Universidad de las Ciencias Informáticas

Facultad 2

Título: Selección e integración de una herramienta para monitorear la plataforma PlaTel.

Trabajo de diploma para optar por el título de Ingeniero en Ciencias Informáticas.

Autores:

Miguel Makay Pérez

Raymon Tapia Castellanos

Tutor(es): Ing. Tte. Duany Baro Menéndez

Ciudad de La Habana, 2010

Año 52 de la Revolución

DECLARACIÓN DE AUTORÍA

Declaramos ser autores de la presente tesis y reconocemos a la Universidad de las Ciencias Informáticas los derechos patrimoniales de la misma, con carácter exclusivo.

Para que así conste firmo la presente a los _____ días del mes de _____ del año _____.

_____	_____
Firma del autor.	Firma del autor.
Miguel Makay Pérez.	Raymon Tapia Castellanos.

_____

Firma del tutor.

Ing. Tte Duany Baró Menéndez.

"El futuro de nuestra patria tiene que ser necesariamente un futuro de hombres de ciencia, tiene que ser un futuro de hombres de pensamiento…"

Fidel Castro Ruz.

Agradecimientos

Quiero empezar con mis padres y con mi hermana, pues no tengo forma de agradecerles por todo su amor, comprensión, por su maravilloso ejemplo, por el todo el apoyo que me han brindado, por confiar siempre en mí y por ser las personas más especiales en mi vida.

Agradecerle igualmente a toda mi familia por estar siempre a mi lado, especialmente a mis tías Amarilis, Norma y Milagros y mis abuelas Carmen y Rafaela.

A mi amigo y compañero de tesis Makay por los buenos y malos momentos que hemos pasado en el desarrollo de su trabajo de diploma.

A mis compañeros de grupo tanto el antiguo como el actual, a todos los amigos tan especiales que he conocido en esta universidad, gracias por su amistad.

A todos quienes compartieron las noches de insomnio y las buenas y malas noticias de estos años a mi lado, mil gracias.

A mi compañera Dailien por brindarme su apoyo en todo momento, gracias por ser tan especial.

A mi tutor Duany y al tribunal de tesis, gracias.

Raymon

Dedicatoria

Dedico este trabajo primeramente a mi mamá y mi papá, que siempre han confiado en mí y me han apoyado incondicionalmente en cada uno de mis pasos en la vida. A mi hermana, que es la niña de mis ojos y la quiero con la vida. A mis tías Norma, Amarilis, Milagros, a mis abuelas Rafaela y Carmen, que todos son como mis otros padres, que me criaron e hicieron de mí un hombre del que hoy, sin dudas, pueden estar orgullosos. A todos los demás miembros de mi familia que de una forma u otra siempre se han preocupado por mi futuro.

En fin, le dedico este trabajo a todos los que me quieren, y a los que no también, por haberme ayudado a ser como soy.

Raymon

Resumen

El presente trabajo de diploma, tiene como objetivo seleccionar una herramienta que pueda llevar un control permanente sobre un servidor Asterisk y se integre con la plataforma PlaTel, conociéndose que no se dispone de un sistema que alerte los posibles fallos que puedan ocurrir en la red de dicha plataforma; facilitando entre otras ventajas evitar errores, aumento de la productividad, la automatización de las actividades y establecer mejoras en el sistema VoIP.

En este documento quedan plasmados los resultados del estudio realizado sobre algunas de las herramientas de código abierto existentes en el mundo. Se definen los conceptos fundamentales relacionados con el tema, las características de los sistemas de monitoreo así como algunas PBX basadas en software. Nagios fue el software seleccionado entre una gran variedad ya que puede monitorear la plataforma para asegurar que los sistemas, aplicaciones, servicios y procesos de negocio estén funcionando correctamente. Si se produjera alguna falla puede alertar al personal técnico del problema, que iniciarían los correctivos del caso, antes que los fallos afecten a los procesos de negocio, usuarios finales o clientes. Se describe además el proceso de instalación y configuración de la herramienta seleccionada.

Palabras Claves: control, monitoreo, Asterisk, VoIP, PBX, alertar.

TABLA DE CONTENIDO

ÍNDICE DE IMÁGENES

ÍNDICE DE TABLAS

INTRODUCCIÓN

La comunicación siempre ha sido un tema muy importante para el hombre y al mismo tiempo un punto que ha conseguido la atención y la investigación para satisfacer la necesidad continúa de comunicarse. En la nueva era de las comunicaciones digitales, las centrales telefónicas han evolucionado hasta convertirse en potentes máquinas de enrutamiento y gestión de llamadas, capaces de usar líneas análogas convencionales, acceso a Internet y telefonía IP (***I****nternet* ***P****rotocol*).

La telefonía de voz sobre IP es una tecnología que toma señales de voz analógicas para convertirlas en paquetes de datos, de modo que pueda ser trasmitida a través de cualquier red de datos. Esta tecnología está revolucionando el mundo de la telefonía como lo conocemos hoy en día y es por ello que las compañías telefónicas se sienten un tanto amenazadas.

Para Cuba es importante buscar el equilibrio adecuado entre la generación propia de tecnología y la asimilación de las mismas, disponibles en el mercado, que permitan reducir, de forma acelerada, la brecha tecnológica y alcanzar un nivel de competitividad en el desarrollo de la telefonía IP.

Las Fuerzas Armadas Revolucionarias (FAR), con la participación de la Universidad de las Ciencias Informáticas (UCI), están dirigiendo el desarrollo de la Plataforma de Telecomunicaciones Unificada PlaTel, que tiene como misión unificar la telefonía IP con la telefonía tradicional, mensajería instantánea, correo electrónico, fax y todos los servicios que brinda una central telefónica, reduciendo de esta forma los costos que proporciona la compra de PBX (***P****rivate* ***B****ranch* ***E****xchange*) extranjeras. Esta plataforma telefónica utiliza como elemento fundamental de su núcleo la PBX Asterix, cuyo código fuente está disponible para adicionarle funcionalidades e incluso realizar mejoras permitiendo construir un sistema robusto y eficiente.

En la Unidad de Compatibilización, Integración y Desarrollo de Software Integrado a la Defensa (UCID), que es el centro designado por las FAR para el desarrollo de productos informáticos y donde precisamente se desarrolla la plataforma PlaTe, no existe un sistema que alerte los posibles fallos que puedan ocurrir en la red de dicha plataforma telefónica, por ejemplo, la caída de un servidor, router, switch, o cualquier otro dispositivo, lo que puede traer como consecuencia la imposibilidad de brindar los servicios pertinentes a sus usuarios. De esta forma surge la necesidad de monitorear el

correcto funcionamiento de los elementos que componen la plataforma telefónica, con el objetivo de obtener, interpretar y decidir ante los fallos que puedan detectarse durante el monitoreo de la misma.

Las diversas problemáticas planteadas conllevan a determinar el siguiente **problema científico** ¿Cómo monitorear la plataforma PlaTel? Definiéndose como **objeto de estudio** los sistemas de monitoreo de red, identificándose como **campo de acción** monitoreo de los servicios de red para la plataforma PlaTel. El **objetivo general** consiste en seleccionar una herramienta que se integre con la plataforma PlaTel y permita monitorear los servicios que ésta ofrece. De ahí se derivan los siguientes **objetivos específicos**:

- Proponer una herramienta que brinde la posibilidad de monitorear la plataforma PlaTel.
- Instalar y configurar la herramienta propuesta.
- Integrar la herramienta con la plataforma PlaTel.
- Realizar pruebas a la solución propuesta en el centro UCID con el propósito de verificar su funcionamiento.

La **idea a defender** que rige esta investigación es la siguiente:

Si se selecciona e integra correctamente una herramienta apropiada para el monitoreo de los elementos y servicios que componen la red se logrará supervisar el funcionamiento de la plataforma PlaTel.

Con el propósito de organizar el trabajo realizado y garantizar una mayor comprensión, el documento se estructuró en 3 capítulos que recogen toda la información de la investigación realizada.

Capítulo 1: Fundamentación Teórica. Aborda los conceptos de protocolo, monitoreo, conmutación, entre otros, para facilitar la comprensión del documento. Se describen los protocolos VoIP, las PBX basadas en software así como algunas herramientas de monitoreo de red existentes. Además se exponen características de los sistemas de monitoreo así como su funcionamiento.

Capítulo 2: Proceso de Instalación y Configuración. Incluye un análisis donde se detallan los aspectos esenciales que facilitaron la selección de la herramienta. Recoge además la estructura de la misma así como los requisitos y el procedimiento que se debe tener en cuenta para su instalación. También se explican los procedimientos a seguir para efectuar una configuración completa del software a emplear.

Capítulo 3: Proceso de Prueba. Precisa los detalles de la puesta en marcha de la herramienta y recoge los resultados obtenidos en el monitoreo de los diferentes servicios.

CAPÍTULO 1. FUNDAMENTACIÓN TEÓRICA

1.1. Introducción

Hoy día el acelerado desarrollo de las tecnologías de la informática y las telecomunicaciones trae como consecuencia que las redes de cómputo se vuelvan cada vez más complejas. Éstas soportan numerosas aplicaciones y servicios estratégicos para las organizaciones en las que se implementan, y la exigencia de su apropiado funcionamiento es sumamente solicitada por sus usuarios. El monitoreo de redes está estrechamente atado a este avance y se ha convertido en una importantísima labor de carácter primordial para evitar cualquier problema que se pueda presentar.

En este capítulo se definen los principales conceptos asociados al tema de monitoreo de plataformas telefónicas. Se abordan, entre otros aspectos, características de las plataformas telefónicas de código abierto (open source) existentes en el mundo además de las distintas herramientas para el monitoreo de los elementos de una red. En fin se realiza un estudio sobre el estado actual de las mismas.

1.2. Conceptos asociados al dominio del tema

Para entender el significado de monitoreo de plataformas telefónicas es necesario realizar un estudio de los conceptos que están totalmente ligados al dominio del tema, y que su desconocimiento puede dificultar la comprensión del documento.

1.2.1. Red informática

Según la Real Academia Española una red, desde el punto de vista informático, es un conjunto de ordenadores o de equipos informáticos conectados entre sí que pueden procesar, intercambiar y almacenar información.

También se les conoce como red de ordenadores o red de computadoras, a una red conformada por un conjunto de dispositivos conectados por medio de cables, señales, ondas o cualquier otro método de trasmisión de datos que comparten información, recursos, servicios, etc. incrementando la eficiencia y productividad de las personas que acceden a ella. (1)

1.2.2. Monitoreo de red

El término monitoreo de red describe el uso de un sistema que monitoriza una red de computadoras en búsqueda de cualquier comportamiento desfavorable, para luego informar a los administradores mediante correo electrónico, mensajería instantánea, etc.

Los recursos usados en una red informática tienen que ser continuamente vigilados debido a que cualquier falla lleva al deterioro del funcionamiento de un recurso específico, un conjunto de recursos o la red, y por lo tanto debe ser corregido. Esto es más una acción preventiva que una reactiva. Los recursos tienen que ser controlados, lo que significa que se debe vigilar cómo se comportan, a fin de que su función se realice apropiadamente.

1.2.3. Protocolo

Término tomado del lenguaje diplomático que se utiliza para designar las reglas y convenciones necesarias para intercambiar información en un sistema de telecomunicaciones. Un protocolo funciona como un lenguaje común que tiene que poder ser interpretado por cualquier ordenador conectado a una red. (2)

En la informática protocolo es una palabra muy utilizada, refiere a un conjunto de reglas usadas por computadoras para comunicarse unas con otras a través de una red. Es una estándar que controla o permite la conexión, comunicación y transferencia de datos entre dos puntos finales.

En su forma más simple, un protocolo puede ser definido como las reglas que dominan la sintaxis, semántica y sincronización de la comunicación. Los protocolos pueden ser implementados por hardware, software, o una combinación de ambos.

1.2.4. Conmutación

Conmutación es el vocablo general usado para describir la operación de un conmutador. Debido a que se asocia con el hardware, la conmutación suele tener una velocidad mayor que el enrutamiento. Un conmutador es un dispositivo electrónico que forma el centro de una red de topología en estrella. Los conmutadores usan la dirección destino de un paquete o paquetes de información para determinar la computadora que debe recibirlos. (3) En el mundo de las telecomunicaciones es un

término elemental a la hora de referirse a cualquier dispositivo telefónico, ya que se puede clasificar como el interconectar manual o automáticamente de los terminales telefónicos.

A continuación se mencionan algunas de las principales funcionalidades que ofrecen estos dispositivos.

Funciones del equipo de conmutación

- Identificar al abonado solicitante.
- Analizar la información de selección.
- De acuerdo a esta información, seleccionar la vía o canal a utilizar.
- Transferirle la información de selección.
- Investigar el estado libre/ocupado del abonado solicitante.
- Informar al abonado A/B lo que le corresponde.
- Establecer/liberar el enlace.
- Supervisar conexión.
- Y liberar los caminos establecidos cuando la comunicación haya finalizado.

Si no existiese una herramienta como esta, fuera muy difícil o casi imposible que las personas se comunicaran por vía telefónica.

1.3. Funcionamiento de los sistemas de monitoreo

Los sistemas de monitoreo realizan tareas de control constantemente. Se comunican con procesos que supervisan el sistema operativo, que contienen información sobre el ordenador y para capturar los datos, utilizan funciones de bajo nivel. Por lo general estas aplicaciones están implementadas en el lenguaje de programación C/C++.

La monitorización de los sistemas puede realizarse a través de dos mecanismos, monitorización remota y agentes locales instalados. La primera de estas, se realiza desde un ordenador hacia uno o varios de estos. Para establecer una conexión entre ambas partes, utilizan un protocolo de red. Este tipo de monitoreo, puede representar de manera gráfica las acciones que se cometen en el ordenador que se está controlando.

El agente local, consiste en una aplicación que supervisa recursos del sistema operativo en el ordenador instalado. Su funcionamiento frente al monitoreo remoto básicamente es el mismo, la diferencia radica en que las herramienta locales no requieren de la conexión a una red, y por lo tanto la implementación es menos compleja y riesgosa.

La actividad de monitoreo varía en cuanto a la necesidad de lo que se quiera controlar, puede ser, el estado de los servicios de red, procesos de un ordenador o parámetros físicos del hardware. Teniendo en cuenta el propósito para el que se controla, el sistema puede ser visible o no al usuario objeto de vigilancia.

1.4. Características de los sistemas de monitoreo

El funcionamiento de los sistemas de monitoreo remoto, exigen una alta velocidad de conexión para obtener un rendimiento óptimo cuando la distancia y la cantidad de equipos son considerables. Son muy usados por la comodidad con que reflejan sus datos y generalmente están orientados al control de redes. Se recomienda su uso cuando se cuenta con un servicio de red fiable, ya que dependen totalmente de esta, por lo que no garantizan el control total de los recursos del sistema permanentemente y su empleo puede ser muy costoso.

Las aplicaciones locales son ligeras, escasamente requieren recursos del sistema operativo y aseguran el control del mismo mientras es usado. Son independientes de la conexión a una red y facilitan integrarse a esta. Se sugiere su empleo, cuando es indispensable que un ordenador sea chequeado constantemente. El uso de estas herramientas pueden ser aplicadas con tecnología barata.

Existen al menos dos puntos de vista para abordar el proceso de monitorear una red: el enfoque activo y el enfoque pasivo. Aunque son diferentes entre sí ambos se complementan.

1.4.1. Monitoreo activo

Este tipo de monitoreo se realiza inyectando paquetes de prueba en la red o enviando paquetes a determinadas aplicaciones midiendo sus tiempos de respuestas. Este enfoque tiene la característica de agregar tráfico en la red y es utilizado para medir el rendimiento de la misma. (4)

- **Técnicas de monitoreo activo**
  - *Basado en ICMP (**I**nternet **C**ontrol **M**essage **P**rotocol)*
    - Diagnóstico de problemas en la red.
    - Detectar retardo y pérdida de paquetes.
    - Disponibilidad de host y redes.
  - *Basado en TCP (**T**ransmission **C**ontrol **P**rotocol)*
    - Tasa de transferencia de datos.
    - Diagnóstico de problema a nivel de aplicación.
  - *Basado en UDP (**U**ser **D**atagram **P**rotocol)*
    - Pérdida de paquetes en un sentido.

1.4.2. Monitoreo Pasivo

Este enfoque se basa en la obtención de datos a partir de recolectar y analizar el tráfico que circula por al red. Se emplean diversos dispositivos como sniffers, ruteadores, computadoras con software de análisis de tráfico y en general dispositivos con soporte para SNMP (***S**imple **N**etwork **M**anagement **P**rotocol*) y RMON (**R**emote **M**onitor). Además no agrega tráfico en la red como lo hace el enfoque activo. Es utilizado para caracterizar el tráfico de la red y para contabilizar su uso. (4)

- **Técnicas de monitoreo pasivo**
  - *Solicitudes remotas mediante el protocolo SNMP*

Esta técnica es utilizada para obtener estadísticas sobre la utilización de ancho de banda en los dispositivos de red, para ello se requiere de tener acceso a dichos dispositivos. Al mismo tiempo este protocolo genera paquetes llamados trampas que indican que un evento inusual se ha producido. Además se pueden confeccionar *scripts* que tengan acceso a dispositivos remotos para obtener

información importante para el monitoreo. En esta técnica se pueden emplear módulos de Perl, SSH (del inglés ***S**ecure **Sh**ell*) con autenticación de llave publica, entre otros. (4)

- *Captura de tráfico*

Se puede llevar a cabo de dos formas: mediante la configuración de un puerto espejo en un dispositivo de red, el cual hará una copia del tráfico que se recibe en un puerto hacia otro donde estará el equipo que realizará la captura; y mediante la instalación de un dispositivo intermedio que capture el tráfico, el cual puede ser una computadora con el software de captura o un dispositivo extra. Esta técnica es utilizada para contabilizar el tráfico que circula por la red. (4)

- *Análisis de tráfico*

Se utiliza para la caracterizar el tráfico de la red, es decir, para identificar el tipo de aplicaciones que son mas utilizadas. Se puede implementar haciendo uso de dispositivos que envíen información mediante RMON o a través de un dispositivo intermedio con una aplicación capaz de clasificar el tráfico por aplicación, direcciones IP origen y destino, puertos origen y destino, etc. (4)

- *Flujos*

También utilizado para identificar el tipo de tráfico utilizado en la red. Un flujo es un conjunto de paquetes con:

  - La misma IP origen y destino.
  - El mismo puerto TCP origen y destino.
  - El mismo tipo de aplicación.

Los flujos pueden ser obtenidos de ruteadores o mediante dispositivos que sean capaces de capturar tráfico y transformarlos en flujos. También es usado para tareas de facturación. (4)

1.5. Protocolos VoIP

La Voz sobre IP es una tecnología que toma señales de voz analógicas para convertirlas en paquetes de datos de modo que pueda ser transmitida a través de cualquier red de IP, la cual conjuga dos mundos históricamente separados: la transmisión de voz y la de datos. Se trata de transportar la voz, previamente convertida a datos, entre dos puntos distantes. Esto posibilitaría utilizar las redes de datos para efectuar las llamadas telefónicas y desarrollar una única red que se encargue de cursar todo tipo de comunicación, ya sea vocal o de datos. (5)

Esta tecnología se apoya de una serie de protocolos para su funcionamiento, estos son detallados a continuación.

1.5.1. SIP

EL protocolo SIP (del inglés ***S****ession* ***I****nitiation* ***P****rotocol*) es un protocolo de control y señalización usado principalmente en los sistemas de telefonía IP. El mismo posibilita crear, modificar, y terminar sesiones con unos o más participantes de la red. Estas sesiones incluyen llamadas telefónicas por Internet, distribución video, voz y mensajería instantánea. (6)

SIP permite la interacción entre dispositivos, esto se consigue con distintos tipos de mensajes propios del protocolo, proporcionando capacidades para registrar y/o invitar un usuario a una sesión, negociar los parámetros de una sesión, establecer una comunicación entre dos a más dispositivos y por último, finalizar sesiones. (6)

En definitiva, se puede observar que SIP es un protocolo con una gran escalabilidad y muy apto para convertirse en el futuro inmediato de la VoIP.

1.5.2. MGCP

El protocolo MGCP (del inglés ***M****edia* ***G****ateway* ***C****ontrol* ***P****rotocolo*) permite vigilar los elementos de control de llamadas externas en las pasarelas de los medios de comunicación, llamados Gateway o Agente de Llamada. La pasarela de medio es, típicamente, un elemento de la red que proporciona la conversión entre señal de audio de un teléfono conmutado por circuito y la señal de paquete que se puede transportar a través de Internet o sobre la red de conmutación de paquete. Presenta una arquitectura de control de llamada donde la “inteligencia” está fuera de las pasarelas y es manejado por elementos de control de llamada externos, conocidos como Agentes de Llamada.

El MGCP presupone que estos elementos del control de llamada o Agentes de Llamada se sincronizan entre sí para enviar órdenes coherentes y respuesta a las pasarelas. Si esta suposición se viola, debe esperarse una conducta incoherente. No define un mecanismo para sincronizar a los Agentes de Llamada, implementa la Interfaz de control de Gateway de comunicación como un conjunto de transacciones compuestas por un orden y una respuesta obligatoria permitiendo comunicar al controlador de Gateway con los Gateway de telefonía.

1.5.3. H.323

El estándar H.323 proporciona una base para las comunicaciones de audio, video y datos a través de una red IP como Internet. Los productos que cumplen con este protocolo pueden ínter operar con los productos de otros, permitiendo de esta manera que los usuarios puedan comunicarse sin preocuparse por problemas de compatibilidad.

Es un conjunto de normas para comunicaciones multimedia que hacen referencia a los terminales, equipos y servicios estableciendo una señalización en redes IP. No garantiza una calidad de servicio, y en el transporte de datos puede, o no, ser fiable; en el caso de voz o vídeo, nunca es fiable.

Incluye desde dispositivos específicos hasta tecnologías embebidas en ordenadores personales, además de servir para comunicación punto-punto o conferencias multipunto. Trabaja también sobre control de llamadas, gestión multimedia y gestión de ancho de banda, además de los interfaces entre redes de paquetes y otras redes. (7)

1.5.4. IAX2

El protocolo IAX2 (del inglés ***I**nter-**A**sterisk e**X**change v**2***) como indica su nombre fue diseñado como un protocolo de conexiones VoIP entre servidores Asterisk aunque hoy día también sirve para conexiones entre clientes y servidores que soporten dicho protocolo. Utiliza como protocolo de transporte UDP (del inglés ***U**ser **D**atagram **P**rotocol*, Protocolo de Datagrama de Usuario), normalmente sobre el puerto 4569.

Es un protocolo robusto más simple en comparación con otros protocolos. Permite gestionar una gran cantidad de codificadores y un gran número de emisiones, lo que significa que puede ser utilizado

para transportar virtualmente cualquier tipo de dato. Esta capacidad lo hace muy útil para realizar videoconferencias o realizar presentaciones remotas.

Soporta trunking, donde un simple enlace permite enviar datos y señalización por múltiples canales. Cuando se realiza Trunking, los datos de múltiples llamadas son manejados en un único conjunto de paquetes, lo que significa que un datagrama IP puede entregar información para más llamadas sin crear latencia adicional. Esto es una gran ventaja para los usuarios de VoIP, donde las cabeceras IP son un gran porcentaje del ancho de banda utilizado. (8)

1.6. PBX basadas en software

Las PBX (del inglés ***P**rivate **B**ranch E**x**change*) son conocidas como pequeñas centrales telefónicas privadas, implantadas en las medianas y grandes empresas por su fácil manejo. La palabra “private” significa que el administrador del sistema es dueño y señor absoluto del mismo y es el que decide cómo compartir las líneas con los usuarios. Estas centrales telefónicas tienen la capacidad de redirigir entre un terminal telefónico, o varios, las llamadas entrantes. Admiten además que un teléfono escoja una de sus líneas para realizar una llamada al exterior, de la misma forma que el router es encargado de dirigir los paquetes en la red, una PBX se encarga de dirigir las llamadas. (9)

También permiten que los usuarios se puedan comunicar fácilmente, incluso si un trabajador se encuentra lejos de su puesto de trabajo. Para esto se establece un número de teléfono que tiene la peculiaridad de aceptar las llamadas externas pulsando la extensión a la cual se quiere comunicar. Como se puede apreciar las PBX son realmente cómodas tanto para las empresas, como para los usuarios que la integran (terminales telefónicos). Existen varios software que presentan características de PBX, como Asterisk, FreeSwitch, Yate. Estas PBX basadas en software son capaces de soportar protocolos VoIP. (9)

1.6.1. Asterisk

Asterisk es una aplicación para controlar y gestionar comunicaciones de cualquier tipo, ya sean analógicas o digitales mediante todos los protocolos que implementa. Además es de código abierto basada en licencia GPL (del inglés ***G**eneral **P**ublic **L**icense*) y por lo tanto con las ventajas que ello

representa, haciéndolo libre para desarrollar sistemas de comunicaciones profesionales de gran calidad, seguridad y versatilidad. (10)

Poco a poco, esta aplicación se ha convertido en la evolución de las tradicionales centralitas analógicas y digitales permitiendo también integración con la tecnología más actual: VoIP. Convirtiéndose así en el mejor, más completo, avanzado y económico sistema de comunicaciones existente en la actualidad.

Otra de sus mejoras es su capacidad de ser programada, logrando realizar labores que hasta el día de hoy lo llevaban efectuando sistemas extremadamente costosos y complicados y, gracias a Asterisk, esta misma labor se realiza de una forma más económica lo que fomenta el uso de sistemas libres como Linux y estándares abiertos como SIP, H323 o IAX. (11)

Una de las ventajas más interesantes es su posibilidad como sistema híbrido, ya que permite gestionar comunicaciones telefónicas tradicionales (analógicas, digitales, móviles, etc.) como comunicaciones IP mediante el uso de los protocolos estándares de VoIP.

Proporciona además adaptabilidad a los usuarios, permitiendo que los mismo implementen nuevas funcionalidades creando un nuevo plan de marcado (dialplan) en el lenguaje script de Asterisk o agregando un nuevo módulo en algún lenguaje de programación soportado por GNU/Linux, además tiene funcionalidades solo presente en PBX privadas como buzón de voz, conferencia, respuesta de voz interactiva (IVR), distribución automáticas de llamadas, entre otras.

1.6.2. FreeSwitch

Es una aplicación software libre bajo la licencia de MPL (del inglés ***M**ozilla **P**ublic **L**icense*), clasificada como un softswitch[1] de bajo costo, pero se puede implantar como una PBX. Es multiplataforma y permita conexión con los protocolos de VoIP, SIP, H.323, IAX2, Google Talk, entre otros. Además brida servicio de conferencia altamente estable y de múltiples velocidades de muestreo, también llamadas de alta definición, video y mensajería instantánea. Presenta desventajas ya que su

[1] Dispositivo encargado de controlar, procesar llamadas, entre otros servicios, sobre una red de conmutación de llamadas

configuración es en XML, su documentación se encuentra en inglés y la comunidad hispana es pobre, aunque es muy estable, escalable y extensible. (12)

1.6.3. Yate

Al igual que los dos ejemplos anteriormente descritos, Yate es código abierto basado en la licencia pública general GPL, pero a diferencia de Asterisk, fue desarrollado en C++. Esto trae consigo que sea un poco difícil de compilar tanto el Linux como en Windows. Se puede encontrar en Yate un motor impulsor con gran alcance en la telefonía fácilmente aplicable que incluye voz, video, datos y mensajería instantánea, todo unido a un motor de enrutamiento flexible. Esta PBX aunque está escrito en C++ es compatible con pequeñas secuencias de otros lenguajes de desarrollo como Perl, PHP, Python con el objetivo de facilitar el desarrollo de funcionalidades externas.

1.7. Herramientas para el monitoreo de red

Antiguamente, cuando no se disponía de las herramientas y las tecnologías que hoy existen para el monitoreo de redes, era necesario que una persona, generalmente el administrador de red, supervisara constantemente el estado de las computadoras, servicios y de la red en general, esto trae consigo que una parte del día dichos elementos no fueran chequeados, trayendo problemas a la entidad. Precisamente esto una de las principales ventajas que poseen estas aplicaciones, monitoreo las 24 horas del día, además de una serie de características que las distinguen a unas de otras.

Tras un estudio realizado de las principales herramientas de código abierto utilizadas en el mundo para el cumplimiento a esta labor, se exponen a continuación las de mayor aceptación para la investigación en curso.

1.7.1. Nagios

Es una herramienta de código abierto bajo la licencia GPL, útil en la monitorización de servicios y host de redes tanto locales como remotas. Está implementado en lenguaje C y ofrece conocer en cada momento qué ordenadores y dispositivos están activos, cuáles no, cuáles están fallando, cuáles funcionan correctamente, qué servicios funcionan correctamente y cuáles no; en definitiva, sirve para cuestionar el estado en tiempo real de una red, sea grande o pequeña. (13)

Entre sus principales características se encuentran: monitoreo de servicios de red (SMTP, POP3, HTTP, NNTP, PING, etc.), monitoreo de recursos de equipos (carga en el procesador, uso de disco duro, etc), diseño simple de plugins permitiendo a los usuarios un desarrollo fácil de sus propias verificaciones de servicios, monitorización remota a través de túneles SSL cifrados o SSH y la habilidad de definir una jerarquía de los equipos de la red. Otra de las características es que envía notificaciones a contactos cuando un servicio o equipo presenta problemas y necesita resolverse vía email o método definido por el propio usuario. También posibilita soporte para implementar equipos redundantes para monitoreo, interfaz web opcional para ver el estado actual de la red, notificaciones, historial de problemas, archivo log, etc. Un aspecto negativo que este tiene es que se puede hacer muy compleja su instalación y manejo. (13)

1.7.2. Cacti

Es una solución completa para la monitorización de redes diseñada para aprovechar el poder de almacenamiento y la funcionalidad de graficar que poseen las RRDtool. Proporciona un esquema rápido de obtención de datos remotos, múltiples métodos de obtención de datos, un manejo avanzado de creación de plantillas, gráficos y una completa interfaz de gestión de usuarios. Además ofrece un servicio de alarmas mediante el manejo de umbrales, todo ello en una sola consola de administración fácil de configurar.

Su instalación no es realmente compleja, lo que lo hace uno de los sistemas más completos de código abierto publicado bajo la licencia GNU GPL. Esta herramienta está implementada en PHP (***P****HP* ***H****ypertext* ***P****re-processor*) y utiliza MySql para el almacenamiento de información sobre los gráficos y datos recogidos, utilizando el protocolo SNMP para la comunicación con los distintos equipos.

1.7.3. Munin

Otro de los programas que nos permiten monitorizar una o varias computadoras es Munin, herramienta de monitorización de servidores y host pertenecientes a una red de computadoras que genera estadísticas sobre el funcionamiento de los mismos tales como, memoria, disco duro y servicios. Utiliza las herramientas RRDTool para generar gráficas de rendimiento de los parámetros

del sistema analizados. Utiliza una interfaz web para mostrar las gráficas generadas permitiendo visualizar la información de varios servidores y de esta manera trabajar de forma distribuida. (14)

Dicha aplicación está implementada con el lenguaje de programación Perl y admite la incorporación de plugins para aumentar su funcionalidad, lo cual lo hace realmente versátil. Pero posee la dificultad de recolectar información sin previa autenticación en la interfaz web permitiendo el acceso a la información sensible o confidencial que se maneja por la red.

1.8. Conclusiones

En este capítulo se realizó un estudio de los conceptos fundamentales entorno al monitoreo de redes de cómputo. Se abordaron temas tales como: las herramientas libres más utilizadas en el mundo para monitorear elementos de una red, los principales protocolos VoIP, así como las características de algunas de las PBX basadas en software. Es válido destacar que de las herramientas descritas Nagios ofrece funcionalidades de interés para el propósito de este trabajo.

CAPÍTULO 2: PROCESO DE INSTALACIÓN Y CONFIGURACIÓN.

2.1. Introducción

En el presente capítulo se describe la estructura de la herramienta Nagios. Se detallan los requisitos necesarios para establecer la misma así como el procedimiento que se debe llevar a cabo para su instalación y puesta en marcha. Quedan plasmados además los elementos y archivos a tener en cuenta para realizar la configuración de las diferentes herramientas utilizadas.

2.2. Análisis de selección de Software

Para seleccionar la herramienta de monitoreo a utilizar en la investigación se hizo necesario establecer parámetros técnicos generales y específicos que sirvieran de apoyo en la elección, estos son detallados en las Tabla 1 yTABLA **2**.

Descripciones	Cacti	Munin	Nagios
Interfaz Web	x	x	x
Alertas y notificaciones			x
Basta información en la red	x		x
Flexible a plugins	x	x	x
Escalable	x	x	x
Complejidad en instalación y configuración			x
Reportes			x
Autenticación de usuarios	x		x
Usado para redes locales	x	x	x
Usado para redes empresariales			x
Licencia libre	x	x	x
Potente			x
Facil de usar	x	x	x
Orientado a VoIP			x

Tabla 1. *Indicación general.*

Como se puede observar Nagios cumple con todos los aspectos mostrados en la primera tabla, siendo Alertas y Notificaciones y Orientado a VoIP las de mayor peso para la elección. Otro aspecto que influyó es la Licencia libre aunque en este caso las tres herramientas la cumplen, publicadas bajo la GNU/GPL.

Descripciones	Cacti	Munin	Nagios
Grado de dificultad(fácil= 1, medio= 2, difícil= 3)			
Manejo de la interfaz Web	1	1	1
Instalación	1	1	2
Configuración	2	2	3
Implementado en una red local	1	1	1
Implementado en una red empresarial	2	3	2
Información en internet	2	3	1
Grado de características funcionales(muy bueno= 1, bueno= 2, regular= 3)			
Alertas y notificaciones	3	2	1
Versatilidad	3	3	1
Potente	3	2	1
Robusto	2	3	1
Escalable	2	3	1
Flexibilidad	3	2	1
Grado de características para el negocio(si=1, no=0)			
Licencia libre	1	1	1
Orientado a VoIP	0	0	1

Tabla 2. *Indicaciones cuantificables*

Estudios realizados en la Dirección de Redes y Seguridad Informática de la Universidad de las Ciencias Informáticas (UCI), revelaron que la herramienta que se utiliza para monitorear los servidores del nodo central, hace más de 4 años, es precisamente Nagios. Según Eduar Palomo Gené, especialista general en el área, esta herramienta es muy potente, flexible, consume poco recursos y gracias a su condición de código abierto se le puede incluir funcionalidades que se necesiten y no estén programadas.

2.3. Estructura de Nagios

Con Nagios se puede saber en todo momento el estado en el que se encuentran las computadoras y los dispositivos de la red, si están encendido o apagados, cuales están fallando, como se encuentra el estado de los elementos de hardware, cuáles servicios están funcionando correctamente y cuáles no. Se utiliza para tener conocimiento en tiempo real de todo aquello que pueda ser monitoreado en una red. Esto es posible porque presenta una arquitectura muy simple y muy adaptable, por lo que es fácil de escribir plugin en cualquier lenguaje de programación posibilitando agregarle funcionalidades según la necesidad del usuario que lo esté utilizando. Además no se puede omitir que su configuración es poco amigable ya que todo se hace escribiendo de forma manual en los ficheros de configuración y por lo tanto necesita de usuarios avanzados para realizar estas operaciones.

En la siguiente tabla se visualizan las rutas de acceso a los diferentes directorios en los que se encuentra estructurada la herramienta Nagios.

Directorios	**Descripción**
/usr/local/nagios/bin/	Ejecutable principal de Nagios
/usr/local/nagios/etc/	Ficheros de configuración.
/usr/local/nagios/sbin/	CGIs
/usr/local/nagios/share/	Ficheros HTML del interfaz web y documentación.
/usr/local/nagios/var/	Directorio vacío para logs, etc.
/usr/local/nagios/libexec/	Plugins, ejecutables que realizan los chequeos.

Tabla 3. *Rutas de acceso a directorios*

2.4. Requisitos para la instalación

Para que la herramienta sea instalada correctamente se hace necesario tener en cuenta los siguientes requisitos:

- Tener una PC (***P****ersonal* ***C****omputer*) ejecutando Linux o una variante de Unix y un compilador de C.

- Un servidor web (preferiblemente Apache 2).
- Instalar las librerías de desarrollo y compilación GCC.
- Instalar las librerías de desarrollo GD
- Disponer de los lenguajes de programación Perl y Python.

2.5. Instalación y puesta en marcha

Antes de iniciar la instalación de la herramienta se debe realizar las siguientes acciones:

1. Crear un usuario con el nombre: nagios.
   useradd –m nagios

2. Generar el grupo nagcmd para permitir el envío de comandos desde la consola y agregar los usuarios nagios y apache.
   groupadd nagcmd

   usermod –a –G nagcmd nagios

   usermod –a –G nagcmd apache

3. Crear una carpeta donde se descargará Nagios.
   mkdir /opt/nagios

4. Descargar dentro de la carpeta creada el código fuente de:
   - Nagios Core 3.2.0

   wget http://prdownloads.sourceforge.net/sourceforge/nagios/nagios-3.2.0.tar.gz

   - Nagios Plugins 1.4.14

   wget http://prdownloads.sourceforge.net/sourceforge/nagiosplug/nagios-plugins-1.4.14.tar.gz

   - Nagios nrpe 2.12 (esto servirá para monitorea PC y servidores remotos).

wget http://prdownloads.sourceforge.net/sourceforge/nagios/nrpe-2.12.tar.gz

5. Una vez realizada las acciones anteriores se procede a la descompresión de Nagios.
   cd /opt/nagios

   tar xzf nagios-3.2.0.tar.gz

   cd nagios-3.2.0

Ahora se está en condiciones de comenzar con la instalación de la herramienta.

6. Se configura y compila
   ./configure –with-command-group=nagcmd

   make all

   make install

   make install-init

   make install-config

   make install-commandmode

7. Con la realización de esta acción Nagios queda instalado en /usr/local/nagios pero se debe proseguir con la instalación de la interfaz Web y la creación del usuario Admin con su respectiva contraseña.
   cd /opt/nagios/nagios-3.2.0

   make install-webconf

   htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin

   service httpd restart

No se debe olvidar la contraseña que especificó ya que la requerirá para ingresar a la interfaz web.

8. Se descomprime Nagios Plugins para proceder con su instalación y configuración.
   cd /opt/nagios

tar xzf nagios-plugins-1.4.14.tar.gz

cd nagios-plugins-1.4.14

9. Se instala y se configura.
   ./configure --with-nagios-user=nagios --with-nagios-group=nagios

   make

   make install

10. Se verifican los archivos de configuración.
    /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg

Si no surgiera ningún error se debe mostrar en la consola la siguiente salida:

Total Warnings: 0

Total Errors: 0

11. Posteriormente se le permite a Nagios y al Apache que inicien cada vez que se inicie el sistema operativo.
    chkconfig --add nagios

    chkconfig nagios on

    chkconfig httpd on

12. Y como último paso se inicia Nagios.
    service nagios start

Una vez ejecutados todas estas acciones se tiene la herramienta instalada y funcionando. Para poder ingresar al portal de Nagios debe utilizar la dirección http://dirección-servidor/nagios autenticarse con el usuario nagiosadmin y la contraseña que se le fue asignada en pasos anteriores.

Para buscar las versiones estables más recientes se puede visitar el sitio oficial de Nagios en la siguiente dirección:

http://www.nagios.org/download/download.php

2.6. Instalación del demonio NRPE

2.6.1. En el servidor de monitoreo

Con la instalación del demonio NRPE (***N****agios* ***R****emote* ***P****lugin* ***E****xecutor*) se puede extender la funcionalidad de Nagios. Como bien indica su nombre permite que Nagios ejecute plugins en equipos remotos, principalmente en host que tengan instalado como sistema operativo GNU/Linux.

Para realizar dicha instalación se debe auxiliar de las siguientes acciones:

1. Primeramente se descomprime el archivo nrpe-2.12 que fue descargado con anterioridad.
   cd /opt/nagios

   tar xzf nrpe-2.12.tar.gz

   cd nrpe-2.12

2. Luego se configura y compila el archivo nrpe.
   ./configure

   make all

   make install-plugin

3. El siguiente paso a ejecutar es comprobar la comunicación del demonio NRPE con el servidor de Nagios.
   /usr/local/nagios/libexec/check_nrpe -H <ip-servidor>

Una vez ejecutada esa línea se debe obtener como salida:

NRPE v2.12

En caso de no obtener dicha salida debemos revisar lo siguiente:

- Verificar que ningún firewall este bloqueando la comunicación entre ambos servidores.

- Verificar que el demonio NRPE este funcionando correctamente en el servidor a monitorizar.
- Asegúrese que el servidor a monitorizar no tenga tablas IP que bloquen el tráfico de entrada o salida.

4. Por último se edita el archivo /usr/local/nagios/etc/object/commands.cfg para poder usar el plugin.
   vi /usr/local/nagios/etc/object/commands.cfg

   define command{

   command_name check_nrpe

   command_line $USER1$/check_nrpe -H $HOSTADDRESS$ -c $ARG1$

   }

2.6.2. En los host remotos

Para realizar la ejecución de la instalación del demonio NRPE se debe usar los plugins que se utilizaron al instalar el servidor de Nagios.

1. Primeramente se crea un usuario nagios y para esto debe autenticarse como usuario root en la consola.
   /usr/sbin/useradd nagios

   passwd nagios

2. Se crea una carpeta donde se descargara y descomprimirá los plugins de Nagios.
   mkdir /opt/nagios

   cd /opt/nagios

   wget http://prdownloads.sourceforge.net/sourceforge/nagiosplug/nagios-plugins-1.4.14.tar.gz

tar xzf nagios-plugins-1.4.14.tar.gz

3. Seguidamente se configuran e instalan dichos plugins.
   cd nagios-plugins-1.4.14

   ./configure

   make

   make install

4. Se le cambian los permisos al usuario nagios con contraseña nagios.
   chown nagios.nagios /usr/local/nagios

   chown –R nagios.nagios /usr/local/nagios/libexec

5. Se instala el paquete xinetd.
   apt-get install xinetd

6. Se descarga y descomprime el demonio NRPE.
   cd /opt/nagios

   wget http://prdownloads.sourceforge.net/sourceforge/nagios/nrpe-2.12.tar.gz

   tar xzf nrpe-2.12.tar.gz

   cd nrpe-2.12

7. Se compila e instala el demonio NRPE.
   ./configure

   make all

   make install-plugin

   make install-daemon

   make install-daemon-config

8. Seguidamente se instala el demonio como un servicio en Xinetd.
   make install-xinetd

9. Se edita el archivo /etc/xinetd.d/nrpe para agregar el ip del servidor Nagios.
   gedit /etc/xinetd.d/nrpe

   only_from = <dirección-servidor-nagios>

10. Se edita el archivo /usr/local/nagios/etc/nrpe.cfg para agregar el ip del servidor Nagios.

    gedit /usr/local/nagios/etc/nrpe.cfg
    server_address = <dirección-servidor-nagios>
    allowed_hosts = <dirección-servidor-nagios>

11. Se le agrega la siguiente línea al demonio NRPE en el archivo /etc/services.

    gedit /etc/services

    nrpe 5666/tcp # NRPE

12. Se reinicia Xinetd.

    service xinetd restart

13. Seguidamente se comprueba el demonio NRPE localmente.
    netstat -at | grep nrpe

Se debe obtener como resultado en la consola:

tcp 0 0 *:nrpe *:* LISTEN

En caso de no obtener este resultado se revisará lo siguiente:

- Si se agregó correctamente la entrada en el archivo /etc/services.
- Si en la línea only_from del archivo /etc/xinetd.d/nrpe todavía contiene 127.0.0.1.
- Si Xinetd está correctamente instalado y corriendo.

Para verificar que el demonio NRPE se instaló correctamente se utilizará el plugin check_nrpe ubicado en /usr/local/nagios/libexec.

/usr/local/nagios/libexec/check_nrpe -H localhost

Con la ejecución de esta línea se debe obtener el siguiente resultado en la consola.

NRPE v2.12

Hasta el momento se tiene instalado completamente la herramienta Nagios, el NRPE Cliente y NRPE Servidor, solo queda la instalación del plugin para la monitorización del Asterisk.

2.7. Instalación de NSClient++

Antes de comenzar a controlar los servicios y los atributos privados de las computadoras con sistema operativo Windows, se tendrá que instalar un agente en esos ordenadores. Se recomienda usar el addon NSClient++, que se puede encontrar en http://sourceforge.net/projects/nscplus. A continuación se enumeran las instrucciones que guiarán al lector a través de una instalación básica del complemento NSClient++, así como la configuración de Nagios para el control de estas PCs.

1. Descargar la última versión estable del complemento NSClient++ desde la dirección http://sourceforge.net/projects/nscplus.
2. Descomprimir el archivo NSClient++ en una nueva C:\NSClient o en cualquier otra dirección que se desee.
3. Abrir el intérprete de comandos de Windows e introducirse en la dirección C:\NSClient++ o donde se descomprimió la aplicación.
4. Se registra el servicio NSClient++ en el sistema mediante esta línea de comando.

nsclient++ /install

5. Instalar el servicio en la bandeja del sistema distinguiendo mayúsculas y minúsculas.

nsclient++ /install SysTray

6. Abrir el administrador de servicios y asegurarse de que el servicio NSClient++ se le permite interactuar con el escritorio. Véase la siguiente ilustración.

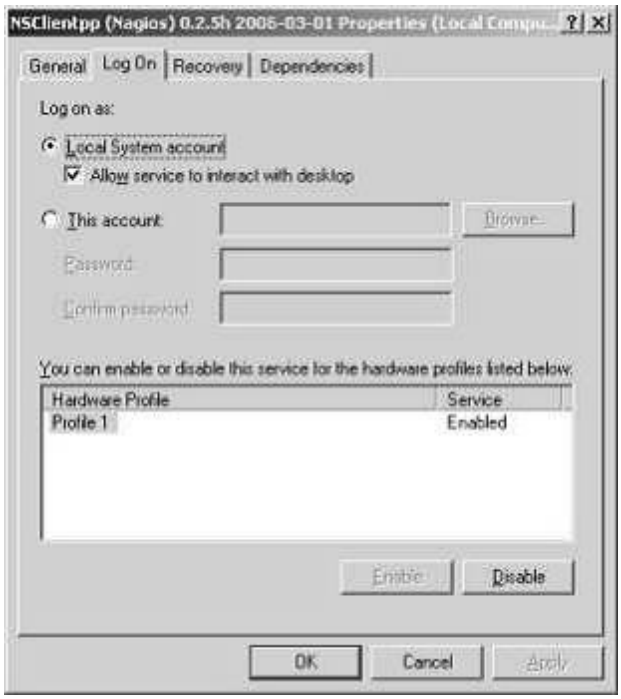

ILUSTRACIÓN 1 PROPIEDADES DEL SERVICIO NSCLIENT++

7. Editar el archivo nsc.ini localizado en el directorio C:\NSClient++ y realizar los cambios que se describen a continuación.

- Eliminar los cometarios a todos los archivos con extensión .dll excepto a los archivos CheckWMI.dll y RemoteConfiguration.dll en la sección [modules].
- Eliminar el comentario a la opción *allowed_hosts* en ubicada en la sección [Settings] y adicionarle la dirección IP del servidor de Nagios.
- Asegurarse que la opción *port* en la sección [NSClient] no esté comentada y tenga el valor 12489 que es el puerto por donde serán controladas la PCs de Windows.
- Iniciar el servicio NSClient++ con el siguiente comando.

nsclient++ /start

Una vez cumplidas todas estas instrucciones se tiene instalada la aplicación que permitirá controlar los ordenadores en los cuales tengan instalados con sistema operativo Windows en conjunto con sus servicios y atributos.

2.8. Instalación de Nagisk

Nagisk no es más que un *script* sencillo implementado con el lenguaje de programación Perl con el objetivo de supervisar el servidor Asterisk. Con este *script* se puede tener el control sobre llamadas concurrentes, los canales que están activos, los protocolos que se están utilizando, los que puedan fallar en determinado momento, así como cuáles de estos son más confiables.

- Se descarga el Nagisk en el servidor Asterisk donde se encuentra el demonio NRPE.

cd /opt/nagios
wget http://prdownloads.sourceforge.net/sourceforge/nagisk/nagisk-1.1.1.tgz

- Se descomprime y se copia el archivo para el fichero libexec.

tar zxvf nagisk-1.1.1.tgz

cd nagisk

cp nagisk.pl /usr/local/Nagios/libexec

- Se le cambian los permisos de dicho archivo

chown nagios.nagios /usr/local/nagios/libexec/nagisk.pl

chown 750 /usr/local/nagios/libexec/nagisk.pl

- Se modifica el archivo /etc/sudoers agregando la siguiente línea.

nagios ALL=NOPASSWD:/urs/sbin/asterisk

Nota: *Este archivo es solo lectura, se debe modificar los permisos de escritura.*

- Según lo que se desee monitorear se modifica el archivo /usr/local/nagios/etc/nrpe.cfg agregándole cualquiera de estas líneas.

command[check_asterisk_version]=/usr/local/nagios/libexec/nagisk.pl –c version

command[check_asterisk_peers]=/usr/local/nagios/libexec/nagisk.pl –c peers

command[check_asterisk_channels]=/usr/local/nagios/libexec/nagisk.pl –c channels

command[check_asterisk_zaptel]=/usr/local/nagios/libexec/nagisk.pl –c dahdi

command[check_asterisk_span]=/usr/local/nagios/libexec/nagisk.pl –c span –s 1

- Al finalizar se reinicia el servicio NRPE

/etc/init.d/xinetd restart

La instalación está completa, solo queda ajustar los archivos de configuración.

2.9. Procedimientos para la configuración de Nagios

Para una configuración simple solo se necesita modificar algunos archivos de configuración (extensión .cfg). En este ejemplo se dividirá la configuración en dos partes, el archivo de configuración general de Nagios y los archivos de configuración de equipos, switch, routers, contactos.

1. Se crea un nuevo directorio que se nombrará elastix o se puede nombrar como se desee.

mkdir /usr/local/nagios/etc/elastix

2. Se accede con el editor de texto preferido al archivo nagios.cfg

gedit /usr/local/nagios/etc/nagios.cfg

3. Se busca la sección

 # You can also tell Nagios to process all config files…..

4. Se agrega la siguiente línea.

cfg_dir=/usr/local/nagios/etc/elastix

5. Se crea un archivo en la dirección /usr/local/nagios/etc/elastix que se nombrará *server.cfg* para definir los nuevos host a monitorizar.

gedit /usr/local/nagios/etc/elastix/server.cfg

6. Se agregan las siguientes definiciones de los nuevos host.

Define host{

use	**elastix**	**; el nombre del template a utilizar**
host_name	**PC1**	**; nombre para identificar el equipo**
alias	**alias_PC1**	**; el alias del equipo**
address	**10.23.45.241**	**; ip o el nombre del equipo**

}

Define host{

use	**elastix**	**; el nombre del template a utilizar**
host_name	**PC2**	**; nombre para identificar el equipo**
alias	**alias_PC2**	**; el alias del equipo**
address	**10.23.45.242**	**; ip o el nombre del equipo**

}

7. Se crea un archivo en la dirección /usr/local/nagios/etc/elastix que se nombrará *servicios.cfg* para definir los nuevos host a monitorizar.

gedit /usr/local/nagios/etc/elastix/servicios.cfg

8. Se agregan las siguientes definiciones de los nuevos servicios para los host ya definidos.

Define service{

use	**generic-service**	**;nombre del template por defecto.**
host_name	**PC1,PC2**	**;nombre de los equipos a monitorear.**

service_description Carga del CPU ;descripción del servicio.

check_command check_nrpe!check_load ;nombre del comando.

}

Define service{

use generic-service ;nombre del template por defecto.

host_name PC1,PC2 ;nombre de los equipos a monitorear.

service_description Usuarios logueados ;descripción del servicio.

check_command check_nrpe!check_users ;nombre del comando.

}

Define service{

use generic-service ;nombre del template por defecto.

host_name PC1,PC2 ;nombre de los equipos a monitorear.

service_description Espacio libre del disco ;descripción del servicio.

check_command check_nrpe!check_hda1 ;nombre del comando.

}

Define service{

use generic-service ;nombre del template por defecto.

host_name PC1,PC2 ;nombre de los equipos a monitorear.

service_description Estado de la swap ;descripción del servicio.

check_command check_nrpe!check_swap ;nombre del comando.

}

9. Se crea un archivo en la dirección /usr/local/nagios/etc/elastix que se denominará *elastixTemplate.cfg* para definir los nuevos host a monitorizar.

gedit /usr/local/nagios/etc/elastix/elastixTemplate.cfg

10. Se agrega la siguiente definición de la nueva plantilla para los host ya definidos.

define host{

name elastix ;nombre del template

use generic_host ;nombre del template por defecto

check_period 24x7 ;nombre del periodo de tiempo

check_interval 5 ;intervalo de chequeo dado un minutos

retry_interval 1 ;intervalo de chequeo cuando falla un host

max_check_attempts 10 ;cantidad de intentos de chequeo

check_command check-host-alive ;nombre del comando

notification_period 24x7 ;período de tiempo para enviar las notificaciones

notification_interval 30 ;intervalo de notificaciones dado un minutos

notification_options d,r ;opciones de notificación

contacs_groups admins ;grupo de contactos a los que se enviarán las notificaciones

register 0 ;no registrarlo es una template.

}

11. Verificar la configuración de los archivos modificados para asegurar que todo está correctamente.

/usr/local/nagios/bin/nagios –v /usr/local/nagios/etc/nagios.cfg

12. Reiniciar Nagios

/etc/init.d/nagios restart

2.10.Configuración avanzada de Nagios.

Se puede realizar pequeños ajustes a conveniencia del administrador de la red, para enviar alertas si fallan algunos de los parámetros personalizados.

1. En el equipo remoto accedemos al archivo /usr/local/nagios/etc/nrpe.cfg y modificaran las siguientes líneas.

   gedit /usr/local/nagios/etc/nrpe.cfg

   command[check_swap]=/usr/local/nagios/libexec/check_swap –w 20% -c 10%

Nota: en este caso si llega al 20% se emitirá una alerta y al 10% una alerta crítica.

2. Para Asterisk se puede adicionar estos comandos mencionados anteriormente y para los servicios que brinda el servidor se agregan las siguientes líneas.

   command[check_asterisk_version]=/usr/local/nagios/libexec/nagisk.pl –c version

   command[check_asterisk_peers]=/usr/local/nagios/libexec/nagisk.pl –c peers

3. En el server de monitoreo se agregan las siguientes definiciones:

   Define service {

   use generic-service ;nombre del template por defecto.

   host_name PC1 ;nombre de los equipos a monitorear.

service_description Chequear versión SIP ;descripción del servicio.

check_command check_nrpe!check_asterisk_version ;nombre del comando.

}

Define service {

use generic-service ;nombre del template por defecto.

host_name PC1 ; nombre de los equipos a monitorear.

service_description Chequear peers SIP ; descripción del servicio.

check_command check_nrpe!check_asterisk_peers ;nombre del comando.

}

4. Se comprueba la modificación verificando que no existan errores.

/usr/local/nagios/bin/nagios –v /usr/local/nagios/etc/nagios.cfg

5. Reiniciar Nagios

/etc/init.d/nagios restart

Hasta el momento se tiene la herramienta Nagios instalada y configurada para el monitoreo de los servidores, host remotos, switch, Asterisk, entre otros, con los servicios personalizados. Existe un grupo de archivos de configuración que presenta Nagios que están en la dirección /usr/local/nagios/etc/objetc/, que se pueden utilizar como guía para un mayor entendimiento y así aumentar la calidad de la configuración de la herramienta.

Una de las grandes ventajas que presenta Nagios es que tiene gran flexibilidad teniendo en cuenta el envío de alertas, ya que puede remitir alertas por casi cualquier vía, correo, jabber, SMS. Un ejemplo de configuración para correo se muestra a continuación:

define contact{

```
        contact_name        Makay           ;nombre corto del contacto
        use             generic-contact     ;utilizar template por defecto de contact
        alias           Nagios Admin        ;nombre completo del contacto
        email       correo@electronico.com  ;dirección de correo
    }
define contact{
        contact_name        Raymon          ;nombre corto del contacto
        use             generic-contact     ;utilizar template por defecto de contact
        alias           Nagios Admin        ;nombre completo del contacto
        email       correo@electronico.com  ;dirección de correo
    }
```

En caso de que existan más de un contacto se puede lograr una mejor organización creando un grupo de contactos definido de la siguiente forma:

```
define contactgroup{
        contactgroup_name   admins      ;nombre pequeño del grupo de contactos.
        alias           Nagios Administrators       ;el alias de grupo de contactos.
        members   Makay, Raymon   ;los nombres de los contactos separados por “,”.
    }
```

Es válido señalar que cuando se define un servicio o un host se pueden encontrar las variables llamadas *contact_groups* y *contact* que se le debe poner el mismo nombre que la variable *contactgroup_name* definida en el grupo de contactos y la variable *contact_name* establecida en la definición de los contactos respectivamente, según como le defina el administrador.

Siempre que realice una modificación el los ficheros de Nagios, compruebe que no existan errores. Todo está listo para un perfecto funcionamiento de la herramienta.

2.11. Instalación del demonio NDOUtils

NDOUtils (***N****agios* ***D****ata* ***O****utput Utils*) es un demonio diseñado para almacenar toda la configuración e información obtenida por Nagios en una base datos. Al ofrecer esta posibilidad de almacenamiento de datos permite una rápida recuperación del sistema en caso de la existencia de algún fallo y el procesamiento óptimo de los datos recogidos, además de ayudar al desarrollo de una nueva interfaz web en el futuro. Este demonio está concebido para trabajar con los gestores de base de datos MySQL y PostgreSQL. Actualmente solo las bases de datos MySQL son soportadas por dicho agente pues el soporte para Postgre está en desarrollo.

Antes de comenzar con la instalación se debe tener ejecutando Nagios 2.0 versión estable para conseguir que este agente funcione como es debido porque no es compatible con Nagios 2.0 beta. NDOUtils también trabaja bajo las actualizaciones 2.x en lo adelante así como con las versiones 3.x.

Para obtener el addon NDOUtils y las versiones estables de Nagios puede visitar el sitio oficial de la herramienta en las siguientes direcciones respectivamente:
http://www.nagios.org/download/addons

http://www.nagios.org/download/core/thanks

2.11.1. Requisitos.

Antes de comenzar con la instalación del addon es preciso instalar el gestor MySQL así como otros paquetes necesarios para su instalación.

- Nagios

- El gestor de base de datos MySQL
- Herramienta de administración de base de datos phpMyAdmin

Este último no es obligatorio instalarlo pero sí ayuda a las personas encargadas del manejo de dicho gestor a alcanzar un mejor entendimiento de la información almacenada.

1. Después de la instalación de estos paquetes se debe verificar el funcionamiento del gestor de base de datos MySQL introduciendo en la consola el siguiente comando.

   ps -ef | grep mysql

2. Luego se crea un usuario y la base de datos donde NDO escribirá las tablas y los datos que proceden de Nagios en el servidor MySQL. En este caso se creará la base de datos nagiosdb, el usuario nagios con contraseña contrase_nagios.

   mysql -u root –p
   (Contraseña de root para MySQL)

Si el usuario root no tiene asignada una contraseña en el gestor de base de datos se puede obviar el comando –p

Una vez realizado este procedimiento se accede al gestor desde la consola.
(Dentro del MySQL)

3. Se crea la base de datos nombrada nagiosdb con la siguiente línea.

   mysql>**create database nagiosdb;**

Si no existe ningún problema a la hora de crear la base de datos mostrara dicho resultado.

Query OK, 1 row affected (0.00 sec)

4. Más adelante se crea un usuario en la base de datos llamada nagiosdb identificado con la contraseña contrase_nagios.
   mysql>**CREATE USER nagios@IP_SERVIDOR_NAGIOS**
   IDENTIFIED BY ' contrase_nagios ';

5. En esta ocasión se le permite al usuario nagios que no tenga restricciones a la hora de conectarse con la base de datos.

   mysql>**GRANT USAGE ON *.* TO nagios@IP_SERVIDOR_NAGIOS**
   IDENTIFIED BY ' contrase_nagios '
   WITH MAX_QUERIES_PER_HOUR 0
   MAX_CONNECTIONS_PER_HOUR 0
   MAX_UPDATES_PER_HOUR 0
   MAX_USER_CONNECTIONS 0;

6. Ahora se le cede a este usuario todos los privilegios sobre la base de datos nagiosdb.

   mysql>**GRANT ALL PRIVILEGES**
   ON nagiosdb.*
   TO nagios@IP_SERVIDOR_NAGIOS
   WITH GRANT OPTION ;

7. En este paso se actualizan los privilegios asignado al usuario creado, de lo contrario si no se ejecuta esta línea se tiene que reiniciar el servidor de base de datos.

   mysql>**flush privileges;**

8. Se verifica si la base de datos nagios fue creada satisfactoriamente.

```
mysql>show databases;
+----------+
| Database |
+----------+
| database |
| mysql    |
| nagios   |
| test     |
+----------+
4 rows in set (0.01 sec)
```

9. Como ultima acción se sale de la consola del MySQL.

```
mysql> quit
```

10. Posteriormente de realizados las acciones anteriores se procede a descargar el paquete ndoutils-1.4b8.

cd /opt/nagios
wget -c http://downloads.sourceforge.net/nagios/ndoutils-1.4b8.tar.gz

11. Se descomprime el paquete.

tar xzvf ndoutils-1.4b8.tar.gz

No es muy frecuente encontrar el comando "make install", se debe hacer la instalación manualmente con un par de componentes, pero no es complicado. Existen dos versiones de ndomod.o módulo NEB (***N****agios* ***E****vent* ***B****roker*) y demonio ndo2db a compilar. Uno para las versiones 2.x y el otro para las 3.x de Nagios.

Para trabajar con Nagios 2.x se deben utilizar los componentes ndomod-2.x.o y ndo2db-2x o si se va laborar con las versiones 3.x corresponde a utilizar los addon ndomod-3x.o y ndo2db-3x.

12. Se compila programa el paquete descomprimido.

    cd /opt/nagios/ndoutils-1.4b8
    ./configure --prefix=/usr/local/nagios --enable-mysql --with-mysql-lib=/usr/lib/mysql
    make

13. Se copian los ejecutables.

    cp -f src/file2sock src/log2ndo src/ndo2db-* src/ndomod-* src/sockdebug /usr/local/nagios/bin/
    cp -p config/ndo2db.cfg /usr/local/nagios/etc/ndo2db.cfg
    cp -p config/ndomod.cfg /usr/local/nagios/etc/ndomod.cfg

En dependencia de la versión de la herramienta que el usuario tenga instalada copiará un ejecutable u otro. Para este ejemplo se usara la versión Nagios 3.

cp -f src/ndomod-3x.o /usr/local/nagios/bin/ndomod.o
cp -f src/ndo2db-3x /usr/local/nagios/bin/ndo2db

14. Ahora se crean las tablas y el modelo de datos en la base de datos:

    cd /opt/ndoutils-1.4b8/db

    ./installdb -u nagios -p contrasenagios -h IP_SERVIDOR_MYSQL -d nagiosdb

15. Se debe cambiar la configuración del NDO en el archivo /usr/local/nagios/etc/ndo2db.cfg y comprobar algunas de las variables como:

    tcp_port=5663

Con el objetivo de evitar problemas con otros plugins, por ejemplo de NRPE.
Indicar la IP del servidor MySQL.

db_host=IP_SERVIDOR_MYSQL

Verificar las credenciales de base de datos.

db_name=nagios_db
db_user=nagios
db_pass=contrase_nagios

Mantener los eventos durante 2 semanas, destacar que el valor de la variable **max_timedevents_age** está dado en minutos.

max_timedevents_age=20160

16. Para que el Nagios sepa donde tiene que buscar el corredor de eventos se tiene que configurar el archivo (/usr/local/nagios/etc/nagios.cfg).

    broker_module=/usr/local/nagios/bin/ndomod.0
    config_file=/usr/local/nagios/etc/ndomod.cfg

Hay que tener en cuenta que cuando se pone esta línea en el fichero nagios.cfg debe ser antes de la variable event_broker_options=-1 y además de ponerse todo consecutivo, sin “Enter”.

17. También se necesita configurar el puerto que debe escuchar el NDO se edita el fichero /usr/local/nagios/etc/ndomod.cfg o asegurarse que esta por ese puerto.

    tcp_port=5663

18. Crear el script de arranque del servicio NDO para iniciar el demonio cada vez que se encienda la computadora.
    cp -f /opt/nagios/ndoutils-1.4b8/daemon-init /etc/init.d/ndo2db
    chmod a+x /etc/init.d/ndo2db
    chkconfig ndo2db on
19. Y para terminar, se reiniciarán todos los servicios y se comprobará que las tablas empiezan a llenarse con nuevos datos.

    /etc/init.d/ndo2db stop
    /etc/init.d/ndo2db start
    /etc/init.d/nagios restart

Otra forma de terminar el proceso de instalación sin tener que configurar el script de arranque del servicio NDO.

/usr/local/nagios/sbin/ndo2db -c /usr/local/nagios/etc/ndo2db.cfg

Si al reiniciar el NDO2DB y se visualiza en la consola que el fichero ndo.sock está en uso, hay que borrarlo y volver al paso 19.
rm /usr/local/nagios/var/ndo.sock

2.12.Conclusiones

En el presente capítulo se exponen los aspectos esenciales que sirvieron de apoyo para la selección de la herramienta Nagios para el monitoreo de la plataforma Platel. Se explica paso a paso la instalación de esta, el procedimiento a seguir para su configuración y quedan plasmadas algunas notas que no deben ser obviadas. Además, se debe cumplir los requisitos descritos para lograr un funcionamiento adecuado de la misma.

CAPÍTULO 3: PROCESO DE PRUEBA

3.1. Introducción

En este capítulo se precisan los detalles de la puesta en marcha de la herramienta Nagios, mostrándose los resultados obtenidos en el proceso de prueba de la misma. Haciendo énfasis en el monitoreo de los elementos de hardware, servicios de red y en los protocolos VoIP. En fin se realiza un bosquejo de todos los servicios y dispositivos monitoreados.

3.2. Escenario de Pruebas

Las pruebas se llevaron a cabo en un total de diez ordenadores y dos switches, de ellos, cinco computadoras y un switch se encuentran en el laboratorio número cinco perteneciente al UCID, donde se está desarrollando el proyecto Platel. Los restantes ordenadores poseen la peculiaridad de ser servidores y están ubicados, uno en el nodo central del UCID junto al segundo switch y el otro en el nodo central de la UCI. Este laboratorio cuenta con un servidor de telefonía IP Asterisk y la herramienta Nagios instalada en uno de sus ordenadores.

De los cuatro ordenadores que funcionaban como clientes en el laboratorio del UCID, dos se instalaron con sistema operativo Windows y el resto con Linux, la otra computadora es el servidor Asterisk anteriormente mencionado, de esta forma se abarca la totalidad de los incidentes que se puedan presentar. En todas se hizo necesario instalarles agentes o demonios pues estos posibilitan ejecutar los plugin que necesita Nagios para obtener la información de los ordenadores remotos. Para las computadoras con sistema operativo Linux se les instaló el demonio NRPE y en las computadoras con Microsoft Windows como sistema operativo, el addon NSClient++ vistos en el capítulo anterior.

A continuación se muestra el mapa de los elementos de la red que se están analizando y monitoreando.

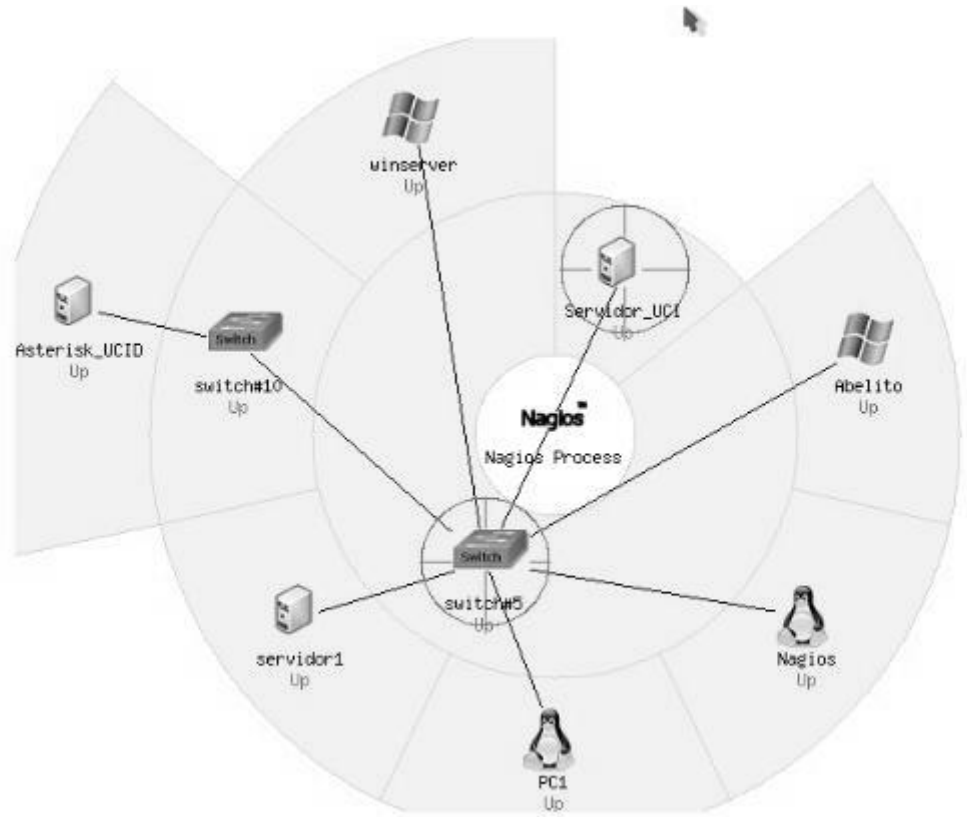

ILUSTRACIÓN 2 *MAPA DE LOS ELEMENTOS DE RED*

3.3. Monitoreo de los elementos

Como bien se ha indicado en capítulos precedentes, entre de las principales características de Nagios figuran la monitorización de servicios de red, de recursos de sistemas de hardware independientemente del sistema operativo que se esté utilizando. En esta sección se presentarán los resultados obtenidos con la utilización de esta aplicación.

3.3.1. Hardware

A todos los ordenadores donde se llevaron a cabo las pruebas se les monitoreo los elementos de hardware. Los que tenían como sistema operativo Windows se supervisó el espacio libre y utilizado de los discos, la carga del microprocesador, los porcientos del comportamiento de la memoria RAM. Adicionándose algunos de los procesos que están siendo ejecutados en por el ordenador como son:

el proceso Explorer.exe y Avp.exe en este caso el explorador de Windows y el antivirus Kaspersky respectivamente, además del tiempo que lleva encendido dicho equipo. El adecuado monitoreo y funcionamiento de todos estos parámetros se pueden observar en la siguiente Ilustración **3**.

Service	Status	Last Check	Duration	Attempt	Status Information
C:\ Drive Space	OK	05-18-2010 16:35:20	0d 1h 18m 40s	1/4	c: - total: 25,15 Gb - usado: 18,45 Gb (73%) - libre 6,70 Gb (27%)
CPU Load	OK	05-18-2010 16:35:20	0d 1h 20m 15s	1/4	Carga de la CPU 0% *1 promedio min)
D:\ Drive Space	OK	05-18-2010 16:35:24	0d 1h 19m 30s	1/4	d: - total: 93,46 Gb - usado: 88,20 Gb (94%) - libre 5,26 Gb (6%)
Memory Usage	OK	05-18-2010 16:35:20	0d 1h 20m 13s	1/4	UtilizaciÃ³n de memoria: total:1229,41 Mb - utilizado: 621,10 Mb (51%) - libre: 608,31 Mb (49%)
Explorer	OK	05-18-2010 16:35:20	0d 1h 18m 40s	1/4	Explorer.exe: Running
Kaspersky	OK	05-18-2010 16:35:20	0d 1h 18m 40s	1/4	avp.exe: Running
Uptime	OK	05-18-2010 16:35:20	0d 1h 18m 40s	1/4	System Uptime - 0 day(s) 5 hour(s) 58 minute(s)

ILUSTRACIÓN 3 *MONITOREO DE HARDAWARE EN WINDOWS*

Por otro lado las computadoras que tienen instalado Linux como sistema operativo se les chequeó la carga del microprocesador, el uso de la memoria RAM, de la memoria de intercambio (Swap), el espacio libre que presenta la partición del disco duro. Por último la cantidad de procesos que están siendo ejecutados por el ordenador. Para lograr una mayor comprensión sobre este tema se puede ver la Ilustración 4**Ilustración 4**.

Service	Status	Last Check	Duration	Attempt	Status Information
Carga del CPU	OK	05-18-2010 16:37:20	0d 17h 51m 26s	1/4	OK - carga media: 0.32, 0.23, 0.32
RAM++	OK	05-18-2010 16:37:24	0d 17h 49m 49s	1/4	OK - Memory usage is 40.0%
Uso de la Swap	OK	05-18-2010 16:37:20	0d 17h 51m 21s	1/4	SWAP OK - 88% free (847 MB out of 972 MB)
Root Partition	OK	05-18-2010 16:37:20	0d 17h 51m 15s	1/4	DISK OK - free space: /home 28344 MB (58% inode=94%):
Cantidad de Procesos	OK	05-18-2010 16:37:24	0d 15h 50m 43s	1/4	PROCS OK: 204 processes
Usuarios Loguedos	OK	05-18-2010 16:37:20	0d 17h 47m 56s	1/4	USERS OK - 1 users currently logged in

ILUSTRACIÓN 4 *MONITOREO DE HARDAWARE EN LINUX*

3.3.2. Servicios de Red

La utilidad de una red para los sistemas informáticos es precisamente que los usurarios puedan hacer un correcto uso de los recursos y de esta forma puedan gozar de las ventajas del uso de las redes en sus entornos de trabajo, como mayor facilidad de comunicación, mejora de la competitividad, mejora de la dinámica de grupo, entre otras. Esto solo es posible si la red presta una serie de servicios a sus usuarios. Servicios que están basados principalmente en la web y brinda una lista de disímiles vías para que los clientes puedan interactuar, como el chat, mensajería, correo electrónico, chat de voz, el uso compartido de archivos, blogs, grupos de discusión, tienda virtual, etc. En la Ilustración 5 se muestran los servicios supervisados en el escenario de prueba. De los mismos se muestra la información de su estado, duración, último momento en que fue chuequeado, entre otros.

Service	Status	Last Check	Duration	Attempt	Status Information
Servicio HTTP	OK	05-18-2010 16:37:20	0d 17h 48m 11s	1/4	HTTP OK: HTTP/1.1 200 OK - 376 bytes in 0,001 second response time
Servicio SSH	OK	05-18-2010 16:37:20	0d 15h 50m 33s	1/4	SSH OK - OpenSSH_5.1p1 Debian-5ubuntu1 (protocol 2.0)
PING	OK	05-18-2010 16:38:20	0d 0h 9m 10s	1/4	PING OK - Packet loss = 0%, RTA = 4.01 ms
POP3	OK	05-18-2010 16:37:20	0d 1h 22m 54s	1/4	POP OK - 0,008 second response time on port 110 [+OK POP3 ready]

ILUSTRACIÓN 5 *MONITOREO DE LOS SERVICIOS DE RED*

3.3.3. Protocolos VoIP

Otro de los elementos monitoreados fue los servicios y protocolos VoIP del servidor Asterisk. En la Ilustración 6 se puede observar las llamadas concurrentes, las llamas activas mediante los protocolos SIP e IAX2. Además se muestra el estado de la tarjeta de telefonía Sangoma que permite la conexión de la red telefónica con la red de datos. Todo esto es de gran importancia supervisarlo constantemente pues se necesita conocer los protocolos más estables, el que más problemas presenta, cómo se comportan los elementos de hardware ante los diferentes estados del servidor, entiéndase por estado, múltiples llamadas concurrentes, saturación de la red, etc.

Es importante destacar que el escenario de prueba estuvo compuesto por 10 usuarios portando softphones para un total de 5 llamadas concurrentes, consumiendo cada una de ellas entre 8.3 y 8.4 Kb de acho de banda. Durante las mismas el servidor Asterisk mostró en su comportamiento que solo utilizó el 6,32% de la memoria RAM, dejando el 100% libre de la memoria de intercambio para una carga media del microprocesador.

Service	Status	Last Check	Duration	Attempt	Status Information
ASTERISK_SPAN	CRITICAL	06-21-2010 23:12:52	35d 0h 22m 9s	4/4	Zaptel card not detected
ASTERISK_VERSION	OK	06-21-2010 23:12:52	0d 1h 19m 23s	1/4	Asterisk 1.6.1.12 built by root @ debian-server on a i686 running Linux on 2010-06-04 00:03:40 UTC
ASTERISK_ZAPTEL	CRITICAL	06-21-2010 23:12:52	35d 0h 25m 18s	4/4	Zaptel card not detected
Carga del CPU	OK	06-21-2010 23:12:52	0d 0h 55m 40s	1/4	OK - carga media: 0.37, 0.43, 0.46
LOCAL_CHANNEL	OK	06-21-2010 23:12:52	0d 1h 15m 47s	1/4	13 active SIP dialogs
LOCAL_IAX2	OK	06-21-2010 23:12:52	0d 1h 19m 23s	1/4	17 iax2 peers [0 online, 0 offline, 17 unmonitored]
LOCAL_IAX_CHANNELS	OK	06-21-2010 23:12:52	0d 1h 19m 23s	1/4	0 active IAX channels
LOCAL_MGCP	OK	06-21-2010 23:12:52	0d 1h 19m 23s	1/4	Gateway '9004' at 0.0.0.0 (Dynamic)
LOCAL_PEERS	OK	06-21-2010 23:12:52	0d 1h 19m 23s	1/4	22 sip peers [Monitored: 0 online, 0 offline Unmonitored: 21 online, 1 offline]
Llamadas Concurrentes	OK	06-21-2010 23:12:52	0d 1h 19m 23s	1/4	5 active calls
PING	OK	06-21-2010 23:12:40	0d 1h 19m 23s	1/4	PING OK - Packet loss = 0%, RTA = 2.59 ms
RAM++	OK	06-21-2010 23:12:52	0d 1h 19m 23s	1/4	OK - Memory usage is 6.32 %
Root Partition	OK	06-21-2010 23:12:52	0d 1h 19m 23s	1/4	DISK OK - free space: / 84069 MB (94% inode=97%):
Total Procesos	OK	06-21-2010 23:12:52	0d 1h 19m 23s	1/4	PROCS OK: 106 processes
Uso swap	OK	06-21-2010 23:12:52	0d 1h 19m 23s	1/4	SWAP OK - 100% free (956 MB out of 956 MB)
Usuarios Logueados	OK	06-21-2010 23:12:52	0d 1h 19m 23s	1/4	USERS OK - 0 users currently logged in

ILUSTRACIÓN 6 *MONITOREO DEL SERVIDOR ASTERISK*

3.4. Envío de alertas y notificaciones

Una de las ventajas que presenta Nagios y que fue de vital importancia para la selección de esta es precisamente la posibilidad de enviar alertas y notificaciones a las personas encargadas de la supervisión de la plataforma telefónica. Permitiendo de esta forma que estas personas no necesiten estar las 24 horas del día frente a la aplicación observando lo que pasa en ella.

En estos momentos Nagios fue configurado para que alerte y notifique a los administradores mediante correo electrónico y mensajería instantánea. Eficazmente ante la caída del servidor Asterisk la herramienta notificó a sus administradores mediante correo electrónico comprobándose la validez de la misma. Está claro que si el administrador no se encuentra frente a un ordenador no puede dar respuesta inmediata ante un problema presentado con urgencia, es por esto que se recomienda que se notifique o alerte también por SMS y beeper, aunque para esto se tienen que involucrar las empresas de telecomunicaciones del país.

3.5. Conclusiones

En este capítulo fueron expuestos los resultados obtenidos monitoreando la plataforma PlaTel con la herramienta Nagios. Se explica además la composición del escenario donde se realizaron las pruebas de dicha aplicación y los elementos monitoreados. Por último se manifiesta como Nagios alerta y notifica a los administradores de red.

CONCLUSIONES

Se concluye al término de la presente investigación sobre la selección de una herramienta que se pueda integrar a la plataforma PlaTel y permita monitorear los servicios que esta ofrece, que el objetivo general fue cumplido.

Alcanzándose los siguientes resultados:

- Se presentó una herramienta que ofrece la funcionalidad de monitorear la plataforma PlaTel con el objetivo de mejorar y optimizar la labor de dicha plataforma.
- Se desarrolló exitosamente la etapa de instalación y configuración de la herramienta propuesta.
- Se integró sin ningún problema la herramienta seleccionada con la plataforma PlaTel.
- Se le realizaron las pruebas a la solución propuesta en el centro UCID con el propósito de verificar su funcionamiento.

RECOMENDACIONES

En el desarrollo de un trabajo investigativo, siempre quedan un conjunto de aspectos relevantes, que por cuestiones de prioridad y tiempo, no siempre pueden ser analizados en profundidad. Esta investigación no queda exenta de ello; por tanto, a continuación se mencionan un conjunto de ideas que se consideran necesarias para darle continuidad a este trabajo, contribuyendo a la obtención de un producto más acabado:

- Cambiar la interfaz web de la aplicación atendiendo a los estándares que propone el centro UCID.
- Integrar la herramienta con el proyecto GIS (***G****eografic* ***I****nformation* ***S****ystem*) desarrollado en el centro UCID.
- Incorporar la funcionalidad de enviar alertas vía SMS (***S****hort* ***M****essage* ***S****ervice*).

BIBLIOGRAFÍA Y REFRENCIAS BIBLIOGRÁFICAS

1. **Equipo Técnico - Pedagógico de Ceibal .** Plan Ceibal. *¿Qué es una red? .* [Online] 2006. [Cited: Enero 13, 2010.] http://www.ceibal.edu.uy/index.php?option=com_content&view=category&layout=blog&id=81&Itemid=227.

2. **Avogadro, Marisa.** Razón y Palabra. *Glosario de Nuevas Tecnologías de la Información y la Comunicación.* [Online] Primera revista electrónica en América Latina especializada en comunicación, Febrero 2007. [Cited: Enero 23, 2010.] http://www.razonypalabra.org.mx/comunicarte/2007/febrero.html.

3. **Enrique Melrose Aguilar, Gerardo Chávez Díaz, Erick Huesca Morales.** Red La comunidad de expertos en TICs. *Glosario.* [Online] febrero 2008. [Cited: Enero 21, 2010.] http://www.red.com.mx/letter.php?recD=230.

4. **Altamirano, Ing. Carlos Alberto Vicente.** Seguridad Perimatral. *Monitoreo de recursos de red.* [Online] Junio 2005. [Cited: Febrero 15, 2010.] http://www.seguridad.unam.mx/eventos/admin-unam/Monitoreo.pdf.

5. Demetrixs. *Miércoles de Tecnología: VoIP.* [Online] Julio 18, 2007. [Cited: Enero 26, 2010.] http://demetrix.net/2007/07/18/miercoles-de-tecnologia-voip/.

6. **Quarea ITC Management & Consulting.** Quarea: Vos Datos IP. *SIP: Session Initiation Protocol.* [Online] 2007. [Cited: Febrero 3, 2010.] http://www.quarea.com/tutorial/sip_session_initiation_protocol.

7. **Tomas de Miguel Moro, Alberto Pérez Gómez.** Red Iris. *Información General sobre H.323 .* [Online] Enero 7, 2010. [Cited: Febrero 10, 2010.] http://www.rediris.es/mmedia/H323Info.es.html.

8. **Dueñas, Joel Barrio.** Alcance Libre. *El protocolo IAX2 es oficialmente desde hoy el RFC 5456.* [Online] Febrero 23, 2009. [Cited: Febrero 2, 2010.] http://www.alcancelibre.org/article.php/protocolo-iax2-es-oficialmente-rfc5456.

9. 3CX Software based PBX for Windows. *¿Qué es un sistema telefónico PBX?* [Online] 2009. [Cited: Enero 25, 2010.] http://www.3cx.es/voip-sip/sistema-telefonico-pbx.php.

10. Asterisk-ES Comunidad de usuarios de Asterisk-ES. *Introducción a Asterisk.* [Online] 2007. [Cited: Febrero 5, 2010.] http://comunidad.asterisk-es.org/index.php?title=Introduccion_a_Asterisk.

11. **Herrero, Lic. Alejandro fernández.** Universidad de Mendoza. *Maestría en teleinformática.* [Online] 2009. [Cited: Febrero 3, 2010.] http://www.um.edu.ar/nuke6/imagenes-contenido/UM-MTI-FernandezA.pdf.

12. FreeSWITCH La Primera comunidad hispana. [Online] 2009. [Cited: Febrero 5, 2010.] http://www.freeswitch.es/.

13. **Cayuqueo, Sergio.** Monitoria y análisis de Red con Nagios. *Sergio Cayuqueo.* [Online] Mayo 29, 2009. [Cited: Marzo 20, 2010.] http://cayu.com.ar/files/manual-nagios-2009.pdf.

14. **Instituto de Investigaciones Económicas.** 2o Foro Nacional de Software Libre FONASOL 2008. *Monitoreo de redes con Munin.* [Online] Mayo 28, 2008. [Cited: febrero 20, 2010.] http://gwolf.org/files/munin.pdf.

15. *In Vestigium Revista Oficial de la Dirección de Investigación y Desarrollo.* **Universidad de Aquino.** 12, Bolivia : UDABOL, 2006, Vol. 1. ISSN 1990-7028.

16. **Nagios Core Development Team and Community Contributors.** Official Nagios Documentation. *Nagios.* [Online] Agosto 29, 2007. [Cited: Marzo 11, 2010.] http://nagios.sourceforge.net/docs/ndoutils/NDOUtils_DB_Model.pdf.

17. —. Official Nagios Documentation. *Nagios.* [Online] Abril 18, 2007. [Cited: Marzo 11, 2010.] http://nagios.sourceforge.net/docs/ndoutils/NDOUtils.pdf.

18. —. Official Nagios Documentation. *Nagios.* [Online] Mayo 1, 2007. [Cited: Marzo 11, 2010.] http://nagios.sourceforge.net/docs/nrpe/NRPE.pdf.

19. —. Official Nagios Documentation. *Nagios.* [Online] Junio 16, 2009. [Cited: Marzo 5, 2010.] http://nagios.sourceforge.net/docs/nagios-3.pdf.

20. *Telemática, REVISTA DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES.* **Francisco, Ing. Abel Diogo.** No.27, Ciudad de La Habana : s.n., 2004, Vol. II. ISSN:1729-3804.

21. **Leyla Dinora Rivera Rivera, Hugo Miguel Colato Rodríguez, Nelson Antonio Tesorero.** Tesis de maestía. *Sistema WDS para la Administración remota de servidores.* [Online] Octubre 2007. [Cited: Enero 16, 2010.] http://wwwisis.ufg.edu.sv/wwwisis/documentos/TE/005.75-R621s/005.75-R621s.pdf.

GLOSARIO DE TÉRMINOS

Gateway: Dispositivo mixto de hardware y software que permite enlazar dos redes de datos con estructuras físicas y/o protocolos diferentes; permitiendo la adaptación y conversión de la información cursada entre ambas.

Plugin: Es una aplicación que se relaciona con otra, aportándole una función nueva y generalmente muy especifica. Esta aplicación adicional es ejecutada por la aplicación principal.

Router: Dispositivo para la interconexión de redes informáticas que permite determinar la ruta que deben tomar los paquetes de datos que viajan por la estas redes.

RRDTool: Sistema que permite almacenar y mostrar datos temporales almacenados en bases de datos de forma muy compacta y que no crece con el tiempo. Procesando los datos extraídos de forma tal que se puedan representar gráficamente los valores almacenados.

Sniffer: Es un programa que generalmente está programado en lenguaje C y tiene como utilidad monitorear y analizar el trafico en una red de computadoras, detectando los cuellos de botellas y problemas que existan en ella.

Script: Conjuntos de instrucciones que permiten la automatización de tareas, posibilitando la creación de nuevas utilidades. Son ejecutados por un intérprete de órdenes y frecuentemente se almacenan en archivos de texto.

Softphone: Es un software que realiza una simulación de un teléfono convencional por computadora, permitiendo usar la misma para realizar llamadas a otros softphones o a otros teléfonos convencionales.

Trunking: Es una función para conectar dos servidores, del mismo modelo o no, mediante 2 cables en paralelo en modo Full-Duplex. Permitiendo evitar cuellos de botella en la conexión de varios segmentos y servidores.