“MONTAJE DE PRACTICAS DE LABORATORIO EN LA INSTALACION, IMPLEMENTACIÓN Y USO DE LA HERRAMIENTA DE MONITOREO NAGIOS EN UNA RED LAN.”

JHON JAIRO GAMBA MEJIA

UNIVERSIDAD TECNOLOGICA DE BOLIVAR
FACULTAD DE INGENIERIA
DIRECCION DE PROGRAMA DE INGENIERIA DE SISTEMAS
CARTAGENA DE INDIAS, D. T Y C.
2010

“MONTAJE DE PRACTICAS DE LABORATORIO EN LA INSTALACION, IMPLEMENTACIÓN Y USO DE LA HERRAMIENTA DE MONITOREO NAGIOS EN UNA RED LAN.”

JHON JAIRO GAMBA MEJIA

.

ROYECTO PRESENTADO COMO REQUISITO FINAL PARA OPTAR AL TITULO DE INGENIERO DE SISTEMAS

DIRECTOR
GONZALO GARZON

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR
FACULTAD DE INGENIERÍA
DIRECCION DE PROGRAMA DE INGENIERÍA DE SISTEMAS
CARTAGENA DE INDIAS D. T. Y C.
2010

Cartagena de Indias D. T. y C., Julio de 2010.

Señores
Comité Curricular
Programa de Ingeniería de Sistemas
Facultad de Ingeniería

Asunto: Presentación de proyecto de Trabajo de Grado

Cordial Saludo

Por medio de la presente quiero hacerle llegar a ustedes la presentación del anteproyecto del trabajo de grado "MONTAJE DE PRACTICAS DE LABORATORIO EN LA INSTALACION, IMPLEMENTACIÓN Y USO DE LA HERRAMIENTA DE MONITOREO NAGIOS EN UNA RED LAN." presentado a ustedes para así poder optar el título de Ingeniero de Sistemas

Cordialmente.

_____

Jhon Jairo Gamba Mejía
C.C # 1'047.374.026 de Cartagena

Cartagena de Indias D. T. y C., Julio de 2010.

Señores
Comité Curricular
Programa de Ingeniería de Sistemas
Facultad de Ingeniería

Asunto: Presentación de proyecto de Trabajo de Grado

Cordial Saludo

Por medio de la presente quiero hacer llegar a ustedes la presentación del anteproyecto del trabajo de grado “MONTAJE DE PRACTICAS DE LABORATORIO EN LA INSTALACION, IMPLEMENTACIÓN Y USO DE LA HERRAMIENTA DE MONITOREO NAGIOS EN UNA RED LAN.”, presentado por los estudiantes, Jhon Jairo Gamba Mejía, cód. T00013741.

Cordialmente.

_____

Gonzalo Garzón
C.C #

Cartagena de Indias, D. T y C. Julio de 2010

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____
PRESIDENTE DEL JURADO

_____
JURADO

_____
JURADO

Cartagena de Indias, D. T y C. Julio de 2010

AUTORIZACIÓN

Yo JHON JAIRO GAMBA MEJIA, identificado con la cedula de ciudadanía número, 1’047.374.026 de Cartagena, autorizo a la Universidad Tecnológica de Bolívar, para hacer uso de este proyecto de tesis, y publicarla en el catalogo online de la biblioteca institucional.

_____

JHON JAIRO GAMBA MEJIA
C.C # 1’047.374.026 de Cartagena

TABLA DE CONTENIDO

LISTADO DE TABLAS

LISTADO DE FIGURAS

RESUMEN

Hoy en día, hay una ampliación constante de equipos de cómputo, que solicitan conexiones a una red de área local, esto, para poder realizar trabajos de campo, investigaciones, clases virtuales, entre otras, conllevando a elevar el nivel de consumo de ancho de banda por parte de los usuarios de la red.

De acuerdo a esto han surgido diferentes mecanismos para medir la Calidad de Servicio (QoS), los cuales ofrecen la prioridad con algunos tipos específicos de tráfico sobre tecnologías diferentes incluyendo: Frame Relay, Modo de Transferencia Asincrónico (ATM), LAN, WLAN y líneas dedicadas, para garantizar entrega de tráfico según la importancia de cada uso en caso de competición para recursos de red.

La medición de la Calidad de Servicio, se hace necesaria mediante la presencia de una herramienta de monitoreo en una red LAN, para así, poder analizar el tráfico en la red y poder dar más cobertura de ancho de banda a aquellos servicios que más son utilizados, mejorando la calidad del servicio prestado a los usuarios finales de esta red.

Los sistemas de calidad de servicio medidos con un sistema de monitoreo en las redes de datos que actualmente están aplicados a nivel mundial no deben ser ajenos para aquellas empresas que quieran mejorar la calidad de servicio que prestan a los usuarios finales de una red LAN. Uno de los factores que disminuyen la velocidad de transmisión de datos en una red pueden ser los espías (troyanos), "que ocupan una pequeña porción del ancho de banda ocasionando deterioros en la red" [23], impidiendo mantener una calidad prestada en el servicio.

También otro factor que puede llegar a afectar el rendimiento de esta, es la calidad de los equipos de cómputo y de red, entre los cuales están los computadores, los Routers, el cableado físico instalado en la red, como

también el hilo de fibra óptica y los Swiches y Routers. Un programa adecuado de monitoreo para esta red orientado hacia una red más confiable y rápida, garantizará ofrecer un servicio competitivo, agradable y manejar un nivel de calidad de servicio óptimo en la red.

Para esto, se debe tener en cuenta unos aspectos de monitoreo de redes de datos que son importantes para medir la calidad de servicio:

- La recuperación rápida y completa de los sistemas de información, esto en caso de un ataque directo a la red.
- La integridad de la información, todos los datos trasmitidos por la red lleguen a su destino.
- La disponibilidad de los sistemas de información en todo momento sin importar el estado de la red.
- La confidencialidad de la información, este es uno de los aspectos más importantes ya que si una red no tiene un grado de seguridad, se podría decir que la red no es confiable.

Ya definidos los aspectos principales para poder implementar una herramienta de monitorización y así medir la calidad de servicio, se podrá analizar el tráfico que se presenta en la red LAN para el mejoramiento del servicio prestado.

Para poder realizar está simulación, se aplicará la herramienta de monitorización dentro de una práctica de laboratorio, en donde se contara con un cableado estructurado, Swiches y Routers y se monitorearan servicios prestados en la red.

MONITOREO CON NAGIOS

El administrador de la red iniciara la monitorización a través de la herramienta de monitoreo NAGIOS, la cual será instalada en un servidor LINUX por ser software libre y que medirá la transmisión de datos, servicios prestados por otros servidores y medición de carga de cada equipo se encuentre dentro de la red LAN.

La red es considerada un recurso valioso y de alta importancia, por lo que garantizar su disponibilidad y buen funcionamiento es una tarea esencial; no es fácil asegurar dicha labor debido a las constantes amenazas que se presentan día tras día, como son el robo de información, los virus, las fallas en los dispositivos de red y los ataques de denegación de servicios, las cuales pueden generar o conducir a pérdidas de información, interrupciones dentro del servicio prestado y una posible disminución global de la credibilidad y rentabilidad de una entidad.

En conclusión, es válido el uso de la herramienta de monitorización Nagios, ya que es una manera fácil, rápida, económica y eficiente, frente a las demás herramientas de monitorización.

INTRODUCCION

El presente estudio está relacionado con el monitoreo de red, que se puede definir como "un sistema que constantemente monitoriza una red de computadoras en busca de componentes defectuosos o lentos, para luego informar a los administradores de redes mediante correo electrónico, pager u otras alarmas su estado" [1]. Dichas actividades, métodos y procesos son realizados por una herramientas de monitoreo de red existentes en la actualidad, cuyo objetivo es el de brindarle a los usuarios, una serie de tareas automatizadas o manuales que les permitan monitorear de una manera eficiente las redes LAN.

La característica principal de la monitorización de una red es la importancia y trascendencia que ha tomado en la actualidad, siendo considerada por muchas organizaciones como una tarea primordial que se debe realizar de manera constante debido a los grandes beneficios que ofrece al momento de mejorar los servicios con el monitoreo. Hoy en día, el problema que existe con la monitorización, es por la falta de información con relación a la manera de cómo monitorizar, y la poca información que se posee sobre las diferentes herramientas que existen para este fin.

La investigación de esta problemática se realizó por el interés de conocer la herramienta NAGIOS y las ventajas y desventajas que esta posee al momento de monitorear las redes LAN, cuya actividad es considerada como uno de los principales procesos que permite el mejoramiento continuo al momento de prestar un servicio con calidad en una red LAN. Permitiéndonos así, identificar y comprender la variedad de características e inconvenientes, protocolos y servicios, con el fin de desarrollar prácticas para comprobar lo fundamental que puede llegar a ser la implementación de esta herramienta.

En concreto, esta investigación está centrada en los sistemas de monitorización de redes LAN. La cual, pretende investigar y profundizar sobre la herramienta NAGIOS, sus ventajas y desventajas al momento de monitorear una red para el mejoramiento continuo de la misma.

OBJETIVOS

GENERAL

Realizar una implementación de la herramienta de monitoreo NAGIOS mediante una simulación de laboratorio para analizar el tráfico de una red mediante la monitorización.

ESPECIFICOS

1. Establecer cada una de las características, ventajas y desventajas de la herramienta NAGIOS, su importancia en la monitorización de redes y el contenido que aporta a la investigación.

2. Elaborar documentos o manual de lectura de la herramienta NAGIOS con la cual se pueda explicar la lectura de esta.

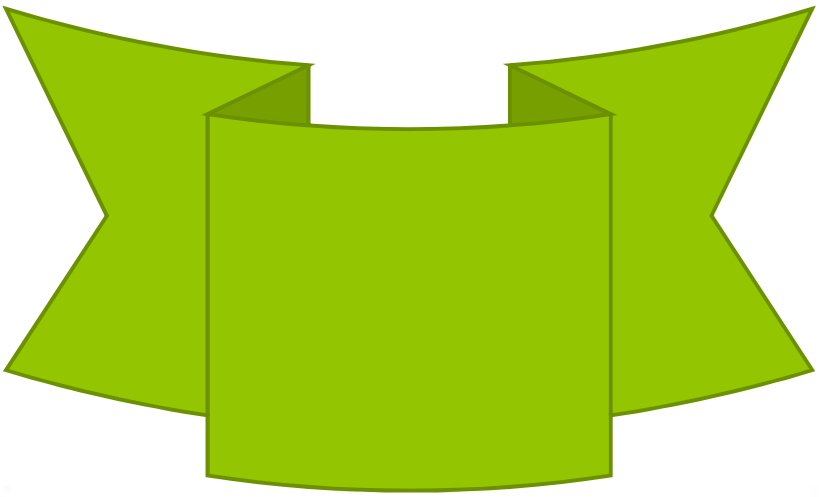
3. Elaborar un manual de instalación y configuración de la herramienta NAGIOS para la implementación de esta, en las prácticas de laboratorios.

4. Brindar un conjunto de resultados recolectados en la práctica simulada, para su interpretación, evaluación y análisis.

1

CAPITULO

MONITOREO DE REDES



1. MONITOREO DE REDES

1.1 Introducción al monitoreo de redes

Inicialmente, el monitoreo de redes se puede definir como “un sistema que constantemente monitoriza una red de computadoras en busca de componentes defectuosos o lentos, para luego informar a los administradores de redes mediante correo electrónico, pager u otras alarmas su estado”, pero a ciencia cierta, al momento de llevarlo a la computación, se ha obtenido un auge enorme en el área de redes. Se han realizado diferentes prospectos de definición y la más acertada es “Una función que busca conocer cómo se están realizando las tareas definidas en el plan operativo” [16] .Aunque esta definición que se ha considerado como la más acertada, no está relacionada con el área en la que se estudia, nos proporciona una mirada extensa en donde se puede llevar más allá de lo dicho para nuestra investigación.

En nuestra área, este concepto debe tener una orientación más práctica, en el área de redes, todas las acciones que se hacen son actividades activas y se requiere tener conjetura y relación con el equipo de trabajo, y este es el tema a investigar, supervisar y analizar todas las actividades que se realizan dentro de una red LAN. Teniendo en cuenta esto, podemos darnos cuenta que el monitoreo se encuentra muy ligado con el concepto de Inteligencia Competitiva la cual se define como: “conocimiento generado a partir del análisis resultante de la integración de información sobre el entorno de la organización, que está disponible lícitamente” [17]

Definiendo y teniendo en cuenta estos dos conceptos, podemos decir que “el término monitoreo de red describe el uso de un sistema que constantemente monitorea una red de computadoras para detectar sistemas lentos o en mal funcionamiento y que notifica a quien monitorea la red en caso de falla vía

correo electrónico, beeper u otras alarmas. Es un subconjunto de las funciones implicadas en la administración de la red" [18].

La monitorización tiene unos alcances increíbles, desde sus inicios en los años 90, se consolido como unos de los campos de acción más fuertes dentro del área administrativa de una red LAN, convirtiéndose así en una forma de ahorrar dinero en el rendimiento de la red, la productividad de los empleados y los excesos de costos de infraestructura.

1.2 Definición de monitoreo de redes.

A la pregunta ¿Qué es Un monitoreo de red?, podemos decir que es un sistema que supervisa una red interna LAN para brindar un servicio estable a los usuarios finales. De igual forma, ayuda a encontrar y a resolver problemas dentro de la red como puede ser los equipos hardware, los procesos ejecutados por usuarios, o procesos que sobrecarguen el sistema y que provoquen la caída de servidores, o la caída de conexiones de red u otros dispositivos.

El objetivo principal, de plantear un sistema de monitorización de red LAN, es prevenir las incidencias y conocer la importancia de los recursos tecnológicos y de comunicaciones TIC's. Teniendo en cuenta que estos objetivos son importantes dentro de una empresa, se puede decir que cada una debería contar con un sistema de monitorización.

Aunque se diga que implementar un sistema de monitoreo de red LAN es complicado, mucha de las actividades que se desarrollan dentro de este proceso no lo son. Para esto se desarrollan ciertos pasos, que simplifican al administrador de red LAN la utilización de herramientas que permitan esto.

Antes que una instalación, se debe realizar un análisis detallado del sistema informático a monitorizar para, entre otras cosas, detectar los sistemas críticos (tanto máquinas, como servicios) para el buen funcionamiento de una

red LAN y así poder formular políticas de actuación frente a incidencias en dichos sistemas. Podría destacarse como interesante, asegurarse de que un servidor web o de datos esté siempre en marcha o estar sobre aviso de emergencias en el sistema de correo electrónico monitorizado.

Ya teniendo este punto resuelto, se puede continuar con la redacción del plan de instalación e integración del nuevo sistema de monitorización en nuestro sistema informático, para lo cual es imprescindible respetar estas tres reglas[1]:

- Mantener las medidas de seguridad existentes.
- Minimizar el impacto en el propio sistema a estudiar.
- Minimizar el número de sistemas intermedios entre el sistema de monitorización y los sistemas críticos.

1.2.1 Implementación de un Monitoreo de Red

Como plan adicional a este proceso, habría que saber qué ocurre o cómo actuar si el sistema de monitorización deja de estar disponible, es decir, hay que contestar a la pregunta ¿quién monitoriza al monitorizador?. Aunque parezca una verdad de verdades, no todo el mundo tiene en cuenta este importante detalle.

Para tener en cuenta esto se puede elegir un buen paquete de software especializado y proceder a su instalación y configuración. Para esto, se cuenta con opciones de licencia libre como Nagios que ofrece ventajas frente a sus alternativas comerciales de competencia, destacando especialmente su inmensa flexibilidad para poder monitorizar todo lo que queramos en el modo que lo necesitemos.

Se puede pensar que no hay necesidad de añadir un sistema de monitorización si la red tiene un funcionamiento correcto, sin embargo, existen razones para insistir en la supervisión de la red, y se pueden resumir

en un alto nivel en el mantenimiento de la estabilidad actual de la red, para garantizar la disponibilidad y mejorar el rendimiento.

Para la implementación de un plan operativo de un sistema de monitorización de red LAN se pueden utilizar distintos programas informáticos en conjunto con una combinación de hardware plug-and-play y soluciones de software. Prácticamente cualquier tipo de red puede ser monitorizada teniendo en cuenta estos aspectos. No hay que tener cuidado si es una red WAN, LAN WLAN o VPN, puede monitorizar los dispositivos en sistemas operativos diferentes con multitud de funciones, que van desde la conectividad de BlackBerry y teléfonos celulares de manera Wi-Fi, a los servidores, Routers y Switches. Estos sistemas pueden ayudar a identificar las actividades específicas y medición de desempeño, produciendo resultados que permiten a una empresa atender las necesidades diversas y variadas dentro de su red LAN.

Como segunda medida, hay que decidir lo que específicamente se quiere supervisar dentro de la red, ya que es importante mantener la estabilidad de la red desde una perspectiva general, hasta llegar a los usuarios finales.

Para esto, hay que tener seguridad en la ejecución del plan de inserción de la herramienta de monitoreo, antes que nada, se debe estar seguro de que el mapa de topología de red LAN esté actualizada. Este mapa debe establecer con precisión los diferentes tipos de redes que deben controlarse, los servidores que se ejecutan y las aplicaciones del sistema operativo, cómo muchos equipos finales.

1.2.2 Practica de Monitoreo

Inicialmente la práctica consiste en la implementación de una herramienta de monitorización de redes LAN, con la cual, se podrá observar el tráfico que se da en la red, y analizar qué tanta utilidad se da en los puertos y en el consumo del ancho de banda, teniendo en cuenta esto, podemos definir como una buena práctica, aquella en la cual, al momento de la implementación, diseño e instalación de la monitorización todo funcione adecuadamente y se logren los objetivos trazados en esta, de igual forma se requiere un conocimiento previo del tema, el cual se basara la persona para poder desarrollar las competencias académicas exigidas por la herramienta para su correcto uso y buen funcionamiento. Tomando esta información como base inicial de una buena práctica de monitoreo LAN se podrá decir, que se realizó con éxito el desarrollo de dicha práctica.

1.2.3 Que es lo que se Monitorea

En un entorno corporativo o institucional, la red es un activo completo, expansivo y dinámico. Está en funcionamiento las 24 horas, los siete días de la semana y típicamente acceden a ella tanto los usuarios internos como externos en forma continua. Después de todo, los sitios Web nunca cierran y siempre hay usuarios en alguna parte del mundo que están enviando mensajes de correo electrónico y que están trabajando en proyectos, y esperan tener acceso disponible independientemente de su zona horaria y de la ubicación de los activos. Esto quiere decir que la red se debe monitorear en todo momento, se debe recopilar información sobre niveles de desempeño, utilización y estado operativo. Esta información se debe guardar y colocar a disposición para su análisis, con el fin de que se puedan realizar seguimientos de tendencias y generar informes.

Por lo tanto, en una red se debe monitorear todo. Enrutadores, concentradores, conmutadores, estaciones de trabajo y otros dispositivos conectados a la red, a través de agentes de protocolo simple de administración de redes (Simple Network Management Protocol, SNMP) y bases de administración de información (Management Information Base, MIB). Además, se deben tener en cuenta las aplicaciones de Windows por medio de agentes de Instrumental de administración de Windows (WMI), las bases de datos y archivos, los cortafuegos, filtros de spam y virus., las redes privadas virtuales (VPN) y las LAN virtuales (VLAN). Si cualquiera de estos elementos falla o está comprometido de cualquier forma, puede generar consecuencias graves, como por ejemplo:

- Si los empleados no pueden acceder a las aplicaciones y a la información que necesitan para hacer su trabajo, se pierde productividad y no se puede cumplir con los plazos estipulados por la empresa y sus clientes.
- Cuando los clientes no pueden completar sus transacciones en línea, significaría ingresos perdidos, usuarios frustrados y reputación dañada.
- Cuando los socios no pueden colaborar o comunicarse con la compañía, se deterioraría esta relación y afectaría a su resultado general.
- Las regulaciones de seguridad y privacidad hacen que las organizaciones sean responsables de las amenazas para los datos, incluso cuando los sistemas como un servidor de correo electrónico no están funcionando.

En conclusión, las redes son tan complejas y dinámicas, que siempre hay posibilidades de que algo salga mal. La monitorización de la red no puede prevenir todos los problemas, pero puede minimizar la pérdida de servicio y el impacto del tiempo que no funcione. Por ejemplo, cuando aumentan los índices de utilización, el desempeño tiende a sufrir y crece el riesgo de un error grave. Si el administrador de red puede ver que se está llegando a un cierto límite, se

pueden tomar medidas correctivas y agregar más capacidad y evitar que un problema potencial se convierta en un desastre total. O, si una alerta indica que un servidor tiene un error, el administrador puede poner en línea uno redundante rápidamente mientras reinicia el servicio en el primero.

1.3 SOLUCION DE CONFLICTOS

La monitorización de red no ayuda a solucionar conflictos de un día a otro, esto es considerado un proceso de ejecución a mediano plazo, y hay que tener en cuenta que la implementación de la herramienta de monitoreo, cumpla con los ideales anteriormente mencionados. La vigilancia del tráfico es una tarea fundamental y vitalicia para el funcionamiento de una red LAN, esta es la actividad base de las demás actividades que se ejecutan en el proceso. Por lo general, los recursos que apoyan los usuarios finales internos son centrados, permitiendo así, poder reconocer de manera rápida y eficaz, que proceso puede fallar, o que hardware está presentando inconvenientes. Concluyendo esto, los sistemas de monitoreo de red, permiten la observación continua de los diferentes dispositivos de red como son:

- BlackBerry
- Teléfonos celulares
- Servidores y equipos de sobremesa
- Routers
- Switches.

Cabe albergar un punto importante como lo son algunos sistemas de monitorización de red, que vienen con el automatic discovery[2], (Descubrimiento automático), que es la capacidad para grabar continuamente los dispositivos de una red LAN a medida que se agregan, quitándose o

sometiéndose a los cambios de una configuración dentro de la red. Algunos dispositivos comunes suelen ser:

1. Dirección de IP
2. Servicio
3. Tipo (switch, router, etc.)
4. Ubicación física

Más allá de la obvia ventaja de saber exactamente y en tiempo real lo que han desplegado, el descubrimiento automático y clasificación de los segmentos le ayuda a planificar para el crecimiento de su red LAN. El Hardware subutilizado puede asumir nuevas funciones, por ejemplo, ayudaría a identificar los problemas con la sustitución de equipo defectuoso. Si todos los dispositivos de red LAN en un lugar determinado son de poca envergadura, podría haber un problema de gestión de recursos para hacer frente.

Del mismo modo, las grandes redes a menudo son subredes de redes principales. Los segmentos pueden variar según el proveedor ISP, la generación, la misión y otros factores. Llegando a este punto podemos ver que las herramientas de monitoreo puede tener sentido en la organización de la complejidad de una red LAN. Algunos tipos de redes más comunes son:

- Conexión inalámbrica o por cable
- Una red corporativa de área local (LAN)
- Una red privada virtual (VPN)
- red de área amplia Un proveedor de servicios (WAN)

1.4 HERRAMIENTAS O SISTEMAS DE MONITOREO DE REDES LAN

Habiendo definido los tipos de redes más comunes a monitorear, Un sistema de monitoreo de red ayudará a dar sentido a estos entornos complejos de las LAN, mediante la generación de reportes de que los administradores de red utilizan para:

- Confirmar el cumplimiento normativo y de políticas
- Hacer hincapié en los posibles ahorros por la búsqueda de recursos redundantes, por ejemplo:
  - Resolver la eficiencia minando misterios como caído sesiones de correo
  - Ayudar a determinar la productividad del empleado
  - Spot sobrecargando equipo antes de que pueda bajar de una red
  - Identificar los débiles vínculos de red de ancho de banda y otros cuellos de botella
  - Medir la latencia, o retraso en el traslado de los datos
  - Encontrar tráfico anómalo interno que puedan indicar una amenaza para la seguridad.

Los sistemas de monitorización de red pueden ser software o firmware, simples o complejos. Entre los más simples existen herramientas que permiten la interconexión entre diferentes dispositivos de red, permitiendo observar servicios básicos como son el PING, FTP, entre otro.

Las herramientas de monitoreo de red más relevantes para la mayoría de los administradores de red son aquellas que se incluyen por si mismas dentro de un rango de comparación ya sea en pruebas comunes y las secuencias de comandos de control y que pueden producir informes con gráficos ricos que resuman las condiciones de un dispositivo específico para toda la red.

Las herramientas de código abierto son innovadores, de bajo costo y numerosas, permiten trabajar con la mayoría de las herramientas y plataformas de Sistemas Operativos. Teniendo en cuenta esto, se investiga agresivamente que tan importante es trabajar bien dentro de su red LAN, teniendo como pieza clave la diversidad de sistemas operativos que puede llegar a monitorizar.

1.4.1 Complejidad de las Herramientas de Monitoreo

Las herramientas de monitorización de red vienen en diferentes niveles de complejidad. Un ejemplo claro es el Ping, una herramienta simple y fiable que sirve para operar bajo los distintos sistemas operativos mediante la evaluación de conectividad que se da en los host, en particular si es accesible a través de una red IP, ya que funciona mediante el envío de paquetes de solicitud de eco ICMP al host de destino y la escucha de las respuestas de eco de respuesta. Ping estima el tiempo de ida y vuelta en milisegundos, los registros de cualquier pérdida de paquetes y arroja un resumen cuando haya terminado.

Obviamente, hay diversidad de sistemas de acuerdo a niveles de gestión, como por ejemplo una gran cantidad de soluciones de interfaz gráfica de usuario basada en reportes Webs incluyendo informes detallados y características gráficas en donde los detalles de los informes es lo primordial . Estas herramientas pueden ser más fáciles de configurar y utilizar. Muchos vienen con configuraciones prediseñadas. Además, los resúmenes que producen son muy útiles al momento de rendir informes sobre el estado de la red LAN.

Las herramientas de código abierto, son siempre una opción principal, abundan para implementarlas como monitoreo de red. Son en general, innovadoras, irreverente, pero con estilo, en su mayoría gratuitos o en su defecto, económicos. Además, las herramientas de código abierto son compatibles con casi todas las herramientas de otras plataformas. Los datos de estas herramientas de código abierto son casi siempre objeto de dumping en XML, e incluso los principales proveedores tienden a usar XML en un momento u otro.

Por ejemplo, una herramienta que es software libre bajo la GNU GPL comenzó su vida como un guión insignificante, con poca definición para graficar el uso de una conexión LAN dentro de una empresa. Después fue utilizado como una herramienta que permite graficar otras fuentes de datos como la velocidad, voltaje, temperatura y el número de impresiones. Así se dio inicio a que los administradores de red comenzaran a utilizar el software dentro de una red LAN, para sondear los valores de los dispositivos de red, recuperar el MIB (Management Information Base) y SNMP (Simple Network Management Protocol), y el uso de scripts de Perl para enviar los resultados en gráficos en páginas web. La herramienta se convirtió rápidamente en una fuerte solución a la monitorización de redes, no sólo por la gente de código abierto, ya que improvisaban sus propias soluciones en conjunto, sino también por vendedores de software con licencia muy grandes que tomaron algunas de las capacidades de la herramienta para enriquecer sus propias soluciones.

Cambiando a la otra perspectiva, varios fabricantes de equipos de red como CISCO, HUAWEY, entre otros, han desarrollado herramientas que proporcionan información muy detallada de su propio hardware, añadiendo un valor significativo a la compra de los equipos. Sin embargo existe una falencia al momento de contractar estas herramientas con otras que sean de tipo genérico, ya que la compatibilidad entre el hardware y el software suele ser un inconveniente para poder monitorear una red LAN con este tipo de sistemas.

1.4.2 Diferentes Herramientas de Monitoreo de Redes LAN

Teniendo la claridad sobre que es un monitoreo de red LAN y cuál es su importancia dentro de una empresa, se procede a la búsqueda de una herramienta que permitiera poder visualizar el comportamiento que está teniendo una red LAN, facilitando así, la búsqueda de problemas que se presenten dentro de esta.

La comparación que se muestra a continuación se realiza con diferentes herramientas, en donde se tienen en cuenta los aspectos o características más importantes, como costos, licencia, operatividad, entre otras:

Nombre	Gráficas	Informes	Estadística	Plataforma	SNMP	Complement	Alertas	Aplic. web	Precio
Entuity	✓ Sí	✓ Sí	✓ Sí	Windows	✓ Sí	✓ Sí	✓ Sí	✓ Cotrol total	Comercial; € 900
PacketTrap	✓ Sí	✗ No	✓ Sí	Windows y Linux	✓ Sí	✓ Sí	✓ Sí	✓ Visualización	Comercial; $ 99
Nagios	✓ Sí	✓ Sí	✓ Sí	Linux	✓ Con Plugins	✓ Sí	✓ Sí	Sólo visualización	GPL: LIBRE
Zenoss	✓ Sí	✗ No	✓ Sí	Linux	✓ Sí	✓ Sí	✓ Sí	✓ Control total	GPL: LIBRE
Hobbit Monitor	✗ No	✓ Sí	✓ Sí	✓ Linux, Solaris	✓ Sí	✓ Sí y soporta BB	✓ Sí	Viewing, nowledging,	GPL: LIBRE
Op Manager	✓ Sí	Desconocido	✓ Sí	Windows	✓ Sí	✓ Sí	✓ Sí	✓ Control total	Comercial; € 1.079,12

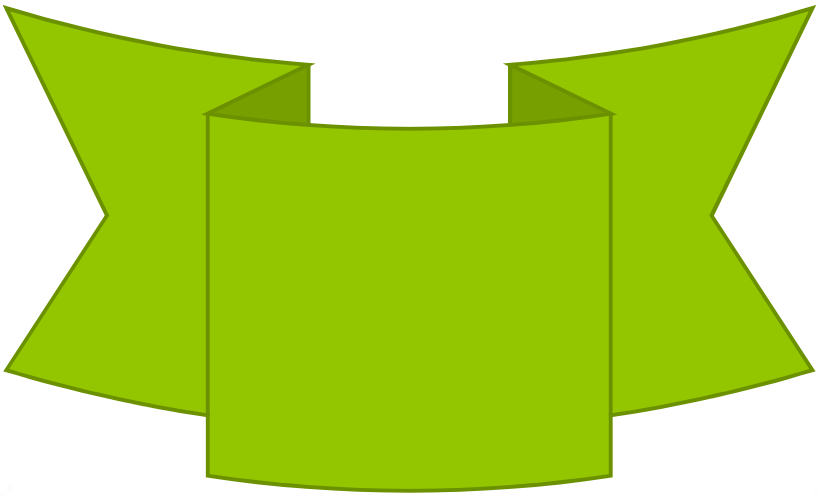
TABLA 1: COMPARACIÓN DE NAGIOS CON OTRAS HERRAMIENTAS

Como se observa, la herramienta Nagios, y analizando las diferentes características, se puede observar que cumple con todas, y que se simplifica la selección de esta herramienta, gracias a que no tiene costo alguno su licencia, ni la de la plataforma en la que corre.

2

CAPITULO

HERRAMIENTA DE MONITOREO NAGIOS



2.1 Introducción a Nagios

Nagios, Inicialmente llamado Netstat, se ha convertido en uno de los sistemas de monitorización más utilizados por los administradores de red que buscan un funcionamiento correcto de su hardware en la red.

Nagios fue creado y se sigue manteniendo por el grupo de desarrolladores de software Ethan Galstad en el año de 1997. Originalmente diseñado para ser ejecutado en Linux, en la actualidad también corre sobre algunas variantes de Unix. Anteriormente era llamado Netstat, herramienta que inicio como proyecto universitario. Cambio su nombre debido a inconvenientes con registros de nombre comercial, Nagios proviene del acrónimo Nagios (Ain't Gonna Insist On Sainthood) [3]. Este programa es comprendido como modular, que puede descomponerse en tres partes:

El motor de la aplicación que ordena las tareas de supervisión.

La interfaz web, que permite tener una vista conjunta del sistema de información y de las posibles anomalías.

Los Plugins, una centena de mini programas que se pueden completar en función de nuestras necesidades para supervisar cada servicio o recurso disponible sobre el conjunto de ordenadores o elementos en red.

Una gran cantidad de características hacen de Nagios una potente herramienta de monitorización de la red. Algunas de las más significativas pueden ser su monitorización de servicios como SMTP, POP3, PING, así mismo, en conexión con otras plataforma permite la verificación de carga del procesador, utilización del disco y memoria RAM, como los ficheros log, entre otros, una de las características nuevas que se incluyeron en la versión 2, fue la monitorización de factores ambientales como la temperatura. Por ser una aplicación GNU, permite el desarrollo y la inclusión de Plugins que permiten a los usuarios crear de manera sencilla eventos propios de chequeo del sistema.

Nagios es un aplicativo de monitoreo de sistemas de redes que observa a los host y servicios que se especifican, alertando cuando se presenten inconvenientes dentro de la red.

La complejidad de las redes y sistemas modernos es algo sorprendente, ya que cualquier administrador no está al cien por ciento de sus capacidades para monitorear una red compleja, inclusive, las redes pequeñas ya no suelen encontrarse en pequeñas o medianas empresas, y pueden tener altos niveles de complejidad en los sistemas que corren.

Nagios fue diseñado como un software sólido para el control, programación y alerta de diferentes eventos dentro de la red, así mismo, contiene algunas características de gran alcance, y el aprovechamiento de estas no sólo es una cuestión de entender cómo funciona Nagios, si no también cómo funciona el sistema que está monitoreando. Este es un logro importante, Nagios no enseña de manera automática acerca de los sistemas complejos, pero es considerada una herramienta valiosa para ayudar en la solución de conflictos.

2.2 Soluciones que brinda la Herramienta

De aquí nos derivamos a la pregunta importante, ¿qué soluciones puede brindar Nagios al monitorizador de red LAN? Nagios puede hacer mucho más que una observación del hardware de la red, sin embargo se nombran las principales actividades que se pueden desarrollar con esta herramienta.

2.2.1 Comprobar si un servidor está activo y en funcionamiento

Esta comprobación se realiza a través de la implementación de la herramienta NSCLIENT++, la cual corre bajo sistemas Windows, para poder realizar el enlace entre la plataforma y la herramienta de monitorización LAN.

2.2.2 Notificar si un servidor está caído

Esta configuración se presta mediante la configuración de un sistema SMS del proveedor de servicio, y en el caso de correo electrónico, mediante el enlace que se da entre la cuenta de correo electrónico establecida para este uso y la cuenta del local host de monitorización (por correo electrónico / / SMS)

2.2.3 Comprobación de Ejecución de un servicio

Análisis y observación continua 24–7 de los diferentes servicios que se prestan en la red, mediante la configuración y agregación de servicios en los ficheros de configuración *.cfg (correo, http, pop, ssh).

2.3 ¿Por qué utilizar Nagios?

Nagios es una excelente opción si se desea llevar a cabo algún tipo de control. Las principales fortalezas de Nagios son:

- Open Source
- Robusto y fiable
- Altamente configurable
- Fácilmente extensible
- Active el Desarrollo
- Comunidad Activa

2.3.1 Como trabaja la Herramienta

Nagios se ejecuta en un servidor web, por lo general como un daemon (o servicio). Nagios periódicamente ejecutar los Plugins que residen en el mismo servidor, se ponen en contacto con hosts y servidores de su red o en Internet.

También puede hacer que la información enviada a Nagios sea recibida como alerta sonora o visual. De igual forma, se pueden activar Plugins que sirvan como atacantes a los eventos que puedan pasar dentro de la red LAN.
Entre los años de 2001 y 2006, Se siguieron desarrollando Plugins de Nagios, con los cuales se implementan nuevas características a la herramienta en su segunda versión, una de las principales, es la visualización web de todo el sistema de monitorización que se está implementando, así mismo, cambia su sistema de log, se implementa la opción de contacto, en la cual se describe a quien se le contacta en cada inconveniente que se encuentre dentro de la red.

Habiéndose cumplido la primera década de la existencia de la herramienta NAGIOS, sale su tercera versión, llamada Nagios Core, en la cual su principal destacamento se basa en la documentación y un nuevo sistema de detección de errores, diferenciados con banderas de colores, así mismo, sigue permitiendo Plugins externos a la herramienta, diseñadas para exportar documentación, y generar mapas completos del estado actual de la red.

Abarcando todo estos datos cronológicos podemos hacer actividades específicas en caso de que una infraestructura de una red, pueda llegar a presentar algún inconveniente, de esta manera podemos diferenciar entre un simple análisis, como el de Nagios en su primera versión, a la actual, que consta de un sistema que se pueda hacer llamar “completo”.

En caso del monitoreo además de realizar un análisis detallado acerca de las acciones que suceden en la red, también se realizan las acciones de supervisar y reaccionar ante algún imprevisto. Estos imprevistos se pueden traducir en eventos como es el caso de “problemas de ruido en la línea de transmisión y que crean situaciones que no existen tales como direcciones de computadoras que no pertenecen a ninguno de los nodos, errores en la información, por mencionar algunos” [8].

Nagios, por ser una herramienta de monitorización, permite su instalación en un servidor web bajo la plataforma Linux, el cual se puede conectar en un punto específico dentro de una red LAN, como se muestra a continuación:

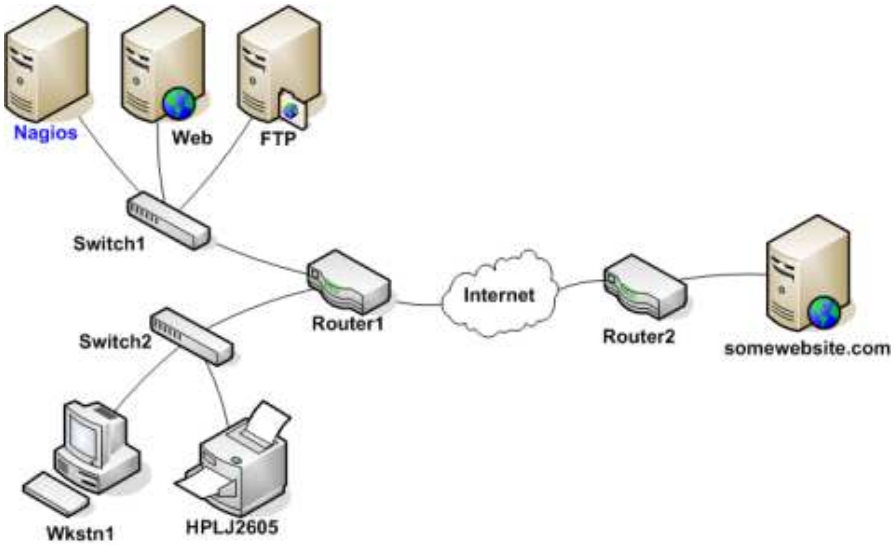


Figura 1: Esquema de Monitorización de la herramienta Nagios

Así mismo, la herramienta Nagios se implementa dentro de los estándares de la IEEE, que es el caso del estándar 802.2 permitiendo así, establecer un Esquema general de monitoreo como se muestra:

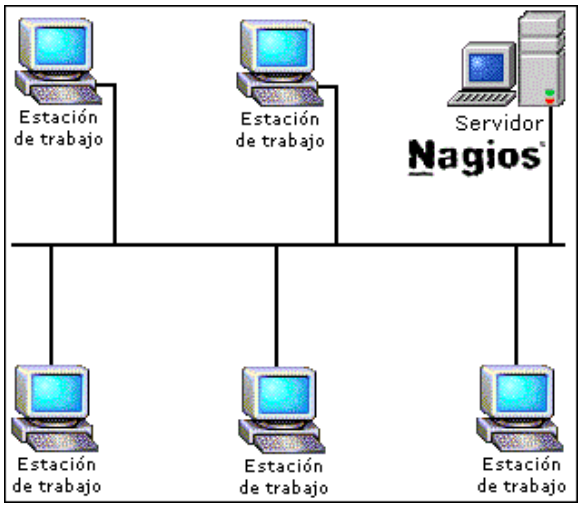


Figura 2: Topología de Bus estándar 802.2 IEEE

Bajo los estándares de la IEEE, enfatizando más en el estándar 802.x se puede ver que como interactúa la herramienta Nagios con los demás equipos.

Para prevenir errores en un sistema existente podemos utilizar un equipo que se ocupe de estar “controlado y observando” el funcionamiento de la red, esto podemos realizarlo por medio de la herramienta anteriormente descrita Nagios.

Esta herramienta nos asegura una rápida ejecución y su licencia que lo determina como Software Libre nos asegura que siempre tendremos actualizaciones disponibles y que hay una gran comunidad de desarrolladores soportándolo.

Creada para ayudar a los administradores a tener siempre el control de lo qué está pasando en la red que administran y conocer los problemas que ocurren en la infraestructura antes de que los usuarios de la misma los perciban, para así no sólo poder tomar la iniciativa, sino asumir la responsabilidad de hacer que las cosas sucedan; decidir en cada momento lo que queremos hacer y cómo lo vamos a hacer, debido a que este software nos permite obtener datos, interpretarlos y tomar decisiones en base a ello como:

Conservar y almacene 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

Generar reportes sustentados para justificar las necesidades de actualización de la red

2.4 Plugin de Nagios

Para facilitar tareas de explotación de datos, hay diferentes aditivos como un visor de reportes integrados, en el cual se puede ver el histórico de actividad y performance de servicios, y además un visor de diagramas de red con el estado actual de cada equipo.

El mismo, está constituido por un Núcleo que construye la interfaz de usuario los cuales representan los “ojos y oídos” de Nagios y por lo cual se encargan de

recopilar información (bajo demanda). Los mismos pueden estar programados en diversos lenguajes como C, C++, Python, Perl, PHP, Java, Bash etc, ya que Nagios es independiente del lenguaje en el cual que se desarrolle el plugin y solo procesa los datos recibidos de este, para la posterior elaboración y envío de notificaciones a los encargados de la administración del sistema en cuestión.[26]

Las necesidades principales de Nagios o del administrador de red es conocer el estado de diferentes servicios brindados por equipos como servidores corriendo diferentes sistemas operativos, Routers de los cuales dependen varios equipos.

Obtener información de los mismos como estado en red, tiempo de subida, puertos abiertos, servicios y procesos corriendo, carga de CPU, carga de memoria física, carga de memoria virtual, espacio en disco, interfaces de red activas. Es posible conocer los estados y datos de estos diferentes equipos para una posterior elaboración de reportes etc, elaborando una configuración personalizada de Nagios para cada caso en particular, por medio de testeo de paquetes de red, o haciendo uso de diferentes funciones que provee el protocolo SNMP (Simple Network Management Protocol) que nos permite gestionar y/o supervisar datos de diferentes elementos y componentes de la red como Routers, Switches, servidores etc y al ser un protocolo standard es posible monitorizar una amplia variedad de casos en escenarios con sistemas o equipos diferentes[26].

El impacto de Nagios desde su primer uso después de su correcta configuración se da mediante la mejora de productividad, antelación de problemas, reporte y aviso de incidentes, agilidad en su tratamiento y, mejor y mayor relación e integración de sectores adjuntos con los plugin ad-don como se muestran a continuación:

2.4.1 NDOUtils

El generador de graficas Nagvis necesita que Nagios almacene sus datos dentro de una base de datos MySQL ya que por defecto lo hace en archivos de texto, para que Nagios pueda hacer eso, deberemos instalar el módulo NDO que viene dentro del paquete NDOUtils descargable vía el sitio web de Nagios. Este módulo es el que se encarga de generar las consultas en formato MySQL, que son cargadas sobre un socket El proceso NDO2DB corriendo como daemon lee de ese socket y carga los datos en una base de datos MySQL.[26]

Hay 4 componentes principales que inician las utilidades NDO:

- NDOMOD Event Broker Module (Modulo de evento corredor)
- LOG2NDO Utility
- FILE2SOCK Utility
- NDO2DB Daemon

2.4.1.1 NDOMOD Event Broker Module

Las utilidades NDO incluyen un Nagios Even Broker Module (NDOMOD.O) que exporta datos desde el demonio de Nagios.

Asumiendo que Nagios fue compilado con el Modulo Event Broker activado (esto es por default), usted puede configurar que Nagios cargue el módulo NDOMOD en tiempo de ejecución. Una vez que el modulo fue cargado por el daemon de Nagios, este puede acceder a todos los datos y lógicamente presente el proceso de Nagios que está corriendo.

El módulo NDOMOD tiene designado exportar la configuración, como información variada de eventos en tiempo de ejecución que ocurre en el proceso de monitoreo, por el daemon de Nagios. El modulo puede enviar esta información a un archivo estándar, a un Socket Unix de Dominio o un a socket TCP.

El NDOMOD escribe la info en un formato que el demonio NDO2DB puede entender.

Si el NDOMOD está escrito para un archivo de salida, usted puede configurarlo para rotarlo periódicamente y/o procesarlo en otra máquina físicamente (usando SSH, etc.) y envía este contenido al daemon NDO2DB usando la utilidad FILE2SOCK (que describiremos más adelante) [26].

2.4.1.2 LOG2NDO

Esta es designada para permitir importar un historial de logs de Nagios a una BD vía el NDO2DB daemon (describiremos luego). La utilidad trabaja enviando archivos de logs históricos a un archivo estándar, un unix sock o un tcp sock en un formato que NDO2DB daemon entienda. El NDO2DB daemon puede luego usarlo para procesar la salida y almacenar en un archivo de log histórico informándolo en una BD [26].

2.4.1.3 FILE2SOCK

Esta utilidad es muy simple, solo lee de un archivo estándar (o STDIN) y escribe todo sobre un socket de dominio unix o un tcp socket. Estos datos son leídos y no son procesados por nada, antes de ser enviados al socket [26].

2.4.1.4 NDO2DB

La utilidad es diseñada para tomar los datos de salida de los componentes NDOMOD y LOG2NDO y almacenarlos en una BD MySQL o BD PostgreSQL [26].

Cuando este inicia, el daemon NDO2DB crea un socket y espera que los clientes se conecten. NDO2DB puede correr independientemente, bajo un demonio multiproceso o bajo inetd (si está usando un socket TCP).

Múltiples clientes pueden conectarse al daemon NDO2DB y transmitir simultáneamente.

2.4.2 Nagvis

Es un ad-don para Nagios, con el cual podemos tener gráficos a modo de diagrama estructural de red, dinámicos, con lo cual podemos conocer el estado actual de la red mirando un gráfico amigable al usuario final [26].

2.5 Estructura de archivos de Nagios

Una vez que se compila e instala el paquete Nagios, termina quedando una nomenclatura de directorios como la siguiente:

Bin: Dentro de este directorio encontramos los ejecutable principales, como el binario Nagios que es el que se ejecuta como proceso en segundo plano, el objeto ndomod.o que es el modulo que se encarga de traducir las estadísticas de Nagios en formato de consultas MySQL, y ndo2db que el proceso en segundo plano que se encarga conectarse con la base de datos para posteriormente ejecutar esas consultas. [26]

Etc: Este directorio guarda la configuración de Nagios, sus componentes, hosts/servicios a chequear, comandos de ejecución, contactos de notificación, intervalos de chequeos. Dentro del hay diferentes subdirectorios y archivos [39].
Libexec: Allí se contienen lo ejecutables de los Plugins que efectúan los chequeos, SNMP, SAP, Oracle, SSH, que pueden ser binarios, scripts en Perl, PHP, Shell, Java, etc [26].

Sbin: Aquí se almacenan los ejecutables cgi que se ejecutaran para la visualización por web de la consola Nagios [26].

Share: Aquí encontramos el contenido web, imágenes, logos, los aditivos como PNP, Nagvis y los datos que necesitan para funcionar estos [26].

Var: Aquí se guardan los datos internos de Nagios, estadísticas de los chequeos, información de ejecución actual, archivos de sockets, registros de logs, colas de ejecución de chequeos [26].

Para mostrar una escala final del sistema Nagios como tal en su configuración correcta se muestra la siguiente gráfica, en donde se detalla la organización recomendada de la configuración de este aplicativo de monitorización.

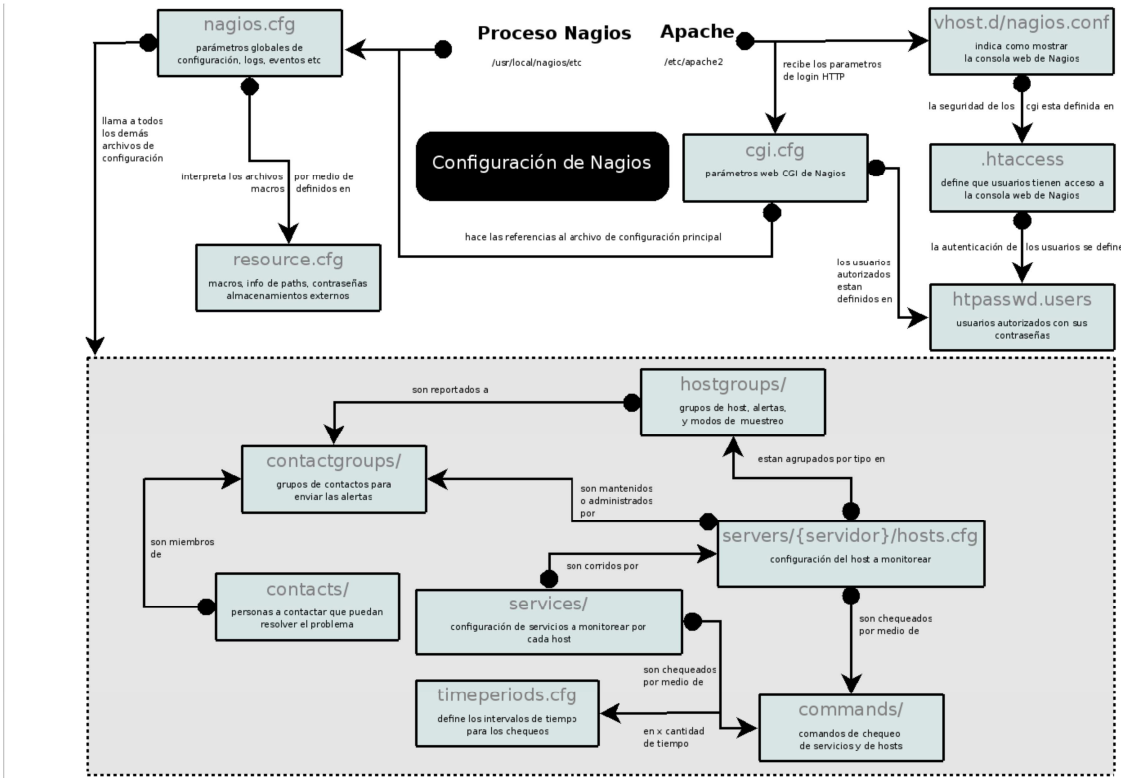


FIGURA 3: COMPILACION TOTAL DE LOS ARCHIVOS DE NAGIOS

2.6 Estados de Servicio

La implementación y configuración correcta de Nagios, conlleva a que se pueda observar el estado de cada uno de los servicios agregados para la monitorización, existen 4 salidas de información, las cuales permiten clasificar cada uno de los estados de servicio, para luego reflejar esos estados en su código de retorno o Exit status, dependiendo de la interpretación que el mismo Nagios muestre.

Exit Status	Estado del Servicio	Estado Del Host	Descripción
0	OK	UP	UP El plugin es capaz de verificar el servicio y que parece estar funcionando correctamente
1	WARNING	UP / DOWN / UNREACHABLE	El plugin es capaz de verificar el servicio, pero que parecía estar por encima de un umbral de “advertencia” o parece no estar funcionando correctamente
2	CRITICAL	DOWN / UNREACHABLE	El plugin detecta que o bien el servicio no funciona o que está por encima de un umbral “crítico”
3	UNKNOWN	DOWN / UNREACHABLE	Argumentos de línea de comandos no válida o fallas internas del plugin (por ejemplo error en un socket o dns) que le impiden realizar las operaciones especificadas

TABLA 2: DESCRIPCION DE LOS ESTADOS DE NAGIOS [26]

2.7 Principales Comandos de plugin de Nagios.

Después de la definición de los estados de servicio, se procede a definir los comandos principales con los que el sistema Nagios funciona. El sistema Nagios incorpora un gran número de comandos por default que se pueden utilizar. Algunos de ellos hacen uso de librerías y paquetes que deben estar instalados en el sistema, estos comandos son:

2.7.1 check_by_ssh

Permite la ejecución de comandos en ordenadores remotos vía SSH (por tanto, de manera segura). El resultado de ese comando será tomado por Nagios [26].

2.7.2 Check_Disk

Este comando sirve para comprobar el espacio libre de un volumen montado en el sistema de ficheros donde se esté ejecutando Nagios. Permite especificar dos umbrales y generar disparadores advertencias cuando se supera el menor, y errores críticos cuando se supera el segundo [26].

2.7.3 Check_DNS

Este comando permite hacer una consulta DNS para averiguar la dirección IP de un equipo dado el nombre o viceversa. Utiliza nslookup para ello; permite especificar el servidor DNS a usar o si no usa el o los especificados en /etc/resolv.conf [26].

2.7.4 Check_FTP

Este comando realiza comprobaciones de conexión a un servidor FTP remoto. Permite conocer el estado de este servicio [26].

2.7.5 Check_HTTP

Este comando comprueba servicios HTTP y HTTPS en equipos remotos. Permite además realizar el seguimiento de redirecciones, tiempos de conexión,

la expiración de los certificados para SSL, etcétera. Es especialmente útil para servidores web que sirvan de base para aplicaciones de comercio electrónico [26].

2.7.6 check_ifoperstatus

Este comando comprueba el estado de operación de interfaces de red remotas por medio de SNMP v1 o SNMP v3 [26].

2.7.7 Check_ifstatus

Este comando comprueba el estado general de interfaces de red remotas por medio de SNMP v1 o SNMP v3 [26].

2.7.8 Check_imap

Este comando realiza conexiones contra un servidor IMAP para comprobar su estado de funcionamiento. Permite generar advertencias y errores críticos [26].

2.7.9 Check_ircd

Este comando comprueba el funcionamiento de un servidor de IRC remoto. Realiza conexiones para ello, está escrito en Perl [26].

2.7.10 Check_ldap

Este comando realiza conexiones y búsquedas LDAP contra un servidor remoto y comprueba así su estado de funcionamiento y si responde dentro del tiempo esperado o no [26].

2.7.11 Check_load

Este comando trabaja en local en la máquina que está ejecutando el sistema Nagios. Comprueba la carga del sistema en función de unos umbrales que tiene preestablecidos y permite generar advertencias o errores severos según sea esta carga [26].

2.7.12 Check_log

Este comando es muy interesante para administradores del sistema. Funciona en local y permite buscar coincidencia de patrones en ficheros de suceso. Cuando el patrón que se busca es encontrado, Nagios recoge esta incidencia [26].

2.7.13 Check_mailq

Este comando funciona en local en la máquina que corre Nagios. Permite comprobar el número de mensajes que hay en espera en las colas de Sendai. Se puede establecer un límite para que se genere una notificación en ese caso [26].

2.7.15 Check_mrtg

Este comando también trabaja en local en la máquina que está ejecutando Nagios y permite monitorizar los ficheros de sucesos de MRTG; en concreto permite monitorizar cualquiera de los parámetros que se vuelcan sobre dichos ficheros como por ejemplo conexiones, carga del procesador, entrada, salida, etcétera. Permite establecer umbrales que si se superan generan notificaciones [26].

2.7.15 Check_mrtgtraf

Este comando permite comprobar el servicio UPS en un equipo remoto y establecer umbrales para, según el valor devuelto, disparar una advertencia, un error severo o nada [26].

2.7.16 Check_nagios

Este comando se ejecuta en la máquina que está ejecutando Nagios y permite comprobar que el archivo de sucesos del sistema de monitorización no sea más antiguo de lo que se especifique [26].

2.7.17 Negate

Este comando sirve para, en combinación con cualquiera de los otros Plugins, negar su valor. Por ejemplo, el uso normal del comando Check_FTP es que devuelve OK cuando el servicio esté funcionando y CRITICAL cuando no. Con este comando se invierten los valores. Es útil para cuando se desea tener notificación explícita de que algo está funcionando bien en lugar de cuando falla[26].

2.7.18 Check_nntp

Este comando establece conexiones NNTP contra un servidor remoto especificado para comprobar que el servicio de NEWS esté activo [26].

2.7.19 Check_nt

Este comando realiza peticiones a un equipo Windows NT/2000/XP remoto que esté ejecutando el servicio NSClient para comprobar parámetros locales a dicho equipo como por ejemplo uso de la CPU, de la memoria, del disco, etcétera [26].

2.7.20 Check_ntp

Este comando ejecuta ntpdate para comprobar que el timestamp de la máquina local que ejecuta Nagios no difiere en más de lo especificado del timestamp de una máquina remota dado [26].

2.7.21 Check_nwstat

Planificación, especificación, diseño y evaluación de redes Este comando realiza peticiones a un equipo Novell remoto que esté ejecutando el servicio MRTGEXT NLM para comprobar parámetros locales a dicho equipo como por ejemplo uso de la CPU, de la memoria, del disco, etcétera[26].

2.7.22 Check_oracle

Este comando permite comprobar el estado de un SGBD Oracle en un ordenador remoto así como el estado de los tablespaces, de bases de datos, de las caché, etcétera, de dicho servidor [26].

2.8 Protocolo SNMP

Una vez instalado el sistema de monitorización Nagios, sólo se tienen que definir los equipos y servicios que queremos monitorear. Para esto es conveniente conocer la forma en que Nagios funciona. En resumen, Nagios utiliza los plugin para monitorear los servicios y equipos. Los plugin pueden utilizar varios métodos para llevarlo a cabo, como ejecutar un simple ping, hacer una consulta vía SNMP o comunicarse con un cliente instalado en el equipo a monitorear. Lo que debemos hacer es definir las propiedades del equipo o servicio a monitorear en los archivos de configuración. En estas directivas es donde mandamos llamar a los plugin dependiendo de lo que queremos hacer. A partir de aquí, podemos comenzar a explotar todas las herramientas de Nagios, como definir contactos para enviar alertas, definir las veces que se monitorea un servicios, escalamiento de las alertas, etc.[24].

Un ejemplo de cómo funciona Nagios para monitorear un Router o un switch se ve en la siguiente imagen

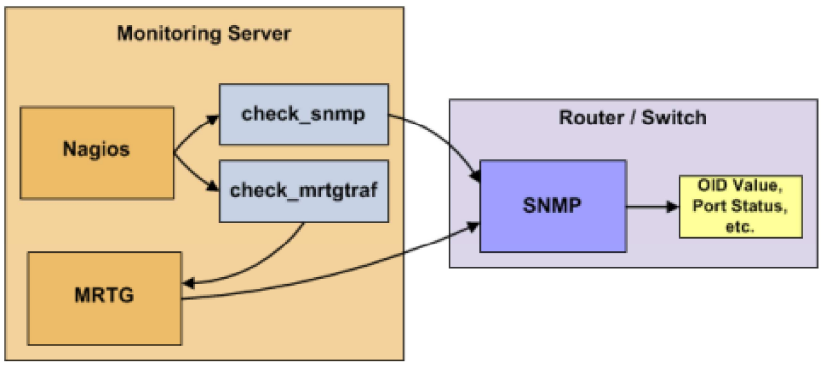


FIGURA 4: funcionamiento de Nagios mediante CHECK_SNMP

2.8.1 Definicion de SNMP

SNMP (Simple Network Management Protocol) es un protocolo de red diseñado para monitorear dispositivos conectados a la red. Utiliza OID (identificadores de objetos) para la definición de la información, conocida como MIB (Management Information Base), que pueden ser monitoreados.
El Management Information Base (MIB) presenta variables que permiten realizar un seguimiento diverso a atributos que describen el estado de los componentes críticos con el apoyo de su sistema.

Los identificadores de objetos asociados, proporcionan el estado general de todos los subsistemas críticos que estamos monitoreando y que proporcionan mucho más detalle, pero en esta situación, el requisito era que se le avise si un servidor tenía un problema y para indicar el subsistema particular que tenía el problema. Un subsistema no se abordó en el "Estado del sistema" Grupo capítulo-el subsistema RAID. Hay, sin embargo, un OID de control de ésta".

Para el desarrollo de la gestión de redes en inter-redes basadas en TCP/IP, el IAB (Internet Activities Board) decidió seguir la estrategia de usar a corto plazo el Simple Network Management Protocol (SNMP) para gestionar los nodos, proponiendo para largo plazo la estructura de gestión de redes OSI. Se escribieron entonces dos documentos para definir la gestión de la información: RFC 1065 que definía la Estructura de la Información de Gestión (Structure of Management Information, SMI), y RFC 1066, que definía la Base de Información de Gestión (Management Information Base, MIB). Ambos documentos fueron diseñados para ser compatibles con la estructura SNMP y la de gestión de redes OSI.

2.8.1.1 Ventajas de Monitoreo con SNMP [25]

La ventaja fundamental de usar SNMP es que su diseño es simple por lo que su implementación es sencilla en grandes redes y la información de gestión que se necesita intercambiar ocupa pocos recursos de la red. Además, permite al usuario elegir las variables que desea monitorizar sin más que definir:

- El título de la variable.
- El tipo de datos de la variable.
- Si la variable es de sólo lectura o también de escritura.
- El valor de la variable.

Otra ventaja de SNMP es que en la actualidad es el sistema más extendido. Ha conseguido su popularidad debido a que fue el único protocolo que existió en un principio y por ello casi todos los fabricantes de dispositivos como puentes y enrutadores diseñan sus productos para soportar SNMP.
La posibilidad de expansión es otra ventaja del protocolo SNMP: debido a su sencillez es fácil de actualizar.

2.8.1.2 Desventajas de monitoreo con SNMP [25]

El protocolo SNMP en su versión 1 no es ni mucho menos perfecto. Presento fallos que con el tiempo se han ido corrigiendo.
La primera deficiencia de SNMP en la versión uno es que presentaba fallos de seguridad que permitían a intrusos acceder a información que lleva la red. Todavía peor, estos intrusos podían llegar a bloquear o deshabilitar terminales.
La solución a este problema es sencilla y se ha incorporado en la nueva versión SNMPv2. Básicamente se han añadido mecanismos para resolver:
Privacidad de los datos, que los intrusos no puedan tomar información que va por la red.

Autentificación, para prevenir que los intrusos manden información falsa por la red.
Control de acceso, que restringe el acceso a ciertas variables a determinados usuarios que puedan hacer caer la red.
El mayor problema de SNMP es que se considera tan simple que la información está poco organizada, lo que no lo hace muy acertado para gestionar las grandes redes de la actualidad. Esto se debe en gran parte a que SNMP se creó como un protocolo provisional y no ha sido sustituido por otro de entidad.
De nuevo este problema se ha solucionado con la nueva versión SNMPv2 que permite una separación de variables con más detalle, incluyendo estructuras de datos para hacer más fácil su manejo. Además SNMPv2 incluye dos nuevas PDU's orientadas a la manipulación de objetos en tablas.

2.8.2 CHECK_SNMP.

Nagios ejecuta el comando check_snmp, al cual se le pasan los parámetros definidos en la directiva “define host”. El comando a su vez lanza una petición SNMP para obtener los valores que nos interesan. El Router/switch envía la información de vuelta para que Nagios la procese y actúe conforme se tiene definido.

Los Switches y Routers pueden ser monitoreados fácilmente haciendo un simple ping para determinar pérdida de paquetes, RTA, etc. Si el switch soporta SNMP, se puede monitorear el estado de los puertos, etc. con el plugin check_snmp
El plugin utilizado check_snmp, puede ser utilizado si se compila e instala los paquetes net-snmp y net-sn, p-utils en el sistema Nagios, ´para corroborar esto, se puede visualizar la existencia del plugin en /usr/local/Nagios/libexec. Si estos paquetes no están instalados no se puede monitorear a través de SNMP.

2.8.3 Funcionamiento de CHECK_SNMP

El sistema de monitorización Nagios simplifica la instalación de su configuración al traer preinstaladas por decirlo de cierta forma algunos parámetros importantes para el chequeo que se realiza por SNMP como la agregación de dos definiciones de comandos principales una de esas corresponde a check_snmp, que se encuentra dentro del archivo de configuración Commands.cfg. Esto le permite utilizar los Plugins check_snmp para monitorear Routers de red.

Este archivo puede ser localizado en el directorio raíz /usr/local/Nagios/etc/objects/.

Por ser la configuración inicial de monitorización de Nagios, se hace necesario que se observe si el router o switch soporta SNMP, teniendo en cuenta esto, se podrá saber que equipos se pueden monitorear y a su vez, acceder a la información con la utilización de este plugin.
Al tener este punto claro se procede a la implementación del plugin en el sistema Nagios mediante el siguiente código:

```
Define service {
 Use   generic-service ; Inherit values from a template
 host_name   linksys-srw224p
 service_description Uptime
 check_command  check_snmp!-C public -o sysUpTime.0
 }
```

Esta sentencia sirve para monitorear el tiempo de actividad (Uptime) de un switch.

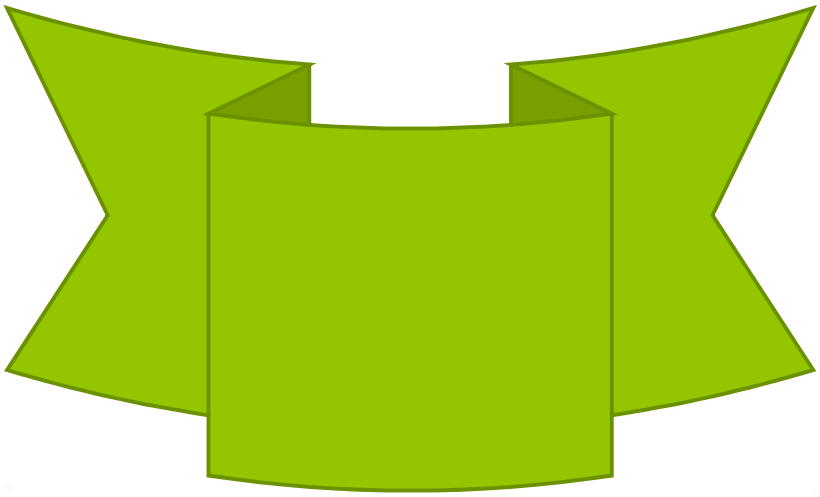
En la directiva check_command de la definición de servicio anterior, el "-C public" le dice al plugin que la comunidad SNMP que va a ser utilizada es "public" y el "-o sysUpTime.0" indica cual OID deberá ser revisada.

Una vez agregada la nueva definición de servicio y equipo en el archivo switch.cfg, se puede iniciar el proceso de monitorización de Switches y Routers, para esto se hace necesario reiniciar el sistema Nagios mediante la línea de comando ingresada en la consola terminal del sistema operativo UNIX.

3

CAPITULO

INSTALACIÓN DE NAGIOS Y SISTEMAS UTILIZADOS



3.1 Descripción de Herramientas Utilizadas Para el Monitoreo de Red

Para el desarrollo de la práctica se hace necesaria la implementación de diferentes herramientas que relacionadas entre sí, permiten mostrar el funcionamiento de la herramienta de monitorización. Estas herramientas son:

3.1.1 Programas

3.1.1.1 VMware Workstation Versión 7.1

Es un sistema de virtualización por software compatible con ordenadores x86. El software VMware puede funcionar en las plataformas Windows, Linux y Mac. Un sistema virtual por software es un programa que simula un sistema físico con características de hardware determinadas.

Un virtualizador de software permite ejecutar o simular varios ordenaros dentro de un mismo hardware de manera simultánea, permitiendo así el mayor aprovechamiento de recursos. Es posible decir que VMware es parecido al programa Virtual PC, aunque existen discrepancias entre ambos que afectan en la forma como el software interactúa con el sistema físico. Mientras que Virtual PC emula una plataforma x86, VMware la virtualiza, de forma que la mayor parte de las instrucciones de VMware se ejecuten directamente sobre el hardware físico, ya que en el caso de Virtual PC se traducen en llamadas al sistema operativo que se ejecuta en el sistema físico.

VMware brinda una versión de prueba por 30 días, la cual es posible descargar en:
http://downloads.vmware.com/d/info/desktop_downloads/vmware_workstation/7_0

3.1.1.2 Nagios

Es la herramienta Open Source de monitorización de sistemas Unix/Linux más conocida. Nagios puede también monitorizar sistemas Windows mediante la instalación de un agente en la máquina a monitorizar, aunque la parte servidor de Nagios debe residir en un servidor Unix/Linux. Debido a que es una aplicación de código abierto la cual se rige por los reglamentos de la licencia pública general de GNU es posible su obtención mediante su página principal. La última versión se puede localizar en http://www.nagios.org/download/core/thanks/

3.1.1.3 Plugin de Nagios

Son complementos que se integran con la aplicación o herramienta Nagios y tienen como función principal la de evaluar y monitorear una aplicación, un servicio o un protocolo en particular. La versión oficial de Nagios nos brinda un conjunto de Plugins que pueden ser usados para monitorear una variedad de servicios y protocolos. El sitio web de Nagios nos provee la posibilidad de descargar sobre 50 plugins para empezar a monitorear todos los servicios y protocolos básicos. Estos se pueden encontrar en la dirección web http://www.nagios.org/download/plugins.

3.1.1.4 NetMeeting

Es una herramienta de videoconferencia VoIP y multipunto que se incluyen en muchas versiones de Windows, desde Windows 95 hasta Windows XP. En este estudio, se utilizó para general tráfico entre los distintos computadores y de esta manera monitorear los diferentes servicios y protocolos que esta aplicación brinde y utilice. Se puede conseguir de manera gratuita en el centro de descarga de Microsoft por medio de la dirección web

http://www.microsoft.com/downloads/details.aspx?familyid=26c9da7c-f778-4422-a6f4-efb8abba021e&displaylang=en

3.1.1.5 Unreal Tournament

Es un videojuego de acción en primera persona. Lanzado al mercado en 1999, es la continuación del juego Unreal de Epic Games, y su principal enfoque es la acción para multijugador. Es considerado uno de los mejores videojuegos multijugador debido al enorme rendimiento que brinda a sus usuarios. Su utilidad es similar a la herramienta NetMeeting, que nos permitirá monitorear protocolos tanto UDP como TCP usados por esta videojuego en línea.

3.1.1.6 Network Traffic Emulator

Software que genera trafico IP/ICMP/TCP/UDP/HTTP para evaluar y testear servidores, Routers, ordenadores y cortafuegos mediante una carga robusta de red. Es u programa muy simple y rápido el cual puede simular la actividad del cliente. Para generar un tráfico específico nos provee de parámetros sobre la fuente/destino, además de especificar el número de paquetes a simular. El programa de simulación de tráfico se puede descargar desde la dirección de web http://www.brothersoft.com/trafficemulator-35615.html

3.1.1.7 Microsoft Office 2010

Es una versión de la suite ofimática Microsoft Office de Microsoft y sucesora de Microsoft Office 2007 conocida también como Office 14. Office 2010 incluye compatibilidad extendida para diversos formatos de archivos, actualizaciones de la interfaz de usuario, y una experiencia de usuario refinada. Una versión trial de esta herramienta se puede obtener en http://office.microsoft.com/en-us/try/try-office-2010-FX101868838.aspx?WT.mc_id=MiG_Products

3.1.2 Sistemas Operativos:

3.1.2.1 Microsoft Windows XP

Proporciona un nuevo estándar en confiabilidad y desempeño. Este sistema operativo está diseñado para negocios de todos tamaños y para usuarios que demandan el máximo desempeño de su experiencia informática. Tomando como punto de partida el ya probado sistema operativo Windows 2000, Windows XP Professional representa una base de total confianza que mantendrá los equipos en perfecto funcionamiento siempre que sea necesario.
Se brinda una versión con el service pack 2 en http://www.microsoft.com/downloads/details.aspx?familyid=049c9dbe-3b8e-4f30-8245-9e368d3cdb5a&displaylang=es

3.1.2.2. Ubuntu

Es una distribución de Linux orientada a escritorio, basada en Debian GNU/Linux pero enfocado en la usabilidad, lanzamientos regulares y fáciles de instalación.
Ubuntu es patrocinado por la empresa Canonical Ltd. de Mark Shuttleworth, y es un sistema operativo libre y de código abierto. Además, al mantenerlo libre y gratuito, la empresa es capaz de aprovechar los desarrolladores de la comunidad en mejorar los componentes de su sistema operativo. Canonical también apoya y proporciona soporte para cuatro derivaciones de Ubuntu: Kubuntu, Xubuntu, Edubuntu y la versión de Ubuntu orientada a servidores. Una versión de Ubuntu se localiza en http://www.ubuntu.com/desktop/get-ubuntu/download

3.2 Topología de Red

La topología de red se puede definir como la disposición física en la que se conecta una red de ordenadores. Si una red tiene diversas topologías se la llama mixta. Entre las más comunes encontramos:

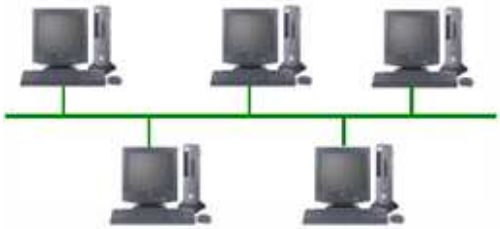
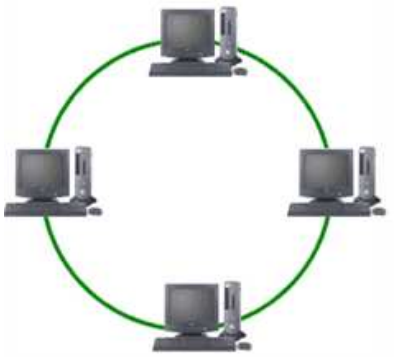
<table>
<tr><td>  </td><td>  </td></tr>
<tr><td>Topología en Malla</td><td>Topología de Bus</td></tr>
<tr><td colspan="2">  </td></tr>
<tr><td colspan="2">Topología en Estrella</td></tr>
<tr><td>  </td><td>  </td></tr>
<tr><td>Topología de Anillo</td><td>Topología en Árbol</td></tr>
</table>

TABLA 3: Topologías de red más comunes.

3.2.1 Selección de Topología

En nuestra implementación de monitoreo de red se utilizó la topología de red tipo árbol como se puede observar a continuación:

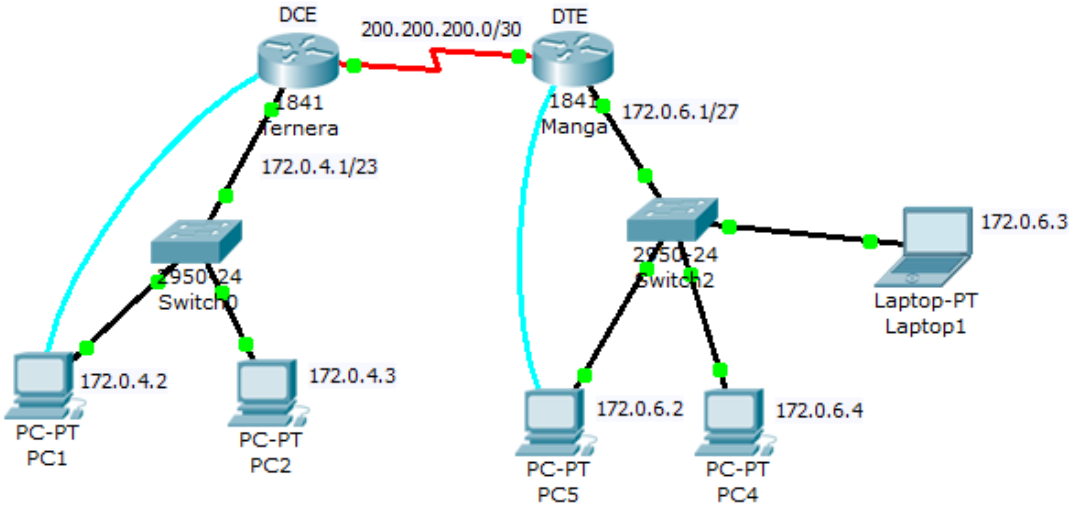


FIGURA 5: Topología de Red implementada en la práctica.

Como se puede observar en la figura x1, la red utilizada en la implementación de un monitoreo con la herramienta Nagios encuentra constituida por los siguientes elementos:

- 2 Routers: 1 Puertos Seriales DCE y DTE.
- 2 Switches: 2 Puertos FastEthernet, es decir, 1 Puerto por Switch.
- Computadores Personales: 4 Puertos Ethernet (uno por cada PC).
- 2 Cables de Consola.
- 7 Cables Directos.

3.3 Descripción de los Elementos Utilizados en la Topología:

Los distintos materiales que se usaron para la implementación de la red en las instalaciones de la UTB, se describen a continuación con sus respectivas características y especificaciones.

3.3.1 Routers

Cantidad Usada: 2

Marca: Cisco 2800 Series

Especificaciones: Descripción del producto

- Modelo de Producto: Router de servicios integrados 2811 Bundle de voz
- Gama de Producto: 2800
- Interfaces/Puertos: 2 x 10/100Base-TX LAN
- Detalles de Interfaces/Puertos: 2 x RJ-45 10/100Base-TX LAN 2 x USB 1.1 1 x RJ-45 Auxiliar Gestión 1 x RJ-45 Consola Gestión
- Ratio de Transferencia de Datos: 10Mbps Ethernet 100Mbps FastEthernet Hasta 115,2Kbps Consola Hasta 115,2Kbps Auxiliar
- Tipo de Conexión: Par Trenzado 10/100Base-TX
- Ranuras Expansión: 9 x Ranura de expansión
- Protocolos: TCP/IP SNMP v3 SSH v2 SRTP VoIP H.323 MGCP VoFR ATM VoATM

Características:

- Fabricante: Cisco Systems, Inc.
- Integración con Cisco Unified Communications Manager Express para soporte de procesamiento de llamadas de hasta 96 usuarios.
- Integración con Cisco Survivable Remote Site Telephony (SRST) para mantener los servicios de voz locales en caso de pérdida de la conexión.
- Mayor confiabilidad y flexibilidad que le permite dar prioridad al tráfico de voz o al intercambio de datos para que la entrega de información se adapte a las necesidades de su empresa.
- Soporte para conexiones de red privada virtual para conectar Socio de Negocios u oficinas remotas.
- Diferentes opciones de conectividad de banda ancha y red.

3.3.2 Switches

Cantidad Usada: 2

Marca: Cisco Catalyst 2960 Series

Características:

- Soportan voz, video, datos y acceso seguro.
- Opción de Fast Ethernet (transferencia de datos de 100 megabits por segundo) o Gigabit Ethernet (transferencia de datos de 1000 megabits por segundo), en función del precio y sus necesidades de rendimiento.
- Varias configuraciones de modelo con la capacidad de conectar escritorios, servidores, teléfonos IP, puntos de acceso inalámbrico, cámaras de TV de circuito cerrado u otros dispositivos de red.

- Capacidad de configurar LAN virtuales de forma que los empleados estén conectados a través de funciones de organización, equipos de proyecto o aplicaciones en lugar de por criterios físicos o geográficos.
- Seguridad integrada
- Funciones de supervisión de red y solución de problemas de conectividad mejoradas.
- Actualizaciones de software sin gastos adicionales.

Especificaciones:

Descripción del producto:

- Cisco Catalyst 2960-24TT
- Tipo de dispositivo Conmutador Factor de forma Externo
- Dimensiones(An x Pro x Al): 44.5 cm x 23.6 cm x 4.4 cm
- Peso 3.6 kg
- Memoria RAM 64 MB
- Memoria Flash 32 MB
- Cantidad de puertos 24 x Ethernet 10Base-T, Ethernet 100Base-TX
- Velocidad de transferencia de datos 100 Mbps
- Protocolo de interconexión de datos Ethernet, Fast Ethernet
- Puertos auxiliares de red 2x10/100/1000Base-T
- Protocolo de gestión remota SNMP 1, RMON, Telnet, SNMP 3, SNMP 2c

3.3.3 Computadores Personales

Cantidad: 4

Marca: Dell

Serie: OptiPlex 755 Desktop

Características: Ofrece una personalización sencilla, una implementación rápida y gran capacidad de adaptación sean cuales sean las necesidades de su empresa.

Especificaciones:

Descripción del producto:

- Microprocesador Core 2 Dúo
- Tarjeta gráfica ATI Radeon 2400 de 256MB
- 2GB RAM DDR2
- Disco duro de 250 GB
- Grabadora de DVD
- Teclado
- Mouse
- Sistema Operativo Microsoft XP

3.3.4 Cables Seriales

Cantidad: 1 DTE y 1 DCE

Marca: Cisco System

Características: Estos cables son capaces de trabajar con Routers incluyendo los modelos más populares como el 2801, 2811, 2821, 3825, 3845, 2621, 1721 y muchos otros.

Especificaciones: Los 26 pin del cable serial son usados para conectar una tarjeta de interfaz Cisco WAN incluyendo WIC-2T y WIC-2A/S.

3.3.5 Cables directos

Cantidad: 7

Características: Son aquellos que implementan una conexión pin a pin y se suelen utilizar para conectar un PC a un HUB Ethernet, a un Router, a un switch, etc.

Especificaciones:

- Soportan tanto su uso en redes de 10, 100 o 200 Mbits/seg
- Están provistos en sus extremos de conectores del tipo RJ45 macho

- Se ha utilizado cables mallados multipar de categoría 5 E (CAT5E) lo cual garantiza un muy bajo nivel de pérdida de señal y minimiza o anula totalmente las interferencias electromagnéticas del ambiente

3.3.6 Cables de Consola

Cantidad: 2
Marca: Cisco Systems
Serie: Cable de Consola de DB9 a RJ45
Características:

- Usada para conectar el puerto serial del computador al puerto consola RJ45 de un router cisco.
- El conector DB9 al puerto serial de la computadora.
- Largo del Cable: 1.9 metros.
- Peso: 79.2 g

3.4 Instalación de Nagios con Ubuntu

Por medio de esta guía, se pretende proveer con simples instrucciones sobre cómo instalar Nagios en el sistema operativo Ubuntu y tenerlo monitoreando una maquina local dentro de 20 minutos. La instalación fue realizada con la versión de Ubuntu 7.10.

Mediante el correcto seguimiento de las instrucciones, al finalizar se tendrá a:

- Nagios y los plugins instalados en /usr/local/Nagios
- Nagios configurado para monitorear unos pocos aspectos del ordenador local, ya sea, carga de CPU, uso del disco, memoria, etc.
- La interfaz web de Nagios será accesible en http://localhost/nagios/

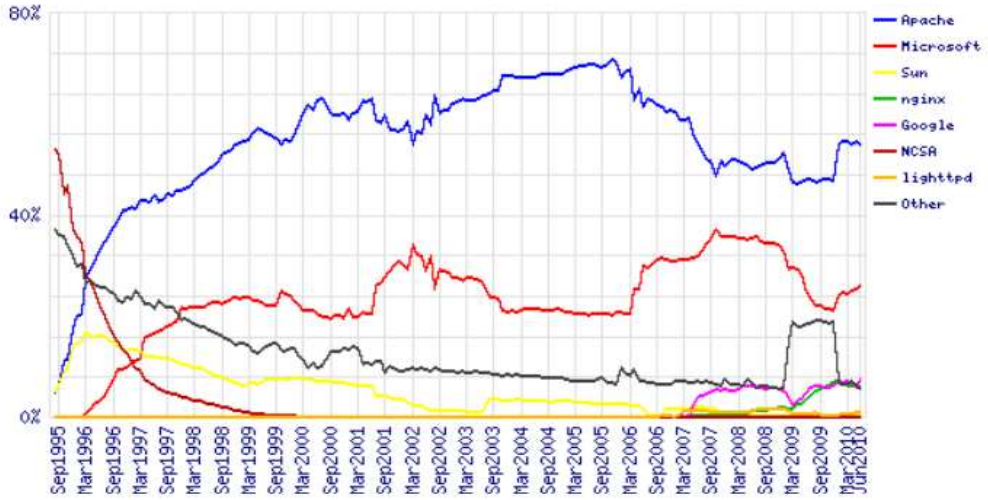
3.4.1 **Paquetes Requeridos**

1. Apache 2: Es un servidor de páginas web gratuito que se acopla muy bien con el lenguaje PHP y herramientas de gestión de bases de datos como MySQL, además es uno de los más utilizados en los últimos 11 años de acuerdo a la gráfica brindada por el sitio web http://www.netcraft.com/, el cual se puede observar en la figura X.

   Apache presenta características configurables, bases de datos de autenticación y negociación de contenido, pero fue criticado por la falta de una interfaz gráfica que ayude en su configuración. Entre otras características se tiene:

   - ✓ Apache es un servidor web multiplataforma y de código abierto.
   - ✓ Puede ser adaptado a diferentes entornos y necesidades, y gracias a esto se han desarrollado diversas extensiones entre las que destaca PHP.
   - ✓ Basado en hebras[1] en la versión 2.0.

[1] Característica que permite a una aplicación realizar varias tareas a la vez. http://es.wikipedia.org/wiki/Hebra_%28software%29



Developer	May 2010	Percent	June 2010	Percent	Change
Apache	112,663,533	54.68%	111,792,321	54.02%	-0.67
Microsoft	52,062,154	25.27%	53,865,345	26.03%	0.76
Google	12,357,212	6.00%	15,375,950	7.43%	1.43
nginx	13,490,726	6.55%	11,264,229	5.44%	-1.11
lighttpd	1,869,658	0.91%	1,704,797	0.82%	-0.08

FIGURA 6: Comparación de Servidores Web.

2. PHP (PHP Hipertext Preprocessor): Se trata de un lenguaje de programación del lado del servidor. Es un lenguaje que brinda una licencia de código abierto certificada por la iniciativa de código abierto[2]. Su funcionamiento consta de que en el momento que un usuario envía una petición HTML al servidor, este interpreta el código PHP y envía la correspondiente respuesta al usuario en cuestión.

   Una gran ventaja de PHP es la posibilidad de conexión con servidores de bases de datos como Postgress o como MySQL, lo cual permite realizar consultas SQL mediante PHP.

[2] Licencia de PHP - http://www.php.net/license/

3. Compilador GCC y librerías de desarrollo: Conjunto de compiladores creados por el proyecto GNU. tiene como objetivo mejorar el compilador usado en los sistemas GNU incluyendo la variante GNU/Linux. Es compilador de software libre distribuido por la fundación del software libre bajo la licencia GPL[3].

4. Librerías de desarrollo GD: Es una librería de código abierto para la creación de imágenes dinámicas por programadores. Está escrito en C, y se encuentra disponible para PERL, PHP y otros lenguajes. GD crea imágenes de tipo GIF, JPEG y PNG.

   Nagios lo utiliza para generar estadísticas por medio de gráficas, reportes, imágenes en miniatura, entre otras.

3.4.2 **Instalación de paquetes Prerrequisitos.**

Ingresando a la Terminal del sistema operativo Ubuntu es posible obtener los paquetes requeridos a través de los siguientes comandos, teniendo en cuenta que es necesaria una conexión a internet.

Apache 2: *sudo apt-get install apache2*
PHP: *sudo apt-get install libapache2-mod-php5*
Compilador GCC y Librerías de Desarrollo: *sudo apt-get install build-essential*
Librerías de Desarrollo GD: *sudo apt-get install libgd2-xpm-dev*

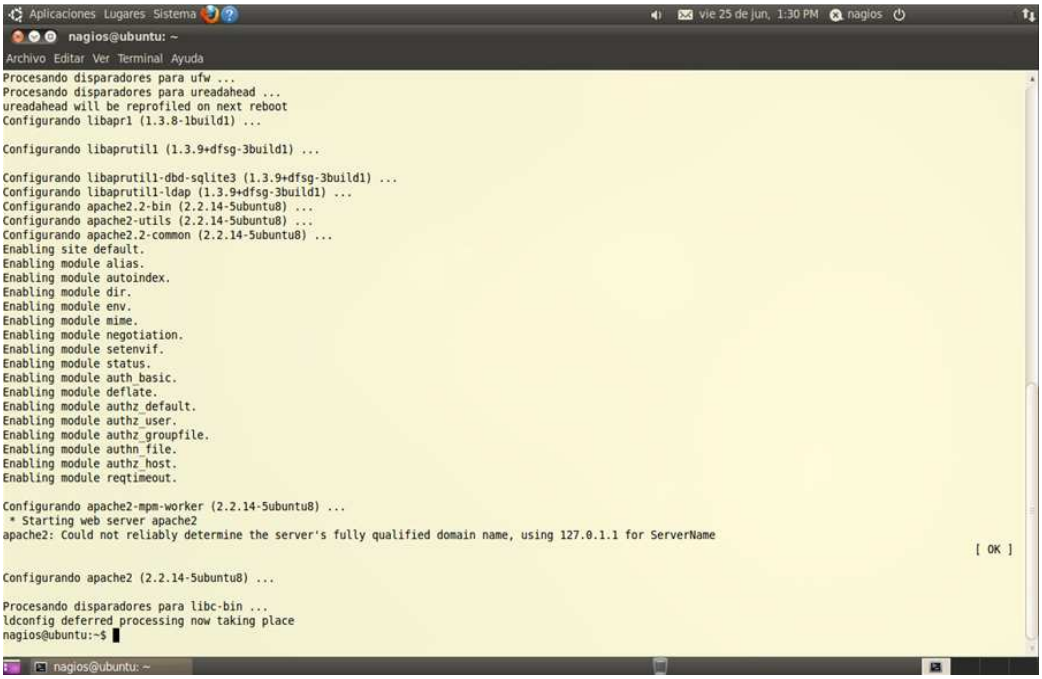
A continuación por medio de representaciones visuales se puede observar la instalación de cada uno de estos paquetes. Luego de finalizar la instalación, se seguirá con el siguiente paso, el cual es la creación de una cuenta de usuario y su respectivo password.

[3] GNU General Public License - http://www.gnu.org/copyleft/gpl.html

3.4.3 Instalación de Paquete de Apache 2 en Ubuntu

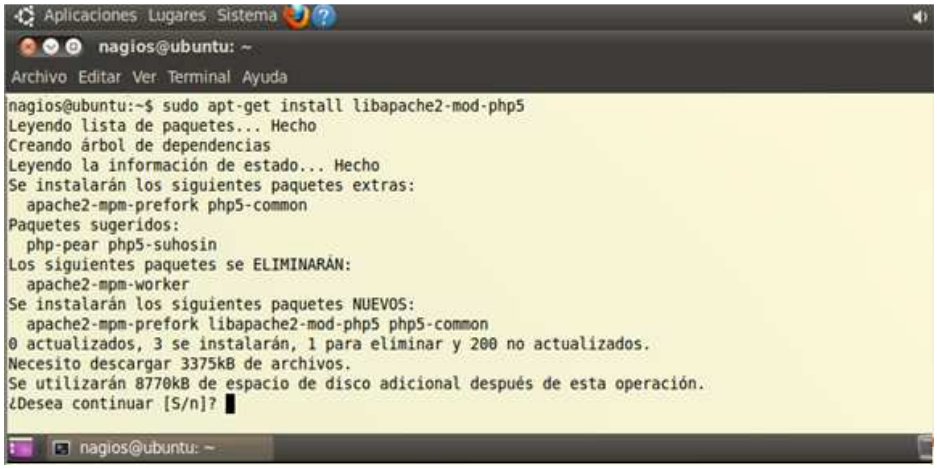
Para la instalación de cada uno de los paquetes requeridos por la herramienta de monitoreo Nagios, es necesario ingresar a la consola del sistema operativo utilizado en este caso Ubuntu y estar conectado a Internet. Desde la consola escribir *sudo apt-get install apache 2* para descargar apache.

Se confirma la utilización del espacio por la descarga y su próxima instalación como nos muestra el siguiente gráfico.

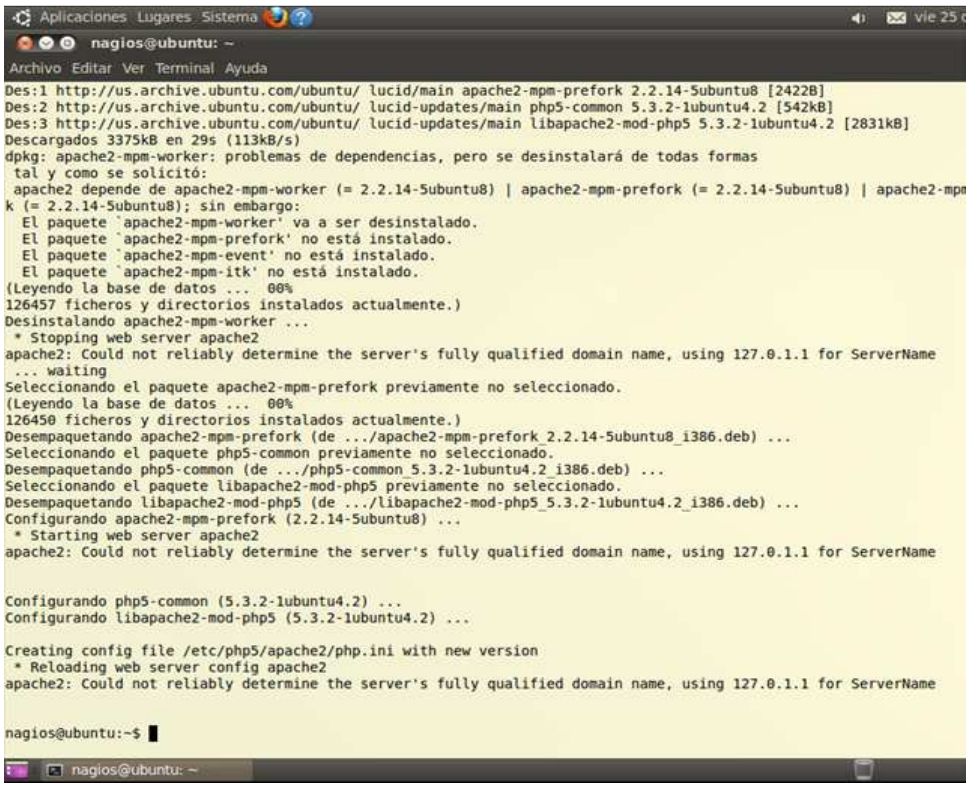


3.4.4 Instalación de Paquete de PHP

Desde la consola escribir *sudo apt-get install libapache2-mod-php5* para descargar el soporte a PHP.



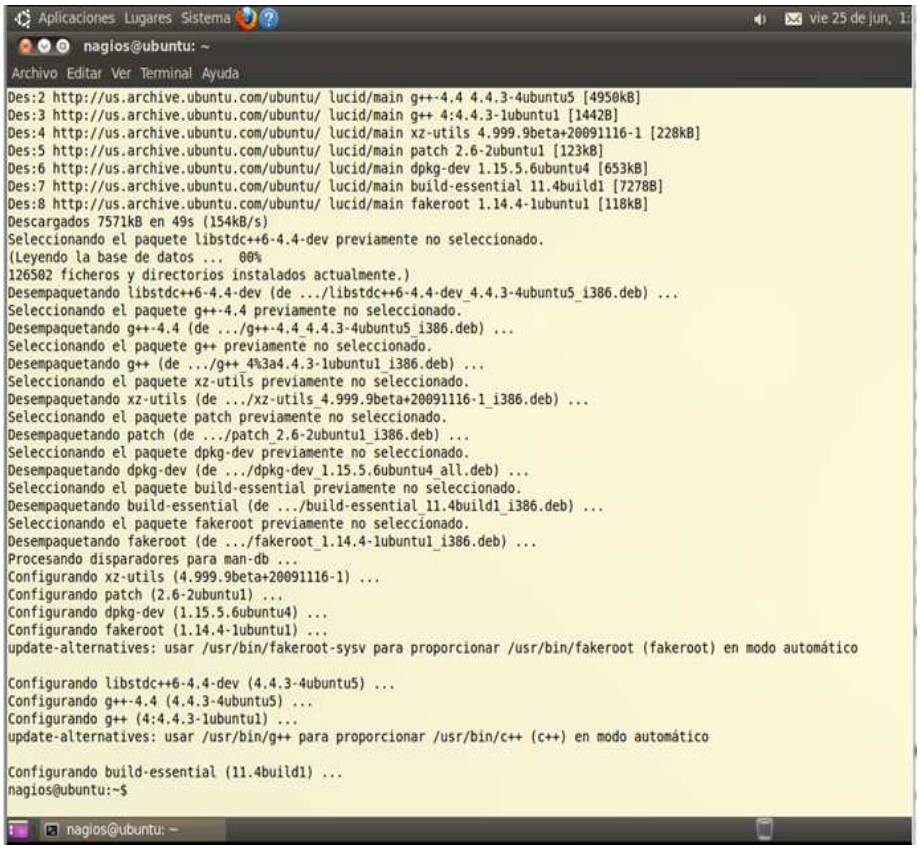
Confirmar el uso de espacio e instalación.



3.4.5 Instalación del Compilador GCC y Librerías de Desarrollo

Desde la consola escribir *sudo apt-get install build-essential* para descargar las librerías y el compilador GCC

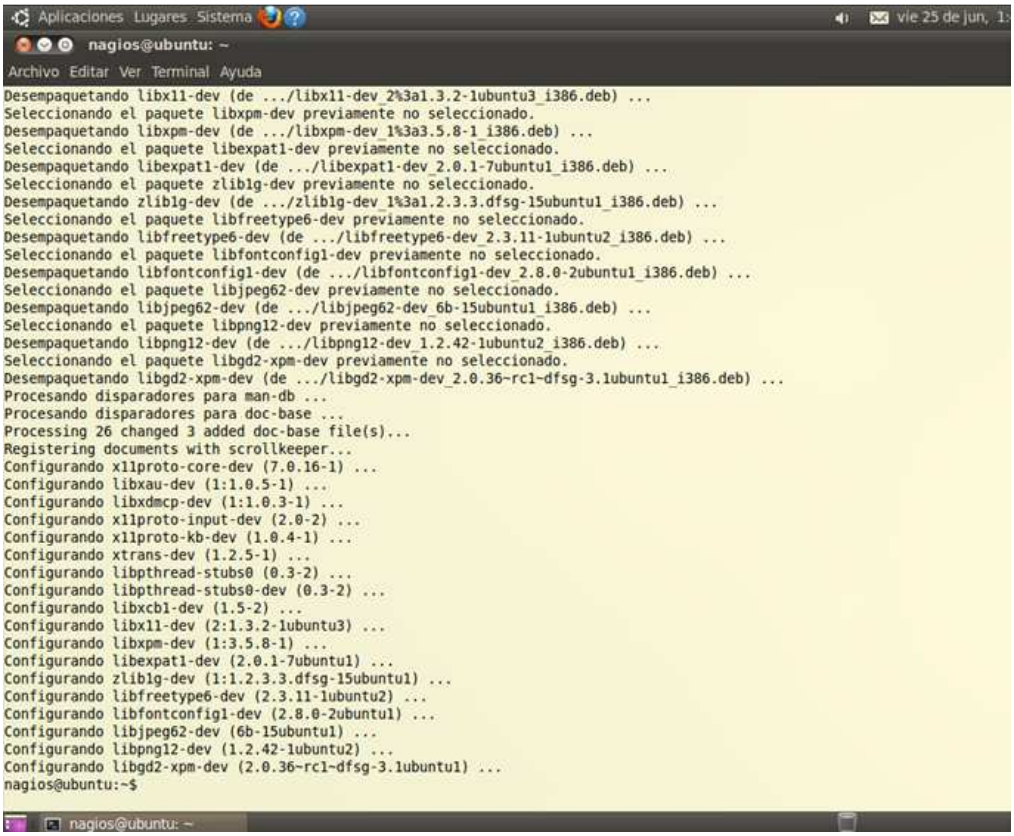
Confirmar el uso de espacio en disco e instalación.



3.4.6 Instalación de las Librerías de Desarrollo GD

Desde la consola escribir *sudo apt-get install libgd2-xpm-dev* para descargar las librerías de desarrollo GD

Confirmar el uso de espacio en disco e instalación.



3.4.7 Crear Cuenta de Usuario

Para la utilización y administración de la herramienta Nagios, es requerida una cuenta de usuario que permita gestionar la aplicación y así agregar cada una de las utilidades que nos brinda.

1. Convertirse en usuario root con el comando: *sudo –s*
2. Crear un nuevo usuario Nagios y darle una contraseña
   /usr/sbin/useradd –m –s /bin/bash nagios
   passwd Nagios
3. Crear un nuevo grupo denominado *nagcmd* para permitir que comandos externos admitidos a través de la interfaz web. Adicionar el usuario Nagios y el usuario apache al grupo.
   /usr/sbin/groupadd nagcmd
   /usr/sbin/usermod –a –G nagcmd nagios
   /usr/sbin/usermod –a –G nagcmd ww-data

Ya creado el usuario y agregado al grupo nagcmd. El siguiente paso es la descarga de Nagios y de los Plugins.

3.4.8 Descargando Nagios y sus Plugins

Crear un directorio para almacenar las descargas.
mkdir ~/downloads
cd *~/downloads*

Descargar el código fuente de Nagios y de sus plugins. Las siguientes direcciones fueron testadas con Nagios 3.1.1 y Nagios Plugins 1.4.11.

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

wget http://prdownaloads.sourceforge.net/sourceforge/nagios/nagios-plugins-1.4.11.tar.gz

3.4.9 Compilación e Instalación de Nagios

Se extrae el archivo descargado del código fuente de Nagios.

cd *~/downloads*
tar xzf nagios-3.2.0.tar.gz
cd nagios-3.2.0

Ejecutar el script de configuración de Nagios, pasándole el nombre del grupo que fue creado previamente.

./configure –with-command-group=nagcmd

Compilar el código fuente de Nagios.

make all
make install
make install-init
make install-config
make install-commandmode

Aun no se debe iniciar Nagios, ya que es necesario realizar algunas configuraciones.

3.4.10 Configuraciones Específicas

Los archivos de configuración han sido instalados en el directorio /usr/local/Nagios/etc. Estos archivos deberían trabajar bien en la ejecución de Nagios. Pero, se requiere realizar algunos ajustes antes de proceder.

Editar el archivo de configuración */usr/local/Nagios/etc/objetcs/contacts.cfg* con algún editor y cambiar la dirección de correo asociada con el contacto *nagiosadmin* y colocar una en la cual se desee recibir alertas.

vi /usr/local/Nagios/etc/objetcs/contacts.cfg

3.4.11 Configuración de la Interfaz Web

Instalar el archivo de configuración web de Nagios en el directorio de configuración de apache.

make install-webconf

Crear una cuenta de nagiosadmin para loguearse en la interfaz web de Nagios. Recordar la contraseña asignada a esta cuenta.

htpasswd –c /usr/local/Nagios/etc/htpasswd.users nagiosadmin

Reiniciar el servidor Apache para que las nuevas configuraciones tengan efecto.

/etc/init.d/apache2 reaload

3.4.12 Compilación e Instalación de los Plugins de Nagios

Se utiliza un método parecido a la instalación de la herramienta de red Nagios. Primero se extrae los archivos descargados:

cd *~/downloads*
tar xzf nagios-plugins-1.4.11.tar.gz
cd nagios-plugins-1.4.11

Posteriormente, se compila e instalan los plugins.

./configure –with-nagios-user=nagios –with-nagios-group=nagios
make
make install

3.4.13 Iniciación de Nagios

Configurar Nagios para que se inicie automáticamente cuando el sistema se carga.
ln –s/etc/init.d/Nagios /etc/rcS.d/s99nagios

Verificar los archivos de configuración de Nagios.
usr/local/Nagios/bin/Nagios –v /usr/local/Nagios/etc/nagios.cfg

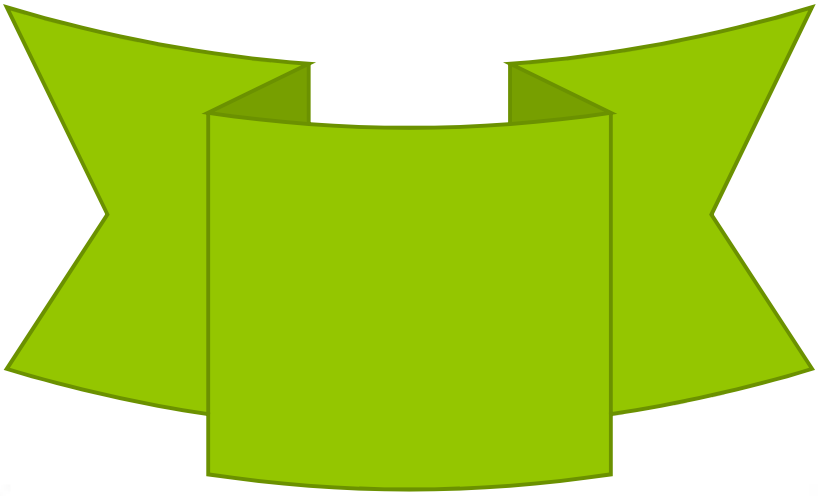
Si no hay algún error, inicie Nagios.
/etc/init.d/Nagios start

De esta manera, se podrá tener una instalación satisfactoria de la herramienta de monitorización Nagios bajo el sistema Ubuntu.

4

CAPITULO

GESTION Y REPORTE DE UNA RED CON NAGIOS



GESTION Y REPORTE DE UNA RED CON NAGIOS

La finalidad de este capítulo es explicar la manera de cómo configurar los dispositivos de una red, y así mismo establecer las configuraciones que se dan dentro de los archivos de configuración de la herramienta de monitorización NAGIOS, para así poder definir los reportes del estado de la red mediante histogramas y reportes habilitados por la misma herramienta.

4.1 Configuración de Red

Las configuraciones de red se realizaron teniendo en cuenta como principal ayuda el manual de la herramienta NAGIOS. A continuación se muestra de manera general los diferentes ajustes que se hicieron:

Se usó la versión 1 de SNMP en todos los dispositivos.

Comunidades:
ComunidadPublic: Permisos de solo lectura.
ComunidadPrivate: Permisos de solo lectura y escritura.

Se configuro el protocolo de gestión de red SNMP para cada dispositivo.

Se definieron 2 grupos para los Routers y computadores respectivamente.

Para cada grupo se definieron los dispositivos correspondientes teniendo él cuenta el tipo de dispositivo.

A cada dispositivo, se le especificaron los diferentes servicios a monitorear.

Se generaron estadísticas definidas por la herramienta NAGIOS, como por ejemplo, top 25 de Ping más rápido, etc.

4.1.1 CONFIGURACIÓN DE ROUTER.

Para configurar los router de la red, se usaron los siguientes comandos los cuales especificaran en detalle a continuación por cada router.

Router 1:

- ✓ Interfaces Seriales:

```
Interface Serial0/3/0
Ip address 192.168.1.1
255.255.255.0
Clock rate 125000
No shutdown
```

```
Interface Serial0/3/1
no ip address
shutdown
```

Se usó la serial 0/3/0, en la cual se define la ip 192.168.1.1 que corresponde a la primera WAN con su respectiva mascara. Esta interfaz se definió como la DCE, cuyo clock rate es de 125000. La otra interfaz serial no se utilizó, por lo que se encuentra abajo o shutdown.

- ✓ **Interfaces FastEthernet:**

```
Interface fastethernet0/0
Ip address 192.168.10.1
255.255.255.0
Duplex auto
Speed auto
No shutdown
Ip nat inside
```

```
Interface fastethernet0/1
Ip address dhcp
Duplex auto
Speed auto
No shutdown
Ip nat outside
```

Para definir la primera LAN, se utilizó la interface FastEthernet 0/0 del router 1, con la ip 192.169.10.1 y mascara 255.255.255.0. Así mismo se definió la interface FastEthernet 0/1 para la entrada de internet bajo NAT, en la cual se muestra la siguiente configuración en el router, no en las interfaces.

```
Ip route 0.0.0.0 0.0.0.0 fastethernet0/1 dhcp
Access-list 100 permit ip 192.168.10.0 0.0.0.255 any
Access-list 100 permit ip 192.168.12.0 0.0.0.255 any
Ip nat inside source list 100 interface fastethernet0/1
overload
```

Mediante la secuencia de estos comandos, se puede tener navegación a internet dentro de un router. La primera línea se aplica para indicar que enrrute todo el tráfico, la segunda se aplica, para controlar que segmentos de la red pueden salir a internet, se definieron los dos router que tienen salida, y la tercera línea se realiza este comando para realizar NAT al segmento de ip privada.

- ✓ **Definiendo las Subredes:**

```
router rip
version 2
network 192.168.1.0
network 192.168.10.0
```

Mediante el comando router rip, se definieron cada una de las subredes que hacen parte de la red.

Configuración Router 2:

- ✓ Interfaces Seriales:

```
Interface Serial0/3/1
Ip address 192.168.1.2
255.255.255.0
No shutdown
```

```
Interface Serial0/3/0
no ip address
shutdown
```

Se usó la serial 0/3/1, en la cual se define la ip 192.168.1.2 con su respectiva mascara. Esta interfaz hace el papel de DTE con respecto al primer router. La otra interfaz serial no se utilizó, por lo que se encuentra abajo o shutdown.

- ✓ **Interfaces FastEthernet:**

```
Interface fastethernet0/0
Ip address 192.168.12.1
255.255.255.0
Duplex auto
Speed auto
No shutdown
```

```
Interface fastethernet0/1
no Ip address
No shutdown
```

Para definir la segunda LAN, se utilizó la interface FastEthernet 0/0 del router 2, con la ip 192.169.12.1 y mascara 255.255.255.0. por no utilizar la segunda interface fastethernet no se activa y se deba abajo.

- ✓ **Definiendo las Subredes:**

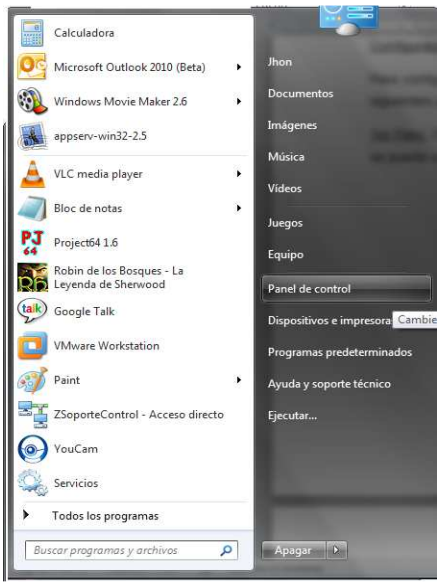
```
router rip
version 2
network 192.168.1.0
network 192.168.12.0
```

Mediante el comando router rip, se definieron cada una de las subredes que hacen parte de la red.

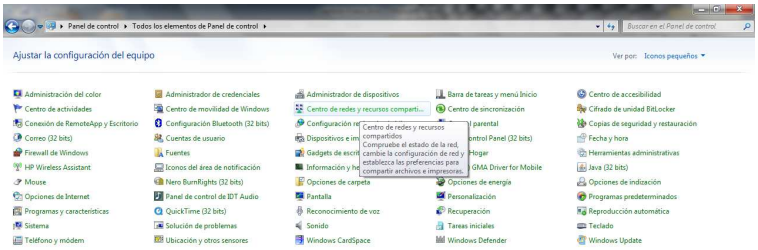
4.1.2 CONFIGURACIÓN DE EQUIPOS.

Para configurar la dirección ip asignada a un pc determinado se deben seguir los siguientes pasos:

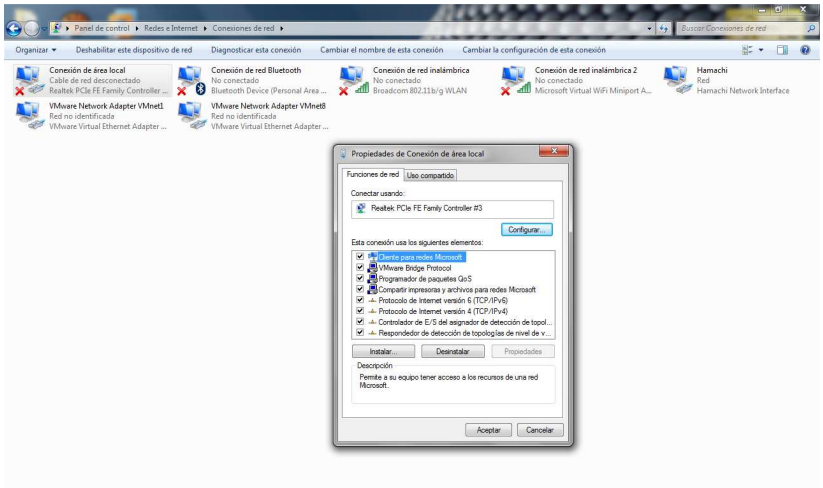
1er Paso: Dirigirse al Panel de Control ubicado en Inicio – Panel de Control como se puede observar en la siguiente gráfica.



2do Paso: Dentro del Panel de Control, localizar el icono denominado Centro de Redes y recursos compartidos y pulsar doble clic sobre él.



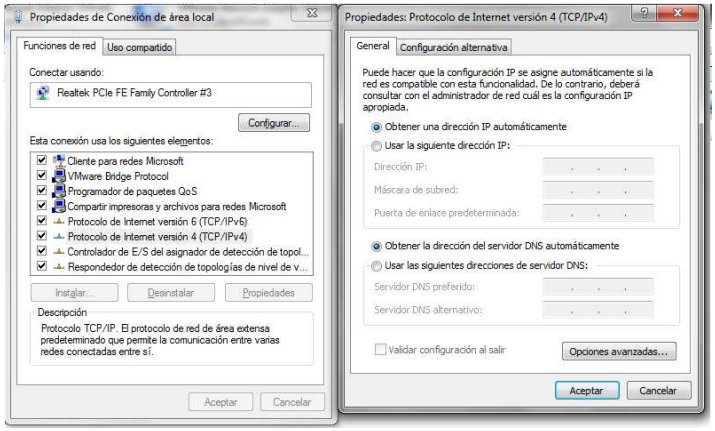
3er Paso: Estando en la carpeta Centro de redes, seleccionamos la Opción de Cambiar la configuración del adaptador de red. Se selecciona el área local que se está usando, y luego se pulsa doble clic sobre dicha conexión. Esto muestra una nueva ventana como la observada en la parte derecha de la siguiente gráfica.



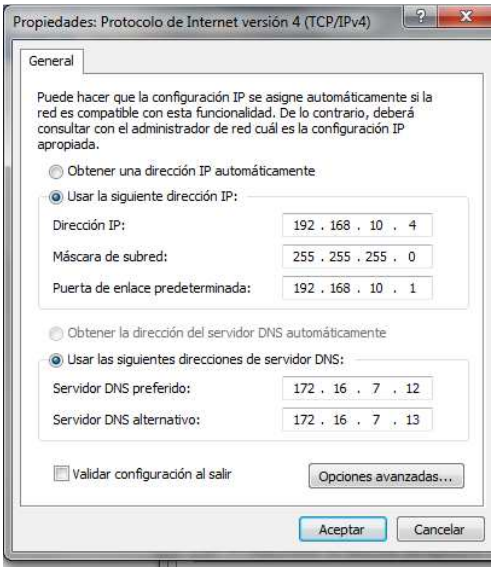
4to Paso: Como cuarto paso, nos dirigimos a las propiedades de la conexión, lo cual haremos pulsando clic sobre el botón Propiedades de la anterior gráfica. Esto nos presentará las propiedades de la conexión de área local.

5to Paso: Seleccionar el elemento denominado “Internet Protocol (TCP/IP)” que se encuentra en la pestaña general. Después, pulsar clic en las propiedades de este elemento, con el fin de ingresar las direcciones que deseamos asignar a la conexión de red de la PC.

En la gráfica siguiente, podemos observar cada uno de los campos que posee el protocolo de internet.



El grafico que se muestra a continuación nos da una vista de la configuración básica que se debe tener al momento de configurar cada equipo dentro de una red.



4.1.3 CONFIGURACION DE SNMP

La finalidad de esta parte es describir cada una de las configuraciones del protocolo SNMP realizadas a cada uno de los dispositivos que hacen parte de la red.

4.1.3.1 SNMP en Routers

En esta sección se presenta la configuración del protocolo de gestión de red SNMP para cada uno de los Routers. Los comandos se introdujeron ingresando a la configuración del router mediante la consola y la terminal Telnet.

```
Snmp-server community public RO
```

Se define una primera comunidad por defecto que es la public, con permisos de solo lectura.

```
Snmp-server community comunidadpublic RO
Snmp-server community comunidadprivate RW 4
```

Comandos que nos permiten definir dos comunidades comunidadpublic de solo lectura y comunidadprivate de lectura y escritura.

```
Access-list 3 permit 192.168.10.2
```

Se crea una lista de control de acceso o ACL, la cual contiene direcciones IP de los gestores SNMP a los que se permite acceder al agente empleando el nombre de comunidad especificado.

```
Snmp-server host 192.168.10.2 comunidadpublic
Snmp-server host 192.168.10.2 comunidadprivate
```

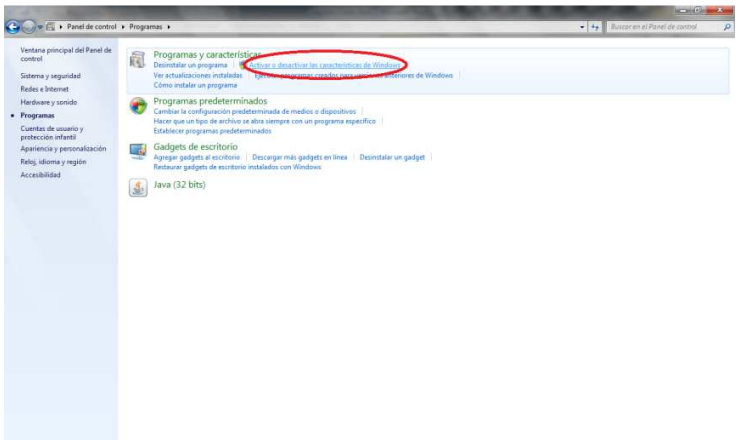
Se definen los hosts (Entidad Gestora) a los cuales se les enviarán las notificaciones. Por defecto emplea SNMP v1, la cual es la que usamos.

```
Snmp-server enable traps
```

Se habilitan las interrupciones. Es posible habilitar un conjunto determinado de interrupciones o notificaciones, o habilitarlas todas como podemos realizar con el anterior comando.

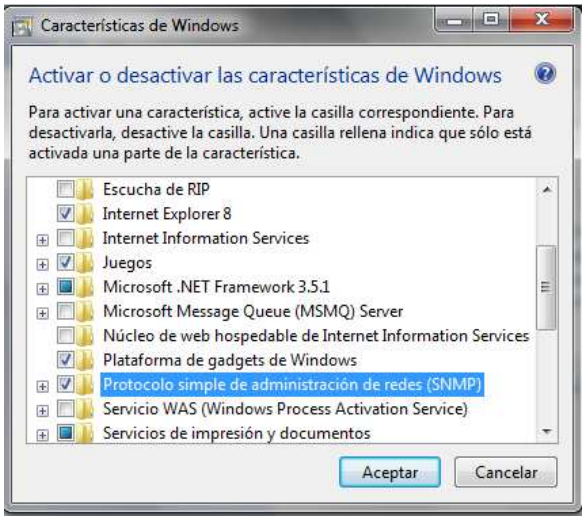
4.1.3.2 SNMP EN EQUIPOS

Para instalar el agente snmp en un sistema basado en Microsoft Windows, debemos instalar el servicio, haciendo clic en inicio, panel de control, Programas, y finalizar dando click en Activar o Desactivar las Características de Windows.

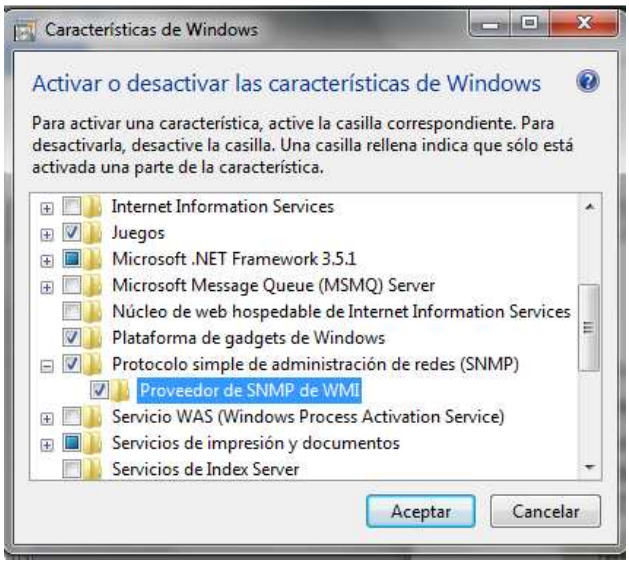


.

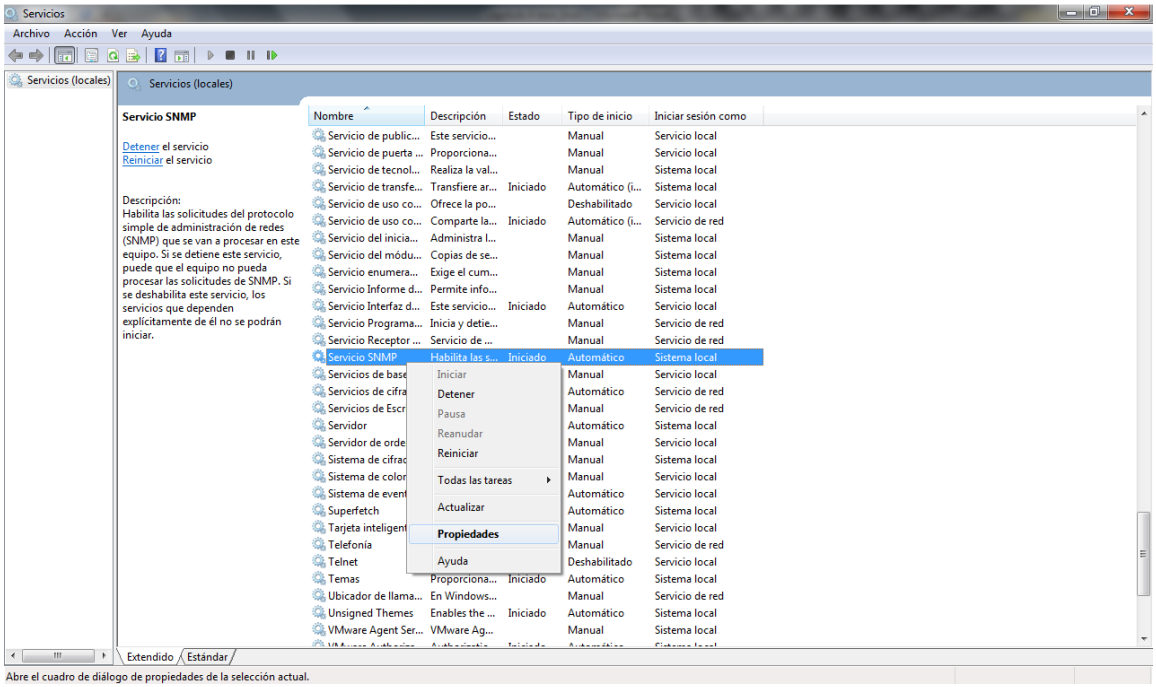
Dentro del asistente, damos clic en la pestaña Agregar o Quitar Componentes de Windows, luego buscamos y seleccionamos las herramientas de administración y supervisión, después pulsamos clic en la pestaña detalles.



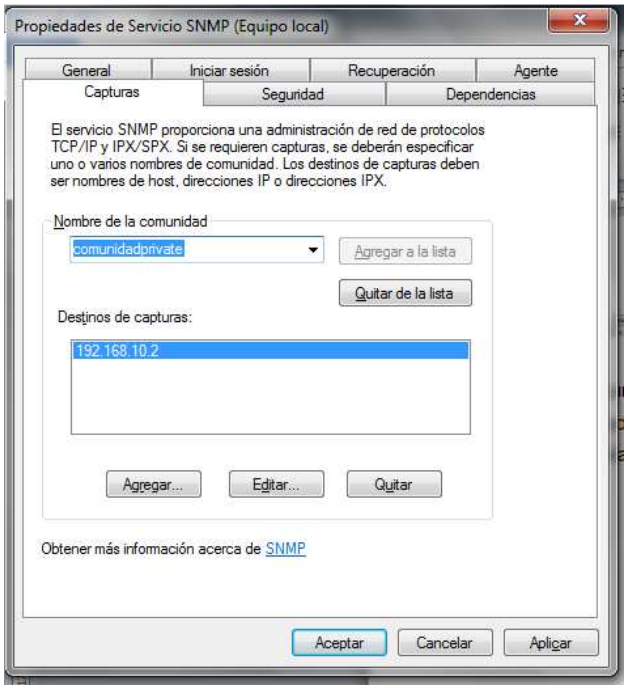
Cuando hacemos clic en detalles aparecen dentro del asistente varias herramientas de administración y supervisión. Se debe seleccionar las opciones relacionadas con snmp y posteriormente aceptar.



Una vez instalado el protocolo, el paso siguiente es configurar el agente definiendo la comunidad snmp y correr el servicio snmp. Para esto, nos vamos a inicio panel de control herramientas administrativas servicios. Cuando estemos dentro de la ventana de la consola de servicios, buscamos el servicio SNMP, pulsamos clic derecho sobre él y nos vamos a las propiedades.



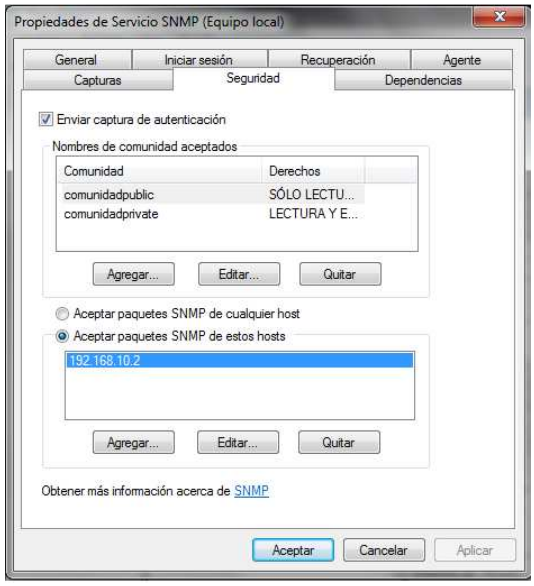
Ahora configuraremos las comunidades definidas en los Routers. Nos vamos a la pestaña llamada capturas y en el apartado que nos indica, escribimos el nombre de la comunidad que este caso será public, luego hacemos clic en agregar lista.



En la anterior gráfica, podemos observar que la comunidad definida fue denominada como com1, la cual es public.

Además, podemos notar que la entidad gestora en la cual se recolectaran todos los datos usando SNMP tiene IP 192.168.10.2.

En la pestaña de seguridad es posible configurar las siguientes opciones, de acuerdo a la gráfica:



Enviar capturas de autenticación: Cuando el agente recibe una solicitud que no contiene un nombre de comunidad valido o bien el host emisor del mensaje no está en la lista de los permitidos, el agente puede enviar un mensaje de captura o alarma a uno o más destinos de capturas con el mensaje de fallo de autenticación.

Nombres de comunidad aceptados: La comunidad predeterminada es public y tienes permisos de solo lectura. Se recomienda el cambio de public a otro nombre pues éste no es seguro. Solo se procesarán los mensajes provenientes de una comunidad que esté en esta lista.

Derechos de comunidad: Se pueden configurar con que permisos se procesan las solicitudes de los miembros de comunidades determinadas.

Aceptar paquetes SNMP de cualquier host: Cuando esta opción está habilitada nunca se descartan paquetes SNMP en base a la dirección o nombre del host fuente.

Aceptar paquetes SNMP de estos host: Cuando esta opción está habilitada sólo se aceptan paquetes de los host de la lista de los permitidos. Esto añade un nivel de seguridad más alto que el nombre de la comunidad.

4.2 IMPLEMENTACIÓN DE NAGIOS

4.2.1 COMANDOS

Son los que nos permiten configurar y verificar la herramienta de monitoreo Nagios. Entre los más utilizados se destacan:

sudo /usr/local/Nagios/bin/Nagios -v /usr/local/Nagios/etc/nagios.cfg

Permite comprobar Nagios con el objetivo de conocer si las diferentes configuraciones realizadas no posean algún error o fallo. Y luego de esto, reiniciar el servicio de Nagios para que lo cambios se realicen. A continuación se presenta un resultado de la verificación de Nagios:

Nagios Core 3.2.0
Copyright (c) 2009 Nagios Core Development Team and Community Contributors
Copyright (c) 1999-2009 Ethan Galstad
Last Modified: 08-12-2009
License: GPL

Website: http://www.nagios.org
Reading configuration data...
Read main config file okay...
Processing object config file '/usr/local/nagios/etc/objects/commands.cfg'...
Processing object config file '/usr/local/nagios/etc/objects/contacts.cfg'...
Processing object config file '/usr/local/nagios/etc/objects/timeperiods.cfg'...
Processing object config file '/usr/local/nagios/etc/objects/templates.cfg'...
Processing object config file '/usr/local/nagios/etc/objects/mynetwork.cfg'...
Read object config files okay...
Running pre-flight check on configuration data...
Checking services...

Checked 41 services.

Checking hosts...

Warning: Host 'Switch1' has no services associated with it!

Warning: Host 'Switch2' has no services associated with it!

Checked 9 hosts.

Checking host groups...

Checked 4 host groups.

Checking service groups...

Checked 0 service groups.

Checking contacts...

Checked 1 contacts.

Checking contact groups...

Checked 1 contact groups.

Checking service escalations...

Checked 0 service escalations.

Checking service dependencies...

Checked 0 service dependencies.

Checking host escalations...

Checked 0 host escalations.

Checking host dependencies...

Checked 0 host dependencies.

Checking commands...

Checked 25 commands.

Checking time periods...

Checked 5 time periods.

Checking for circular paths between hosts...

Checking for circular host and service dependencies...

Checking global event handlers...

Checking obsessive compulsive processor commands...

Checking misc settings...

Total Warnings: 2

Total Errors: 0

Things look okay - No serious problems were detected during the pre-flight check

sudo /etc/init.d/Nagios restart

Nos permite reiniciar el servicio de la herramienta Nagios.

sudo gedit mynetwork.cfg

Nos provee la posibilidad de modificar el archivo mynetwork.cfg por medio de la aplicación gedit dándole permisos de super usuario.

4.2.2 ARCHIVOS DE CONFIGURACIÓN

4.2.2.1 NAGIOS.CFG

Principal archivo de configuración usado por la herramienta Nagios, en el cual se definieron los objetos de configuración. Para nuestra práctica fue creado un nuevo archivo denominado mynetwork.cfg donde se definieron cada uno de los objetos. Como nota, podemos decir que el símbolo # es el utilizado para definir comentarios.

```
# NAGIOS.CFG - Sample Main Config File for Nagios 3.2.0
#
# Read the documentation for more information on this configuration
# file.  I've provided some comments here, but things may not be so
# clear without further explanation.
#
# Last Modified: 12-14-2008
#
# LOG FILE
# This is the main log file where service and host events are logged
# for historical purposes.  This should be the first option specified
# in the config file!!!

log_file=/usr/local/nagios/var/nagios.log

# OBJECT CONFIGURATION FILE(S)
# These are the object configuration files in which you define hosts,
# host groups, contacts, contact groups, services, etc.
# You can split your object definitions across several config files
# if you wish (as shown below), or keep them all in a single config file.
```

```
# You can specify individual object config files as shown below:
cfg_file=/usr/local/nagios/etc/objects/commands.cfg
cfg_file=/usr/local/nagios/etc/objects/contacts.cfg
cfg_file=/usr/local/nagios/etc/objects/timeperiods.cfg
cfg_file=/usr/local/nagios/etc/objects/templates.cfg

# Definitions for monitoring the local (Linux) host
#cfg_file=/usr/local/nagios/etc/objects/localhost.cfg

# Definitions for monitoring a Windows machine
#cfg_file=/usr/local/nagios/etc/objects/windows.cfg

# Definitions for monitoring a router/switch
#cfg_file=/usr/local/nagios/etc/objects/switch.cfg

# Definitions for monitoring a network printer
#cfg_file=/usr/local/nagios/etc/objects/printer.cfg

# Definitions for monitoring a gamba network
cfg_file=/usr/local/nagios/etc/objects/mynetwork.cfg

# You can also tell Nagios to process all config files (with a .cfg
# extension) in a particular directory by using the cfg_dir
# directive as shown below:

#cfg_dir=/usr/local/nagios/etc/servers
#cfg_dir=/usr/local/Nagios/etc/printers
#cfg_dir=/usr/local/Nagios/etc/Switches
#cfg_dir=/usr/local/Nagios/etc/Routers
```

4.2.2.2 COMMANDS.CFG

Se definen los plugins que se van a utilizar en la herramienta de Nagios. Como por ejemplo los plugins de la aplicación Net-SNMP o NSClient++ que nos permiten monitorear propiedades de los host y Routers.

```
##############################################################################
#
# COMMANDS.CFG - SAMPLE COMMAND DEFINITIONS FOR NAGIOS 3.2.0
# Last Modified: 05-31-2007
# NOTES: This config file provides you with some example command definitions
#        that you can reference in host, service, and contact definitions.
```

```
#       You don't need to keep commands in a separate file from your other
#       object definitions.  This has been done just to make things easier to understand.
###############################################################################
#
###############################################################################
#
# SAMPLE SERVICE CHECK COMMANDS
# These are some example service check commands.  They may or may not work on
# your system, as they must be modified for your plugins.  See the HTML
# documentation on the plugins for examples of how to configure command definitions.
# NOTE:  The following 'check_local_...' functions are designed to monitor
#       various metrics on the host that Nagios is running on (i.e. this one).
###############################################################################
#
# 'check_local_disk' command definition
define command{
        command_name    check_local_disk
        command_line    $USER1$/check_disk -w $ARG1$ -c $ARG2$ -p $ARG3$
        }
# 'check_local_load' command definition
define command{
        command_name    check_local_load
        command_line    $USER1$/check_load -w $ARG1$ -c $ARG2$
        }
define command{
        command_name    check_snmp_int_v1
        command_line            $USER1$/check_snmp_int.pl   -H   $HOSTADDRESS$   -C
$USER7$ -n $ARG1$ $ARG2$
        }
define command{
        command_name    check_snmp
        command_line      $USER1$/check_snmp  -H  $HOSTADDRESS$  -C  $ARG1$  -o
$ARG2$ -p $ARG3$
        }
```

4.2.3 PROGRAMAS INSTALADOS

En la herramienta Nagios existen una cantidad inmensa de programas o plugins que permiten la monitorización de todas las propiedades y características de los diferentes dispositivos que hacen parte de una red. En ese apartado se mostrarán los programas usados en nuestro monitoreo así como sus respectivas características.

4.2.3.1 NSCLIENT++

Es un complemento que se instala en los ordenadores bajo el sistema operativo Windows, cuya función es interrogar al servicio instrumental de Windows y obtener los valores de la CPU, memoria y discos. Es posible conseguirlo a través de su sitio web http://nsclient.org/nscp/. Los comandos integrados por la herramienta son denominados módulos entre los cuales se encuentran CheckDisk, CheckCPU, CheckUptime, CheckMem, CheckFile.

4.2.3.2 NET-SNMP

Es un conjunto de aplicaciones utilizados para implementar SNMP en sus versiones 1, v2c y v3 usando IPv4 o IPv6. Está compuesto por una librería genérica para el cliente, una suite de aplicaciones de líneas de comandos, un agente SNMP altamente extensible y módulos PERL.

Algunas de las aplicaciones SNMP incluidas en Net-SNMP son:

- **snmpd:** Un agente SNMP que responde a las solicitudes SNMP para un host determinado.
- **snmptrapd:** Un demonio SNMP que escucha SNMP TRAPS o informa y registra información sobre ellos.
- **snmpset:** SE comunica con una red completa usando solicitudes SNMP SET.

- **mib2c:** Es una utilidad de conversión de la MIB que traduce estructuras MIB en otros informes, tales como C-code.

4.2.4 SERVICIOS

Un servicio se define como el conjunto de acciones y actividades que se llevan a cabo sobre determinado dispositivo para un fin determinado, en este caso nuestro objetivo es conocer las diferentes datos que transcurren en cada uno de los dispositivos de la red. Para ellos, se definieron diferentes servicios para cada dispositivo. La estructura que se utilizó fue la siguiente:

```
define service{
    use                     generic-service
    host_name               UbuntuNagios,WinPC1,WinPC2
        WinPC3,WinPC4,Router1,Router2
    service_description     PING
    check_command                       check_ping!100.0,20%!500.0,60%
    normal_check_interval 5
    retry_check_interval 1
    }
```

La estructura para la definición de los servicios, ordenadores, Routers y grupos e están compuestos por los siguientes parámetros:

- **use:** Es la respectiva plantilla que va a utilizar la definición de dispositivo o servicio que se desee hacer, por ejemplo si es un servidor el que se quiere definir utilizaría *linux_servers***.**
- **host_name:** Define el nombre del dispositivo que se esté definiendo para la herramienta Nagios. En el caso de ser un servicio, este atributo define el conjunto de dispositivos a los cuales se les aplicará el servicio.
- **service_description:** Se refiere al tipo de servicio que se va a monitorear, puede ser PING, HTTP, FTP, entre otros.

- **host_group:** Conformado por un grupo de dispositivos o servicios que posean características similares o estén relacionados entre sí.
- **alias:** Es un seudónimo que se le coloca a un dispositivo para hacer más ameno para el usuario su entendimiento y monitorización.
- **members**: Son los diferentes dispositivos que van a hacer parte de un grupo.
- **address:** Dirección IP que hace referencia al host o router que se está definiendo.
- **normal_check_interval**: Parámetro que permite definir el intervalo de chequeo del dispositivo en segundos.
- **retry_check_interval:** Parámetro que define los intentos a realizar por un plugin.
- **contact_groups**: En este parámetro se definen las personas que tendrán acceso a la herramienta con sus respectivos servicios.
- **max_check_attempts**: Número máximo de intentos que se pueden realizar por un plugin.
- **parents:** Parámetro usado para jerarquizar los dispositivos, en nuestra práctica, empezando por el servidor, luego con los router y Switches y por ultimo con los ordenadores.
- **check_command:** Permite definir el plugin con sus diferentes parámetros, comprobándolo en la definición localizada en el archivo commands.cfg
- **notificaction_interval**: Intervalos de envió de notificación a la persona gestora definida en el archivo contacts.cfg.
- **notification_period**: Define el periodo de notificación que se realizará.

4.2.5 GRUPOS

Son muy utilizados para reportes y asociaciones grupales de dispositivos relacionados con grupos de servicios relacionados. Por ejemplo, un ISP podría crear un único host group para cada cliente. El ISP puede entonces ejecutar o crear scripts regularmente que efectúen la disponibilidad y las tendencias de informes para cada cliente.

```
define hostgroup{
        hostgroup_name  linux-servers
        alias           Linux Servers
        members         UbuntuNagios
        }
```

4.2.6 ROUTERS

La estructura utilizada para la definición de un router es bastante parecida a la de los ordenadores, solo diferenciándolas un conjunto de atributos que evalúan la disponibilidad del Routers en cuanto al conjunto de notificaciones que este puede realizar.

```
define host{
        use                     generic-host
        host_name               Router1
        alias                   Router principal
        address                 192.168.1.1
        check_command                   check-host-alive
        contact_groups          admins
        max_check_attempts      10
        notification_interval   480
        notification_period     24x7
        parents                 UbuntuNagios
}
```

4.2.7 HOSTS

Se definieron 5 ordenadores, divididos en 4 con sistema operativo Windows y uno con Linux, específicamente Ubuntu en el cual estuvo instalada el servidor con la herramienta de monitorización Nagios. La estructura usada para su definición se puede observar a continuación, la cual es parecida para la definición de cualquier host.

```
#PC Linux con Nagios
define host{
        use                     linux-server
        host_name               UbuntuNagios
        alias                   UNagios
        address                 192.168.10.2
        }
```

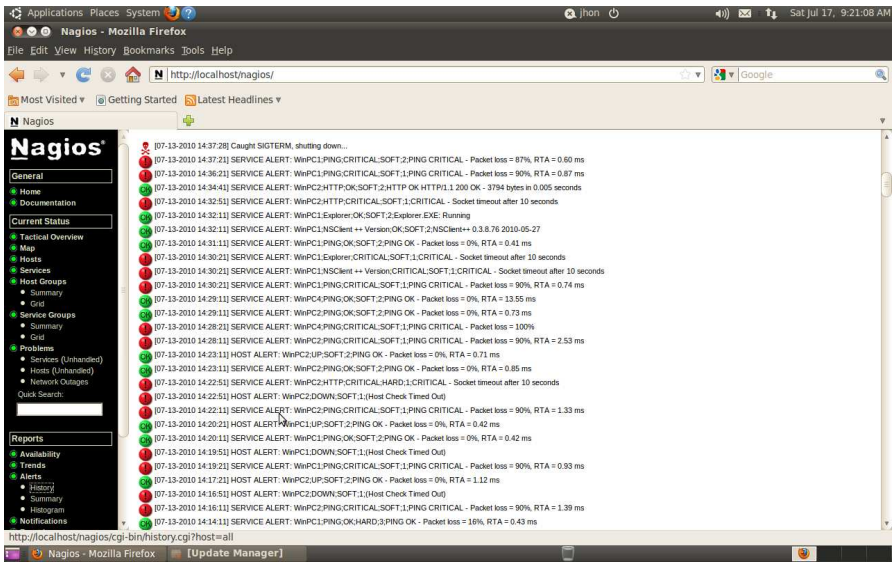
4.3 ALERTAS

Las alertas se definen como avisos que brinda el sistema por alguna información de cambio que se presenta en los servicios.

Dentro de la herramienta de monitorización NAGIOS, se encuentran definidas dos tipos de alertas:

4.3.1 HISTORIAL

Se define el historial, mediante todos los eventos clasificados por fecha, de los sucesos ocurridos durante la monitorización. Un ejemplo similar de las alertas mostradas en Nagios se da a conocer a continuación:



Dentro de la imagen mostrada, se define el historial de servicios y host presentado durante la prueba de monitorización realizada en la práctica de laboratorio, como se observa, presenta diferentes estados dentro de los cuales se definen los host rechazados, los host que fueron apagados o desconectados de la red, y los que se encuentran cambiando de estado constantemente. Estos se definen en diferentes tipos de iconos que los representan y que a su lado se encuentra la fecha y hora y la información correspondiente a que servicio o host hace referencia:

Da a conocer que el servicio o host perteneciente a la red se encuentra Bien.

Da a conocer que el servicio o host perteneciente a la red fue rechazada la conexión, esto traduce que la IP del host no fue encontrada en la red.

Da a conocer que el servicio o host está cambiando constantemente de estado, esto traduce a que existen servicios que cambian de estado como es el caso del Explorer en sistemas operativos Windows, que cambia al momento de pasar un equipo a hibernar.

Indica que el sistema de monitorización Nagios arranco en determinada fecha y hora.

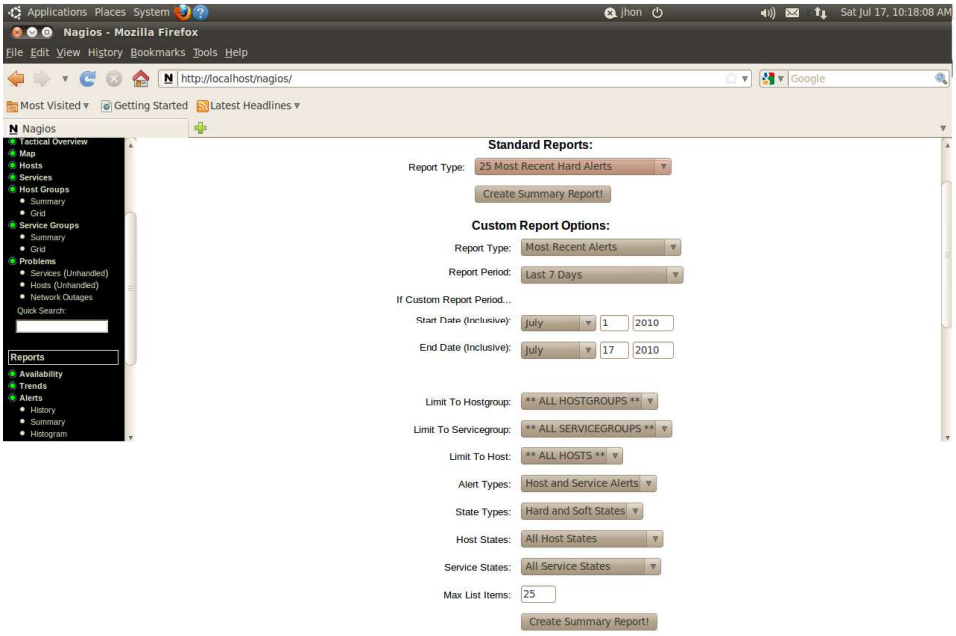
Indica que el sistema de monitorización Nagios se finalizó en determinada fecha y hora.

Indica que un servicio o host en un momento determinado se encontraba OK, y que al momento de generar la siguiente comunicación entre el sistema y el host, no encontró información alguna, es decir no encontró el host.

4.3.2 SUMMARY

Mediante este tipo de alertas, se pueden generar reportes de los TOP de eventos que ocurren en el sistema, de igual forma, genera alertas de host y servicios y permite la escogencia de la fecha que se requiere las alertas. El

sistema de monitorización muestra la siguiente pantalla al momento de generar estas alertas.



Mediante este tipo de alertas se pueden obtener reportes del estado actual de la red, sabiendo que equipos con más continuidad presentan inconvenientes en sus servicios. Las alertas generadas para estos reportes se definen mediante esta imagen:

Totals By Host

Host 'Router1' (Router principal)

Host Alerts

State	Soft Alerts	Hard Alerts	Total Alerts
UP	1	2	3
DOWN	11	3	14
UNREACHABLE	8	1	9
All States	20	6	**26**

Service Alerts

State	Soft Alerts	Hard Alerts	Total Alerts
OK	3	2	5
WARNING	1	0	1
UNKNOWN	0	0	0
CRITICAL	5	3	8
All States	9	5	**14**

Host 'Router2' (Router principal)

Host Alerts

State	Soft Alerts	Hard Alerts	Total Alerts
UP	1	2	3
DOWN	16	2	18
UNREACHABLE	3	1	4
All States	20	5	**25**

Service Alerts

State	Soft Alerts	Hard Alerts	Total Alerts
OK	4	1	5
WARNING	1	0	1
UNKNOWN	0	0	0
CRITICAL	4	3	7
All States	9	4	**13**

Host 'UbuntuNagios' (UNagios)

Host Alerts

State	Soft Alerts	Hard Alerts	Total Alerts
UP	0	2	2
DOWN	9	1	10
UNREACHABLE	0	0	0
All States	9	3	**12**

Service Alerts

State	Soft Alerts	Hard Alerts	Total Alerts
OK	0	4	4
WARNING	1	1	2
UNKNOWN	0	0	0
CRITICAL	6	1	7
All States	7	6	**13**

Host 'WinPC1' (WinPC1)

Host Alerts

State	Soft Alerts	Hard Alerts	Total Alerts
UP	15	2	17
DOWN	37	2	39
UNREACHABLE	0	0	0
All States	52	4	**56**

Service Alerts

State	Soft Alerts	Hard Alerts	Total Alerts
OK	25	8	33
WARNING	10	4	14
UNKNOWN	0	0	0
CRITICAL	35	9	44
All States	70	21	**91**

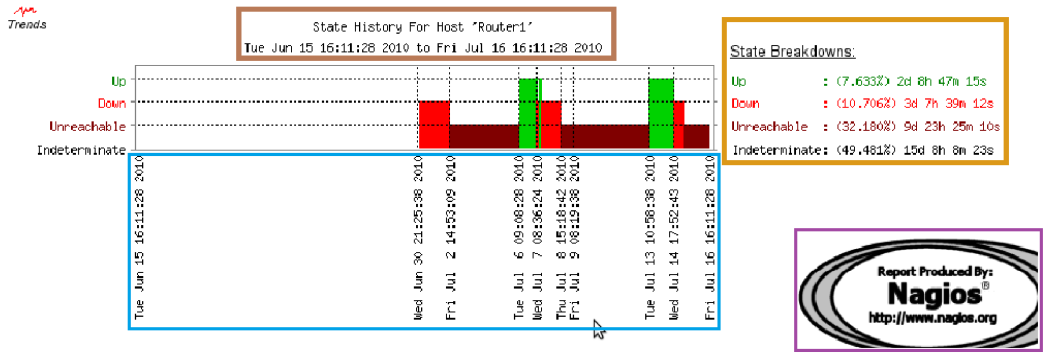
Se puede observar para cada host que cantidad de eventos han ocurrido mientras el sistema realizo su monitorización, para esto se crearon diferentes eventos, como apagar host o desconectarlos de la red.

4.4 REPORTE DE DATOS

4.4.1 DESCRIPCION DE DATOS RECOLECTADOS

El sistema genera reportes estadísticos y gráficos para determinado período de tiempo que indican entre otras cosas estadísticas de tiempo inactivo y activo de los servidores o host y determinados servicios.

La grafica que se muestra a continuación pertenece a una de los reportes generados, con la finalidad de dar a explicar las partes que componen el informe generado.



Como se observa, la gráfica está compuesta por una serie de datos en barras de diferentes colores, en donde cada barra describe un estado diferente como lo describe la leyenda que se encuentra de lado derecho y una serie de datos que la conforman como son:

- **Cuadro Café:** Este campo describe el lapso de tiempo que se seleccionó para la generación de los reportes, así mismo nombra a que se está realizando un historial de estado del Router1.

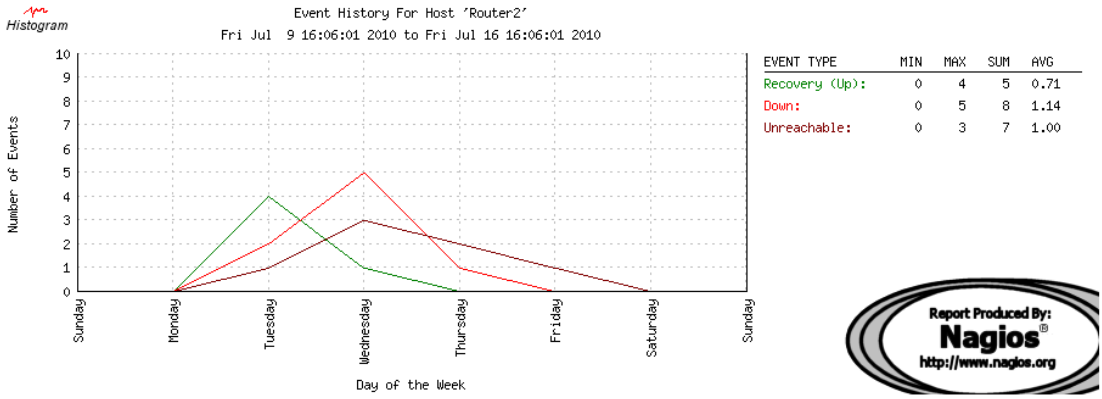
- **Cuadro Dorado:** En este campo se describe los estados por los cuales el host Router1 ha cambiado, de igual forma muestra el porcentaje de tiempo de actividad y la cantidad de días acumulado que se encontró activo.

- **Figura Azul:** En este campo se describe los tiempos de cambio de estado que tuvo el host, es decir en qué días se encontró activo, y en qué días estuvo en otros estados. Al momento de generar los reportes se pueden seleccionar un periodo de tiempo.

- **Figura Morada:** En este campo se muestra el logo de los reportes oficiales impresos por la misma herramienta. Los histogramas, y los reportes de disponibilidad son los únicos que son impresos con este logo.

La grafica como tal, muestra el comportamiento del cambio de estado del host seleccionado

Otro tipo de grafica generada por la herramienta durante la práctica de laboratorio, es el histograma de los servicios y host, como la que se muestra a continuación:



En esta grafica se puede observar un estado de un host y los cambios de eventos ocurridos durante un lapso de tiempo, en donde, de acuerdo con lo mostrado en la gráfica se obtiene una continuidad en los eventos ocurridos en la red, para lograr esto, se apagaron equipos y se desconectaron de la red.

4.4.2 INTERPRETACION DE RESULTADOS OBTENIDOS

Para la interpretación de los datos obtenidos, se determinaron cuatro graficas con mayor contenido para la explicación de su contenido, los reportes son los siguientes:

4.4.2.1 ROUTER 1: con IP: 192.168.10.1

Host State Breakdowns:

State	Type / Reason	Time	% Total Time	% Known Time
UP	Unscheduled	1d 20h 33m 40s	26.524%	26.524%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	**1d 20h 33m 40s**	**26.524%**	**26.524%**
DOWN	Unscheduled	5d 3h 26m 20s	73.476%	73.476%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	**5d 3h 26m 20s**	**73.476%**	**73.476%**
UNREACHABLE	Unscheduled	0d 0h 0m 0s	0.000%	0.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	**0d 0h 0m 0s**	**0.000%**	**0.000%**
Undetermined	Nagios Not Running	0d 0h 0m 0s	0.000%	
	Insufficient Data	0d 0h 0m 0s	0.000%	
	Total	0d 0h 0m 0s	0.000%	
All	Total	7d 0h 0m 0s	100.000%	100.000%

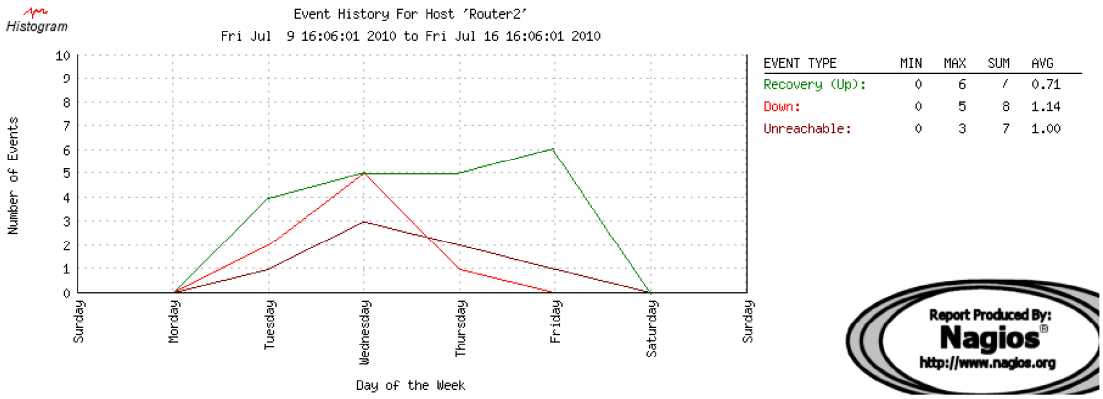
State Breakdowns For Host Services:

Service	% Time OK	% Time Warning	% Time Unknown	% Time Critical	% Time Undetermined
Current Load	44.656% (99.889%)	0.050% (0.111%)	0.000% (0.000%)	0.000% (0.000%)	55.294%
HTTP	26.627% (26.627%)	0.000% (0.000%)	0.000% (0.000%)	73.373% (73.373%)	0.000%
PING	26.371% (26.371%)	0.000% (0.000%)	0.000% (0.000%)	73.629% (73.629%)	0.000%
Root Partition	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
Swap Usage	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	100.000%
Uptime	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	100.000% (100.000%)	0.000%
Average	32.942% (42.148%)	0.008% (0.018%)	0.000% (0.000%)	41.167% (41.167%)	25.882%

Descripción: La grafica permite observar el comportamiento del host durante la implementación de la práctica de laboratorio realizada para este proyecto del Router 1 con IP: 192.168.10.1, realizado durante las dos semanas que se presentó la monitorización. La interpretación de este tipo de graficas es la siguiente:

- El intervalo de tiempo del router fue realizado durante una semana, entre las 10:00 am y las 16:00 pm.
- El servicio que mejor comportamiento tuvo fue el root partition, correspondiente a un 100% del tiempo de actividad total durante la práctica de laboratorio.
- El segundo mejor comportamiento lo tuvo el current load, correspondiente a un 44,656% del tiempo de la práctica.
- El tiempo de inactividad fue mayor que los demás, en donde el Router fue desconectado de la red o apagado, correspondiente a un 73.4%.
- El servicio que peor comportamiento tuvo fue el correspondiente al HTTP, servicio que corrobora el acceso a la Web, porcentaje que equivale a un 73,3%.
- El host nunca fue rechazado, eso quiere decir, que cada vez que se arrancaba el sistema de monitorización NAGIOS, siempre encontraba la dirección IP del router.

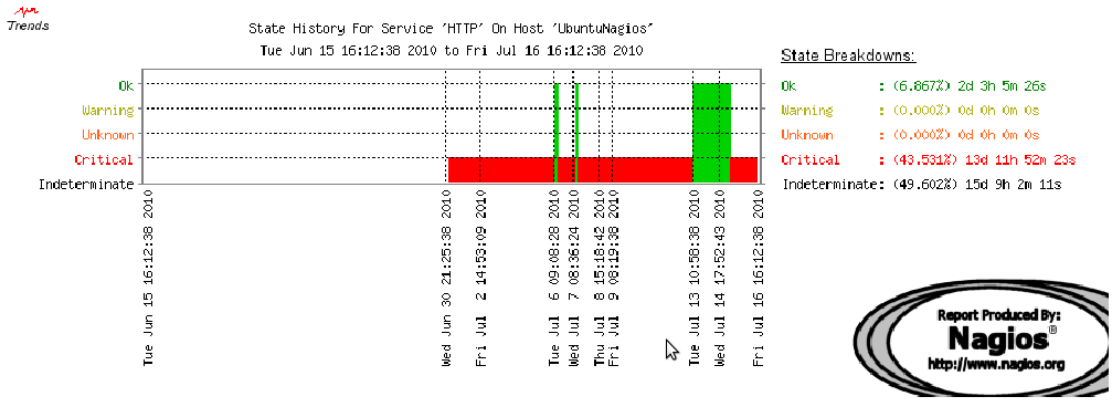
4.4.2.2 ROUTER 2: con IP: 192.168.12.1



Descripción: Grafica que describe la cantidad de eventos presentados durante el día en el router 2 con IP 192.168.12.1. Grafico Generado durante la segunda semana de monitorización entre las 10 am y las 16 pm. La interpretación es la siguiente:

- El tiempo de actividad del router en el transcurso de jueves a viernes de la segunda semana, fue mayor el número de eventos ocurridos, es decir que se obtuvo más comunicación a través de los servicios que se adhirieron a este router.
- En el segundo día, se puede observar mientras se adherían más servicios, el router fue incrementando su número de eventos, pero fueron más los que se rechazaron en ese momento
- Los Servicios dejaron de ser rechazados en los últimos días para así poder llegar a establecer la monitorización de esos servicios.

4.4.2.3 **UBUNTUNAGIOS** con IP: 192.168.10.2



Descripción: Imagen que describe los tiempos en que el sistema cambio de estados en el servicio HTTP, con fecha y hora, comprendida entre junio 15 y julio 16.

- En Junio 30 se inicia el sistema de monitorización de este servicio, empieza abajo, con condición crítica, ya que durante esos días se realizó la instalación de la aplicación.
- En julio 6 se configura el router con IP 192.168.10.1 para que tenga navegación la red, permite el acceso a internet y sube el servicio durante ese día.
- Al día siguiente se configura nuevamente el router después de mediodía para que tenga navegación, y se observa que de manera inmediata navega en la web.
- Durante eso días se generan nuevas configuraciones y no se configura la navegación.
- Se vuelve a probar la navegación y se configura el router antes de prender el equipo y durante todo el día realiza el chequeo comprobando que siempre tiene navegación.
- El sistema colapso durante la mayor parte del tiempo, con un 43,53% y se mantuvo estable durante un 6,86% que son los dos días de navegación que se probó el sistema.

4.4.2.4 TODOS LOS HOST CON SUS SERVICIOS.

Service State Breakdowns:

Host	Service	% Time OK	% Time Warning	% Time Unknown	% Time Critical	% Time Undetermined
Router1	Current Load	44.741% (99.889%)	0.000% (0.000%)	0.000% (0.000%)	0.050% (0.111%)	55.210%
	PING	0.298% (0.298%)	0.000% (0.000%)	0.000% (0.000%)	99.702% (99.702%)	0.000%
	Root Partition	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	100.000%
	Swap Usage	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	100.000%
Router2	Current Load	44.741% (99.889%)	0.000% (0.000%)	0.000% (0.000%)	0.050% (0.111%)	55.210%
	PING	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	100.000% (100.000%)	0.000%
	Root Partition	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	100.000%
	Swap Usage	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	100.000%
UbuntuNagios	Current Load	44.721% (99.889%)	0.050% (0.111%)	0.000% (0.000%)	0.000% (0.000%)	55.230%
	HTTP	26.627% (26.627%)	0.000% (0.000%)	0.000% (0.000%)	73.373% (73.373%)	0.000%
	PING	26.371% (26.371%)	0.000% (0.000%)	0.000% (0.000%)	73.629% (73.629%)	0.000%
	Root Partition	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	Swap Usage	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	100.000%
	Uptime	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	100.000% (100.000%)	0.000%
WinPC1	Current Load	44.721% (99.889%)	0.050% (0.111%)	0.000% (0.000%)	0.000% (0.000%)	55.230%
	Explorer	0.298% (0.298%)	0.000% (0.000%)	0.000% (0.000%)	99.702% (99.702%)	0.000%
	HTTP	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	100.000% (100.000%)	0.000%
	NSClient ++ Version	18.047% (18.047%)	0.000% (0.000%)	0.000% (0.000%)	81.953% (81.953%)	0.000%
	PING	17.636% (17.636%)	0.155% (0.155%)	0.000% (0.000%)	82.208% (82.208%)	0.000%
	Root Partition	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	100.000%
	Swap Usage	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	100.000%
WinPC2	Current Load	44.741% (99.889%)	0.000% (0.000%)	0.000% (0.000%)	0.050% (0.111%)	55.210%
	Explorer	17.484% (17.484%)	0.000% (0.000%)	0.000% (0.000%)	82.516% (82.516%)	0.000%
	HTTP	0.995% (0.995%)	0.000% (0.000%)	0.000% (0.000%)	99.005% (99.005%)	0.000%
	NSClient ++ Version	17.887% (17.887%)	0.098% (0.098%)	0.000% (0.000%)	82.015% (82.015%)	0.000%
	PING	1.154% (1.154%)	16.536% (16.536%)	0.000% (0.000%)	82.309% (82.309%)	0.000%
	Root Partition	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	100.000%
	Swap Usage	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	100.000%
WinPC3	Current Load	44.701% (99.779%)	0.050% (0.111%)	0.000% (0.000%)	0.050% (0.111%)	55.200%
	Explorer	17.219% (17.219%)	0.240% (0.240%)	0.000% (0.000%)	82.542% (82.542%)	0.000%
	NSClient ++ Version	17.156% (17.156%)	0.200% (0.200%)	0.000% (0.000%)	82.644% (82.644%)	0.000%
	PING	17.425% (17.425%)	0.000% (0.000%)	0.000% (0.000%)	82.575% (82.575%)	0.000%
	Root Partition	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	100.000%
	Swap Usage	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	100.000%
WinPC4	Current Load	44.741% (99.889%)	0.000% (0.000%)	0.000% (0.000%)	0.050% (0.111%)	55.210%
	Explorer	17.753% (17.753%)	0.200% (0.200%)	0.000% (0.000%)	82.047% (82.047%)	0.000%
	FTP	17.877% (17.877%)	0.000% (0.000%)	0.000% (0.000%)	82.123% (82.123%)	0.000%
	NSClient ++ Version	17.966% (17.966%)	0.000% (0.000%)	0.000% (0.000%)	82.034% (82.034%)	0.000%
	PING	18.066% (18.066%)	0.000% (0.000%)	0.000% (0.000%)	81.934% (81.934%)	0.000%
	Root Partition	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	100.000%
	Swap Usage	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	100.000%
Average		16.180% (25.594%)	0.429% (0.433%)	0.000% (0.000%)	42.258% (42.265%)	41.134%

Descripción: se observa en la imagen todos los host pertenecientes a la red, y así mismo cada uno de los servicios que se prestan en ellos.

- Se observa que la mayoría de los servicios presentaron inconvenientes, esto se debió a que al momento de realizar las pruebas se desconectaban equipos de la red, y se procedía a realizar otras configuraciones o agregar más servicios.

- El servicio que mejor comportamiento tuvo fue el current load, que cada vez que se iniciaba el sistema de monitorización detectaba que estuvieran encendidos los equipos de manera inmediata.
- En el WinPC1 y en el WinPC2, se instaló para la primera semana la navegación web, y el router 2 no se presentó conexión alguna y es 100% crítico porque se realizaba la monitorización con un solo router.
- Donde más advertencias se presentaron fue en el servicio de WINPC2, en donde el servicio ping cambiaba constantemente de estado, esto traduce a que perdía la conexión con la red, pero no por mucho tiempo, esto se debió a que se cambiaba la IP para que no se detectara el equipo durante 3 minutos, no paso a estado crítico porque el sistema realiza cada secuencia de tiempo el chequeo del estado.
- Lo mismo pasó con el equipo WinPC3, pero a diferencia que este se dejaba por fuera mucho más tiempo que el equipo anterior y por eso el estado de PING fue de 82,575% es decir fue más crítico que OK.
- El chequeo del servicio FTP se realizó en el equipo WinPC4, durante los dos últimos días, por cuestiones de que la red no presentaba navegación, en esos dos últimos días alcanzo a tener un 17,877% de la navegación en directorios FTP.
- Se instaló el NSClient ++ en equipos Windows para tomar el tiempo de actividad de los equipos, es decir que tanto tiempo permanecían encendidos o apagados, esto se realizó durante los 3 últimos días.

Siguiendo estos pasos se podrá realizar la interpretación de los reportes que nos genera la herramienta Nagios.

En NAGIOS existen herramientas externas que permiten la conexión con este para establecer estadísticas y graficas de cada uno de los equipos o servicios que pertenecen a la red o que están siendo monitorizados, una de esas herramientas es PNP4NAGIOS, que permite conexión de los datos obtenidos por la herramienta y este gestor de gráficas. Uno de los ejemplos obtenidos se da mediante la siguiente gráfica.

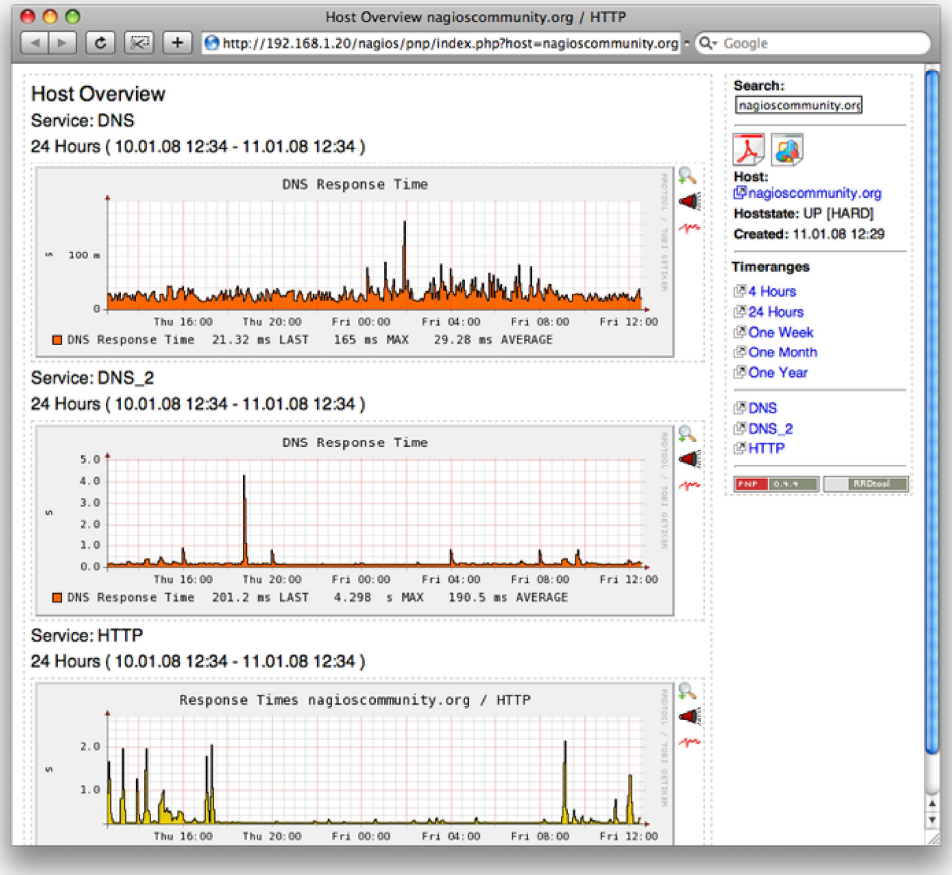


FIGURA 7: Grafica de NAGIOS con PNP4NAGIOS

En este tipo de graficas se puede entender mejor los aspectos técnicos de cada uno de los servicios prestados en la red.

CONCLUSIONES

Se puede destacar a la monitorización de redes como una de las más importantes y primordiales tareas que deben realizar cada una de las entidades que emplean redes en su entorno. La monitorización es un desarrollo tecnológico, el cual brinda una cantidad considerable de recursos para mantener a una red estable, eficiente y segura.

Las herramientas de monitorización brindan un apoyo muy grande a los administradores de red, gracias a estas se puede dar a conocer un estado real de una red de datos, permitiendo corregir de manera oportuna los inconvenientes presentados en esta, permitiendo la confiabilidad y estabilidad, que a la final se traduce a evitar fallas, disminuir costos, optimizar procesos, satisfacer la demanda de los clientes y los requisitos de facilidad de estos.

Como se ve en la práctica, Nagios es un sistema de control sofisticado con un gran potencial para el trabajo de expansión llevando a cabo sus tareas.

También es un software de código libre y abierto, y por lo que es un software ideal para cualquier organización que desee implementar un sistema de gestión de red. Así lo demuestra el gran número de organizaciones entre las empresas y las universidades y organismos gubernamentales que lo utilizan.

Sin embargo, Nagios también es un sistema complejo para configurar e instalar de manera correcta, por este motivo, se recomienda para la monitorización de redes medianas y grandes, equivalentes a más de 3 departamentos con promedio entre 15 o más equipos de cómputo en una empresa.

Además de lo anterior, se hace extraño que el sistema no funcione de forma

nativa con protocolos de gestión de red SNMP, en lugar de esto, Nagios realiza la gestión y red de monitoreo con herramientas propias, denominados Plugins, que podría acarrear inconvenientes con los firewall, o ser dependiente de la bajo la plataforma en que trabaja.

En cualquier caso, Nagios es una herramienta que cada administrador de red debe saber que es una alternativa a los productos de alto costo, es un producto probado, escalable y puede ahorrar costos importantes en licencias de software a organizaciones que se usa.

GLOSARIO

LAN: (Local Area Network, Red de área local). Una LAN es una red que conecta los ordenadores en un área relativamente pequeña y predeterminada (como una habitación, un edificio, o un conjunto de edificios

Administrador de red: Designan a aquellas posiciones laborales en las que los ingenieros se ven involucrados en redes de computadoras, o sea, las personas que se encargan de la administración de la red. Los administradores de red son básicamente el equivalente de red de los

Administradores de sistemas: mantienen el hardware y software de la red.

Banda ancha: Es la transmisión de datos en el cual se envían simultáneamente varias piezas de información, con el objeto de incrementar la velocidad de transmisión efectiva. En ingeniería de redes este término se utiliza también para los métodos en donde dos o más señales comparten un medio de transmisión.

Base de datos: Es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso. En este sentido, una biblioteca puede considerarse una base de datos compuesta en su mayoría por documentos y textos impresos en papel e indexados para su consulta.

Cableado físico: Por definición significa que todos los servicios en el edificio para las transmisiones de voz y datos se hacen conducir a través de un sistema de cableado en común. En un sistema bien diseñado, todas las tomas de piso y los paneles de parchado (patch panels) terminan en

conectores del tipo RJ45 que se alambran internamente a EIA/TIA 568b (conocido como norma 258a).

Descarga: Es copiar datos (generalmente un archivo entero) de una fuente principal a un dispositivo periférico. El término se utiliza a menudo para describir el proceso de copiar un archivo de un servicio en línea a tu propio ordenador. El término descargar puede también referir a copiar un archivo de un servidor de archivos de red a un ordenador en la red.

DNS (Domain Name System): Es una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Aunque como base de datos el DNS es capaz de asociar distintos tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio.

FIREWALL: Un cortafuegos es un elemento de hardware o software utilizado en una red de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de red que haya definido la organización responsable de la red.

FTP (*File Transfer Protocol*): Es un protocolo de transferencia de archivos entre sistemas conectados a una red TCP basado en la arquitectura cliente- servidor, de manera que desde un equipo cliente nos podemos conectar a un servidor para descargar archivos desde él o para enviarle nuestros propios archivos independientemente del sistema operativo utilizado en cada equipo.

Host: Una máquina conectada a una red de computadores y que tiene un nombre de equipo (en inglés, *hostname*). Es un nombre único que se le

da a un dispositivo conectado a una red informática. Puede ser un ordenador, un servidor de archivos, un dispositivo de almacenamiento por red, una máquina de fax, impresora, etc. Este nombre ayuda al administrador de la red a identificar las máquinas sin tener que memorizar una dirección IP para cada una de ellas.

HTTP: El protocolo de transferencia de hipertexto (*HyperText Transfer Protocol*) es el protocolo usado en cada transacción de la Web (WWW). HTTP fue desarrollado por el consorcio W3C y la IETF, colaboración que culminó en 1999 con la publicación de una serie de RFC, siendo el más importante de ellos el RFC 2616, que especifica la versión 1.1.

Mantenimiento de redes: El conjunto de trabajos necesarios para asegurar el buen funcionamiento de las instalaciones.

Monitoreo de red: Para prevenir errores en el sistema existe una computadora que está "monitoreando" el funcionamiento de la red. Estos errores a menudo se deben a problemas de ruido en la línea de transmisión y crean situaciones que no existen, tales como direcciones de computadoras que no pertenecen a ninguno de los nodos, errores en la información, por mencionar algunos.

NAGIOS: Es un sistema open source popular para monitorizar una red. Monitoriza los hosts y servicios que se especifiquen, alertando cuando el comportamiento de la red no es el deseado y nuevamente cuando vuelve a su estado correcto.

Networking: Término utilizado para referirse a las redes de telecomunicaciones en general y a las conexiones entre ellas.

Online: Se utiliza para designar a una computadora que está contactada al sistema, está operativa, está encendida o accede a Internet.

BIBLIOGRAFIA

[1]. Cisco System, “Internetworking Technologies Handbook” 3ra Edition, 2001. Existente en la biblioteca de la Universidad Tecnológica de Bolívar, sede Ternera.

[2]. Craig Hunt, “TCP/IP Network Administration” 2da Edition, Diciembre 1997. http://books.google.com.co/books?id=t7pHu7sIUkQC&dq=TCP/IP+Network+Administration+craig+hunt&printsec=frontcover&source=bn&hl=es&sa=X&oi=book_result&resnum=4&ct=result#PPR7,M1

[3]. Alexander Clemm, “Network Management Fundamentals”, Cisco Press, año 2006. Leer online en http://my.safaribooksonline.com/1587201372?tocview=true

[4]. Nathan J. Muller, “Network Management Handbook”, año 2002 http://books.google.com.co/books?id=a0DNjqpgKYAC&dq=rmon&as_brr=3&source=gbs_navlinks_s

[5]. Tony Kenyon, “Data Networks”, año 2002 http://books.google.com.co/books?id=kipV1OXOygMC&dq=rmon&as_brr=3&source=gbs_navlinks_s

[6]. Harold F. Tipton, Micki Krause, “Information Security Management Handbook”, año 2006 http://books.google.com.co/books?id=cpPGK3ZlzqgC&dq=rmon&as_brr=3&source=gbs_navlinks_s

[7]. Dictionary of Networking, Copyright 2000 SYBEX Inc. Alameda, CA. http://portal.aauj.edu/portal_resources/downloads/networking/dictionary_of_networking.pdf

[8]. IPSWITCH Inc, The Value of Networking, http://www.draware.dk/fileadmin/Ipswitch/wug/Value_of_Network_Monitoring.pdf

[9]. CISCO SYSTEM, “Establishing Best Practices for Network Management”, Session 804, 1999. http://www.scribd.com/doc/5233731/Establishing-Best-Practices-for-Network-Management

[10]. SENA, “Proyecto de Monitoreo y Gestión de Red”, 2008. http://www.scribd.com/doc/8422802/Proyecto-Monitoreo-Y-Gestion-de-Red-Con-Correcciones-a-los-comentarios-del-profe

[11]. Programa de Formación de la Academia de Software Libre, “Unidad 4: Herramientas de Gestión y Monitoreo de Redes”. http://asl.fundacitetachira.gob.ve/file.php/1/Administracion_de_redes/implementacion_de_redes-unidad4.pdf

[12]. José María Peribáñez, “Virtualización y redes en GNU/Linux”, 2007. http://es.tldp.org/Manuales-LuCAS/doc-curso-salamanca-redes/virtualizacionyredes.pdf

[13]. Mario Zaizar, “Resumen de Protocolos de Monitorización”, 2003. http://alumno.ucol.mx/al986138/public_html/MARIO/adm_redes/Resumen%20Protocolos%20de%20Monitorizacion%20por%20Mz%20v1-0.pdf

[14]. Executive Overview, “Network Management Services” http://www.eds.com/services/networkmanagement/

[15]. Linux Magazine, “Introducción a Herramientas de Red – Linux en Red”, http://www.linux-magazine.es/issue/01/Herramientasred.pdf

[16]. IEEE IT Professional Magazine, Vol. 9 No 2, Marzo – Abril del 2007. http://rapidshare.com/files/29402060/IEEE.IT.Professional.Magazine.Vol.9.No.2.Mar-Apr.2007.eBook-TLFeBOOK.pdf

[17]. Interfaz para el monitoreo de redes de comunicaciones mediante una aplicación web, Universidad de las Américas Puebla, Hugo Solano Vera. http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/solano_v_h/capitulo1.pdf

[18]. La integración entre la gestión del conocimiento y la inteligencia competitiva: la aportación de los mapas tecnológicos http://www.revistaespacios.com/a00v21n02/41002102.html

[19]. Herramientas Para el monitoreo del estado de una red. http://seguinfo.wordpress.com/2007/09/12/herramientas-para-el-monitoreo-del-estado-de-red/

[20]. Definición de monitoreo. http://www.cgtichile.com/cgti/index2.php?option=com_content&do_pdf=1&id=30

[21]. Página Oficial de la documentación de Nagios, descripción de Procesos y pasos.
http://support.nagios.com/knowledgebase/officialdocs

[22]. Wikipedia – Monitoreo de Red
http://es.wikipedia.org/wiki/Monitoreo_de_red

[23]. Wikipedia – Definición de Troyano
http://es.wikipedia.org/wiki/Troyano_(informatica)

[24]. ¿Cómo monitorear servidores y equipo de comunicaciones?
http://aspiranteageek.wordpress.com/

[25]. Herramientas de Gestión Basadas en Web. Daniel Arias Figueroa, Trabajo de Tesis.
http://postgrado.info.unlp.edu.ar/Carrera/Magister/Redes%20de%20Datos/Tesis/Tesis%20Arias%20Figueroa.pdf

[26]. Monitoria y Analisis de red con Nagios – Sergio Cayuqueo
http://cayu.com.ar/files/manual-nagios-2009.pdf