Universidad Tecnológica de El Salvador

FACULTAD DE INFORMÁTICA Y CIENCIAS APLICADAS
CARRERA TÉCNICO EN INGENIERÍA DE REDES COMPUTACIONALES

TEMA:

EVALUACION DE DIFERENTES HERRAMIENTAS UTILIZANDO SOFTWARE LIBRE PARA EL MONITOREO DE UNA RED DE DATOS A NIVEL EMPRESARIAL

TRABAJO DE GRADUACION

PRESENTADO POR

CARCAMO RIVERA, JOSUE BENJAMIN
PINEDA AGUILAR, KARLA ALEJANDRA

PARA OPTAR AL GRADO DE:

TÉCNICO EN INGENIERÍA DE REDES COMPUTACIONALES

ABRIL, 2020
SAN SALVADOR, EL SALVADOR, CENTROAMÉRICA

AUTORIDADES ACADÉMICAS

ING. NELSON ZÁRATE SÁNCHEZ

RECTOR

LIC. JOSÉ MODESTO VENTURA ROMERO

VICERRECTOR ACADÉMICO

ING. FRANCISCO ARMANDO ZEPEDA

DECANO DE FACULTAD DE INFORMÁTICA Y CIENCIAS APLICADAS

JURADO EXAMINADOR

LIC. NELSON OSWALDO LOPÉZ CHAVÉZ

PRESIDENTE

ING. DANY SALVADOR CHACÓN

PRIMER VOCAL

ING. ÁNGEL ALFREDO CALDERÓN RODRÍGUEZ

SEGUNDO VOCAL

ABRIL, 2020
SAN SALVADOR, EL SALVADOR, CENTROAMÉRICA

Universidad Tecnológica de El Salvador

ACTA DE EXAMEN PROFESIONAL

HABIÉNDOSE REUNIDO EL JURADO CALIFICADOR INTEGRADO POR:
Ing.Dany Salvador Chacón, Ing.Ángel Alfredo Calderón Rodríguez, Lic.Nelson Oswaldo López Chávez, a las 12:00m.d. del día martes, 3 de diciembre de dos mil diecinueve.
Y LUEGO DE HABER DELIBERADO SOBRE EL EXAMEN PROFESIONAL DE LOS ALUMNOS:

1-Josué Benjamín Cárcamo Rivera Carnet 26-2238-2017
2-Karla Alejandra Pineda Aguilar Carnet 26-2873-2014

QUIENES PRESENTARON DEFENSA DE SU TRABAJO DE GRADUACION TITULADO:
"Evaluación de diferentes herramientas utilizando software libre para monitoreo de una red de datos a nivel empresarial"

PARA OPTAR AL GRADO DE:

TÉCNICO EN INGENIERIA DE REDES COMPUTACIONALES

Y DEL CUAL TAMBIEN EVALUARON LOS CONOCIMIENTOS RELACIONADOS CON EL TEMA DEL MISMO. POR LO QUE ESTE JURADO RESUELVE DECLARAR EL EXAMEN COMO:
APROBADO
YA QUE CUMPLE CON LOS REQUISITOS ESTABLECIDOS EN EL REGLAMENTO DE GRADUACION DE LA UNIVERSIDAD.
San Salvador, 3 de diciembre de dos mil diecinueve.

F._____
PRIMER VOCAL
Ing. Dany Salvador Chacón

F._____
SEGUNDO VOCAL
Ing. Ángel Alfredo Calderón Rodríguez

F._____
PRESIDENTE
Lic. Nelson Oswaldo López Chávez

Calle Arce No. 1020, San Salvador, El Salvador, C.A. Apdo. Postal 1770
Centro de llamadas: (503) 2275-8888, Fax: (503) 2271-4764
Email: contactanos@utec.edu.sv

Introducción.

En el presente trabajo de investigación se tiene como objetivo evaluar el sistema de monitoreo de red de datos a nivel empresarial, para monitorear los equipos y tráfico de red, que ayude a detectar Y prevenir de forma inmediata el momento en el que ocurre un problema o antes de que los usuarios finales noten las fallas.

La detección oportuna de fallas y el monitoreo de los elementos que conforman una red de computadoras son actividades de gran relevancia para brindar un buen servicio a los usuarios. De esto se deriva la importancia de contar con un esquema capaz de notificarnos las fallas en la red y de mostrarnos su comportamiento mediante el análisis y recolección de tráfico.

Hasta hace poco hablar de sistemas de monitoreo de servicios de red en sistemas operativos de red o desktop resultaba casi imposible, ya que no se contaba con las herramientas necesarias para hacerlo. Es muy importante contar con una buena infraestructura de red, tanto como equipos tales como enrutadores de tráfico, switches, puntos de acceso y servidores de servicios, estos deben garantizar un correcto funcionamiento. El documento se divide en cinco capítulos: en el capítulo I se presenta los argumentos que justifican el planteamiento del problema. El capítulo II se refiere a los hallazgos más importantes que se tienen al momento sobre el tema de evaluación de diferentes herramientas, utilizando software libre para monitoreo de una red de datos a nivel empresarial. Capitulo III se presenta de manera clara y concreta los pasos para poder obtener una buena evaluación de monitoreo de red. Capitulo IV se refiere al análisis de

resultados del monitoreo de redes. Y finalmente en el Capítulo V se presenta las conclusiones y el resumen del contenido monitoreo de redes de una red empresarial.

Capítulo I Planteamiento del Problema.

1.1 Antecedentes.

En la actualidad, las redes se han convertido en un elemento determinante en el éxito de una empresa, cuando se produce una falla en la red, los empleados y usuarios quedan incomunicados, de forma que es imposible acceder a información de la compañía; servicios de correo electrónico, aplicaciones o incluso servicios básicos de impresión lo que provoca pérdidas.

El éxito de muchos de los procesos de una organización depende de la calidad de la comunicación existente ante esto las empresas se interesan por adquirir diversos elementos de infraestructura de red que les garantice velocidad, confiabilidad y disponibilidad. Para conseguir este objetivo se debe considerar que un buen servicio de red no depende de una buena infraestructura, también es necesario tener en cuenta un adecuado diseño en la red y un monitoreo de la red entre otras cosas.

El monitoreo es determinante en la prevención y resolución de incidentes con la red de comunicaciones de una empresa, ya que permite la detección oportuna de fallas, la verificación del estado de componentes y la medición del desempeño de la red. Los tipos de aplicaciones de software que existen actualmente presentan diferentes características que permiten el monitoreo de red con funcionalidades distintas. Cada empresa presenta distintas necesidades respecto a un software de monitoreo pero se debe analizar que funcionalidades requiere y con qué recursos cuenta.

Las aplicaciones de software especializadas en el monitoreo de red permiten reducir, prevenir anticipar y gestionar las interrupciones que se puedan presentar, permitiendo una operación continua y evitando perdidas monetarias a la empresa.

1.2 Definición del Problema.

¿Es posible la aplicación e implementación de un sistema de monitoreo para una red de datos a nivel empresarial?

- Cuando se da un determinado servicio en una empresa, las redes son uno de los elementos más importantes a tener en cuenta. Si la red deja de funcionar, por el motivo que sea, y no llegan a transmitirse los datos necesarios, la empresa deja de prestar servicio a los clientes durante el tiempo que dure la caída.
- Todo esto puede de causar grandes problemas en una empresa, causando malestar en los clientes y, en caso de que ocurra de forma repetida, es muy posible que los usuarios decidan cambiar compañía. Es por eso que la implementación de un sistema de monitoreo de red es muy importante para una empresa, porque nos ayuda a detectar esas fallas que se pueden lograr dar en una red y poder buscar el origen del problema a través de la utilización de un software de monitoreo y poder darles un buen servicio a los clientes.

¿Cuáles serían esas ventajas de tener un sistema de monitoreo?

- Control de las rutas y detenciones
- Alertas al instante
- Seguridad en el trasporte
- Mejorar el servicio al cliente

¿En qué puede beneficiar un sistema de monitoreo de red a una empresa?

- Ayuda a mantener la credibilidad: un buen sistema de monitorización siempre habla bien del funcionamiento de la organización.
- Incrementar la eficiencia: los administradores del sistema y los usuarios pueden enfocarse a otras actividades ya que el monitor se encarga de avisar y alertar cuando atención es necesaria.
- Reducción de costos: la solución de problemas de manera preventiva ayuda a reducir los costos ocasionados, incluyendo equipo de staff, hardware y software.

1.3 Objetivo General.

• Evaluar diferentes herramientas para el monitoreo de una red empresarial utilizando software libre.

1.3.1 Objetivos específicos.

- Conocer diferentes tipos de herramientas para el monitoreo de red.
- Obtener o identificar las ventajas de monitoreo de red utilizando software libre.
- Demostrar el funcionamiento de un sistema de monitoreo para una red empresarial.

1.4 Justificación.

Esta investigación tiene como fundamento la necesidad de mejorar la red, cualquiera que sea el método de monitoreo de red a emplear se debe considerar lo siguiente:

El desempeño de la performance de la red, en presencia de aplicaciones restringidas.

El desempeño de la performance de la red, en ausencia de aplicaciones prohibidas.

El desempeño de performance de la red, en presencia y ausencia de aplicaciones que usa la organización.

Cuando se da un determinado servicio en una empresa, las redes son uno de los elementos más importantes a tener en cuenta. Si la red deja de funcionar, por el motivo que sea, y no llegan a transmitirse los datos necesarios, la empresa deja de prestar servicio a los clientes durante el tiempo que dure la caída. Todo esto puede causar grandes problemas en una empresa, causando malestar en los clientes y, en caso de que ocurra de forma repetida, es muy posible que los usuarios decidan cambiar de compañía.

Por estas razones, un sistema de monitoreo de red puede marcar la diferencia en cualquier empresa. El objetivo principal de un administrador de sistemas es asegurarse de que las redes se encuentren funcionando a pleno rendimiento, el 100% del tiempo. Elegir una herramienta de monitoreo de red adecuada nos va a ayudar a detectar posibles problemas antes de que se provoque un colapso o una caída de las redes.

Para poder centrarnos y saber qué es lo que debemos de tener en cuenta para la monitorización de red, es importante saber diferenciar entre el monitoreo de red y la gestión de red. El monitoreo de red nos va a permitir analizar y ver el estado de las redes a un nivel básico. Mientras, la gestión de red va más allá; no solo permite tomar acciones para la gestión, sino que nos va a permitir tomar acciones para paliar los problemas de nuestras redes, dando una visión global de todos nuestros sistemas.

Al obtener los datos que se necesitan, pueden aumentar la seguridad y la escalabilidad, automatizar con eficiencia y alinear mejor los recursos con las necesidades de capacidad.

1.5 Limitaciones.

Limitación científica:

El proyecto está limitado a la utilización de diferentes herramientas de software libre para el monitoreo de redes, ancho de banda, estado de servidores y control de usuarios.

Limitación temporal:

Se planea que la investigación se desarrollara a lo largo del ciclo 02 del año 2019 entre los meses de agosto y noviembre

Limitación espacial:

Se pretende que el proyecto a realizar estará restringido para una red de datos a nivel empresarial

1.6 Alcances

El proyecto se centra en: evaluar las diferentes herramientas, utilizando software libre para el monitoreo de una red de datos a nivel empresarial. De forma específica el proyecto constituye los siguientes alcances:

Evaluar una herramienta que proporcione utilidad y buen monitoreo de una red empresarial.

Proporcionar una solución mediante un software de monitoreo para evitar posibles fallos o caídas de red.

Mantener un control constante de los equipos informáticos dentro de una red empresarial con el propósito de mantener información actualizada sobre el funcionamiento o cambios que se pueden presentar.

Capitulo II Marco Teórico.

2.1 Monitoreo de Red.

El término Monitoreo de red *(Monitorización de red)* describe el uso de un sistema que constantemente monitoriza una red de computadoras en busca de componentes defectuosos o lentos, para luego informar a los administradores de redes mediante correo electrónico, mensáfono (*pager*) u otras alarmas. Es un subconjunto de funciones de la administración de redes.

Mientras que un sistema de detección de intrusos monitoriza una red por amenazas *del exterior* (externas a la red), un sistema de monitorización de red busca problemas causados por la sobrecarga y/o fallas en los servidores, como también problemas de la infraestructura de red (u otros dispositivos).

Por ejemplo, para determinar el estatus de un servidor web un software de monitorización puede enviar, periódicamente, peticiones HTTP (*Protocolo de Transferencia de Hipertexto*) para obtener páginas; para un servidor de correo electrónico, enviar mensajes mediante SMTP (*Protocolo de Transferencia de Correo Simple*) para luego ser retirados mediante IMAP (*Protocolo de Acceso a Mensajes de Internet*) o POP3 (*Protocolo Post Office*). Comúnmente, los datos evaluados son tiempo de respuesta y estadísticas tales como consistencia y fiabilidad han ganado popularidad. Las fallas de peticiones de estado, tales como que la conexión no pudo ser establecida, el tiempo de espera agotado, entre otros, usualmente produce una acción desde del sistema de monitorización. Estas acciones pueden variar: una alarma

puede ser enviada al administrador, ejecución automática de mecanismos de controles de fallas, etcétera.

La generalizada instalación de dispositivos de optimización para redes de área extensa tiene un efecto adverso en la mayoría del software de monitorización, especialmente al intentar medir el tiempo de respuesta de punto a punto de manera precisa, dado el límite visibilidad de ida y vuelta.

Monitorizar la eficiencia del estado del enlace de telecomunicaciones (*subida/bajada*) se denomina *Medición de tráfico de red.*

¿Qué función cumple el monitoreo de red?

Entre las funcionalidades que realizan los MR, se encuentra realizar un seguimiento de cómo se utilizan las PC instaladas a la red, cada vez que se conectan a ésta, indicando el tiempo y hora de conexión, la dirección IP utilizada, el tipo de aplicación que accedió a la red y qué conexión realizó.

En combinación con otros programas, el ***monitoreo de red*** es muy útil para encontrar aquellas conexiones inconvenientes, prohibidas o no autorizadas, así como prevenir fallas de la conexión en momentos de máximo trabajo o flujo de información (horas pico). Hay que tener en cuenta que los monitores sólo muestran información: para controlar el acceso a la red se requiere de firewall o programas similares. (Equipo Editorial, 2019)

Gestión y monitoreo de red

La Gestión define los recursos en una red con el fin de evitar que esta llegue a tener fallas de funcionamiento restando disponibilidad en sus prestaciones.

El monitoreo define un proceso continuo de recolección y análisis de datos con el propósito de predecir problemas en la red. Entonces, los beneficios de tener un sistema de gestión y monitoreo son:

Permiten controlar los elementos de hardware y de software en una red para verificar periódicamente su correcto funcionamiento.

Están diseñados para ver la red entera como una arquitectura unificada con etiquetas y direcciones asignadas a cada punto como atributos específicos en cada elemento del sistema.

2.2 Gestión de Red.

Se trata de una amplia gama de actividades de índole técnica, administrativa y gerencial que se puede resumir en coordinar recursos para: planificar, organizar, diseñar, operar, contabilizar, controlar, analizar, evaluar y expandir las redes 19 de comunicaciones con el objetivo de lograr niveles de servicio óptimos, a un costo razonable y con la máxima eficiencia en el uso de la red y sus recursos. A través de la gestión de redes las organizaciones podrán controlar los recursos estratégicos, controlar la complejidad del diseño de la red, ofrecer mejor prestación de servicios a

los usuarios, reducción de fallas, congestión y tiempos de caídas del servicio y controlar los costos de los recursos que se consumen en la red.

Por otra parte, describe que la gestión de redes en un principio se enfocaba en administrar los equipos de red (switch, router, firewall, enlaces de conexión WAN entre otros), luego evolucionó para abarcar la gestión de la red completa, sin embargo, hoy en día el enfoque está dirigido a la gestión de servicios que toma en cuenta la tecnología y el mantenimiento de los equipos que operan en la red, derivándose en la gestión de equipos y la gestión de la red.

El apropiado uso de las herramientas de apoyo para la gestión de redes, incrementa la satisfacción de los usuarios finales, garantizándoles 20 disfrutar de servicios con mayor disponibilidad disponibles independientemente de la complejidad, crecimiento o cambios que tenga la red En el mismo orden de ideas, se concluye que un sistema de monitoreo es una herramienta de apoyo para la gestión de los dispositivos críticos de la infraestructura TI. A través del correcto uso de esta, los administradores de red mejoran su desempeño y aseguran por mayor tiempo la disponibilidad de los servicios de la plataforma de TI, debido a que podrán visualizar con mayor precisión las causas de las fallas, lo que les permitirá́ brindar soluciones en menor tiempo. Por otro lado, los administradores de red también podrán delegar en un sistema de monitoreo las funciones de supervisión y notificación de fallas, con el fin de concentrar sus esfuerzos en realizar otras funciones de igual importancia para la

infraestructura TI, ahorrando a la organización los costos de contratar personal adicional

Beneficios al implementar servidores de monitoreo de red

Permite la planificación de las capacidades de los recursos, mediante el conocimiento del uso de los recursos de hardware, software y ancho de banda. El desempeño de la red puede ser optimizado a través del uso adecuado de los recursos de la infraestructura TI. La detección y solución de los problemas se torna más rápido abordando problemas específicos. El conocimiento del estado de la red le permitirá a los administradores planificar mantenimientos preventivos y correctivos a la infraestructura de TI, para prever indisponibilidades del servicio. El tiempo de los administradores es empleado en atender otros requerimientos. Con la información de las tendencias de consumos de los servicios permite conocer la tendencia del uso normal, ayudando a configurar la calidad de servicio (QoS) que garanticen la cuota de recursos para los servicios prioritarios. En estas tendencias se pueden detectar problemas.

Gracias al monitoreo de red podrás conocer el estado de los sistemas informáticos en tiempo real para anticiparte a posibles problemas. Por ejemplo, recibir un aviso cuando un disco duro esté por encima del 80%.

La detección de incidentes y su origen es clave para mantener en buen estado los sistemas. Además, también te permite conocer el estado de las instalaciones y comprobar cómo están los activos informáticos más críticos.

El monitoreo de red mejora la eficacia y la eficiencia de las tareas de mantenimiento de los sistemas informáticos, reduciendo así los costes asociados.

El objetivo principal de un software de monitoreo de red tiene que ver especialmente con la optimización del funcionamiento de los equipos y la reducción de errores en la red de la empresa. Sin embargo, las ventajas de este tipo de producto van mucho más allá.

En primer lugar podemos hablar de la posibilidad de comprobar, antes que ocurra cualquier problema, de la presencia de algún elemento que pueda estar ocasionando una bajada en el rendimiento de la red de la empresa. Por tanto, se puede decir que la monitorización no solo sirve para solucionar problemas, sino también para prevenirlos.

Esto se traducirá, entre otras cosas, en una reducción del tiempo empleado en la resolución de problemas, ya que estos se detectarán a tiempo para subsanarlos mejor y más rápidamente. Al mismo tiempo, este monitoreo, que puede hacerse perfectamente con los productos Cisco, nos permitirá sacarle el máximo partido al hardware de la empresa y obtener un mayor control interno sobre los equipos tecnológicos de la compañía, llegando a acceder más fácilmente al estado de los equipos más críticos.

Por otro lado, un software de monitoreo de red nos va a permitir la sistematización de los procesos de mantenimiento de equipos y redes de la empresa. Un hecho que nos facilitará una mayor información a la hora de decidir la adquisición de nuevos equipos para el negocio.

Lo cierto es que hasta ahora sabíamos que un software de monitoreo de red nos iba a ayudar a resolver y detectar los problemas tecnológicos de una empresa. Pero también, como acabamos de comprobar, es un excelente sistema de prevención que repercutirá en los beneficios futuros de la compañía.

¿Cuáles son las posibles consecuencias de no monitorear de forma continua tus sistemas?

Interfaz gráfica de un software de monitoreo (ver imagen)

Imagen 1

El mal funcionamiento de uno o varios componentes de TI puede causar daños importantes que afecten el buen funcionamiento de la empresa. Algunos de estos efectos negativos pueden incluir: Largos períodos de Down time, disminución de la productividad, incumplimiento de SLA, etc. Así mismo, entre las causas más probables de estas fallas encontramos:

- Obsolescencia del sistema.
- Configuración inadecuada del sistema.
- Ataques informáticos no detectados, etc.

En este contexto, se hace esencial la aplicación de medidas que permitan vigilar los sistemas de forma integral; para garantizar el funcionamiento continúo de todos los procesos vitales de la empresa.

¿Qué mide este tipo de monitoreo?

Esta clase de supervisión está dirigida a analizar el comportamiento de cualquier componente del ecosistema de TI. Es decir, puede medir, por ejemplo:

- El estado físico de un equipo, lo que incluye, temperatura, disco duro, memoria, etc.
- La carga de un equipo (número de usuarios, solicitudes, uso de la CPU, rendimiento de la red, entre otros).

- El rendimiento de la red informática (desempeño, aparición de errores, etc.)
- Ataques al sistema. (Rivas, 2018)

2.3 Software de Monitoreo.

Nagios, Cacti y Pandora FMS son tres aplicaciones de monitorización con aproximaciones completamente diferentes: Cacti está enfocada en gráficas, Nagios en estados, y Pandora FMS abarca ambos aspectos, entre muchas otras funcionalidades. Si conoces RRDTool o MRTG, Cacti expande esa filosofía: si tengo una fuente de datos, puedo pintar los datos. Si tengo varias fuentes de datos, puedo combinarlos. Cacti se inició con esa filosofía y evolucionó siguiendo este paradigma: pintarlo todo en gráficas. Y hay que decir que lo hace realmente bien. Algunas de las gráficas de Cacti que utiliza por debajo RRDTool son realmente potentes y atractivas. (Javier, 2016)

Tradicionalmente, en multitud de entornos, se usaba Cacti para crear gráficas y Nagios para gestionar estados y levantar alertas. Esto no significa que Cacti no tenga alertas, ni que Nagios no tenga gráficas, pero en ambos casos son “añadidos” que complementan la funcionalidad principal. No es algo que viniera contemplado en el diseño inicial, por lo que, de alguna forma, esos complementos no dejan de ser una

solución pobre y externa a la aplicación base. Por otro lado, Pandora FMS fue concebido desde sus inicios para hacer ambas cosas simultáneamente, y ofrecerlas como funcionalidades principales.

- NAGIOS.

Nagios es un sistema de monitorización de redes ampliamente utilizado, de código abierto, que vigila los equipos (hardware) y servicios (software) que se especifiquen, alertando cuando el comportamiento de los mismos no sea el deseado. Entre sus características principales figuran la monitorización de servicios de red (SMTP, POP3, HTTP, SNMP...), la monitorización de los recursos de sistemas hardware (carga del procesador, uso de los discos, memoria, estado de los puertos...), independencia de sistemas operativos, posibilidad de monitorización remota mediante túneles SSL cifrados o SSH, y la posibilidad de programar plugins específicos para nuevos sistemas. (Juan Aviles, 2013)

Se trata de un software que proporciona una gran versatilidad para consultar prácticamente cualquier parámetro de interés de un sistema, y genera alertas, que pueden ser recibidas por los responsables correspondientes mediante (entre otros medios) correo electrónico y mensajes SMS, cuando estos parámetros exceden de los márgenes definidos por el administrador de red.

Llamado originalmente Netsaint, nombre que se debió cambiar por coincidencia con otra marca comercial, fue creado y es actualmente mantenido por

Ethan Galstad, junto con un grupo de desarrolladores de software que mantienen también varios complementos. Nagios fue originalmente diseñado para ser ejecutado en GNU/Linux, pero también se ejecuta bien en variantes de Unix.

Nagios está licenciado bajo la GNU General Public License Versión 2 publicada por la Free Software Fundation.

Nagios es una alternativa a plataformas de gestión de infraestructuras TI de reconocidas empresas es esta solución OpenSource de grandes prestaciones llamada Nagios. Nagios es un sistema de monitorización de máquinas y servicios (infraestructura TI) diseñado para informar proactivamente al cliente (administradores de red o clientes finales) de sus posibles problemas de red (sistemas de soporte a la red, elementos de red y aplicaciones de red).

Nagios es una plataforma diseñada para correr bajo sistemas Linux, pero funciona correctamente bajo la mayoría de las variantes UNIX existentes.

Su funcionamiento básico consiste en una arquitectura cliente-servidor mediante ejecución de polling periódico de chequeos de recursos (con agente) y servicios (sin agente) sobre sistemas cliente. Cuando se detecta un error la plataforma es capaz de enviar una notificación (sobre diferentes modos de comunicación) a los contactos administrativos, informando del estado del servicio que ha provocado el error, incluyendo informes de estado, de logs e históricos web).

Nagios proporciona gran cantidad de acciones de monitorización que le permiten ser una potente herramienta de gestión TI.

- Características de NAGIOS.

- Gestión de servicios (SMTP, POP3, HTTP, NNTP, PING, etc.).

- Monitorización de recursos de sistemas.

- Gestión de servicios pasivos generados por aplicaciones o comandos externos (servicios pasivos)

- Monitorización de factores ambientales a través de sondas físicas (temperatura, humedad relativa, luminosidad, líneas de tensión, etc.)

- Arquitectura simple de integración que permita a los usuarios desarrollar fácilmente sus propios agentes de chequeo de servicios y recursos.

- Definición de arquitecturas jerárquicas de los elementos gestionados que nos permitan identificar rápidamente avalanchas masivas de caídas de servicios por no alcanzabilidad

- Diferentes notificaciones de errores por tipo de contacto (vía email, sms, wap u otros servicios de notificación)

- Escalado y distribución de servicios, recursos y nodos gestionados por grupos de contacto.

- Definición de acciones reactivas que permitan solventar un problema de forma inmediata.

- Soporte de arquitecturas de servidor redundantes y distribuidas.

- Interface de comandos externos (triggers, web o terceras aplicaciones) que permitan modificar "on-the-fly" la administración del sistema.

- Retención del último estado de los servicios y recursos que permite paliar pérdidas del sistema gestor.

- Programación de intervalos de tiempo sin notificaciones.

- Visión rápida y sencilla de los elementos gestionados

- Portal web que permite consultar el estado de los elementos gestionados, las notificaciones realizadas, los problemas acontecidos, el estado de los servidores, la administración básica, etc.

- Definición de usuarios de lectura y administración del portal web.

➢ Requerimiento de NAGIOS.

Requisitos mínimos de hardware

Procesador: Pentium 4 a 1.8 GHz

RAM: 1GB

Sistema operativo: Linux

Tarjeta de red: 10/100/1000

Entre las utilidades y funciones de Nagios, se tienen:

Monitorización de servicios de red (SMTP, POP3, HTTP, NTTP, ICMP, SNMP). Monitorización de los recursos de equipos hardware (carga del procesador, uso de los discos, logs del sistema) en varios sistemas operativos, incluso Microsoft Windows con los plugins. Monitorización remota, a través de túneles SSL cifrados o SSH. Diseño simple de plugins, que permiten a los usuarios desarrollar sus propios chequeos de servicios dependiendo de sus necesidades, usando sus herramientas preferidas (Bash, C++, Perl, Ruby, Python, PHP, C#...). Chequeo de servicios paralizados.

Posibilidad de definir la jerarquía de la red, permitiendo distinguir entre host caídos y host inaccesibles.

Interfaz gráfica de NAGIOS (ver imagen 2)

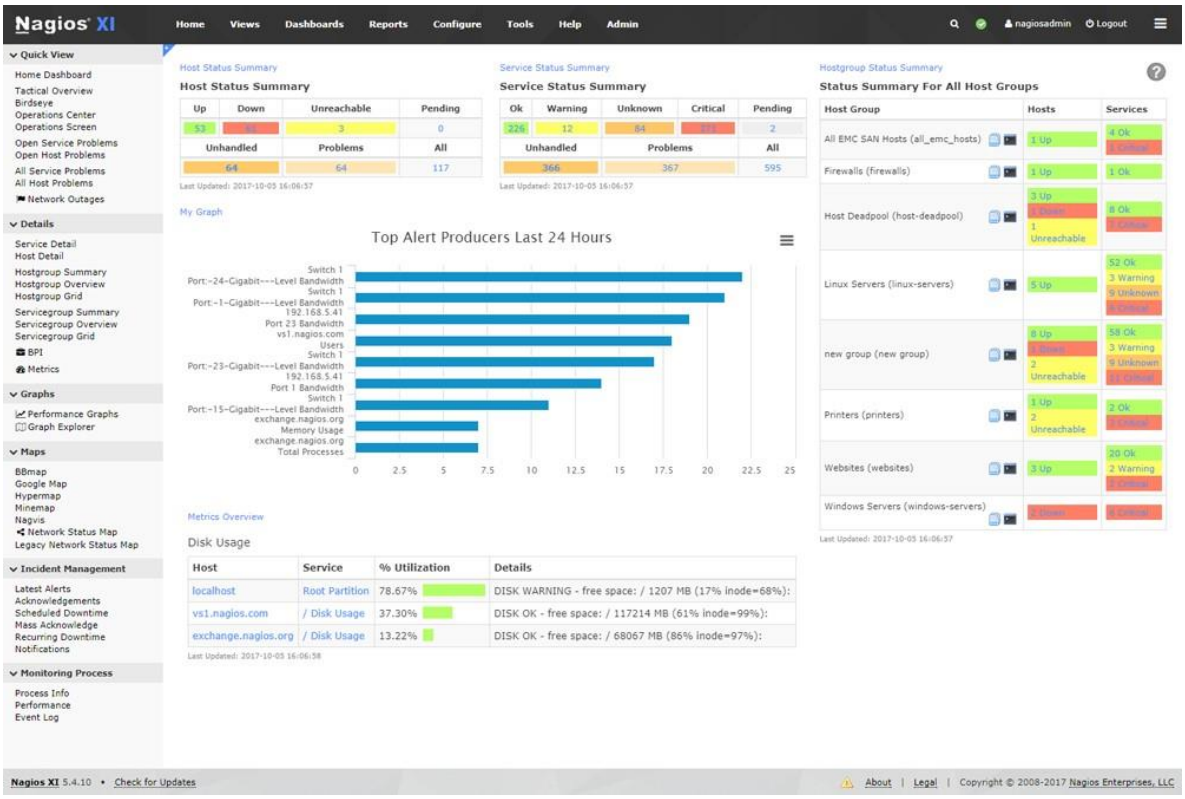

Imagen 2

Notificaciones a los contactos cuando ocurren problemas en servicios o hosts, así como cuando son resueltos a través del correo electrónico, buscapersonas, Jabber (Protocolo abierto basado en el estándar XML para el intercambio en tiempo real de mensajes y presencia entre dos puntos en Internet), SMS, o cualquier método definido por el usuario junto con su correspondiente complemento. Posibilidad de definir manejadores de eventos que ejecuten al ocurrir un evento de un servicio o host para resoluciones de problemas proactivas. Rotación automática del archivo de registro. Soporte para implementar hosts de monitores redundantes. Visualización del estado

de la red en tiempo real a través de interfaz web, con la posibilidad de generar informes y gráficas de comportamiento de los sistemas monitorizados, y visualización del listado de notificaciones enviadas, historial de problemas, archivos de registros...

- CACTI.

Cacti es una interfaz completa para la monitorización de redes mediante gráficos y recopilación de datos, todo ello gracias a la potencia de RRDTool's. Cacti permite tener información prácticamente en tiempo real sobre nuestros routers, switches o servidores, tráfico de interfaces, cargas, CPU, temperaturas, etc. (Mundo Teleco, 2014)

Cacti surge de una evolución de MRTG, un clásico de 1994. Originalmente fue creado para medir tráfico en routers a través de SNMP, y más tarde se amplió para medir cualquier cosa que pudiera devolver información a través de una interfaz SNMP. Finalmente, ha evolucionado hasta ser capaz de medir “cualquier cosa que devuelva un dato numérico”, ya sea el tráfico de una red, el número de paquetes perdidos, o el consumo de CPU de un servidor.

Interfaz gráfica de CACTI (ver imagen 3)

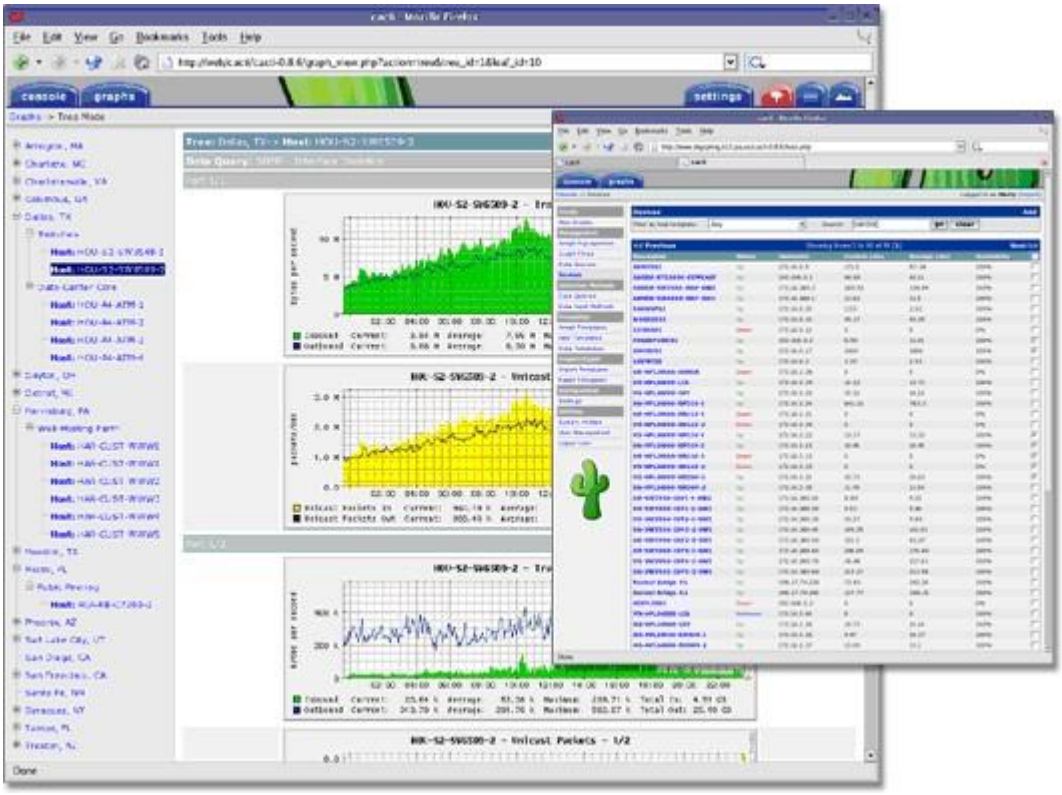

Imagen 3

Este software de monitoreo de redes fue construido bajo las plataformas PHP, Apache y MySql Puede ser manipulado bajo entorno web. Posee un sistema de recolección de datos que utiliza RRDtool, por medio de cual se capturan los datos y se guardan en una base de datos para luego en base a plantilla y gráficos visualizar en su interfaz todo el resultado detallado al usuario.

¿Cómo funciona?

Cacti es una aplicación que funciona bajo entornos Apache + PHP + MySQL, por tanto permite, una visualización y gestión de herramienta a través del navegador

web. La herramienta utiliza RRDtool, que captura los datos y los almacena en una base de datos circular, permitiendo visualizar de forma gráfica los datos capturados.

RRDtool es el estándar de la industria Opensource, registro de datos de alto rendimiento y un sistema de representación gráfica de los datos de series de tiempo. RRDtool se puede integrar fácilmente en los scripts de Shell, Perl, Python, Ruby o aplicaciones TCL.

- Características de CACTI.

Disponibilidad

Fiabilidad

Desempeño

VENTAJAS

Mediciones

- Cacti puede recopilar la utilización del canal en las interfaces de sus equipos, así como los registros de errores.

-Cacti puede medir capacidad, carga del CPU (hardware de red y servidores) y mucho más. Puede reaccionar a ciertas condiciones y enviar alarmas,

Gráficos

-Permite usar toda la funcionalidad de rrdgraph para definir gráficos y automatizar cómo éstos se muestran.

-Permite organizar la información en estructuras jerárquicas (tipo árbol).

Fuentes de datos

-Permite utilizar todas las funciones de rrdcreate y rrdupdate, incluyendo la definición de varias fuentes de datos para cada archivo RRD.

Plantillas

-Puede crear plantillas para reutilizar definiciones de gráficos, datos y fuentes de dispositivos. Gestión de usuarios

-Puede administrar los usuarios localmente o via LDAP y puede asignar niveles detallados de autorización basados en usuarios o grupos.

- Requerimiento de CACTI.

- Sistema operativo Linux como Debían, Gentoo, Redhat, Fedora o SUSE.
- Servicio web Apache.
- PHP.
- MySQL
- RRDTool
- Si se usa SNMP se debe instalar net snmp.
- Un navegador de internet para ejecutar Cacti.

Hardware

Procesador: Pentium 4

RAM: 1GB

Espacio en disco duro: 10 GB

Utilidad de esta herramienta

A través de Cacti, se representan gráficamente los datos almacenados en la RRD: uso de conexión a internet, datos como temperatura, velocidad, voltaje, número de impresiones, etc. La RRD va a ser utilizada para almacenar y procesar datos recolectados vía SNMP.

- PANDORA FMS.

Pandora es una excelente herramienta open source que nos provee de las funcionalidades necesarias para realizar el correcto monitoreo y análisis en nuestra infraestructura de red. Está desarrollado en diferentes lenguajes: C++ y Perl para los agentes, Perl en el servidor, y PHP/JavaScript en la consola WEB. (Tecnopedia.net, 2015)

VENTAJAS

Permite que la tecnología de su negocio funcione de forma más eficiente, rentable y sin sobresaltos, obteniendo la información de todos los elementos críticos de su negocio y detectando los problemas antes de que se conviertan en un mal mayor. Podrá evaluar el nivel de cumplimiento de sus sistemas y mantener a sus clientes informados sobre cualquier incidente. Sus funcionalidades son las ofrecidas por las suites de monitorización de los grandes fabricantes (Big 4), pero a un coste bastante inferior (hasta 7 veces).

Funcionalidad de pandora.

Alertas y eventos.

Registra en tiempo real los acontecimientos en los sistemas monitorizados, los visualiza, gestiona y realiza correlación de eventos. Con un sistema de alertas personalizable y con niveles de escalación.

Monitorización orientada al servicio.

Unifica la monitorización de elementos que contribuyen a un mismo servicio de negocio, comprobando sus interrelaciones para detectar elementos que funcionen mal y comprobar su impacto en el servicio total.

Servidores y redes.

Windows, Mac, Raspberry, Linux, Unix y Android. SNMP y WMI. Ejecución remota de plugins, descubrimiento de red y mapas de red.

Interfaz gráfica de PANDORA (ver imagen 4)

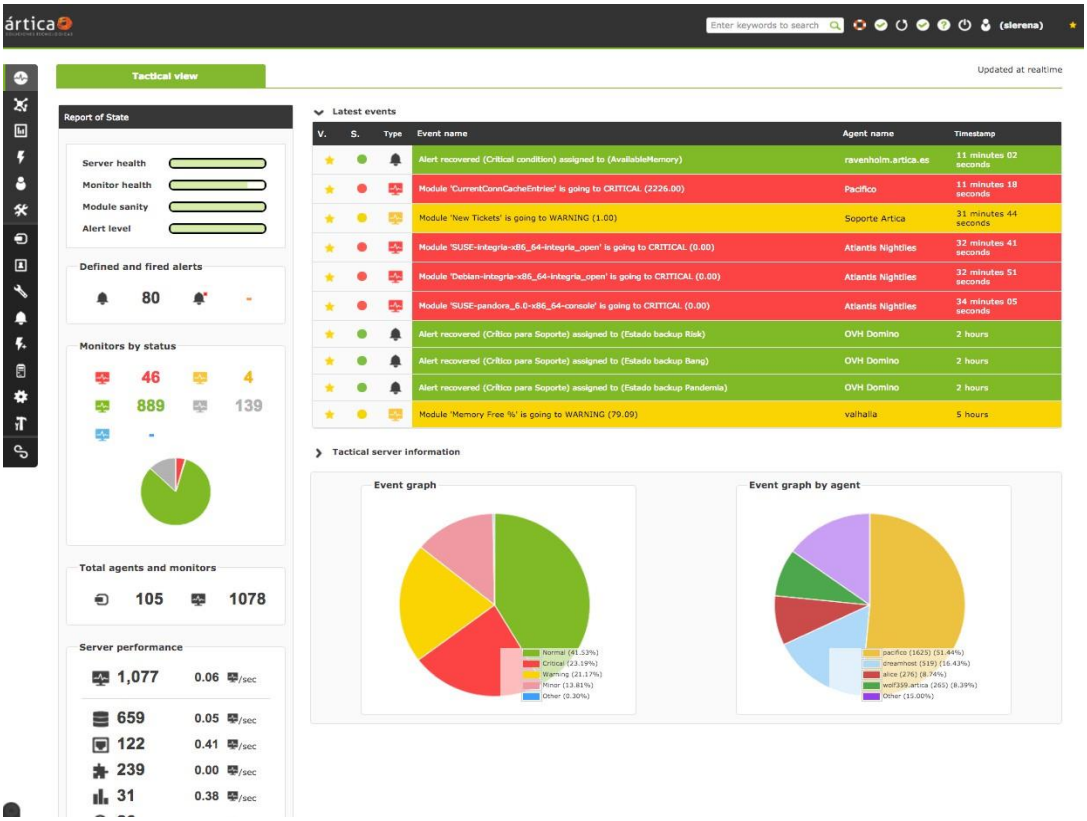

Imagen 4

Beneficios de pandora

Una única herramienta para todos los sistemas y sus fabricantes.

Interfaz Web para configurar y operar la herramienta.

Excelente relación calidad-precio.

Máxima escalabilidad: monitorización de miles de dispositivos.

Gran flexibilidad y capacidad de integración.

Mínimo tiempo de puesta en marcha.

Gran número de funcionalidades out-of-the-box.

Utilizada por empresas de todo el mundo.

Posibilidad de acceso al código fuente.

- Características de PANDORA.

- Autodescubrimiento y detección automática de la topología de red.
- Gestión de Eventos y fallos.
- Agentes multiplataforma para Windows, HP-UX, Solaris, BSD, AIX y Linux.
- Virtualización y cloud computing.
- Monitorización de disponibilidad y rendimiento.
- Consola visual personalizable.
- Agentes para android y dispositivos empotrados.
- Alta disponibilidad.
- Monitorización de red (SNMP, WMI, TCP, ICMP), IPv4 e IPv6.

- Niveles de control de acceso basados en roles.
- Monitorización de SNMP mediante polling y traps.
- Monitorización de servicios.
- Interfaz 100% web con niveles de acceso totalmente personalizables.
- Mapas topológicos de la monitorización personalizables.
- Conexión SSH/Telnet a dispositivos desde el interfaz web.
- SLA y Elaboración de Informes, con ITIL v3 métricas.
- Monitorización de experiencia de usuario.
- Alta escabilidad (monitorización delegada con múltiples instancias y gestión centralizada).
- 4 GB de RAM y un único CPU de 2 GHz. Disco duro rápido 7200rpm o equivalente.
- monitoreo de servidores y estaciones de trabajo ejecutando Linux, Windows o MAC, mediante la instalación de agentes.
- monitoreo de elementos de red mediante SNMP.
- flexibilidad para la integración de scripts que nos brinden datos de tantas funcionalidades como nos imaginemos.
- posee un procesador de querys WMI, recurso que permite monitorear muchos aspectos de terminales Windows sin necesidad de instalación del agente.

• definición de alertas por mail o mensaje de texto las cuales serán disparadas cuando los valores capturados desde los agentes se encuentren dentro de rangos definidos como críticos.

Sistemas Operativos Linux, Windows, Solaris, AIX, HP-UX, BSD, MacOS

Aplicaciones SAP, Tomcat, Weblogic, JBoss, IIS, Exchange, WebSphere, Apache

Comunicaciones

Bases de datos

Cisco, Juniper, 3com, Teldat, Huawei, D-link, etc.

Protocolos soportados SNMP v1, v2c, v3, HTTP, LDAP, ICMP, TCP, UDP, WMI,

Radius, DNS

Virtualización VMware vSphere, Xen VM, Amazon, EC2, RHEV

Sensores hardware Temperatura, humedad, inundación, consumo eléctrico, luz, etc.

Oracle, DB2, Microsoft SQL Server, MySQL, PostgreSQL

Experiencia de usuario Latencias, comprobación contenido, login, proceso de compra, etc.

- Requerimiento de PANDORA.

Tamaño del hardware:

- Hasta 500 agentes o 5000 módulos; 4 GB de RAM y un único CPU de 2 GHz. Disco duro rápido 7200rpm o equivalente.
- Hasta 2000agentes o 10000 módulos: 8 gigas de RAM y un cpu doble de 2,5 Hgz y un disco duro rápido 7200rpm o más.

Agentes:

•AIX 5.x, Solaris, HP-UX11.x, Linux, BSD, Windows NT4, 2000, XP, 2003, Vista y 7, Android y dispositivos empotrados.

Sistemas operativos:

•Para el servidor y la consola: SUSE Linux, Debian, Ubuntu o RHEL/CentOS.

Comparación de herramientas de monitoreo.

Características principales	NAGIOS	CACTI	PANDORA
Escalabilidad	si	si	si
Fiabilidad	si	si	no
Gestión de servicios	si	si	si
Desempeño	si	si	no
Escalado y distribución de servicios	si	no	si
Gestión de usuarios	Si	si	no
Tolerancia a fallos	si	si	si

Tabla 1: Características principales

Requisitos	NAGIOS	CACTI	PANDORA
procesador	Pentium 4	Pentium 4	Pentium 4
RAM	1 GB	1 GB	4 GB
disco duro	20 GB	10 GB	10 GB
sistema operativo	CentOS o Redhat Enterprise Linux	LINUX Y DEBIAN	SUSE LINUX

Tabla 2: Requerimientos de hardware

Descripción	NAGIOS	CACTI	PANDORA
Soporte Técnico	si	no	si

Precio	$2.49	-	$3.75

Tabla 3: Precios por soporte mensual

Descripción	NAGIOS	CACTI	PANDORA
Escalabilidad	si	si	si
fiabilidad	no	si	no
tolerancia a fallos	no	si	si
soporte técnico	si	no	si
requisitos de instalación	bajo	bajo	bajo

Tabla 4: Comparación de los softwares de monitoreo

Descripción	NAGIOS	CACTI	PANDORA
Escalabilidad	9	8	6
Fiabilidad	9	6	5
Tolerancia a fallos	8	6	5
Soporte técnico	9	0	8
Requisitos de instalación	9	9	7
Gestión de usuarios	9	8	7
Precio	8	10	7
Total Promedio	8.7	6.7	6.4

Tabla 5: Elección del software de monitoreo

Capitulo III Metodología.

3.1 *Descripción General de la Metodología.*

El presente trabajo es una investigación de campo lo cual se desarrolló utilizando, investigación bibliográfica, consultando en publicaciones y referente a herramientas que permitan realizar la gestión y monitoreo de la red de datos utilizando software libre. Siendo el proceso más adecuado para obtener información.

Se trata de una investigación debido a que se realizara una evaluación con las herramientas de monitoreo de una red empresarial, los cuales serán visualizados en graficas mostrando capturas de pantalla.

La evaluación de esta metodología ayudara a realizar los siguientes análisis de la factibilidad del proyecto monitoreo de redes, debido a este software, NAGIOS nos permite obtener datos, interpretarlos y tomar decisiones en base a ellos como:

Conservar y almacenar datos de la red para manejar reportes y tendencias. Ver y analizar la red, así como el tráfico de la red a través del tiempo. Monitorear el estado de la red en comparación a los reportes de análisis

3.2 *Método*

Utilizaremos la investigación de campo ya que es aquella que se aplica extrayendo datos e informaciones directamente de la realidad a través del uso de técnicas de recolección (como entrevistas o encuestas) con el fin de dar respuesta a alguna situación o problema planteado previamente.

La investigación de campo es la recopilación de datos nuevos de fuentes primarias para un propósito específico. Es un método cualitativo de recolección de datos encaminado a comprender, observar e interactuar con las personas en su entorno natural.

Cuando los investigadores hablan sobre la metodología de "campo" están hablando de estar en el lugar de los hechos y participar en la vida cotidiana de las personas que están estudiando.

Control de los equipos conectados en la red y ayudara a detectar posibles fallas, que provocaría la caída de la red.

Se utilizará software libre que cuente con las herramientas para recopilar información de la infraestructura y funcionamiento de la red, de manera tal que se cuente con información gráfica de rendimiento y fallas proporcionando un listado de mantenimiento de los equipos tanto tiempo funcionamiento

Encuesta sobre software de monitoreo de red

1. ¿Sabe usted que es un software de monitoreo de red?

SI ☐ NO ☐

2. ¿Conoce usted algún software de monitoreo de red?

SI ☐ NO ☐

3. ¿Cuáles de estos softwares de monitoreo de red conoce?

NAGIOS ☐ CACTI ☐

PANDORA ☐ NINGUNO ☐

4. ¿Qué tan importante considera usted el monitoreo de una red?

EXCELENTE ☐ MUY BUENO ☐ BUENO ☐

5. ¿Cuál considera usted el aspecto más importante de un monitoreo de red?

CONTROL DE USUARIOS ☐ PREVENIR FALLOS ☐

SOLUCION DEL ORIGEN DEL PROBLEMA ☐

REDUCCION DE TIEMPO Y COSTOS ☐ OTROS ☐

RESULTADOS DE LA ENCUESTA DE MONITOREO DE RED		
Sabe usted que es un software de monitoreo de red	SI 4 personas	NO 1 persona
Conoce usted algún software de monitoreo	SI 4 personas	NO 1 persona
Cuál de estos software de monitoreo conoce	NAGIOS y CACTI 4 personas	Ninguna 1 persona
Que tan importante considera usted el monitoreo de una red	Excelente 5 personas	
Cual considera usted el aspecto más importante de un monitoreo de red	prevenir fallos 3 personas	Solución del origen del problema 2 personas

3.3 *Justificación de la Elección de la Metodología*.

Esta investigación de campo se realiza con el fin de realizar una encuesta y dar conocer sobre las herramientas del monitoreo de red para ayudar a tener mejor control de los equipos conectados en la red y ayudara a detectar posibles fallas, que provocaría la caída de la red.

Se utilizará software libre que cuente con las herramientas para recopilar información de la infraestructura y funcionamiento de la red, de manera tal que se cuente con información gráfica de rendimiento y fallas proporcionando un listado de mantenimiento de los equipos tanto tiempo funcionamiento

3.4 *Procedimiento*

- Instalación de Ubuntu server 16.04.5 y NAGIOS XI

Seleccionamos instalar Ubuntu server (Ver imagen 5)

Imagen 5: interfaz de instalación de Ubuntu

Seleccionar el país para fijar su zona hora (Ver imagen 6)

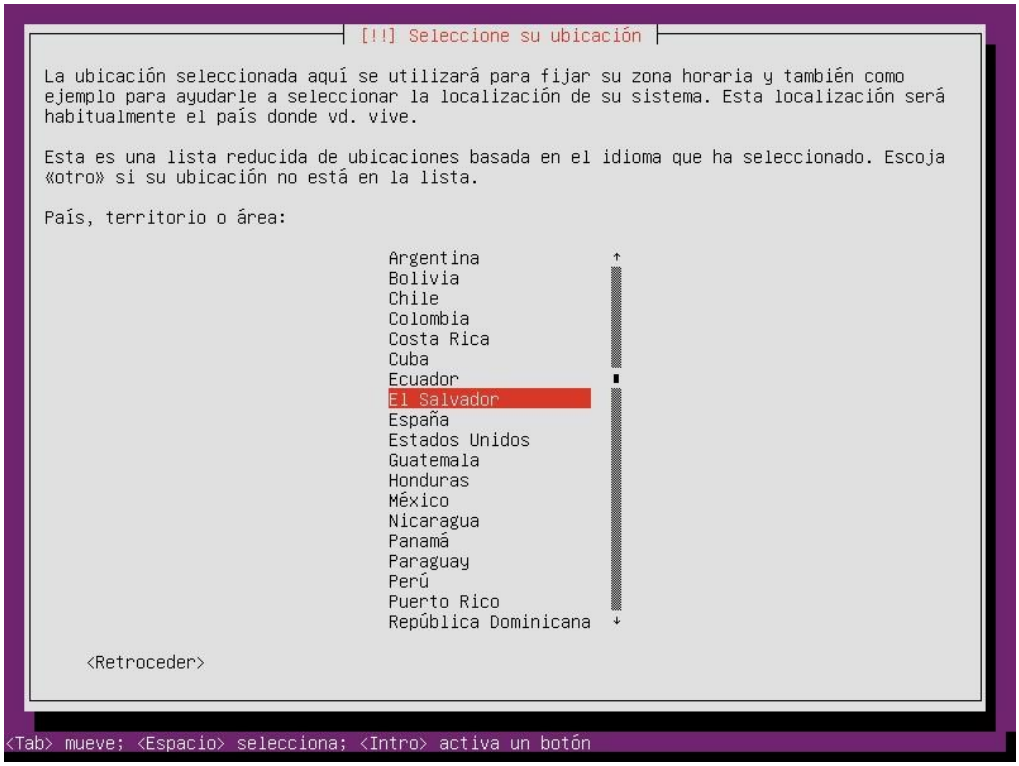

Imagen 6

Seleccionar la interfaz de red en este caso sería enp0s3 (Ver imagen 7)

Imagen 7

Introducir el nombre de la máquina que es nagios-server (Ver imagen 8)

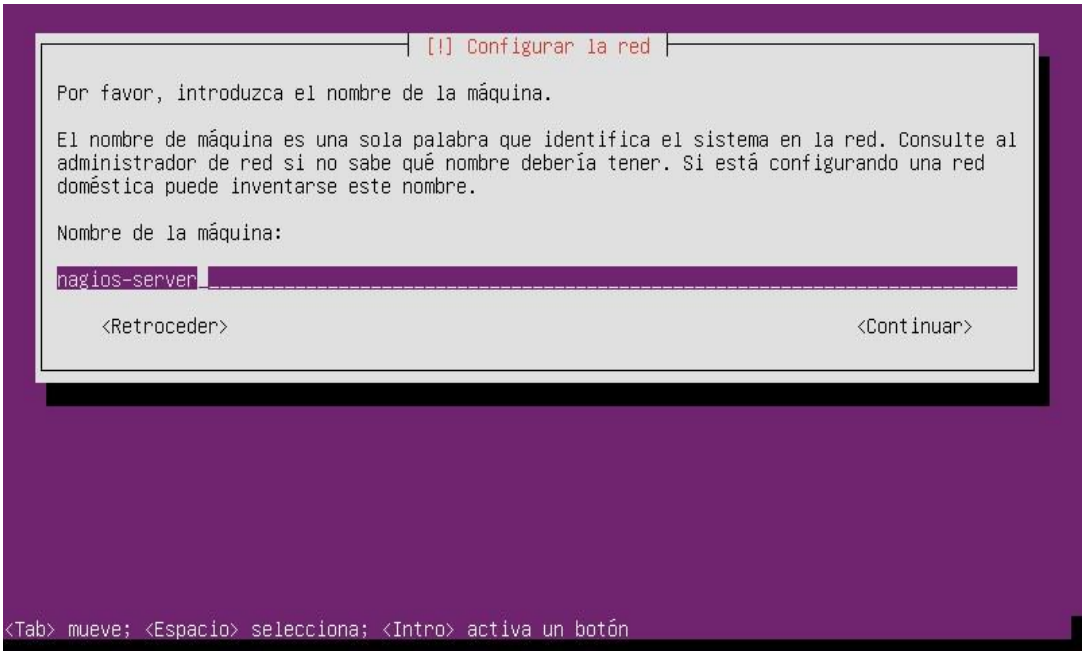

Imagen 8

Creamos una cuenta de usuario y contraseña (Ver imagen 9)

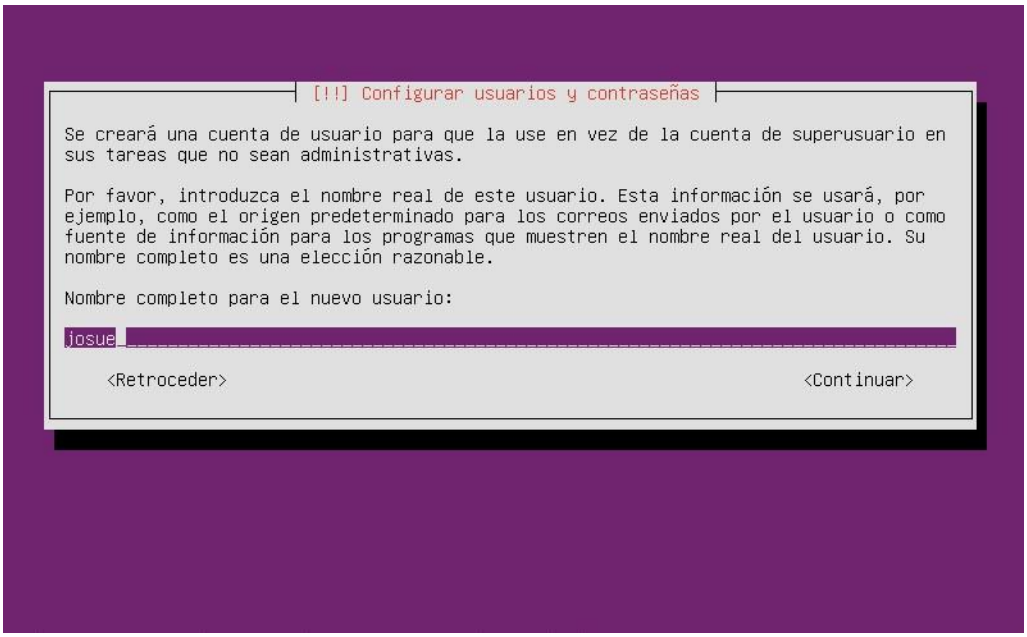

Imagen 9

Seleccionar el programa que se utilizara en este caso es standard system utilities openSSH server. (Ver imagen 10)

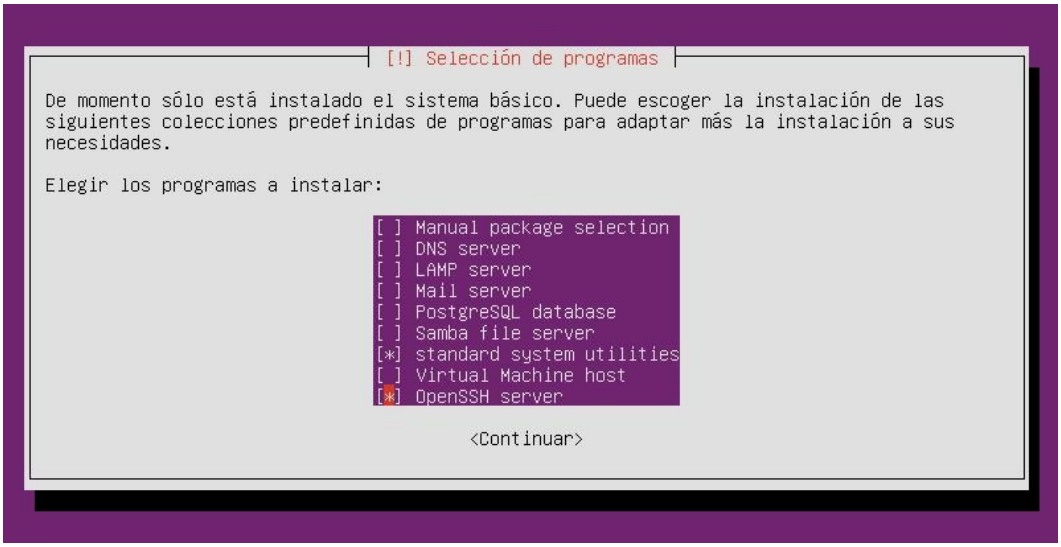

Imagen 10

Instalación terminada Ubuntu server (Ver imagen 11)

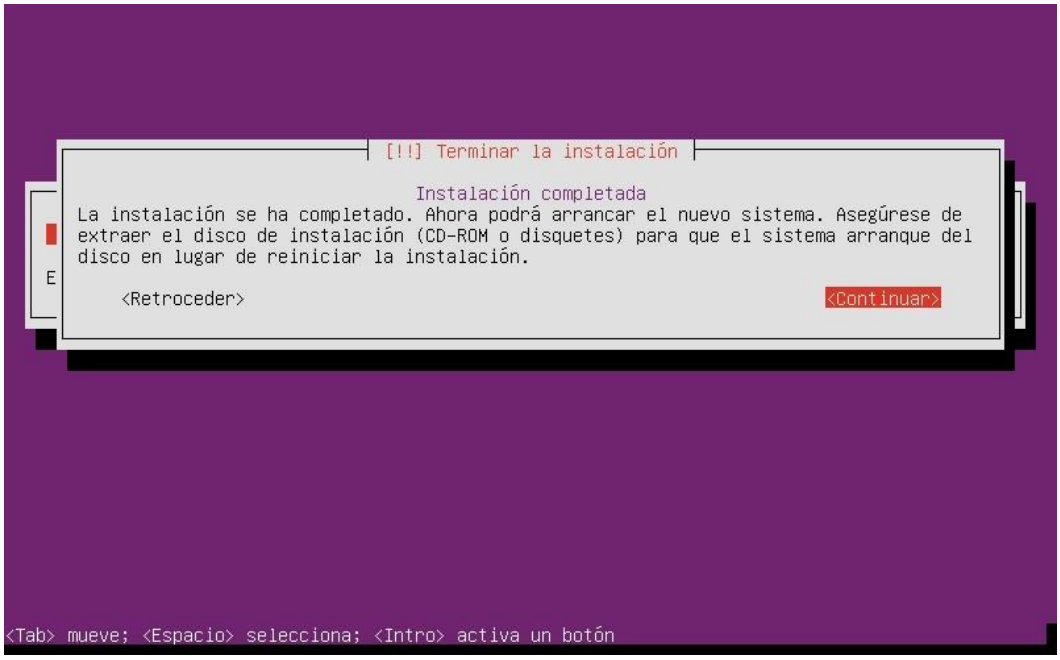

Imagen 11

Entramos a la terminal y establecemos los comandos de sudo apt-get update que sirve para actualizar el listado de paquetes disponibles (Ver imagen 12)

Imagen 12

Luego, establecemos el comando de sudo apt-get upgrade que sirve para actualizar solo los paquetes ya instalados que no necesitan, como dependencia, la instalación o desinstalación de otros paquetes. (Ver imagen 13)

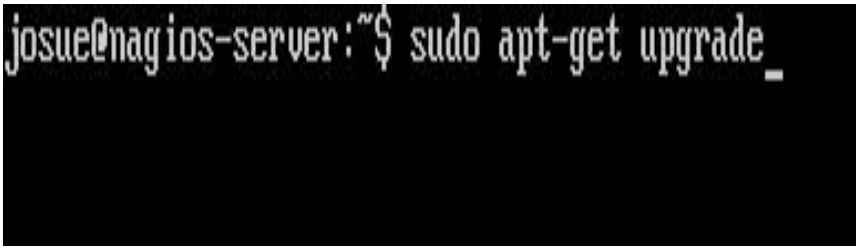

Imagen 13

3.5 *Instalación de NAGIOS XI.*

Digitamos el comando cd /tmp que sirve para acceder al directorio temporal y luego digitamos el comando wget https://assets.nagios.com/dowloads/nagiosxi/5/xi-5.6.7.tar.gz que sirve para descargar nagios xi con la versión más reciente. (Ver imagen 14)

Imagen 14

Establecemos el comando ls para que nos muestre un listado con los archivos del directorio luego digitamos el comando tar xzf xi- 5.6.7.tar.gz que sirve para descomprimir archivos y luego digitamos el comando ls para ver la carpeta que genero al descomprimir el archivo. (Ver imagen 15)

Imagen 15

Colocamos el comando cd nagios xi para ingresar a la carpeta que nos generó al descomprimir el archivo luego digitamos el comando ls para ver el contenido de la carpeta. Después ingresamos el comando ./fullinstall para completar

la instalación de NAGIOS XI. (Ver imagen 16)

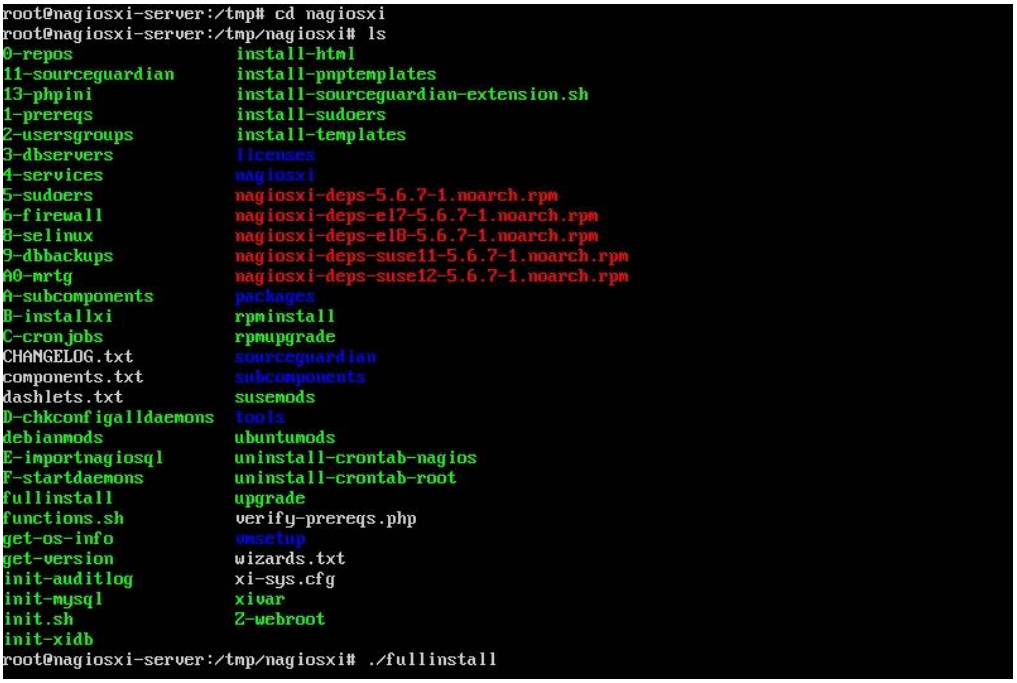

Imagen 16

Instalación finalizada de NAGIOS XI. (ver imagen 17)

Imagen 17

Nagios XI incorpora una serie de funcionalidades exclusivas enfocadas sobre todo en el Interface Web:

Potente interface web: proporciona la capacidad de personalización del diseño, disposición y preferencias del usuario, actualizaciones dinámicas con AJAX que proporcionan información en tiempo real de la infraestructura monitorizada.

Integración de gráficas de rendimiento y capacidad generados automáticamente (con PNP y MRTG).

Dasboards: Potentes paneles de control para un rápido acceso a la información más importante y crítica. Permiten la personalización mediante "dashlets" con acceso y visualización a datos propios e integración con terceros.

Vistas (views): Proporcionan al usuario acceso visual rápido a la información más relevante.

Asistentes de configuración (Wizards) para la motorización de dispositivos. Probablemente unos de los componentes más útiles y prácticos. Nos facilitan la monitorización de todo tipo de componentes (dispositivos, servicios, aplicaciones,…) mediante la configuración mediante asistentes específicos para estos. Si necesidad de entender la lógica compleja que en ocasiones que detrás de estas configuraciones. Debido a su arquitectura modular se crean e incorporan periódicamente nuevos asistentes.

Administrador avanzado de configuración. Mediante herramientas web controlamos y tenemos acceso a toda la configuración tanto de Nagios Core como de otras herramientas. Dispone incluso de la capacidad de importar ficheros de configuración de Nagios Core.

Gestión de usuarios avanzada.

Preferencias y configuración de notificaciones totalmente personalizable por usuario.

Capitulo IV Análisis de Resultados.

4.1 *Demostración y Creación del Usuario NAGIOS XI.*

Creación de usuario de NAGIOS XI. (Ver imagen 18)

Imagen 18

Descargar el agente para comunicarse con el usuario. (Ver imagen 19)

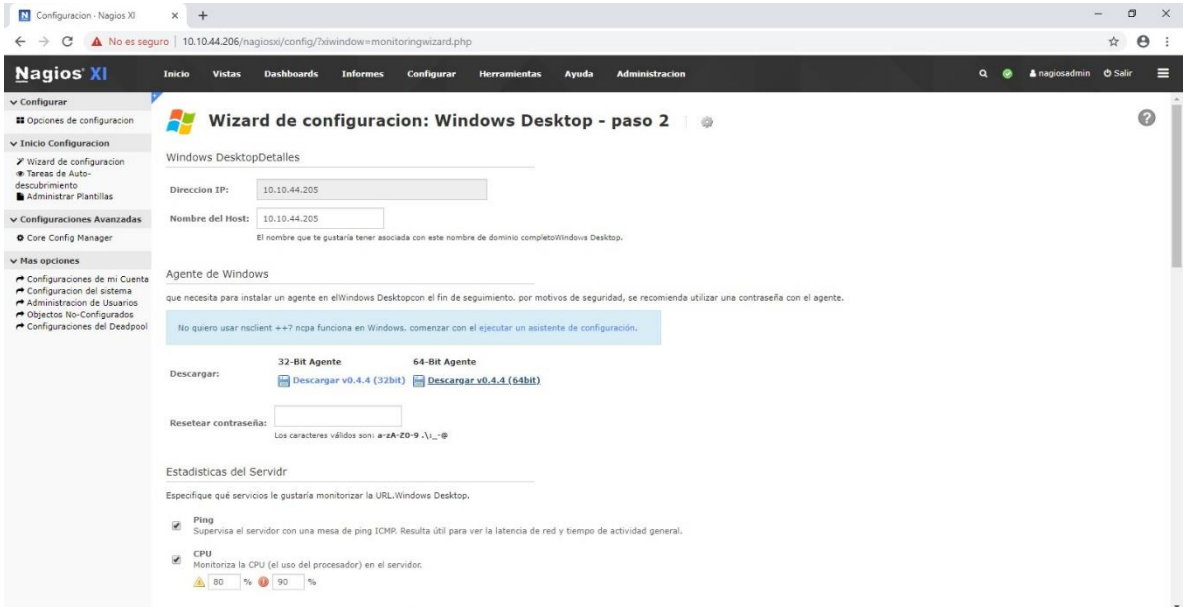

Imagen 19

Ejecutar el agente NSclient. (Ver imagen 20)

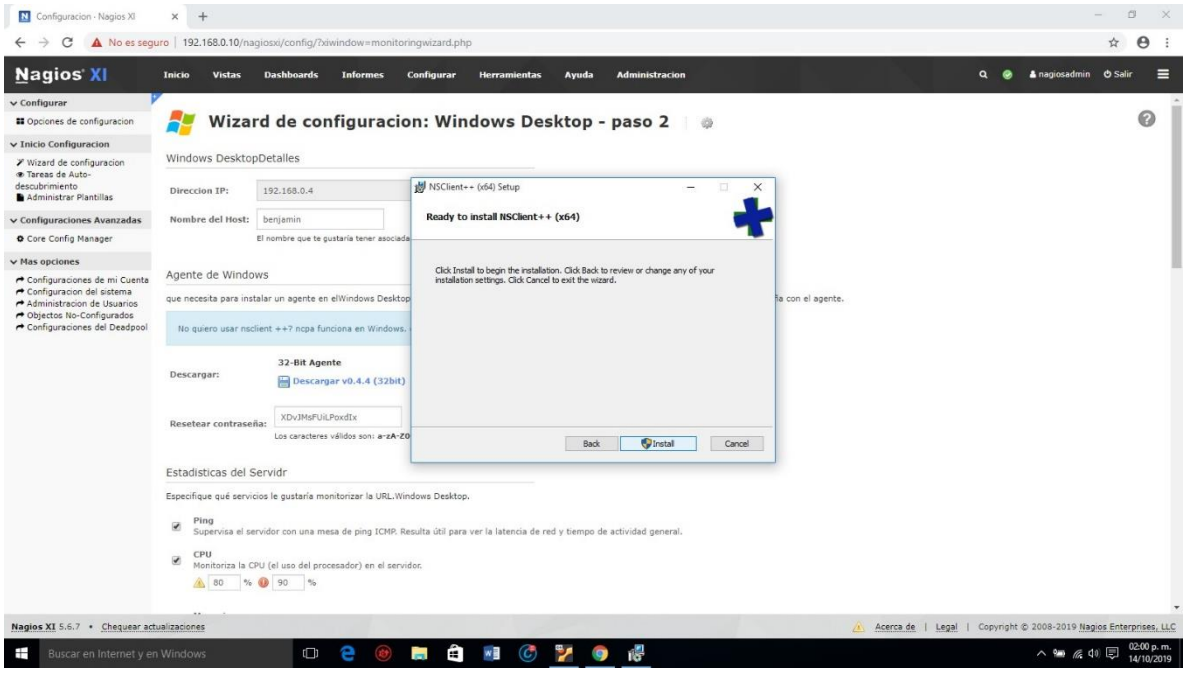

Imagen 20

Seleccionar herramienta de monitoreo (ver imagen 21)

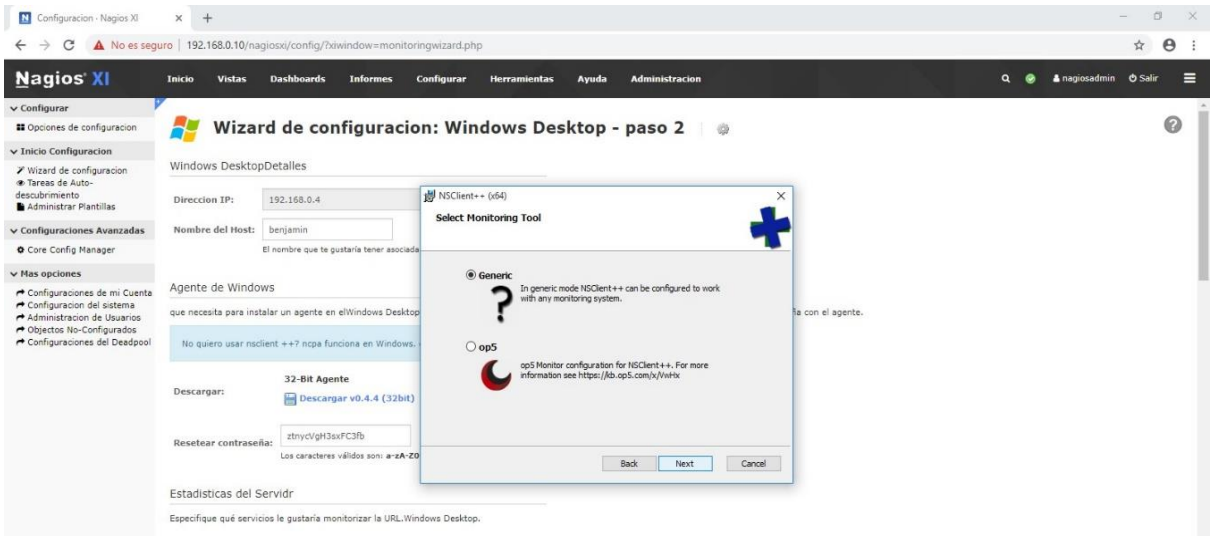

Imagen 21

Seleccionar el tipo de configuración típica. (Ver imagen 22)

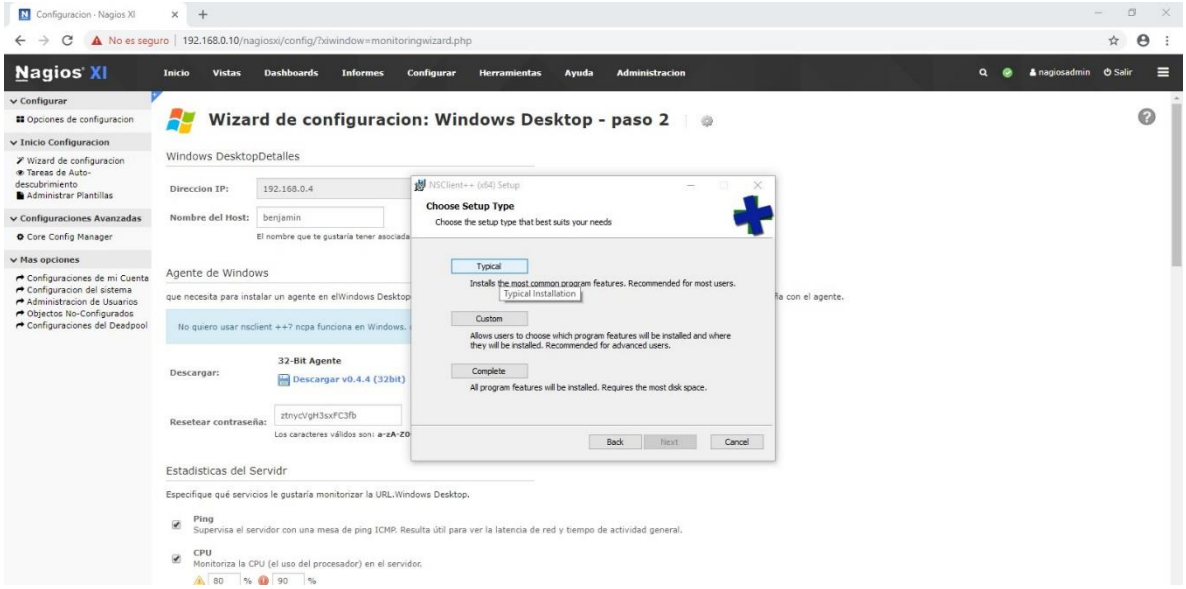

Imagen 22

Configurar el acceso para el servidor. (Ver imagen 23)

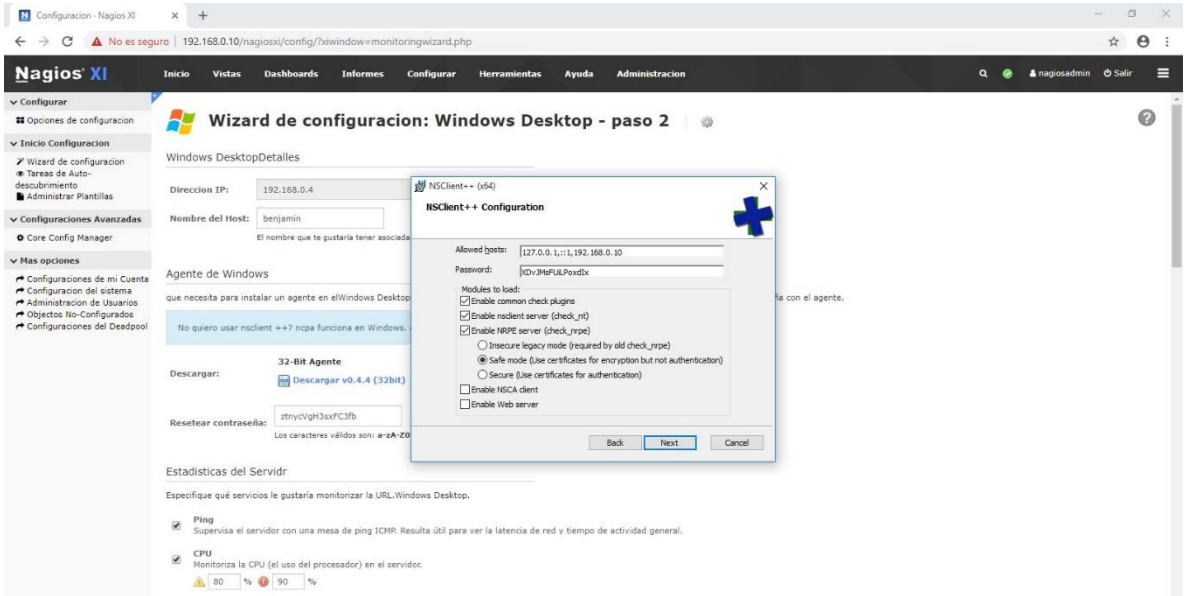

Imagen 23

Finalización de la instalación del agente NSclient. (Ver imagen 24)

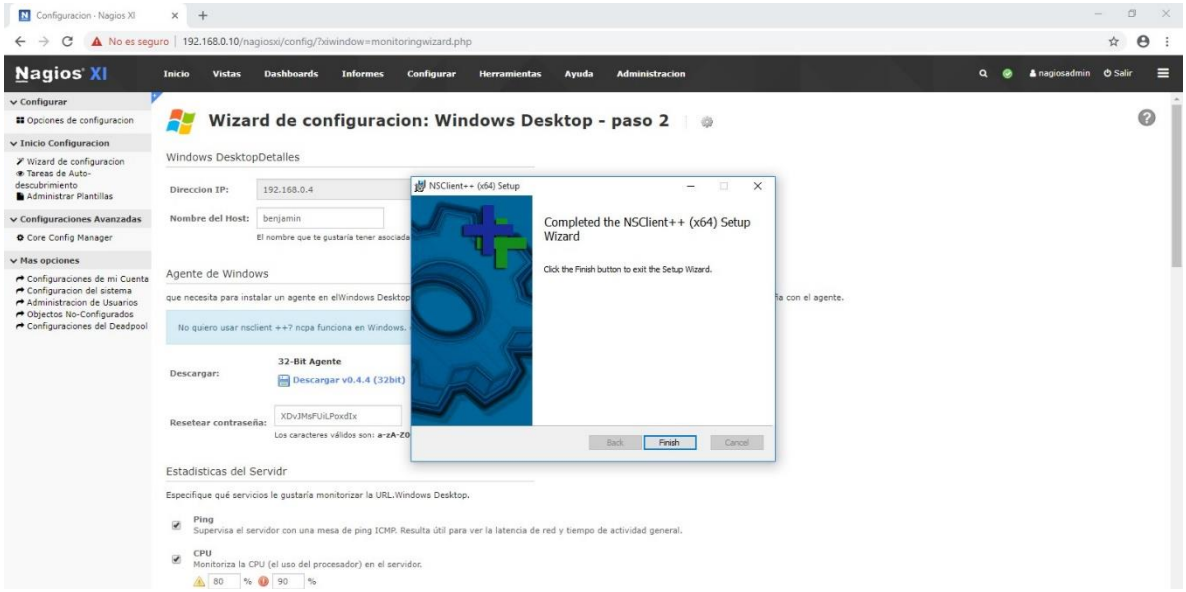

Imagen 24

Finalización de la creación del usuario. (Ver imagen 25)

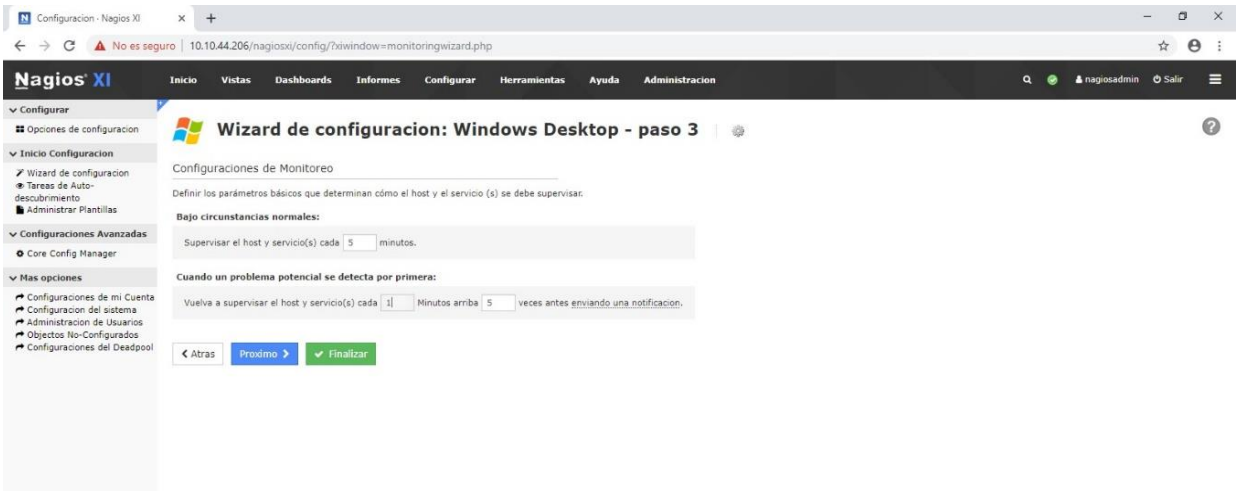

Imagen 25

Estado del servicio del usuario (Ver imagen 26)

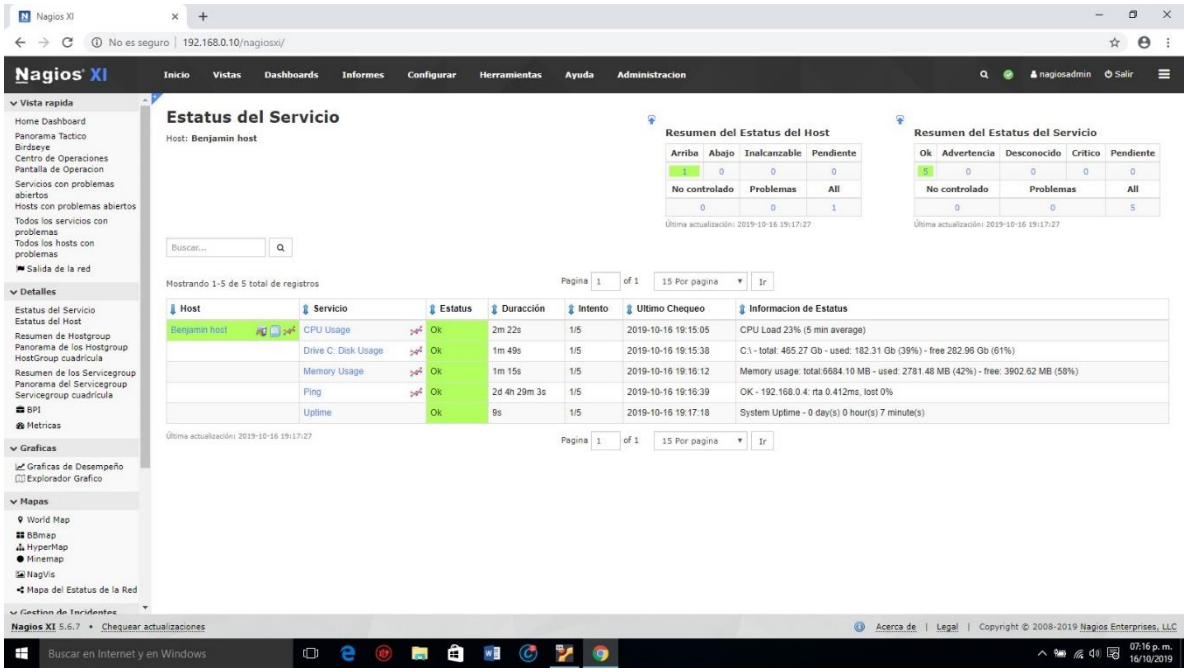

Imagen 26

Detalles del estado. (Ver imagen 27)

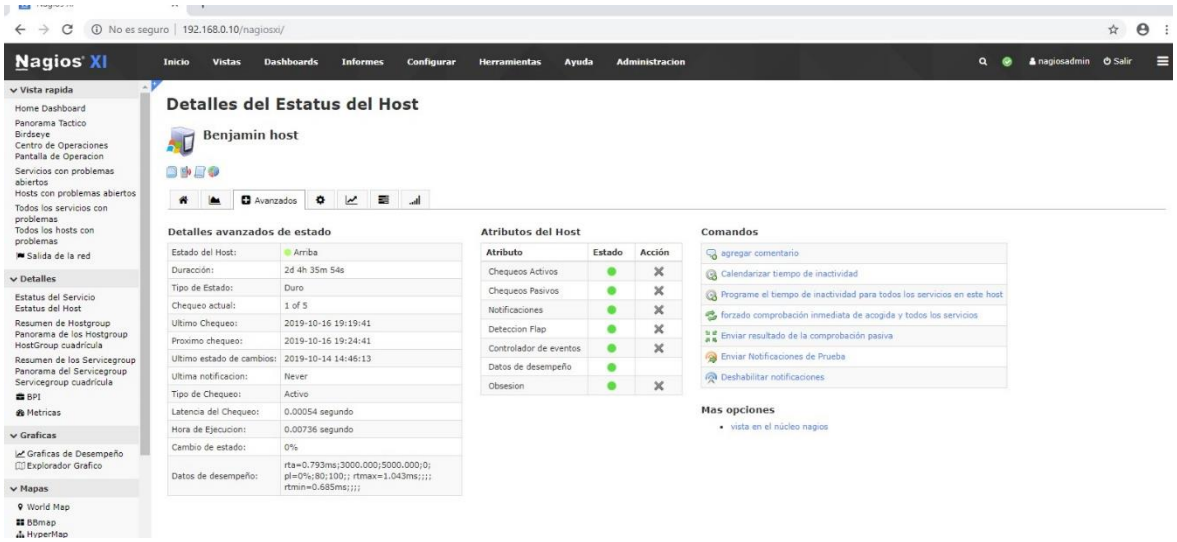

Imagen 27

Informe de notificación (ver imagen 28)

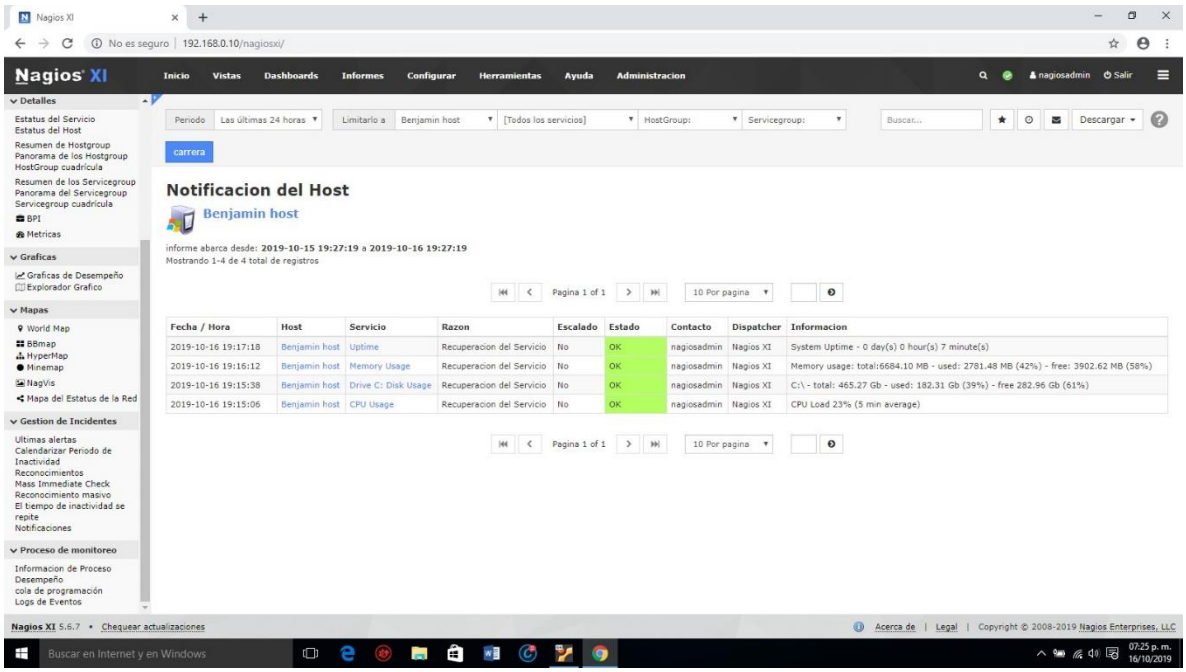

Imagen 28

Gráfico de la disponibilidad y estabilidad del usuario. (Ver imagen 29)

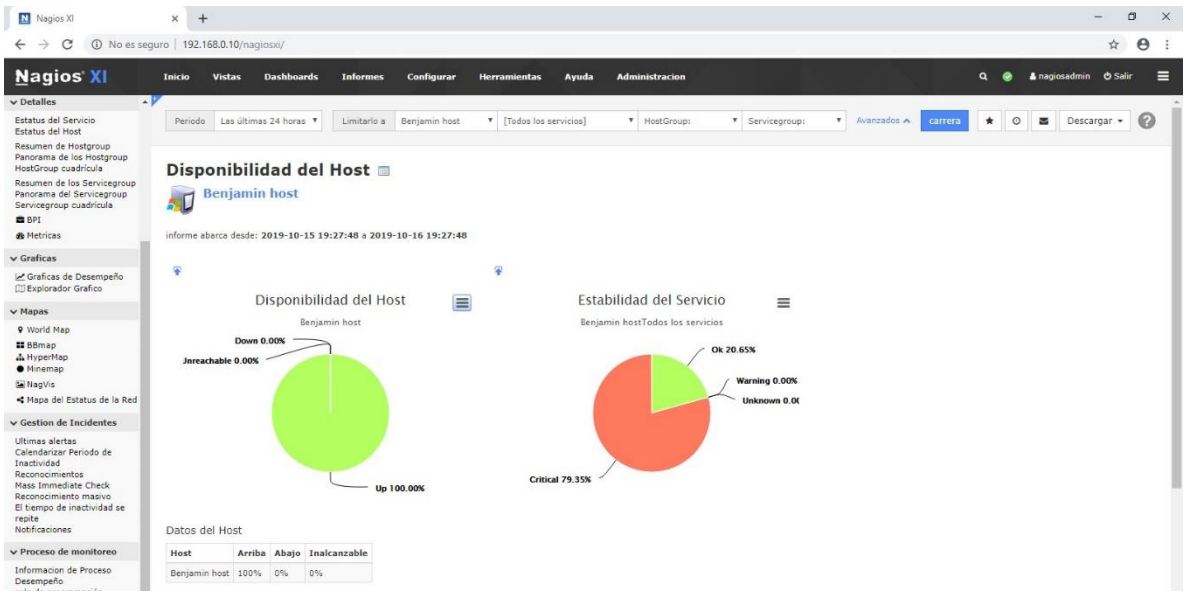

Imagen 29

Datos del servicio. (Ver imagen 30)

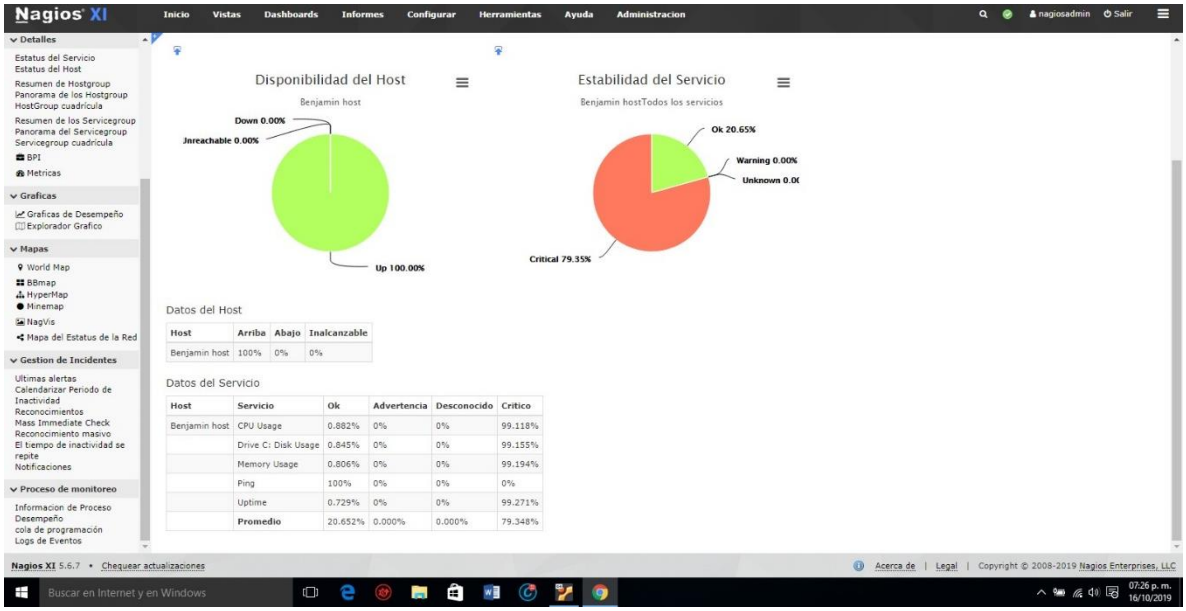

Imagen 30

Capítulo V Conclusiones y Recomendaciones.

5.1 Conclusiones

Concluimos que la implementación de un sistema de monitoreo para una red de datos a nivel empresarial es fundamental, ya que ayuda a prevenir fallos al igual de tener un control internos sobre los equipos de la empresa. Además sistematiza los procesos de mantenimiento de equipos y redes entre otras.

Pero cuales serían las consecuencias o problemas que llevaría al no poseer dicha herramienta, llevaría a la empresa a tener muchos fallos por ejemplo: obsolescencia del sistema, configuración inadecuada del sistema, ataques informáticos no detectados y un mal control para los equipos de la red.

Pero existen herramientas de monitoreo de código abierto, el cual nosotros como grupo elegimos tres herramientas las cuales son: nagios, cacti y pandora. El cual elegimos nagios como herramienta de monitoreo de código abierto a utilizar en nuestro proyecto porque se trata de un software que proporciona una gran versatilidad para consultar prácticamente cualquier parámetro de interés de un sistema y genera alertas por los responsables correspondientes, El cual el único requerimiento para ejecutar nagios es tener un servidor con sistema operativo Linux.

En conclusión la implementación de un sistema de monitoreo de red ayuda a la credibilidad e incrementa la eficiencia y reduce los costos de una empresa permite desarrollar el desempeño y la disponibilidad de la organización desde muchas perspectivas.

5.2 Recomendaciones.

Se recomienda adicionar un módulo de alertas, que permita enviar automáticamente un mensaje vía correo electrónico a las cuentas de los usuarios administradores del sistema, estas alertas indicaran que la fecha de garantía de un activo fijo esta próximo en caerse.

Dentro del servidor NAGIOS toda configuración se realiza por medio de archivos de texto, por lo que es recomendable que se realicen copias de seguridad de estos archivos. Los respaldos y los intervalos de tiempo con el cual se los haga, quede a consideración del administrador de red.

En cuanto a la administración de la herramienta NAGIOS y el directorio activo, se recomienda la creación de los usuarios para el acceso a la información que contiene los servidores y todos los equipos que pertenecen a la red.

El administrador de red debe hacer revisiones constantes del estado de la memoria y almacenamiento de los equipos que contiene las herramientas de NAGIOS, de esta manera se podrá seguir añadiendo más host para monitoreo y si se quiere se realizaran las actualizaciones del software implementado.

Referencias.

Rivas, G. (21 diciembre del 2018). Monitoreo de TI: 5 razones para llevarlo a cabo en tu empresa [Entrada en el blog]. Recuperado de https://www.gb-advisors.com/es/monitoreo-de-ti/

Mundo Teleco. (8 de octubre del 2014). Cacti. [Entrada en el blog]. Recuperado de http://mundotelecomunicaciones1.blogspot.com/2014/10/cacti.html

Javier. (21 de septiembre del 2016). Cacti vs Nagios vs Pandora FMS; comparamos a fondo [Entrada en el blog]. Recuperado de https://pandorafms.com/blog/es/cacti-vs-nagios-vs-pandora-fms/

Equipo Editorial. (2019). *El monitoreo de red dentro de las organizaciones modernas*. Recuperado de https://reportedigital.com/seguridad/monitoreo-de-red/

Avilés. J., Augusto, S., Terán, E. y Fuentes Hernández, A. (2013). *Nagios*. Recuperado de https://es.slideshare.net/juancarlosavilav1/nagios-24210970

Tecnopedia.net. (2015). *Monitoreo de redes y servicios con Pandora FMS*. Recuperado de http://www.tecnopedia.net/software/monitoreo-de-redes-y-servicios-con-pandora-fms/