. Este ejemplo es de un switch, se pueden apreciar los puertos; los clientes conectados; datos tales como IP, VLAN, IP publica, Gateway, DNS, etc.

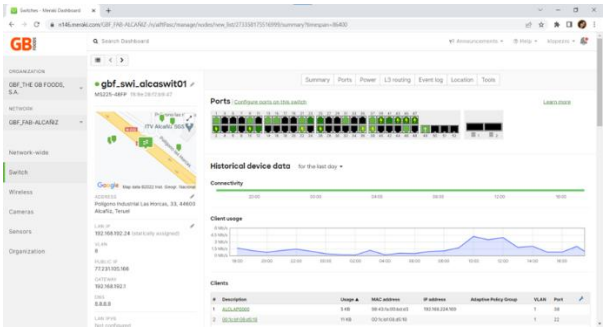


Figura 8. Información desplegada en CISCO Meraki de un switch.

Cuando los equipos no se encuentran en óptimas condiciones, el dashboard de Meraki lo muestra como "offline" o el estado en rojo. La falla de un equipo puede deberse a un problema eléctrico o algún mantenimiento en el sitio el cual no fue notificado a los ingenieros de primer nivel. Ver figura 9.

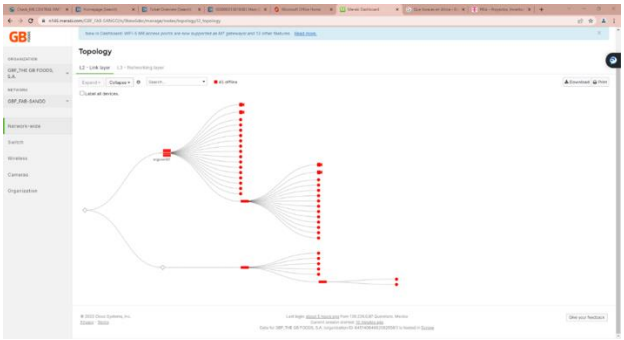


Figura 9. Ejemplo de sede completamente caída.

Otra forma de validar que los equipos tiene algún problema es entrando directamente al dashboard que despliega sus características. Ver figura 10.

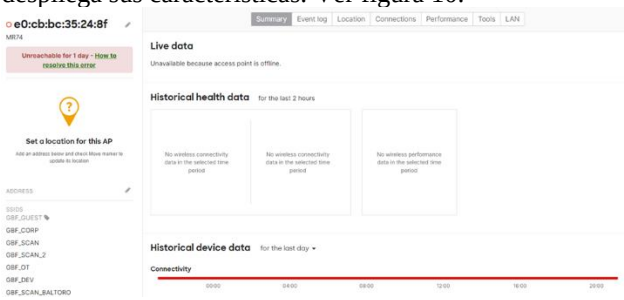


Figura 10. Dispositivo fuera de línea.

Asignación de ticket

Al acceder a la herramienta de ticketing wTTs, mencionada y detallada en párrafos anteriores, se observa una pantalla inicial en cuya parte central aparece un desplegable con los grupos de asignación a los que pertenece el usuario.

Se mostrarán en esta pantalla solo los tickets que estén sin aceptar por ningún miembro del equipo.

En la parte izquierda en "Change User settings" se puede modificar que el aviso de asignación de ticket al grupo/s de pertenencia sea mediante un "pop-up" (eTTs debe estar abierto) o bien vía email. El método por defecto es el "pop-up".

Aparecen las opciones "create new Incident Ticket" o "Ticket overview" para pasar a la página que permite generar un nuevo ticket o ver a la página que muestra la cola de tickets asignados a los grupos de pertenencia. Ver figura 11.

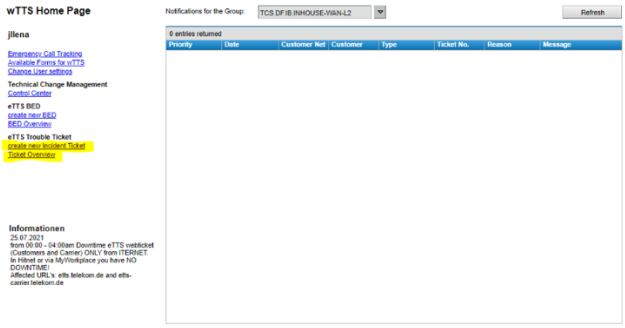


Figura 11. wTTs Home Page

Para buscar tickets, será necesario dar click en "Ticket Overview" (véase figura 12).

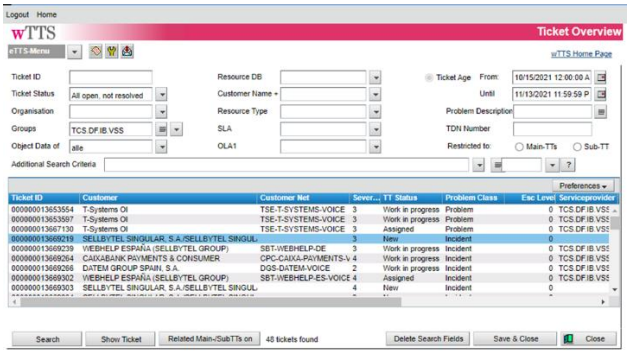


Figura 12. Ticket Overview.

Abrir un ticket en wTTs

Seleccionar la opción abrir ticket (véase figura 13)

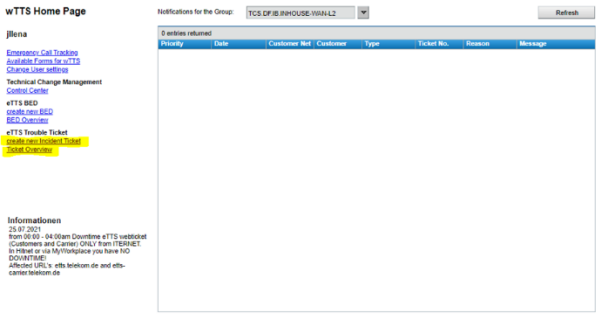


Figura 13. wTTs Home Page. Abrir ticket.

Se abrirá la siguiente ventana. Ver figura 14

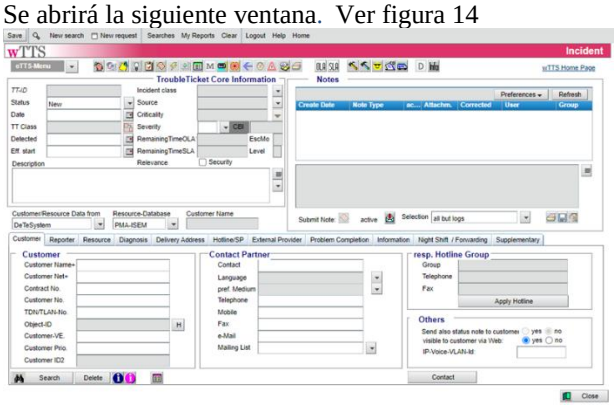


Figura 14. Nuevo ticket.

Datos generales del ticket

El siguiente paso por seguir es rellanar los datos generales del ticket. Los campos para rellenar son los marcados en amarillo en la siguiente figura 15.

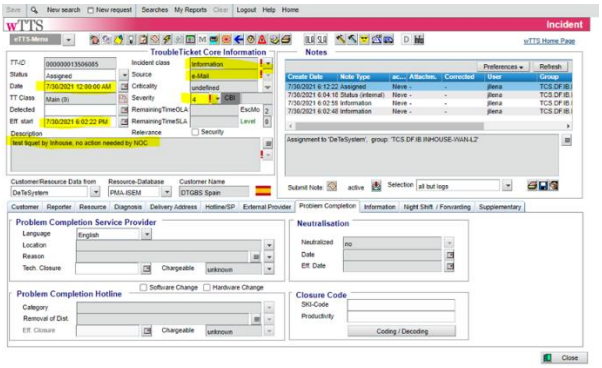


Figura 15. Datos generales para llenar el ticket.

Datos de Cliente

A continuación, será necesario rellenar los datos del cliente, Technical Network y CI afectado. Para realizar esto, se busca en la "Resource-Database" indicada, que por defecto es PMA-ISEM.

Se escribe el cliente o parte de su nombre, por ejemplo, DTGBS y le damos al botón "Search", aparecerá un "pop-up" con ese cliente.

IMPORTANTE: si el nombre del cliente no es correcto (mapping erróneo de SM9, por ejemplo), se da click a la "cruz roja" del "pop-up" que aparece al dar al botón "search" de la pestaña "Customer" y se borra el nombre para poder escribir una parte del nombre correcto y así se pCon el cliente ya seleccionado, en la parte derecha se da click al botón "Network Search" para que reporte la lista de TDN's (Technical Networks). Las TDN's de PMA-ISEM corresponden a los "Grupos Técnicos" la tabla de nuestro interés pueda localizar en la base de datos.

Datos de contacto del solicitante

Se deben indicar los datos del contacto para abrir el ticket. El medio de contacto puede ser teléfono o email, se requerirá rellenar un campo u otro.

Asignar ticket a un Assignment Group (AG) que use wTTs

Desde la pestaña "Hotline/SP" de la parte inferior se selecciona la organización ("Organisation"), la cual siempre será DeTeSystem y el "Org. Group" al que será asignado el ticket.

Asignar ticket a un AG que no usa wTTs

Lo principal es verificar que el ticket está asignado al grupo de wTTs correspondiente al NOC en la pestaña de Hotline/SP.

Desde la pestaña "External Provider", se selecciona "Organisation=" IMTC" y "Org. Group" se selecciona el grupo de destino dentro de los valores del desplegable.

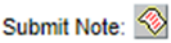
- Grupos de HelpDesk/primer nivel:
- Para clientes Soporte Telefonía asignar a DS.ISD.IB.VSSL1
- Para clientes Voice Services asignar a DS.ISD.IB.24X7.SD
- Para clientes vía CST (por ejemplo, SOC), usar DS.ISD.IB.CST.SD

IPSUMTEC
ISSN: 2594 - 2905

- Para PQIT usar DS.ISD.IB.ANS.SD
- Resto de grupos:
- Para clientes PQIT, GBF y MCM el ticket irá a SM9

Registro de acciones realizadas en la herramienta de ticketing

En la página del ticket abierta, en la sección “Notes” se da clic en el botón “Submit Note”



Se desplegará una ventana en la que agregaremos la nota, el tipo de nota y de ser necesario adjuntar evidencias, como imágenes, correos, archivos, etc (véase figura 16).

En “Note Type”, habitualmente se usarán uno de los siguientes 3 valores:

- "SP Attachment" para adjuntar un fichero (se adjunta en la ventana que hay en este pop-up más abajo, marcada en amarillo en la captura.
- "SP Info to external side" el tipo de nota utilizado para que el update sea visible en la otra herramienta (SM9, SNOW, TT de cliente,)
- "SP Status (internal)”, la nota solo será visible en eTTs. Se utiliza especialmente si se requiere que el primer nivel esté al corriente.

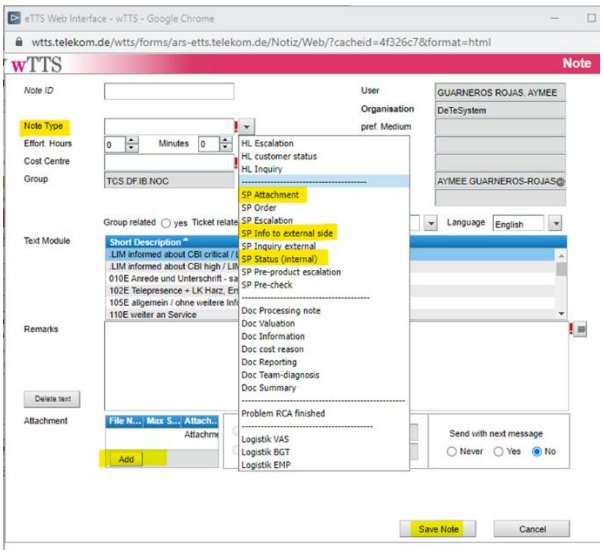


Figura 16. Agregar una nota al ticket en wTTs.

Finalmente se da clic en Save Note y Save al ticket para guardar los nuevos updates agregados al ticket.

Cierre del evento o alarma

Antes de dar por concluida o cerrada una incidencia, es necesario revisar cada uno de los tickets y sus actualizaciones para comprobar que ya haya sido solucionado el problema.

Además, se deberá validar el estado de los equipos tanto en la herramienta de monitoreo NAGIOS, como en el aplicativo de Meraki.

Validaciones

En NAGIOS las alarmas deberían verse de la siguiente forma, imagen 17.

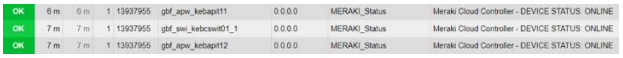


Figura 17. Alarmas o eventos recuperados desde NAGIOS.

Desde Meraki se valida que los equipos estén en estado Online. En el dashboard que despliega la información del equipo podemos ver los cortes que tuvo en el servicio. Ver imagen 18.

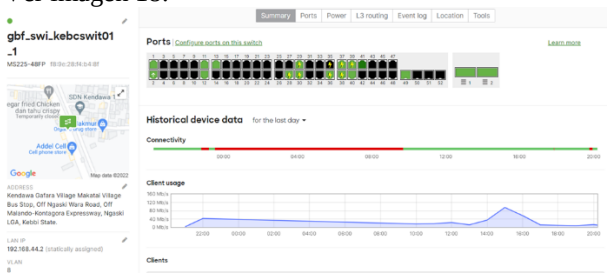


Figura 18. Validar estado del equipo desde CISCO Meraki.

Resolver el ticket en wTTs

Dado que en la solución no podemos escribir comentarios ni adjuntar archivos, primero debemos crear una nota.

- Hacer un "Submit note" (interna si el ticket queda en wTTs o externa si va a otra herramienta).
- Opcional si es necesario adjuntar ficheros: realizar un "Submit note" para attachment y si fuera necesario enviarlo vía "External Provider".

La resolución del ticket se realiza en la pestaña “Problem Completion”.

DISCUSIÓN Y ANÁLISIS DE RESULTADOS

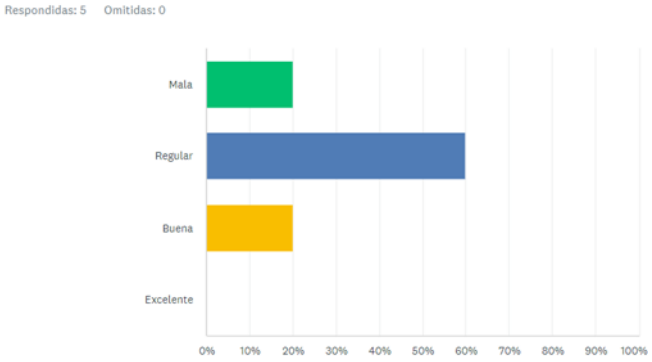
Al lograr concluir las actividades antes mencionada y descritas, se logró llevar a cabo con éxito el proceso de monitorización y gestión de alarmas derivadas de incidencias alertadas en dispositivos de red multiclientes en el área Network Operation Center (NOC) con el apoyo del software NAGIOS.

Encuesta de satisfacción a los clientes

La siguiente encuesta fue realizada para que los clientes calificaran el nivel de satisfacción con la implementación del proceso de monitorización y gestión de alarmas derivadas de incidencia en dispositivos de red.

A continuación, se muestra el análisis y comparación de los resultados obtenidos antes y después de la implementación del proceso de monitorización y gestión de alarmas derivadas de incidencias en dispositivos de red.

Pregunta 1. ¿Cómo califica la atención que recibe para dar seguimiento a sus incidencias? Ver gráfica 1 y 2.



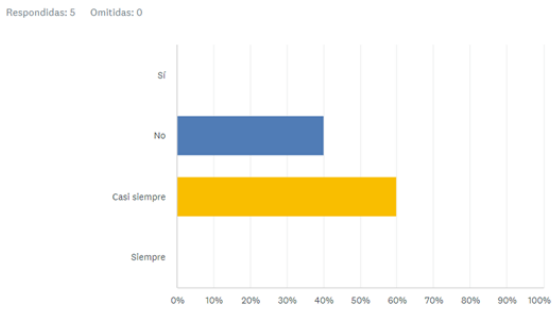
Gráfica 1. Atención que reciben los clientes antes de la investigación.

Al inicio de esta investigación se realiza esta encuesta con el objetivo de conocer el nivel de satisfacción con el tratamiento de alarmas, aplicada a multiclientes en dispositivos de la red para determinar los procesos realizados, los resultados no fueron muy positivos ya que la atención que los clientes recibían para el seguimiento de sus incidencias no era optima y adecuada, y posteriormente con la

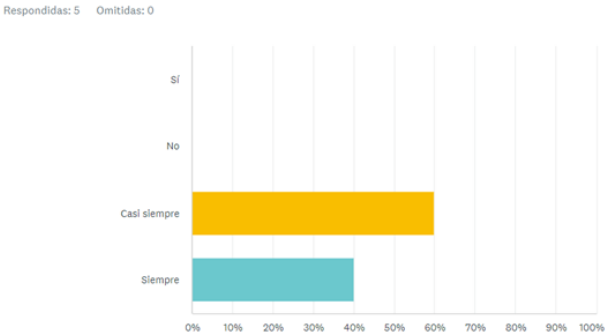
Gráfica 2. Atención que reciben los clientes después de la investigación

Al inicio de esta investigación se realiza esta encuesta con el objetivo de conocer el nivel de satisfacción con el tratamiento de alarmas, aplicada a multiclientes en dispositivos de la red para determinar los procesos realizados, los resultados no fueron muy positivos ya que la atención que los clientes recibían para el seguimiento de sus incidencias no era optima y adecuada, y posteriormente con la implementación del monitoreo y la gestión en la encuesta final se tiene un resultado positivo aumentando de manera significativa la satisfacción de cliente

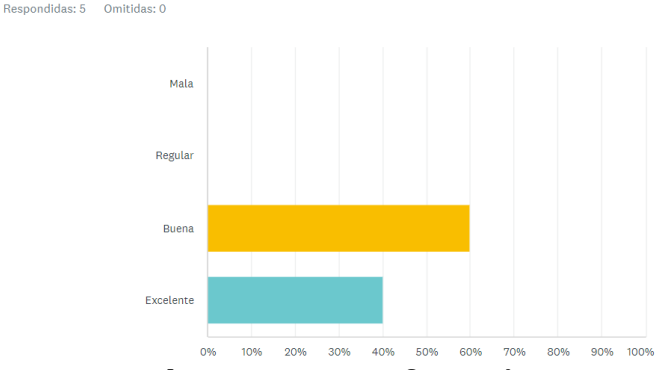
Pregunta 2. ¿Está conforme con el tiempo de resolución de sus incidencias? Ver gráfica 3 y 4.

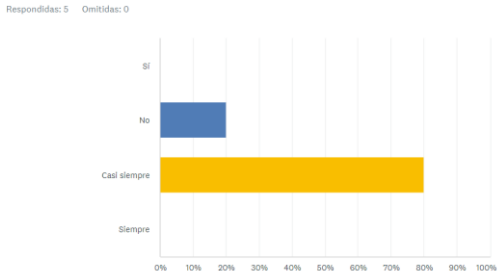


Gráfica 3. Conformidad del tiempo de resolución de incidencias antes de la investigación.

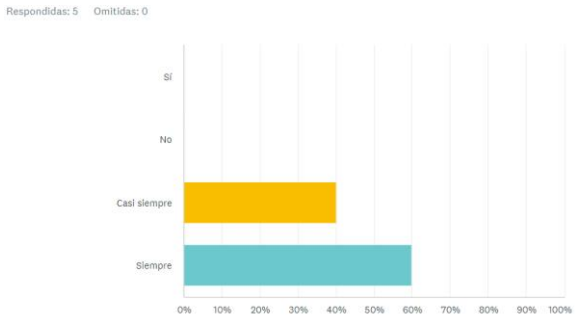


Gráfica 4. Conformidad del tiempo de resolución de incidencias después de la investigación.





Gráfica 5. Conformidad del monitoreo a dispositivos de red antes de la investigación.



Gráfica 6. Conformidad del monitoreo a dispositivos de red después de la investigación

La calificación que el cliente otorgó a la solución de sus incidencias no fue muy positiva ya que no se estaban conformes con la respuesta para resolver sus incidencias no era optima y adecuada, y posteriormente con la implementación del monitoreo y la gestión en la encuesta final se tiene un resultado positivo aumentando de manera significativa la satisfacción de cliente.

Por lo tanto, la discusión versa en el sentido de que las propuestas de solución para la integración de NAGIOS que monitorea el estado de las comunicaciones y disminución los errores presentados por medio de alertas minimizan el tiempo de respuesta para su corrección, tal como lo indica en sus trabajos donde fueron implementados con el objetivo de eliminar el monitoreo manual [15], o siendo capaz de llevar a cabo de forma automática también acciones de prevención y reacción gracias a la posibilidad de definir handlers (es el encargado de recibir datos, manejarlos y realizar una acción como respuesta.) que realicen acciones automáticas durante la monitorización [16] e integrarlo al móvil desde una red social [17].

CONCLUSIONES

La implementación del proyecto "Monitoreo y gestión de alarmas derivadas de incidencias alertadas en dispositivos de red multiclientes en el área NOC, en la empresa líder en servicios digitales de la región con el apoyo del software NAGIOS" logró mejorar la calidad, eficacia y eficiencia del proceso para llevar a cabo el monitoreo y gestión de alarmas.

Gracias a la encuesta realizada para que los clientes calificaran el nivel de satisfacción antes y después de la implementación de la presente investigación fue posible cuantificar los resultados y el impacto que tuvo en el área para la detección de las alarmas reveladas por monitorización, así como el reconocimiento de dichos eventos para buscar una posible solución; revisar la existencia de instrucciones especiales y posteriormente hacer el registro de las acciones realizadas en la herramienta de ticketing; y finalmente gestionar constantemente el tratamiento de las alarmas derivadas de dichas incidencias alertadas en dispositivos de red multiclientes.

Trabajo futuro

Su implementación exitosa facilitaría la inclusión de atender automáticamente las correcciones de bajo riesgo en tiempo real, disminuyendo sensiblemente la presencia física de personal para su corrección; además, se puede anexar notificaciones digitales sobre el móvil de los supervisores en casos de alta maniobrabilidad que ofrecería supervisión de 7/24 los 365 días del año.

BIBLIOGRAFÍA

[1] Portocarrero Miranda, R y Rodríguez Nieva, J. (2017). Implantación del sistema de monitoreo Nagios. Universidad San Ignacio de Loyola. Disponible en https://renati.sunedu.gob.pe/handle/sunedu/3120210

[2] Beviá Cantó, M. (2016). Sistemas de monitorización de infraestructuras de telecomunicaciones basado en Nagios (Doctoral dissertation, Universitat Politècnica de València). Disponible en https://riunet.upv.es/handle/10251/64584

[3] Casado Falcón, A. A. (2015). Despliegue de un sistema de gestión de redes basado en Nagios (Bachelor's thesis, Universitat Politècnica de Catalunya). Disponible en https://upcommons.upc.edu/handle/2117/175746

[4] Martínez Ortega, K. M. (2022). Evaluación de equipos electrónicos a través del sistema de monitoreo Nagios Core en una empresa del sector alimenticio (Doctoral dissertation). Disponible en http://181.39.139.68:8080/handle/123456789/1746

[5] Moreno Calabozo, A. (2015). Diseño e implantación de un sistema de monitarizacion basado en Nagios (Bachelor's thesis). Disponible en https://e-archivo.uc3m.es/handle/10016/23814

[6] NAGIOS. (2022). The Industry Standard In IT Infrastructure Monitoring. Retrieved from The Industry Standard In IT Infrastructure Monitoring: Disponible en https://www.nagios.org/

[7] CISCO Meraki. (2021). Cisco Systems, Inc. Retrieved from Cisco Systems, Inc.: Disponible en https://documentation.meraki.com/

[8] Martí Prats, P. (2016). Máster Universitario en Ingeniería de Telecomunicación. Retrieved from Máster Universitario en Ingeniería de Telecomunicación: Disponible en https://www.uv.es/uvweb/master-ingenieria-telecomunicacion/es/blog/lan-wan-man-otras-redes-1285954593702/GasetaRecerca.html?id=1285959491342

[9] Aruba. (2022). a Hewlett Packard Enterprise Development LP. Retrieved from a Hewlett Packard Enterprise Development LP: Disponible en https://www.arubanetworks.com/es/faq/que-es-la-topologia-de-red/#:~:text=La%20topolog%C3%ADa%20de%20red%20f%C3%ADsica,datos%20dentro%20de%20una%20red

[10] KIO. (2022). KIO Networks. Retrieved from KIO Networks: Disponible en https://www.kionetworks.com/blog/data-center/dispositivos-de-interconexion-de-redes#:~:text=Un%20dispositivo%20de%20interconexi%C3%B3n%20de,repetidores%20y%20puertas%20de%20enlace

[11] Etecé, E. E. (2021). Enciclopedia Concepto. Retrieved from Enciclopedia Concepto: Disponible en https://concepto.de/red-2/

[12] Networking Academy. (2022). Cisco Networking Academy. Retrieved from Cisco Networking Academy: Disponible en https://lms.netacad.com/course/view.php?id=396811

[13] DigiCert. (2022). DigiCert. Retrieved from DigiCert: Disponible en https://www.websecurity.digicert.com/
[14] CloudFlare. (2022). CloudFlare. Retrieved from CloudFlare: Disponible en https://www.cloudflare.com/
[15] Gómez, J. (2010). Monitorizando la red con Nagios. Todo Linux: la revista mensual para entusiastas de GNU/Linux, (114), 28-32. Dsiponible en https://dialnet.unirioja.es/servlet/articulo?codigo=3199007
[16] Hernández Rubio, D. (2021). Sistema experto para la resolución proactiva de problemas de monitorización automática en Nagios. Disponible en https://oa.upm.es/68129/
[17] Pérez Vera, D. I. (2015). Integración de sistema de monitorización Nagios con Twitter. Disponible en http://hdl.handle.net/10609/40561

TABLA DE ROLES DE CONTRIBUCIONES

Rol	Autor (es)
Conceptualización	Violeta Martínez Ramírez
Curación de datos	Aymée Guarneros Rojas
Análisis Formal	Aymée Guarneros Rojas
Financiación de adquisiciones	Violeta Martínez Ramírez
Metodología	Osorio Ramírez Efrén Armando
Administración del proyecto	Aymée Guarneros Rojas
Recursos	Aymée Guarneros Rojas
Software	Aymée Guarneros Rojas
Supervisión	Violeta Martínez Ramírez
Validación	Aymée Guarneros Rojas
Visualización	Teresa Luciano Machorro
Escritura - Preparación del borrador original	Margarita Raquel García Sierra
Escritura - Revisión y Edición	Margarita Raquel García Sierra