

**Implementación de un Servidor de Monitoreo a
los servicios telemáticos que brinda el Nodo
Central de la Universidad de Holguín**

“Oscar Lucero Moya”

Trabajo de Diploma para optar por el Título de Ingeniero Informático

Autor

Alexander Julian Quiala Feria

Tutores

Dr.C Rodolfo García Bermúdez

Ing. Miguel Abellón Medina

Holguín, 2013

Mi trabajo en el software libre está motivado por un objetivo idealista: difundir libertad y cooperación. Quiero motivar la expansión del software libre, reemplazando el software privativo que prohíbe la cooperación, y de este modo hacer nuestra sociedad mejor.

Richard Stallman

Dedicatoria

Dedico este Trabajo de Diploma a mis Abuelos Urbano Feria Hernández y Laura Ávila Vásquez quienes dieron todo su empeño para que llegara hacer el profesional que soy hoy en día a ellos le debo mi vida.

Agradecimientos

Quiero agradecer a la joven que dedico todo su tiempo a darme su amor y cariño y por comprenderme cuando lo necesitaba Mariela Cuba Salinas mi novia para ti lo mejor de este mundo y gracias por ayudarme.

A mi madre por haberme traído al mundo.

A mis tías por cuidarme todo el tiempo y querer lo mejor para mí.

A mis amigos de toda una vida Michel Parra Batista, Livan Sánchez Cabrera, Michel Hechavarria, Napoles, Ángel Julian en fin a todos.

RESUMEN

La implementación de un servidor de apoyo para el monitoreo de los servicios que presta el Nodo Central de la Universidad de Holguín “Oscar Lucero Moya” (Uho); surge de la necesidad de contar con un servidor que favorezca el desempeño y la calidad de las labores que realizan los administradores que trabajan en la misma y demás personas de la institución. En la actualidad los administradores del nodo realizan este trabajo por medio de controles espontáneos dificultando las búsquedas de posibles fallas, la integridad y persistencia de la información, lo que conlleva a la falta de eficiencia.

La vigente investigación pretende solucionar estas dificultades, a partir de la implementación de un Servidor de Monitoreo a los servicios y equipos de la red configurada con sistemas de alertas. La que garantice un satisfactorio trabajo a los administradores del centro, permitiendo menos pérdida de tiempo para darle solución a un problema dado.

Para la implementación de dicho servidor se realizó un exhaustivo estudio del arte de todas las posibles, permitiendo así escoger la más robusta y eficiente y que contara con la característica de nuestro Hardware y características de la Red Uho. Se llegó a la conclusión que el servidor escogido Nagios v3.2.1 garantiza la disponibilidad de los servicios y equipos debido a sus eventos de notificaciones hacia los administradores, de igual manera se contó con la herramienta NagiosGrapher permitiendo hacer comparativas de los servicios en las gráficas que se van generando de los datos de Nagios. Para el bien de la entidad se ha cumplido con los objetivos propuestos garantizando la disponibilidad y eficiencia de los objetivos trazados.

ABSTRACT

The implementation of a server supporting for the monitoring of the services provided by the central node of the University of Holguín "Oscar Lucero Moya" (Uho) arises from the need to have a server that encourages performance and quality work performed by managers working in the same and other people in the institution. At present node administrators does this work by hindering spontaneous controls search possible faults, integrity and persistence of information, leading to lack of efficiency?

The current research aims to resolve these difficulties, from the implementation of a Monitoring Server services and network computers configured with alert systems. The ensuring a satisfactory job center managers, allowing less wasted time for solving a given problem.

To implement the server was made a thorough study of the art of all possible, allowing choosing the most robust and efficient and will feature the characteristic of our Hardware and Network features Uho. It came to the conclusion that the chosen Nagios server v3.2.1 guarantee the availability of services and equipment due to its event notifications to managers, it is equally counted with NagiosGrapher tool allowing to make comparative graphs services in that are generated Nagios data. For the good of the institution has met the objectives by ensuring the availability and efficiency objectives.

Índice

Richard Stallman	I
Introducción	1
1 Fundamentación teórica para la implementación del Servidor de Monitoreo de servicios y equipos del Nodo Central Uho.	7
1.1 Nodo Central de la Red Uho	7
1.1.1 Servicio de Correo Electrónico.....	8
1.1.2 Servicio <i>Web</i>	10
1.1.3 Servicio de transferencia de fichero FTP	11
1.1.4 Servicio de Acceso Remoto.....	12
1.1.5 Servicio de Mensajería Instantánea	14
1.1.6 Servicio de Red Inalámbrica WI-FI	14
1.2 Estudio del Arte de las tecnologías de la información y las Comunicaciones.	17
1.2.1 Sistemas Operativos	17
1.2.1.1 Sistemas Operativos GNU/Linux	17
1.2.1.2 Distribuciones de GNU/Linux	19
1.2.2 Redes informáticas	20
1.2.2.1 Dispositivos de Red	25
1.2.3 Monitoreo de red	25
1.2.4 Virtualización	29
1.2.5 Ventajas del Software Libre sobre el Software Propietario en el mundo de Monitoreo de redes Informáticas.	32
1.2.5.1 Definición de Software Libre	32
1.2.5.2 Ventajas del Software Libre	33
1.2.5.3 Desventajas del software propietario	34
1.2.6 Servidores de Monitoreo. Soluciones de Código Abierto (OpenSource).....	36
1.2.6.1 Pandora FMS	36
1.2.6.2 Zabbix.....	37
1.2.6.3 Zenoss	38
1.2.6.4 Cacti	39
1.2.6.5 Nagios.....	41
1.2.7 Análisis de la selección del software de monitoreo.	44
1.3 Conclusiones de capítulo	45

2	Descripción y Resultados de la propuesta	47
2.1	<i>Implementación en el nodo central del software de monitoreo Nagios</i>	<i>47</i>
2.1.1	Parámetros a Monitorear con Nagios	48
2.1.1.1	Descripción del servicio de correo electrónico mediante (Postfix Dovecot)	48
2.1.1.1.1	Información Cuantitativa y Cualitativa del servidor de correo	48
2.1.1.1.2	Caso 1. Comprobación del servicio	51
2.1.1.2	Descripción del servicio web mediante (Apache)	51
2.1.1.2.1	Información Cuantitativa y Cualitativa del servicio web	51
2.1.1.2.2	Caso 2. Comprobación del servicio web.....	52
2.1.1.3	Descripción del servicio de acceso remoto mediante (FreeRADIUS).....	52
2.1.1.3.1	Información Cuantitativa y Cualitativa del servicio acceso remoto	52
2.1.1.3.2	Caso 3. Comprobación del servicio acceso remoto.....	53
2.1.1.4	Descripción del servicio de FTP mediante (ProFTPD)	53
2.1.1.4.1	Información Cuantitativa y Cualitativa del servicio FTP	53
2.1.1.4.2	Caso 4. Comprobación del servicio FTP.....	54
2.1.1.5	Descripción del servicio de DNS mediante (Bind9)	54
2.1.1.5.1	Información Cuantitativa y Cualitativa del servicio DNS	55
2.1.1.5.2	Caso 5. Comprobación del servicio DNS.....	56
2.2	<i>Instalación del servidor de monitoreo Nagios.....</i>	<i>56</i>
2.2.1	Procedimiento de instalación Nagios	57
2.2.2	Instalación de la Herramienta NagiosGrapher.	58
2.3	<i>Resultados obtenidos con Nagios.....</i>	<i>58</i>
2.3.1	Caso 1. Comprobación del servicio de correo electrónico	59
2.3.1.1	Estado Imap	59
2.3.1.2	Estado Mailq	62
2.3.1.3	Estado POP3	64
2.3.1.4	Estado servicio PING	65
2.3.1.5	Estado servicio SMTP	66
2.3.2	Caso 2. Comprobación del servicio web	67
2.3.2.1	Estado servidor Apache2_HTTP	67
2.3.2.2	Estado del servicio PING	70
2.3.3	Caso 3. Comprobación del servicio Acceso Remoto (FreeRADIUS)	72
2.3.3.1	Estado del servicio PING	72
	Conclusiones.....	76
	Recomendaciones.....	78

Referencias Bibliográficas:79

Anexos.....82

Índice de Figura

Figura 1. Relación entre las estafetas en el servicio de correo.	9
Figura 2. Esquema de ejecución entre maestro-esclavo.....	42
Figura 3. Estado del ServerEmail_1	59
Figura 4. Captura realizada mediante scrip.....	59
Figura 5. Crear reporte de Disponibilidad ServerEmail_1. Estado Imap	60
Figura 6. Averías de estado de servicio ServerEmail_1 Estado Imap.....	61
Figura 7. Entradas del registro del servicio ServerEmail_1 Estado_Imap	61
Figura 8. NagiosGrapher ServerEmail_1 Estado Imap	62
Figura 9. Captura realizada por el script Estado Mailq.....	62
Figura 10. Averías de estado de servicio ServerEmail_1	63
Figura 11. Entradas del registro del servicio ServerEmail_1 Mailq	63
Figura 12. Entradas del registro Criticas del servicio ServerEmail_1 Mailq	63
Figura 13. NagiosGrapher: ServerEmail_1 Estado Pop3	64
Figura 14. NagiosGrapher: ServerEmail_2 Estado Pop3	64
Figura 15. NagiosGrapher: ServerEmail_3 Estado Pop3	65
Figura 16. Captura realizada mediante script Estado Pop3.	65
Figura 17. NagGrapher-ServerEmail_3 Estado servicio Ping.....	66

Figura 18. NagiosGrapher-BalanceadorUho Estado servicio SMTP	66
Figura 19. Estado servicios ServerWebUho.....	67
Figura 20. Captura realizada por script al ServerWebUho	67
Figura 21. Captura realizada por script al ServerWebUho	68
Figura 22.Crear reporte de Disponibilidad ServerWebUho. Estado Apache2_HTTP.....	68
Figura 23. Averías de estado del ServerWebUho. Estado Apache2_HTTP	69
Figura 24.Entradas del registro del servicio ServerWebUho. Estado Apache2_HTTP.....	69
Figura 25. . NagiosGrapher-ServerWebUho. Estado Apache2_HTTP.....	70
Figura 26. Captura realizada por script ServerWebUho. Estado PING	71
Figura 27. NagiosGrapher-ServerWebUho. Estado servicio PING	71
Figura 28. Estado servicio ServerRadius	72
Figura 29. Trama Servicio PING: ServerRadius.....	73
Figura 30.Crear reporte de Disponibilidad: ServerRadius-Servicio PING	73
Figura 31.Averías de estado del ServerRadius: Servicio PING	74
Figura 32.Entradas del registro del servicio ServerRadius: Servicio PING	74
Figura 33. Autenticación de Nagios Interfaz Web	85
Figura 34. Interfaz Web de Nagios.....	86
Figura 35.Estado servicios FTP	88

Figura 36. Trama Servicio Apache_HTTP. FTP-Uho	88
Figura 37. Averías Servicio Apache_HTTP: FTP-Uho	89
Figura 38.Entradas del registro del servicio Apache2_HTTP: FTP-Uho	89
Figura 39. Averías Servicio FTP.....	90
Figura 40.Entradas del registro del servicio FTP: FTP-Uho	90
Figura 41.NagiosGrapher: Servicio Apache2_HTTP: FTP-Uho	91
Figura 42. Estado de los servicio en el Servidor Nagios	91
Figura 43. Trama Servidor Nagios	92
Figura 44. Averías Servidor Nagios.....	92
Figura 45.Entradas del registro del Servidor Nagios.	93
Figura 46. NagiosGrapher Balanceador Servicio PING	93
Figura 47.NagiosGrapher WIFIUHO-1 Servicio PING	94
Figura 48.NagiosGrapher DNS-FH Servicio PING	94

Índice de Tablas

Tabla 1. Análisis de la selección del software de monitoreo.	44
---	----

Introducción

Nadie está ajeno a la enorme influencia que ha alcanzado la informática en la vida diaria de las personas y organizaciones, y la importancia que tiene su progreso para el desarrollo de un país. El comercio, las comunicaciones, los procesos industriales, las investigaciones, la seguridad, la salud entre otras organizaciones. Son todos aspectos que dependen cada día más de un adecuado desarrollo de las tecnologías informáticas[1].

El desarrollo de la computación y su integración con las telecomunicaciones en la telemática[2], han propiciado el surgimiento de nuevas formas de comunicación, que son aceptadas cada vez por más personas. El desarrollo de los servicios informáticos posibilitó su conexión mutua y, finalmente, la existencia de Internet, una red de redes gracias a la cual una computadora puede intercambiar fácilmente información con otras situadas en regiones lejanas. [3]

Los servicios de red constituyen un elemento de singular importancia en el desarrollo de los procesos sustantivos de cualquier institución de educación superior, a partir del soporte que significan para elementos tan disímiles como el control de estudiantes, la enseñanza a distancia, las comunicaciones internas y externas del centro, entre muchos otros. En su funcionamiento se destacan aspectos de relevancia, que tienen que ver con la vitalidad de estos servicios y su calidad, además de lo concerniente con las regulaciones relativas al uso adecuado de la red LAN. [4]

El uso creciente de los servicios de red en la actividad diaria ha dado lugar a un incremento sustancial en el número de usuarios que reciben el mismo.

La red[5] 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 institución de educación.[6]

Las características principales 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. [7]

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 a través de correo electrónico, localizadores u otras alarmas. Es un subconjunto de las funciones implicadas en la administración de la red. La monitorización tiene unos alcances increíbles, desde sus inicios en los años 90, se consolidó como uno 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 administradores y los excesos de costos de infraestructura. [6]

Actualmente aunque las redes y sus componentes sean seguros y confiables, no se puede dejar a un lado la tarea de vigilar y monitorear la red para lograr un correcto funcionamiento, si esta no posee una correcta administración y mantenimiento pueden surgir muchos problemas, que generarían pérdidas de tiempo y de recursos, es por ello que existen numerosas herramientas para la gestión de una red.

Es donde surge la necesidad de mantener un excelente funcionamiento, que es la función principal del administrador, por lo que necesitaría un conjunto de herramientas potentes que le permitan llevar a cabo todas las tareas, involucrando aun mas al supervisor en la correcta gerencia y gestión de la red, en este campo siempre existen muchos obstáculos que impiden el buen

desempeño de los servicios, por lo tanto el monitoreo tiene que ser una actividad primaria en la gestión de la organización. Por lo que es necesario poseer un instrumento que permita saber con anticipación la causa y lugar exactos del problema para solucionarlo a tiempo y evitar mayores complicaciones. [8]

En fin existen numerosos problemas en la administración y gestión de una red[8], por lo que es sumamente importante contar con un servidor como Nagios enfocado en el monitoreo, con base en esto la finalidad de la tesis es proporcionar una herramienta fácil de usar, administrable desde cualquier ordenador, de bajo costo, que sea potente y eficaz que prometa aumentar la productividad y precisión en el mantenimiento, por medio del monitoreo y determinar de manera exacta en que punto o nodo de la red se está generando un problema y así solventar la situación con rapidez para evitar el colapso de las conexiones, por lo que le ofrecerá al administrador mayor conocimiento acerca de su red de manera remota y así mantener la calidad del servicio.

La implementación de este tipo de servidor trae numerosas ventajas tales como:

Reducción de costos

Con la reducción de costos se espera disminuir los gastos en adquisición de equipos por averías, ya que se podrá realizar mantenimiento preventivo a todos componentes de la red, siendo planificados de acuerdo con su ubicación.

Solución rápida de los problemas

Con la determinación exacta del foco del problema mediante el mapa de la red que arroja el sistema Nagios, se podrá ahorrar tiempo en revisar uno a uno los puntos de conexión para determinar donde ocurre el inconveniente, ya que con el método de monitoreo implementado se tendrá la ubicación del dispositivo o nodo de la red donde está fallando y así solucionar el altercado lo más pronto posible.

Mejoras en la calidad del servicio

Al localizar rápidamente la afectación se procederá a la solución más rápida del problema, que se esté presentando en la red, y como consecuencia el usuario final no perderá mucho tiempo del trabajo y contara con un servicio de internet y de transmisión de datos de mejor calidad.

Organización estructurada de la red

Mediante Nagios se realizara la organización estructurada de la red, ya que esta organiza los dispositivos por jerarquización, determinando el parentesco que tenga los dispositivos entre, además que se podrá organizar por tipo de dispositivo, y el mapa final mostrado estará organizado.

Mayor aprovechamiento del personal

Con la reducción del tiempo necesario para ubicar el problema y solucionarlo, es posible el aprovechamiento del personal (Admón. Nodo Central Uho) para orientarlo a su constante documentación, es decir, que el empleado tendrá disponibilidad de tiempo para el estudio de nuevas herramientas para el control y monitoreo de la red, además de mejorar y renovar sus conocimientos informáticos, con el tiempo disponible los administradores de la red estarán en la capacidad de organizar y mantener en buen estado su área de trabajo y contar con un espacio confortable, igualmente el personal podrá planificar con bastante antelación programas de mantenimiento preventivo y correctivo en toda la red Uho.

Alcance

La implementación de un servidor para el monitoreo de la red en el Nodo Central Uho, mejorara y optimizara las labores de diagnostico de fallas en la red localizando de manera exacta el problema, la gestión y administración de los dispositivos de red, además de brindar a los administradores una visión y ubicación de todos los dispositivos que conforman su red. Logrando llevar al nodo de redes a tener un mayor control sobre su red.

El nodo central de la red de la Universidad de Holguín concentra la gestión de la red de la institución en su nivel jerárquico superior y la totalidad de las comunicaciones externas que incluye asimismo todo el equipamiento necesario para esto. En este último caso se incluyen servicios de alta significación para los procesos de la universidad: el correo electrónico nacional e internacional, el acceso a la red nacional, el servicio de mensajería instantánea, de transferencia de ficheros, el acceso a internet y el servicio de comunicación remota, tanto para profesores desde su hogar, como para las sedes universitarias municipales.

Además de ser muy importantes estos servicios se han caracterizado por presentar problemas frecuentes de tiempos de establecimiento alto, baja estabilidad, calidad de las conexiones. Hasta el momento, la manera de conocer de estos problemas por parte del personal de administración es por medio de controles espontáneos, realizados sin planificación al estado de los servidores y por las quejas de los usuarios, cuando no pueden acceder de manera satisfactoria a esto.

Por lo tanto, se hace necesaria la implantación de un servidor de monitorización de los servicios y equipos de la red, configurado con sistemas de alertas ante las anomalías que se puedan presentar, que permita conocer en tiempo real el comportamiento de los principales parámetros que describen su funcionamiento, y contribuya a que el personal técnico pueda responder en los plazos más breves a los eventos que afecten la calidad de los servicios de red, y por otro lado proteger el equipamiento de red. Estos aspectos constituyen la situación problemática que conduce a la existencia de insatisfacciones en los usuarios de la red.

Tras el estudio de esta situación surgió el siguiente **problema científico**:
¿Cómo realizar la monitorización de los servicios de red del nodo central de la Universidad de Holguín?

A partir del problema se define el **objeto de estudio**: los procesos informáticos de la red de la Universidad de Holguín “Oscar Lucero Moya que se desarrollan en su Nodo Central”. Para la solución del problema planteado se persigue el siguiente **objetivo general**: realizar la monitorización de los servicios informáticos de red del Nodo Central de la Universidad de Holguín “Oscar Lucero Moya” que permita elevar la calidad y persistencia con que se desarrollan los mismos.

El objeto que delimita el **campo de acción** de la investigación: La monitorización de los servicios de red del nodo central de la Universidad de Holguín. Para guiar la investigación, se trazo la siguiente **hipótesis**: Implementación de un servidor de monitoreo, que realice la vigilancia del estado de los servicios y equipos de la red en el nodo central de la Universidad de Holguín “Oscar Lucero Moya” contribuirá a elevar su calidad y persistencia, beneficiando así la Confiabilidad, Disponibilidad e Integridad para las conexiones y comunicaciones del Nodo Central de la Uho.

Con el propósito de desarrollar la investigación con la mayor calidad posible, las siguientes **tareas** fueron ejecutadas:

1. Estudio del marco teórico referencial de la monitorización de los servicios de redes locales.
2. Caracterización de los servicios de la red de la Uho.
3. Evaluación y selección de herramientas de monitorización.
4. Implantación de las herramientas seleccionadas.
5. Valoración de la solución propuesta.

Para el cumplimiento de estas tareas se emplean los siguientes métodos de investigación científica:

Métodos Empíricos:

- *Entrevista:* Permitió la interacción directa con el personal que trabaja en el nodo, recoger las informaciones importantes y las necesidades de los trabajadores y estudiantes para ayudar en su labor y determinar los principales requerimientos de la investigación.
- *Observación:* Permitió realizar un análisis detallado de las condiciones de los medios informáticos con que cuenta el centro, para valorar el nivel de eficiencia y calidad que deberá tener el proceso de investigación acorde a las condiciones reales.

Métodos Teóricos:

- *Análisis-Síntesis:* Se utilizó para determinar los fundamentos teóricos de la investigación, conceptos relacionados con el objetivo, la comprensión de las relaciones esenciales y características generales del proceso, así como la elaboración de las conclusiones de la investigación.
- *Histórico-Lógico:* Se lleva a cabo un análisis del proceso de gestión de las políticas rectoras para conocer con mayor profundidad los antecedentes y las tendencias actuales.
- *Hipotético-Deductivo:* Se emplea actualmente para la elaboración y comprobación de la hipótesis bajo el análisis de las deducciones y conclusiones que emiten la investigación.

Se espera, como **Aportes Prácticos** la implantación de un servidor de Monitorización a los servicios y equipos de la red Uho donde se incluya sistemas de alertas beneficiando al personal técnico que lo administra y así obtener la información que se genera de los servicios que presta el nodo. Además la solución estará basada en tecnología de código abierto.

La presente Tesis está estructurado en dos capítulos de acuerdo a los siguientes contenidos:

Capítulo 1: Fundamentación teórica del tema

Recoge la fundamentación del tema donde se expone claramente la situación actual de todos los servicios que se brindan en el Nodo Central de la Red Uho. De igual forma se expone con vista a escoger la mejor solución un estudio de las últimas tendencias en el campo de los Servidores de Monitorización de servicios y equipos de redes LAN los que se han resumido en este capítulo y donde se muestran las características de dichos servidores de monitorización además de proponer una solución eficaz atendiendo al problema científico.

Capítulo 2: Implantación y resultados de la propuesta

En este capítulo se describe todo el proceso que se llevara a cabo para la puesta en marcha de la monitorización de los servicios y equipos de red, así como se evalúan los resultados obtenidos una vez implantados. Además se recoge en este capítulo el estudio de la factibilidad y de sostenibilidad del Servidor de Monitorización.

Para finalizar, se presentan las conclusiones, recomendaciones, referencias bibliográficas y anexos.

Capítulo

1

1 Fundamentación teórica para la implementación del Servidor de Monitoreo de servicios y equipos del Nodo Central Uho.

Se presenta a continuación la descripción del Nodo Central Red Uho y los diferentes servicios que se brindan, fundamentando el objeto de estudio y el campo de acción donde se realiza la investigación. Se muestra también la situación problémica específica de cada servicio. Y para la realización de la propuesta de solución se hace necesario detallar conceptos relacionados con la fundamentación del tema e investigar las últimas tendencias en el campo de Servidores de Monitorización de servicios y equipos de red, haciendo énfasis en los de Código Abierto.

1.1 Nodo Central de la Red Uho

El nodo central de la red de la Universidad de Holguín concentra la gestión de la red de la institución en su nivel jerárquico superior y la totalidad de las comunicaciones del centro, el mismo es el encargado de prestar todos los servicios de red a los usuarios. Entre los numerosos servicios se encuentran el correo electrónico nacional e internacional, Internet, servicio de transferencia de ficheros, resolución de nombres de dominio, publicación de páginas Web,

mensajería instantánea, acceso remoto tanto para profesores desde sus hogares como para las sedes municipales entre otros.

Además es el centro de la topología existente en la Red Uho. Consta de los principales enrutadores, switches, módems, servidores necesarios para establecer la comunicación de la Universidad de Holguín con el resto del mundo.

1.1.1 Servicio de Correo Electrónico

Uno de los usos más comunes de las redes informáticas desde sus orígenes ha sido el correo electrónico, conocido también como *e-mail*, es un servicio de red que permite a los usuarios enviar y recibir mensajes y archivos rápidamente, también denominados mensajes electrónicos o cartas electrónicas) mediante sistemas de comunicación electrónicos. Principalmente se usa este nombre para denominar al sistema que provee este servicio en Internet, mediante el protocolo **SMTP**. El servicio de correo electrónico consta de dos partes bien diferenciadas: aquella con la que trata el usuario, y la que se encarga de transportar los mensajes del origen al destino. A menudo hay un componente adicional encargado de distribuir el correo que llega a la máquina destino a una ubicación especial dentro de ésta, propia de cada usuario. [9]

Los nombres de estos componentes son:

- Cliente de Correo (MUA – *Mail User Agent*).
- Agente Transporte Correo (MTA. *Mail Transport Agent*).
- Utilidades.

Situación actual

Dentro de la arquitectura del soporte informático para la gestión de correo electrónico de la Universidad, se dispone de un sistema que gestiona todo el tráfico entrante y saliente, aplicando cuantos mecanismos de seguridad y gestión se consideren oportunos. Este sistema es lo que se denomina una

estafeta¹ de primer nivel. En un segundo nivel, se encuentran 8 subnodos que han sido considerados necesarios para las mejores prestaciones del servicio en nuestra universidad, a través de los cuales los usuarios acceden al servicio de correo electrónico.

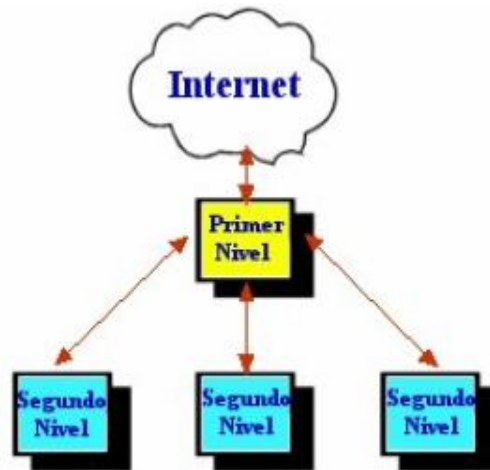


Figura 1. Relación entre las estafetas en el servicio de correo.

Como estafeta de primer nivel se tiene el servidor encontrado en el Nodo Central y como estafetas de segundo nivel se cuenta con los servidores siguientes:

1. Subnodo de la Facultad de Informática y Matemática FACINF.
2. Subnodo de la Facultad de Ingeniería FACING.
3. Subnodo de la Facultad de Ingeniería Industrial FACII.
4. Subnodo de la Facultad de Humanidades FH.
5. Subnodo de la Facultad de Economía FE.
6. Subnodo de ICT y las Vicerrectorías.
7. Subnodo del CADCAM.

¹ Oficina o Nivel del servicio de correos en la que se recibe, clasifica y reparte la correspondencia.

8. Subnodo de la VREA.

1.1.2 Servicio Web

En informática, la **World Wide Web (WWW)** o **Red informática mundial** es un sistema de distribución de información basado en hipertexto o hipermedios enlazados y accesibles a través de Internet. Con un navegador web, un usuario visualiza sitios web compuestos de páginas web que pueden contener texto, imágenes, vídeos u otros contenidos multimedia, y navega a través de ellas usando hiperenlaces. La web es el medio de mayor difusión de intercambio personal aparecido en la *Historia de la Humanidad*, muy por delante de la imprenta. Esta plataforma ha permitido a los usuarios interactuar con muchos más grupos de personas dispersas alrededor del planeta, de lo que es posible con las limitaciones del contacto físico o simplemente con las limitaciones de todos los otros medios de comunicación existentes combinados.[10]

La arquitectura *Web* es del tipo cliente-servidor. En el servidor es donde se almacena la información estática accedida y/o las aplicaciones que la generan. Los clientes por lo general son los programas conocidos como navegadores o *browsers* que gracias al DNS, que es el que se encarga de responder a las peticiones diciéndole a la petición hacia donde se debe de dirigir se encargan de contactar a un servidor ante la solicitud de un usuario y así visualizar el resultado de acuerdo a su implementación propia. El protocolo que emplean el servidor y el cliente para comunicarse es el HTTP (*HyperText Transport Protocol*) o protocolo para cada transmisión de hipertexto. Este es un protocolo orientado a caracteres que sigue el esquema petición-respuesta entre un cliente y un servidor. Por lo general los servidores *Web* escuchan las solicitudes de los clientes a través del puerto 80 y es a este a donde se van a dirigir los clientes por defecto para hacer sus solicitudes.[11]

Situación actual

En la actualidad en la Uho existe un solo servidor Web ubicado en el Nodo Central Uho donde se encuentran publicados los principales sitios web de entidad, pero a la vez en las distintas áreas o subnodos existen otras

máquinas(servidores) que tienen publicados los sitios Web específicos para las especialidades correspondientes a sus facultades y áreas.

1.1.3 Servicio de transferencia de fichero FTP

Uno de los servicios más antiguos de Internet, File Transfer Protocol permite mover uno o más archivos con seguridad entre distintos ordenadores proporcionando seguridad y organización de los archivos así como control de la transferencia. [12]

El servicio FTP tiene dos variantes; *Anónima* donde la conexión al servidor FTP no requiere de una cuenta previamente creada en este, o sea, no se realiza autenticación basada en usuario. Normalmente el *login* que se utiliza en este caso es *anonymous* y el *password* una dirección válida de correo. Los documentos compartidos mediante FTP anónimo normalmente se agrupan en cierta estructura de directorios con permisos bien restrictivos. Además existe la variante *No anónima* donde la conexión al servidor FTP se establece mediante una cuenta de usuario previamente creada en este. El usuario una vez autenticado podrá acceder a todos los ficheros en el servidor de acuerdo a los permisos del sistema de ficheros aplicados a su caso.

El principal problema de este servicio es que fue concebido para realizar las transferencias de ficheros con la mayor velocidad pero con poca seguridad; todo el intercambio de información, desde el *login* y *password* del usuario en el servidor hasta la transferencia de cualquier fichero, se realiza en texto plano con lo que un atacante lo tiene muy fácil para capturar todo ese tráfico y conseguir así un acceso válido al servidor. Incluso puede ser una amenaza a la privacidad de los datos el hecho de que ese atacante también pueda capturar y reproducir los ficheros transferidos. Es por ello que normalmente el servidor está configurado para que el usuario con privilegios de administración no pueda conectarse.

Situación actual

Actualmente este servicio se encuentra implementado en el servidor FTP del Nodo Central de la Red Uho para realizar la transferencia de ficheros entre los

servidores y por parte de los usuarios utilizando las dos variantes de conexión: *Anónima* y *No anónima*. Se encuentra publicado en este servidor un conjunto de datos, documentos, programas necesarios para los usuarios de la Red Uho a los cuales pueden acceder desde sus estaciones de trabajo.

No solamente existe este solo servidor FTP en la Red Uho, también existen otros servidores en otros Subnodos del Instituto donde los administradores han publicado datos, informaciones y programas más específicos a las características de las carreras a las que pertenecen sus usuarios.

1.1.4 Servicio de Acceso Remoto

El servicio de acceso remoto permite a los usuarios conectarse a la red mediante una conexión telefónica. Una vez conectado, gozará de las mismas ventajas que si estuviese conectado físicamente a la red. La tecnología de acceso remoto posibilita la centralización de las aplicaciones que generalmente se ejecutan en un entorno de usuario local, como los procesadores de texto o los navegadores.

Para poder disfrutar de este servicio solamente se necesita una conexión telefónica, siempre acompañado de una encriptación de alto nivel para garantizar la máxima seguridad.

Este tipo de acceso remoto es muy útil para entidades como nuestras sedes debido a que el personal profesional que circula en la misma no siempre está presente en nuestro centro, de ahí que Doctores, Máster, Ingenieros y Jubilados autorizados presenten algún tipo de inconveniente para trasladarse hacia la Uho pues gozaran de tener total acceso a la información y programas que se encuentran en los ordenadores de la oficina. De esta forma, el usuario podrá beneficiarse de toda la información que necesite a la vez que se mantiene en contacto con el resto de usuarios de la red.

Este sistema es de fácil uso porque se pueden ejecutar las mismas tareas que si se estuviese conectado físicamente a la red y la seguridad queda totalmente garantizada ya que si un usuario no dispone de permiso para entrar en un

determinado archivo cuando está conectado localmente, tampoco podrá acceder a él con el acceso remoto. [13]

Para que un usuario sea beneficiado con el servicio, primeramente debe ser trabajador o haber transitado por un periodo largo por la Uho (jubilado), tener teléfono en su casa y por ultimo realizar los trámites pertinentes en el Nodo Central Uho.

Situación actual

Actualmente este servicio se encuentra implementado en el servidor de Acceso Remoto del Nodo Central de la Red Uho para realizar la conectividad desde los hogares hacia la Uho.

El nodo central implementa uno de los servidores más actualizados para esta función el Radius² con las aplicaciones del Freeradius es una alternativa libre hacia otros servidores RADIUS, siendo uno de los más completos y versátiles gracias a la variedad de módulos que le componen. Puede operar tanto en sistemas con recursos limitados así como sistemas atendiendo millones de usuarios. En nuestros días incluye soporte para directorios LDAP este directorio es el que se está implementando en la red Uho, SQL y otras bases de datos, así como EAP, EAP-TTLS y PEAP. Actualmente incluye soporte para todos los protocolos comunes de autenticación y bases de datos. [14]

² Radius: **R**emote **A**uthentication **D**ial-In **U**ser **S**ervice es un protocolo de autenticación, autorización y manejo de cuentas de usuario utilizado para administrar el acceso remoto y la movilidad IP, como ocurre en servicios de acceso por modem.

1.1.5 Servicio de Mensajería Instantánea

Una primera forma de mensajería instantánea fue desde la implementación en el sistema PLATO³ usado al principio de la década de 1970. Más tarde, el sistema Talk⁴ implementado en UNIX/LINUX comenzó a ser ampliamente usado por ingenieros y académicos en las décadas de 1980 y 1990 para comunicarse a través de internet o redes LAN.

La mensajería instantánea (conocida también en inglés como IM) es una forma de comunicación en tiempo real entre dos o más personas basada en texto. El texto es enviado a través de dispositivos conectados a una red, requiere el uso de un cliente de mensajería instantánea que realiza el servicio y se diferencia del correo electrónico en que las conversaciones se realizan en tiempo real.

Situación actual

El Nodo Central de la Red Uho rector de las comunicaciones en la entidad hospeda este servicio en su completo funcionamiento. Implementa Ejabberd servidor de mensajería instantánea de código abierto para plataforma Unix, ejabberd es un potente servidor XMPP estable y con variedad de posibilidades.

1.1.6 Servicio de Red Inalámbrica WI-FI

Wi-Fi es un mecanismo de conexión de dispositivos electrónicos de forma inalámbrica. Los dispositivos habilitados con Wi-Fi, tales como: un ordenador personal, una consola de videojuegos, un smartphone o un reproductor de audio digital, pueden conectarse a Internet a través de un punto de acceso de red inalámbrica. Dicho punto de acceso (o hotspot) tiene un alcance de unos 20

³ Plato: Programmed Logic Automated Teaching Operations o PLATO (Operaciones lógicas programadas para enseñanza automatizada) fue uno de los primeros sistemas generalizados de asistencia por computadora.

⁴ Talk: Programa de UNIX.

metros en interiores y al aire libre una distancia mayor. Pueden cubrir grandes áreas la superposición de múltiples puntos de acceso.

Wi-Fi es una marca de la *Wi-Fi Alliance* (anteriormente la *WECA: Wireless Ethernet Compatibility Alliance*), la organización comercial que adopta, prueba y certifica que los equipos cumplen los estándares 802.11 relacionados a redes inalámbricas de área local.[15]

Existen varias alternativas para garantizar la seguridad de estas redes. Las más comunes son la utilización de protocolos de cifrado de datos para los estándares Wi-Fi como el *WEP*, el *WPA*, o el *WPA2* que se encargan de codificar la información transmitida para proteger su confidencialidad, proporcionados por los propios dispositivos inalámbricos. La mayoría de las formas son las siguientes:[16]

- ✚ *WEP*, cifra los datos en su red de forma que sólo el destinatario deseado pueda acceder a ellos. Los cifrados de 64 y 128 bits son dos niveles de seguridad *WEP*. *WEP* codifica los datos mediante una “clave” de cifrado antes de enviarlo al aire. Este tipo de cifrado no está muy recomendado debido a las grandes vulnerabilidades que presenta ya que cualquier cracker puede conseguir sacar la clave, incluso aunque esté bien configurado y la clave utilizada sea compleja.
- ✚ *WPA*: presenta mejoras como generación dinámica de la clave de acceso. Las claves se insertan como dígitos alfanuméricos.
- ✚ *IPSEC* (túneles IP) en el caso de las VPN y el conjunto de estándares IEEE 802.1X, que permite la autenticación y autorización de usuarios.
- ✚ Filtrado de MAC, de manera que sólo se permite acceso a la red a aquellos dispositivos autorizados. Es lo más recomendable si solo se va a usar con los mismos equipos, y si son pocos.
- ✚ Ocultación del punto de acceso: se puede ocultar el punto de acceso (Router) de manera que sea invisible a otros usuarios.
- ✚ El protocolo de seguridad llamado *WPA2* (estándar 802.11i), que es una mejora relativa a *WPA*. En principio es el protocolo de seguridad más

seguro para Wi-Fi en este momento. Sin embargo requieren hardware y software compatibles, ya que los antiguos no lo son.

Sin embargo, no existe ninguna alternativa totalmente fiable, ya que todas ellas son susceptibles de ser vulneradas.

Situación Actual

Actualmente este servicio se brinda a los usuarios de la red universitaria por medio de equipos destinados para esta función. La dirección de Informatización del centro puso a disposición del Nodo Central de 7 equipos dotados con los mínimos requerimientos para prestar ese servicio estos router con marca TP-Link traen un soporte de protocolos CSMA/CA, CSMA/CD, TCP/IP, ICMP, DHCP, NAT y SNTP. Están ubicados en distintas aéreas de la Uho ya que poseen un radio de acción total de 200 metros y efectiva de 100 metros para tener una buena conectividad, cada día son más los usuarios que dejan atrás la conexión vía cable para unirse a la moderna wifi (llamada así por los hispanoamericanos). Para que un usuario pueda gozar de este medio debe presentar un formulario con los datos que se piden en el mismo y presentarlos en el nodo central Uho allí se le asignara un *user* y *passwd* para la conectividad de la wifi una vez conectado puede hacer uso de todos los servicio que brinda nuestra Universidad.

Como medida de seguridad de los administradores y por requerimientos de la Oficina de Seguridad Provincial al ser este un servicio inalámbrico requiere de algún tipo de seguridad para poder prestar servicio a los usuarios de la red y para prevenir posibles ataques maliciosos, es por ellos que el servicio tiene implementado el soporte de cifrado *WPA2* que se encargan de codificar la información transmitida para proteger su confidencialidad, proporcionados por los propios dispositivos inalámbricos.

1.2 Estudio del Arte de las tecnologías de la información y las Comunicaciones.

Para la realización de la propuesta de solución se hace necesario investigar las últimas tendencias en el desarrollo de software y los servicios de administración de una red, resultados que se muestran en el presente capítulo. Además se recogen las comparaciones realizadas y la decisión final acerca de cuáles sistemas son los idóneos para la solución de la problemática.

1.2.1 Sistemas Operativos

El Nodo Central de la Uho tiene entre sus políticas[17] la utilización de sistemas operativos como GNU/Linux y sus distribuciones.

1.2.1.1 Sistemas Operativos GNU/Linux

Los sistemas GNU/Linux [18] ya no son una novedad, cuentan con una amplia variedad de usuarios y de ámbitos de trabajo donde son utilizados.

Su origen se remonta al mes de agosto de 1991, cuando un estudiante finlandés llamado *Linus Torvalds* anunció en una lista de news (noticias) que había creado su propio núcleo de sistema operativo y lo ofrecía a la comunidad de desarrolladores para que lo probara y sugiriera mejoras para hacerlo más utilizable. Éste sería el origen del núcleo (o kernel) del operativo que más tarde se llamaría Linux.

Por otra parte, la FSF (Free Software Foundation, Fundación Software Libre por sus siglas en inglés), mediante su proyecto GNU, producía software (desde 1984) que podía ser utilizado libremente. Debido a lo que Richard Stallman (miembro de la FSF) consideraba software libre, es decir, como aquél del que podíamos conseguir sus fuentes (código), estudiarlas y modificarlas, y redistribuirlo sin que nos obliguen a pagar por ello. En este modelo, el negocio no está en la ocultación del código, sino en el software complementario añadido, en la adecuación del software a los clientes y en los servicios añadidos, como el mantenimiento y la formación de usuarios (el soporte que les

demos), ya sea en forma de material, libros y manuales, o en cursos de formación.

La combinación (o suma) del software GNU y del kernel Linux, es el que nos ha traído a los actuales sistemas GNU/Linux. Actualmente, los movimientos Open Source, desde diferentes organizaciones (como FSF) y empresas como las que generan las diferentes distribuciones Linux (Red Hat, Mandrake, SuSe, Debian,...), pasando por grandes empresas como HP, IBM, Sun, Novell que proporcionan apoyo, han dado un empujón muy grande a los sistemas GNU/Linux hasta situarlos al nivel de poder competir, y superar, muchas de las soluciones propietarias cerradas existentes.

El sistema ha sido diseñado y programado por múltiples programadores alrededor del mundo. El núcleo del sistema sigue en continuo desarrollo bajo la coordinación de *Linus Torvalds*, la persona de la que partió la idea de este proyecto, a principios de la década de los noventa. Hoy en día, grandes compañías, como IBM, SUN, HP, Novell y RedHat, entre otras muchas, aportan a Linux grandes ayudas tanto económicas como de código.

Día a día, más y más programas y aplicaciones están disponibles para este sistema, y la calidad de los mismos aumenta de versión a versión. La gran mayoría de los mismos vienen acompañados del código fuente y se distribuyen generalmente bajo los términos de licencia de la *GNU General Public License*. Más y más casas de software comercial distribuyen sus productos para Linux y la presencia del mismo en empresas aumenta constantemente por la excelente relación calidad-precio que se consigue con Linux. [19]

También es de destacar que el mercado de Linux crece rápidamente, y los ingresos por software de servidores, escritorios, y empaquetados, que corren bajo este sistema, se mantienen en aumento. La creciente popularidad de Linux se debe a las ventajas que presenta ante otros sistemas operativos, entre otras a su estabilidad, al acceso a las fuentes (lo que permite personalizar el funcionamiento y auditar la seguridad y privacidad de los datos tratados), a la

independencia de proveedor, a la seguridad, a la rapidez con que incorpora los nuevos adelantos tecnológicos (IPv6, microprocesadores de 64 bits), a la escalabilidad (se pueden crear *clusters* de cientos de computadoras), a la activa comunidad de desarrollo que hay a su alrededor, a su interoperabilidad, a la abundancia de documentación relativa a los procedimientos y la ventajas más sobresaliente de Linux se encuentra en lo referido a *redes informáticas*. Cada día más administradores de sistemas eligen Linux, por su costo reducido, sus ventajas y utilidad, mediante soluciones de Servidores para Intranet e Internet. Linux soporta toda la familia de protocolo TCP/IP y todos los servicios y aplicaciones que utilizan este último. [8]

1.2.1.2 Distribuciones de GNU/Linux

El software de Linux se puede conseguir con muchas distribuciones, como Debian, Redhat, Ubuntu, CentOS, SuSE, Slackware, Fedora, Gentoo, Linux Mint entre otras. Cada distribución contiene todo lo necesario para instalar un sistema Linux completo: el núcleo, utilidades básicas, bibliotecas, ficheros de soporte y aplicaciones. Las distribuciones Linux pueden obtenerse a través de diferentes fuentes en línea, como Internet. Cada una de ellas suele tener su sitio de distribución por FTP y un sitio Web.[20]

Cada distribución empaqueta y proporciona ciertas librerías básicas, utilidades de configuración, aplicaciones del sistema y ficheros de configuración. Sin embargo, hay diferencias entre versiones, nombres y localizaciones que hace difícil saber cuáles tienen cada distribución. Esto hace complicado incluir aplicaciones pre compiladas que funcionen bien en todas las distribuciones.

Para intentar solucionar este problema, se ha creado un nuevo proyecto llamado *Linux Standard Base* (Estándar de Sistema Linux Básico). Intenta describir un estándar de ficheros básicos que debe cumplir toda distribución. Así, si un fabricante desea desarrollar una aplicación que funcione en muchas distribuciones sin problemas, basta tener en cuenta la ubicación y versiones de ficheros que el estándar propone. [21]

1.2.2 Redes informáticas

Definición de Red

Una red es un sistema que está compuesto por elementos conectados entre sí, que pueden comunicarse para compartir recursos.

Una red, es más que varias computadoras conectadas, la constituyen varias personas que solicitan, proporcionan e intercambian experiencias e informaciones a través de sistemas de comunicación. [22]

Aplicación de las redes

Debido a los grandes avances en la tecnologías de comunicación se puede decir que la aplicación de las redes es muy extensa, además el estudio de las redes a llevado a comprender como funciona la red del humano es decir la red neuronal, que es aquella que controla todo nuestro sistema nervioso, todo nuestro mundo está formado por redes, para que nos llegue un alimento este debe pasar por un conjunto de procesos que están formados por un conjunto de redes.

Es por ello que su aplicación abarca desde nuestra vida diaria, hasta los procesos más industrializados del planeta que están interconectados y funcionando a través de un sistema de redes. Por lo que tiene una importancia económica ya que de esta manera es posible manejar datos e información de manera rápida y enviarla de un lugar a otro en cuestión de segundos. No solo la parte económica se ve beneficiado sino que todos los campos de la sociedad observan y palpan día a día la influencia de las redes en sus vidas.

Como es el objetivo principal de una red que es la comunicación, surgiendo el tan conocido por todos, el correo electrónico, que nos permite compartir datos, imágenes, documentos en cuestión de segundo y hacia cualquier parte del mundo simplificando en nuestras vida el modo de comunicarnos ya sea por cuestiones personales o profesionales, las redes se han adaptado muy bien a nuestra sociedad.

Estructura de una red

Según Andrew S. Tanenbaum[23]. Establece: “La estructura principal de una red es conjunto de dispositivos o estaciones de trabajo conectadas entre sí,

donde entran en juego las denominadas subredes que son las que permiten la interconexión entre las distintas redes, transmitiendo de un lado a otro la información hasta dar con su destino”.

Aunque la estructura de la red este formada por un conjunto de subredes, no hay que dejar atrás a los componentes y dispositivos que la conforman, ya que sin estos no existiría y no funcionaria la red, porque para que exista la red debe existir los dispositivos que le permitan interconectarse. Por lo que se puede decir que una red está estructurada por un conjunto de dispositivos conectados entre sí transmitiendo datos entre ellos a través de una subred.

Protocolo de redes

Los protocolos de redes son el conjunto de normas y pasos que se deben seguir para enviar y recibir información, no existe solo un modelo por lo contrario esto depende del sistema operativo y del tipo de red que se esté implementando, por lo que un ordenador puede funcionar al mismo tiempo con varios protocolos de red.

Tipos de protocolos de redes

Cuando dos o más equipos están conectados en red, las reglas y procedimientos técnicos que dictan su comunicación e interacción se denominan protocolos. Existen gran variedad de protocolos y trabajan en ciertos niveles del modelo OSI, cada uno tiene una función diferente y realiza distintas tareas. A continuación se definen algunos protocolos:

Protocolo Simple de Gestión de Red (SNMP)

Es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Es parte de la familia de protocolos TCP/IP. SNMP permite a los administradores supervisar el funcionamiento de la red, buscar y resolver sus problemas, y planear su crecimiento. [24]

Protocolo Simple de Transferencia de Correo (SMTP)

Es un protocolo de la capa de aplicación, basado en texto utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos (PDA's, teléfonos móviles, etc.). Se basa en el modelo cliente-

servidor. En el protocolo SMTP todas las órdenes, réplicas o datos son líneas de texto. [24]

Protocolo de Transferencia de Hipertexto (HTTP)

Es el protocolo usado en cada transacción de la Web (www). Especifica las reglas para la comunicación entre los exploradores y servidores Web, por el o define la sintaxis y la semántica que utilizan los elementos de la arquitectura web. Es un protocolo orientado a transacciones y sigue el esquema petición-respuesta entre el cliente y el servidor. [24]

Protocolo de la oficina de correo (POP3)

Este protocolo es usado en clientes locales de correo para obtener los mensajes de correo electrónicos almacenados en un servidor remoto. Está diseñado para recibir correo, no para enviarlo, les permite a los usuarios con conexiones intermitentes, descargar su correo electrónico mientras tiene conexión y revisarlo posteriormente incluso estando desconectados.[24]

Protocolo dinámico de configuración de host (DHCP)

Es un estándar IP diseñado para simplificar la administración de la configuración IP del host. Permite el uso de servidores DHCP para administrar la asignación dinámica a los clientes DHCP de la red, de direcciones IP y otros de tal es de configuración relacionados a partir de la base de datos de direcciones IP del servidor de la red local. [24]

Protocolo de seguridad (IPSEC)

Es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el protocolo de internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. IPSEC también incluye protocolos para el establecimiento de claves de cifrado. [24]

Protocolo de mensajes de control de internet (ICMP)

Es el sub protocolo de control y notificación de errores del protocolo de internet (IP). Se usa para enviar mensajes de error, indicando si un servicio

determinado no está disponible o que un router o host no puede ser localizado.
[24]

Protocolo de Transferencia de Archivos (FTP)

Es un protocolo de comunicación remota para transferir ficheros entre ordenadores. En una sesión FTP, el usuario desea transferir ficheros a un host remoto, para iniciar la sesión debe utilizar un cliente FTP al cual le manda el nombre del host remoto y el login/password en caso de necesitarlo. Esta información de control, se manda al servidor remoto sobre una conexión TCP/IP, luego que autoriza, crea otra conexión para realizar la transferencia.
[24]

Tipos de redes

Red pública: Es una red que puede usar cualquier persona, sin limitaciones y sin ningún tipo de clave de acceso, es usada para compartir información. [22]

Red privada: Este tipo de redes solo puede ser usada por un número determinado de personas que se encuentren registrados en ellas, este tipo de redes es utilizado en la organización y compañías, para poder usar este tipo de red se debe poseer una clave de acceso.[22]

Red de área personal (PAN): Es una pequeña red compuesta por dispositivos personales como computadoras y equipos móviles, se usa para compartir información entre los dispositivos personales, sin que sea necesario el uso de internet, además existe la posibilidad de este tipo de conexión sin cableado gracias a la tecnología bluetooth. [22]

Redes de área local (LAN): Como su nombre lo indica es una red local donde se interconectan los dispositivos que se encuentren dentro del alcance de red, es el tipo de red más usado, ya que es posible interconectar impresoras, computadoras y todo tipo de aparato que tenga posibilidad de conexión a una red.[3]

Red de área local virtual (VLAN): Es un conjunto de equipos y recursos a compartir que se interconectan como si estuvieran en la misma ubicación física

sin importar su ubicación geográfica, para evitar la restricción por la ubicación geográfica.[22]

Red de área metropolitana (MAN): Es una red compuesta por varias redes de área local, hasta alcanzar un tamaño geográfico de una ciudad metropolitana.[22]

Red de área de almacenamiento: Este tipo de red está concebida para conectar servidores, arreglos de discos y librerías de soporte, su conexión se realiza a través de la fibra óptica para mejor transmisión de datos y mayor seguridad en la conexión.[22]

Red irregular: Este es el modelo más usado en la mayoría de las redes, ya que se encuentra compuesto por un conjunto de cables y buses conectados a través de un modem, para conectar una o más computadoras. [22]

Red interna: A este grupo pertenecen las redes privadas, comerciales, industriales o gubernamentales, debido a su tipo de estructura y configuración de ser redes internas conectando dos o más redes o segmentos de red, donde los dispositivos funcionan en, la capa 3 del modelo OSI.[22]

Redes de área extensa (WAN)[22]: Cuando se llega a un punto donde es imposible o tan solo es poco práctico el uso de redes LAN, es donde nace la necesidad de establecer otro tipo de conexión, es por ello que las redes LAN se lleva a otro nivel cuando se establece la conexión sin cables de manera inalámbrica. Las tecnologías WAN funcionan generalmente en las tres capas más bajas del Modelo de referencia OSI: la capa física, la capa de enlace de datos, y la capa de red. Esta a su vez se divide en dos tipos:[7]

- **Centralizado:** Esta consiste en un computador central al que se conectan los otros dispositivos que componen la red.

- **Distribuido:** Una distribuida es aquella que cuenta con dos o más computadoras a los cuales se conectan otros dispositivos que forman otros nodos.

1.2.2.1 Dispositivos de Red

Hub

Conocidos como concentradores, permiten la comunicación entre los equipos de una red. Regenera y sincroniza las señales de red y las envía a cada uno de sus puertos ya que no puede identificar la fuente ni el destino de la información que recibe. Un hub puede enviar o recibir información, pero no puede hacer ambas cosas al mismo tiempo. Los concentradores son dispositivos poco complejos y de bajo costo. [8]

Switch

Trabajan similar a los hubs, con la diferencia que analiza cada paquete de información que llega y que establece una conexión temporal exclusiva entre la fuente y el destino cuando se necesita. Pueden enviar y recibir información al mismo tiempo, por lo que maneja y administra la información más rápido que los hubs, aumenta el ancho de banda, además de evitar que usuarios no autorizados puedan interceptar el tráfico de la red. [8]

Router

Permite interconectar redes y se encarga de determinar la mejor ruta a través de la cual se envía la información en la red. El router recibe el paquete, revisa la dirección de red a través de una operación and con la máscara de red, revisa en su tabla de enrutamiento y desvía el paquete a la interfaz correspondiente. [8]

1.2.3 Monitoreo de red

En el monitoreo interviene dos aspectos muy importantes, la gestión de red que se encarga de mantener el correcto funcionamiento evitando que los recursos de la red funcionen erróneamente bajando el nivel de eficiencia de la red. También el monitoreo como eje central es el proceso continuo de recolección y

análisis de los datos para así poder anticipar cualquier problema que pueda aparecer.[6]

En estos últimos tiempo el monitoreo a tomado gran importancia en el ámbito computacional especialmente en las áreas de redes y seguridad, debido a que una de las funciones principales consiste en supervisar que las tareas definidas en el plan operativo y de presupuesto se estén llevando a cabo sin inconvenientes. A demás de inspeccionar todos los equipos involucrados en la red y su funcionamiento ya que es posible determinar qué espacio de disco está disponible, el uso de memoria, en fin verifica el estado y funcionamiento del ordenador.[7]

De esta manera se puede decir que los sistemas de monitoreo de redes permiten controlar no solo el funcionamiento del hardware sino que también es posible controlar el software. Los sistemas de monitoreo de red están diseñados no solo para el control sino para una visualización completa y exacta de cada una de las direcciones o nodos, etiquetadas con sus atributos, características y enlaces para la modificación de los dispositivos, en un plano estructurado y organizado.

Los sistemas de gestión y monitoreo de redes tienen un conjunto de elementos clave:

Estación de Gestión o NMS (Network Monitoring System - Sistema de Monitoreo de Red por sus siglas en ingles) esta es la que proporciona la interacción entre en administrador de la red y el sistema, además posee una base de datos de información de la gestión de la red que es extraída de cada una de las bases de datos de los dispositivos gestionados.[25]

Otro de los elementos clave del sistema es el Agente quien se encarga de resolver las solicitudes de acción, a demás proporciona información importante de la gestión. Para poder realizar el enlace entre las estaciones de trabajo existe un protocolo específico este es el protocolo SNMP (Simple Network

Management Protocol - Protocolo de Gestión de Red Simple por sus siglas en ingles), que tiene ciertas capacidades clave:[26]

- **Get:** obtiene datos significativos del agente.
- **Set:** establece los valores del agente.
- **Notify:** notificaciones de eventos importantes.

En cuanto al tamaño de la red a monitorear esta se puede dividir en dos tipos o esquemas uno de ellos es el centralizado, este posee una única estación central para la gestión de la red y todos los recursos dispuestos en ella, este especialmente es para uso en redes LAN como nuestro caso.

El esquema descentralizado posee múltiples estaciones distribuidas en un área geográfica grande, a estos se le denominan servidores de gestión, y cada uno está en la posibilidad de gestionar directamente una sección del conjunto total de los agentes. Este tipo de arquitectura es muy usado en redes WAN (Wide Área Network – Red de Área Amplia).

Modelo OSI

El modelo OSI[27] (Open Systems Interconnection – Sistemas de Interconexión Abierto por sus siglas en ingles) abarca una serie de eventos importantes que se producen durante la comunicación entre sistemas. Proporciona las normas básicas empíricas para una serie de procesos distintos de conexión en red. Fue creado por la ISO[28] (International Organization for Standardization - Organización Internacional de Normalización o ISO por sus siglas en ingles), buscando la manera de evitar problemas durante la conexión de distintas arquitecturas de interconexión de sistemas de comunicaciones.

Comprender las distintas capas del modelo OSI no sólo permite internarse en los conjuntos de protocolos de red que actualmente se utilizan, sino que también proporciona un marco de trabajo conceptual del que puede servirse cualquiera para comprender el funcionamiento de dispositivos de red complejos, como conmutadores, puentes y *routers*. [22]

Capas del Modelo OSI

Capa física: en esta capa se realizan todas las conexiones físicas de los dispositivos, en esta entra en juego el cableado, los routers, los modem, conectores, incluso antenas, lentes y la sincronización de bit; etc.

Capa de enlace de datos: esta es donde se realiza el direccionamiento físico estableciendo la conexión a la red, se determina la topología, se realiza control de errores, control de flujo, control de acceso a medios físicos compartidos, para realizar el intercambio de datos de manera confiable.

Capa de red: esta es la capa encargada de asegurar que los datos lleguen a su destino, aunque estos no se encuentran en el mismo espacio físico, aquí entran en juego los enrutadores para determinar el camino o ruta a seguir para que los datos lleguen seguros a su destino, en este nivel actúa el firewall para evitar direcciones de maquinas y evitar archivos infectados.

Capa de transporte: se encarga de realizar el transporte de los paquetes de datos entre los dispositivos desde su enrutamiento hasta su llegada, al conjunto de datos transmitidos se les llama datagramas y es aquí donde se emplean los protocolos el TCP y el UDP, el primero es el comúnmente usado cuando existe conexión y el segundo trabaja en modo sin conexión. Esta capa posee una característica única que permite esconder imperfecciones para ofrecer datos fiables y confiables para ser transmitidos y recibidos.

Capa de sesión: en esta capa se realiza, mantiene y finaliza el enlace entre los dispositivos mientras son transmitidos los datos, de ocurrir una desconexión esta debe ser capaz de restablecerla, mediante la sincronización y recuperación de datos.

Capa de presentación: este nivel trabaja directamente con los datos transmitidos, representándolos para que puedan ser legibles para el sistema receptor, en esta capa se le da formato y significado a la información, es decir, se aplica la sintaxis y la semántica, preparando los datos para la capa de aplicación para ser utilizados por el usuario final.

Capa de aplicación: esta es la ultima capa de modelo de interconexión OSI, ofrece los llamados servicios de aplicación invocados por el usuario, cabe señalar que el usuario no interactúa directamente con esta capa, aunque ya en este nivel los datos pueden ser legibles, es necesario contar con programas de aplicación que interactúan con esta capa para presentar la información al usuario final,

algunas de estas aplicaciones suelen ser el correo electrónico, gestores de base de datos y servidores de ficheros.

Dentro de una red informática, la información es uno de los activos más importante en una institución educacional, y por lo tanto, cualquier organización debiera darle la atención y protección necesaria, ya que en ello se juega el prestigio y la confianza de sus usuarios. La información tiene tres características que deben protegerse:[3]

Confidencialidad: Muy delicada en todo tipo de organización, ya que hay datos que sólo conciernen a algunos, y que pueden ser utilizados de forma indebida por otros, o simplemente pueden afectar el prestigio de la organización si se sabe que no se les da el cuidado adecuado.

Integridad: Da la seguridad que la información no ha sido alterada ni manipulada, y por lo tanto es irrefutable y utilizable.

Disponibilidad: Apunta más a factores externos, ya que se refiere al hecho de poder acceder a la información la mayor cantidad de tiempo posible o todas las veces que se requiera, lo cual se logra con tecnologías de redes y de procesamiento (servidores).

1.2.4 Virtualización

La Virtualización es la técnica empleada sobre las características físicas de algunos recursos computacionales, para ocultarlas de otros sistemas, aplicaciones o usuarios que interactúen con ellos. Esto implica hacer que un recurso físico, como un servidor, un sistema operativo o un dispositivo de almacenamiento, aparezca como si fuera varios recursos lógicos a la vez, o que varios recursos físicos, como servidores o dispositivos de almacenamiento, aparezcan como un único recurso lógico.

Por ejemplo, la virtualización de un sistema operativo es el uso de una aplicación de software para permitir que un mismo sistema operativo maneje varias imágenes de los sistemas operativos a la misma vez.

Esta tecnología permite la separación del hardware y el software, lo cual posibilita a su vez que múltiples sistemas operativos, aplicaciones o plataformas de cómputo se ejecuten simultáneamente en un solo servidor o PC según sea el caso de aplicación. Hay varias formas de ver o catalogar la virtualización, pero en general se trata de uno de estos dos casos: virtualización de plataforma o virtualización de recursos.[29]

✚ **Virtualización de plataforma:** se trata de simular una máquina real (servidor o PC) con todos sus componentes (los cuales no necesariamente son todos los de la máquina física) y prestarle todos los recursos necesarios para su funcionamiento. En general, hay un software anfitrión que es el que controla que las diferentes máquinas virtuales sean atendidas correctamente y que está ubicado entre el hardware y las máquinas virtuales. Dentro de este esquema caben la mayoría de las formas de virtualización más conocidas, incluidas la virtualización de sistemas operativos, la virtualización de aplicaciones y la emulación de sistemas operativos. [30]

✚ **Virtualización de recursos:** esta permite agrupar varios dispositivos para que sean vistos como uno solo, o al revés, dividir un recurso en múltiples recursos independientes. Generalmente se aplica a medios de almacenamiento. También existe una forma de virtualización de recursos muy popular que no es sino las redes privadas virtuales o VPN, abstracción que permite a un PC conectarse a una red corporativa a través de la Internet como si estuviera en la misma sede física de la compañía. [30]

Ventajas de la Virtualización

- Reutilización de hardware existente (para utilizar software más moderno) y optimizar el aprovechamiento de todos los recursos de hardware.
- Rápida incorporación de nuevos recursos para los servidores virtualizados.

- Reducción de los costes de espacio y consumo necesario de forma proporcional al índice de consolidación logrado (Estimación media 10:1).
- Administración global centralizada y simplificada.
- Nos permite gestionar nuestro CPD como un pool de recursos o agrupación de toda la capacidad de procesamiento, memoria, red y almacenamiento disponible en nuestra infraestructura.
- Mejora en los procesos de clonación y copia de sistemas: Mayor facilidad para la creación de entornos de test que permiten poner en marcha nuevas aplicaciones sin impactar a la producción, agilizando el proceso de las pruebas.
- Aislamiento: un fallo general de sistema de una máquina virtual no afecta al resto de máquinas virtuales.
- Mejora de TCO⁵ y ROI⁶.
- Migración en caliente de máquinas virtuales (sin pérdida de servicio) de un servidor físico a otro, eliminando la necesidad de paradas planificadas por mantenimiento de los servidores físicos.
- Balanceo dinámico de máquinas virtuales entre los servidores físicos que componen el pool de recursos, garantizando que cada máquina virtual ejecute en el servidor físico más adecuado y proporcionando un consumo de recursos homogéneo y óptimo en toda la infraestructura.

⁵ **TCO:** Coste total de propiedad. es un método de cálculo diseñado para ayudar a los usuarios y a los gestores empresariales a determinar los costes directos e indirectos, así como los beneficios, relacionados con la compra de equipos o programas informáticos.





⁶ **ROI:** Retorno sobre la inversión. **RSI** o **ROI** de sus siglas en inglés: *Return On investment*— es una razón financiera que compara el beneficio o la utilidad obtenida en relación a la inversión realizada, vale decir, representa una herramienta para analizar el rendimiento que la empresa tiene desde el punto de vista financiero.

- Contribución al medio ambiente -Green IT- por menor consumo de energía en servidores físicos. [31]

1.2.5 Ventajas del Software Libre sobre el Software Propietario en el mundo de Monitoreo de redes Informáticas.

1.2.5.1 Definición de Software Libre

El software libre es aquel que puede ser distribuido, modificado, copiado y usado; por lo tanto, debe venir acompañado del código fuente para hacer efectivas las libertades que lo caracterizan. Dentro de software libre hay, a su vez, matices que es necesario tener en cuenta. Por ejemplo, el software de dominio público significa que no está protegido por el copyright, por lo tanto, podrían generarse versiones no libres del mismo, en cambio el software libre protegido con copyleft impide a los redistribuidores incluir algún tipo de restricción a las libertades propias del software así concebido, es decir, garantiza que las modificaciones seguirán siendo software libre. En términos del citado autor el software libre se refiere a la libertad de los usuarios para ejecutar, copiar, distribuir, estudiar, cambiar y mejorar el software. Y se refiere especialmente a cuatro clases de libertad para los usuarios de software:[32]

-  Libertad 0: la libertad para ejecutar el programa sea cual sea nuestro propósito.
-  Libertad 1: la libertad para estudiar el funcionamiento del programa y adaptarlo a tus necesidades el acceso al código fuente es condición indispensable para esto.
-  Libertad 2: la libertad para redistribuir copias y ayudar así a tu vecino.
-  Libertad 3: la libertad para mejorar el programa y luego publicarlo para el bien de toda la comunidad.

1.2.5.2 Ventajas del Software Libre

Si se analiza la descripción realizada previamente de la definición de software libre se derivan una serie de ventajas principales de este tipo de software sobre el software propietario, algunas de las cuales son muy adecuadas para el mundo de la monitorización de redes informáticas:[32]

- ✚ Al disponer del código fuente de los programas en su totalidad, éste puede ser analizado por terceras personas ajenas a sus autores en busca de fallos de diseño o de implementación. Es decir, cualquiera con los conocimientos necesarios puede realizar una auditoría del código del programa.
- ✚ La posibilidad de realizar modificaciones libremente al código fuente y distribuirlas permite que cualquiera pueda ofrecer mejoras sobre éste. Estas mejoras podrán ser nuevas funcionalidades que se incorporen al mismo o parches que corrijan problemas detectados anteriormente.
- ✚ Las características del software libre hacen que no sea lógico cargar costes sobre el software en sí (dado que se ha de distribuir sin cargo), lo que permite que este tipo de software pueda ser utilizado por organizaciones y personas con menos recursos económicos. Esto se presenta como una ventaja cuando se compara con los precios de lo que cuesta el software de monitoreo propietario hoy en día. El software libre pone en manos de cualquiera el tipo de tecnología que, hoy por hoy, sólo podían tener grandes corporaciones.
- ✚ De igual forma, la posibilidad de modificar libremente el software permite a las organizaciones que lo adapten a sus propias necesidades, pudiendo eliminar funcionalidades que no le sean de interés.

1.2.5.3 Desventajas del software propietario

Se entiende como software propietario aquél que se distribuye en forma de binarios, sin código fuente, por parte de una compañía que licencia dicho software para un uso concreto, con un coste determinado. La comparación no se hace con la nebulosa intermedia de distintos tipos de software cuyas licencias se sitúan entre ambos extremos, por ejemplo: software que se distribuye el código fuente pero no se puede modificar, software que se distribuye con limitaciones para su uso comercial, etc.

Con respecto a la monitoreo, las mismas garantías que ofrece el software libre en el mundo de la monitorización de redes informáticas son problemas que se le pueden achacar al software propietario.

Se puede hablar de las siguientes desventajas del software propietario para el usuario final [32]:

- ✚ Necesidad de confiar totalmente en el fabricante. Esto es así por cuanto éste ha implementado los algoritmos de seguridad y el usuario no puede garantizar por sí mismo que su implementación ha sido correcta y que, por ejemplo, las propiedades matemáticas necesarias para que estos algoritmos funcionen correctamente se cumplan en todas las condiciones.
- ✚ Dependencia de una tercera entidad, ya que es el fabricante del producto el único que puede ofrecer nuevas versiones de éste en caso de fallo o incluir nuevas funcionalidades que puedan ser necesarias. Esto es una desventaja debido a que el usuario no puede transferir esta dependencia a otra entidad, en caso de que el fabricante original haya traicionado su confianza (demasiados errores en la implementación, demasiado tiempo en la generación de parches para arreglar problemas graves, etc).
- ✚ Posibilidad de que existan funcionalidades no deseadas en dicho software. Dependiendo de la programación realizada, algunas funcionalidades podrán ser activadas o desactivadas por el usuario, pero pueden existir también funcionalidades que no se puedan desactivar o que, incluso, no se encuentren documentadas. Llevándolo al extremo se

podría hablar de “puertas traseras” abiertas por el fabricante del software que, después de todo, es un agente comercial y, por tanto, tiene sus propios intereses que pueden ser contrarios a los de la compañía que instala un software de monitoreo específico.

- ✚ Desconocimiento del código por parte del usuario. Esto puede llevar a que el fabricante pueda llegar a tener una falsa sensación de monitoreo por oscuridad, es decir, las vulnerabilidades de su producto no tienen por qué ser conocidas porque nadie tiene acceso a las “tripas” del mismo. De igual forma, esto puede llevar a que el fabricante no tenga interés en desarrollar el código de una forma adecuada porque, al fin y al cabo, el usuario no va a ver dicho código ni evaluar la calidad de su implementación.

Cabe hacer notar que, algunos fabricantes de software, observando las ventajas del modelo Open Source ofrecen, con restricciones o sin ellas, copias del código fuente a terceras entidades interesadas. Tal es el caso, por ejemplo, de fabricantes de sistemas operativos como Sun Microsystems y Microsoft y de fabricantes de productos de monitoreo como IMB.

Independientemente del ritmo de crecimiento del software, del lado del monitoreo, las ventajas ofrecidas por el software libre son evidentes frente a las alternativas propietarias. Máxime en determinados entornos en los que una persona no se puede confiar de aquella compañía que le vende la solución o no puede depender de la seguridad “garantizada” por un determinado producto que no tiene forma de demostrar. Por tanto, si bien el software libre en la actualidad tiene una cobertura desigual de las distintas necesidades del monitoreo de una empresa o corporación, éste es, definitivamente, una apuesta de presente y futuro provechosa en aquellas áreas aún no desarrolladas y una oportunidad real e inmediata en las demás áreas para utilizar soluciones equivalentes a las propietarias con [3]:

- ✚ Un menor coste.
- ✚ Unas mayores garantías de seguridad, debido a la posibilidad de auditar el código en uso.

- ✚ Una mayor flexibilidad en la adaptación e integración, gracias a la posibilidad de modificar dicho código.
- ✚ La posibilidad del mantenimiento asegurado de una solución de seguridad con independencia del origen del producto en sí.

1.2.6 Servidores de Monitoreo. Soluciones de Código Abierto (OpenSource).

Para darle continuidad a la propuesta de solución analizaremos las herramientas o software más populares y utilizados que existen en la actualidad donde todos ellos tienen en común un objetivo: la gestión y monitorización de redes, pero la llevan a cabo por diferentes caminos y de forma diferente.

1.2.6.1 Pandora FMS



Es una herramienta de software libre OpenSource (código abierto) con licencia GPL versión 2 (GNU Public License), la cual está orientada a proteger la libre distribución y modificación de software libre. El proyecto comenzó en 2004 cuando se publicó la primera versión estable 1.0 con el nombre de 'Pandoramon'. Está desarrollado y mantenido actualmente por la empresa Ártica Soluciones Tecnológicas con base en Madrid. [33]

Esta aplicación de monitorización sirve para vigilar y analizar de forma visual todo tipo de sistemas y aplicaciones, utilizando una interfaz o entorno web a través de nuestro navegador. Es una herramienta modular y flexible y está orientada a datos. Puede supervisar todo tipo de parámetros o servicios, Sistemas Operativos mediante agentes específicos que recolectan información, incluso hasta sensores (por ejemplo: humedad, luminosidad, movimiento), electrónica de red, etc.

Pandora FMS puede detectar si una interfaz de red se ha caído, un ataque de "defacement" en una web, una pérdida de memoria en algún servidor de

aplicaciones, o el movimiento de un valor del NASDAQ⁷. Pandora FMS puede enviar SMS si un sistema falla o cuando las acciones de Google bajan de 500 dólares.

Pandora FMS puede recoger información de cualquier sistema operativo, con agentes, específicos para cada plataforma, que recolectan datos y los envían al servidor. Hay agentes específicos para GNU/Linux, AIX, Solaris, HP-UX, BSD/IPSO y Windows 2000, XP, 7, 2003 y 2008.

También puede monitorizar cualquier tipo de servicio TCP/IP, sin necesidad de instalar agentes, y monitorizar sistemas de red como balanceadores de carga, routers, switches, sistemas operativos, aplicaciones o impresoras si se necesita hacerlo de forma remota. Pandora FMS también soporta WMI para comunicarse directamente con sistemas Windows de forma remota y SNMP para recolectar datos.

Algunos ejemplos de recursos comunes que pueden ser monitorizados con Pandora FMS son, la carga del procesador, el uso de disco y memoria, procesos que están corriendo en el sistema, eventos determinados en un log, factores ambientales como la temperatura, la luz o la humedad, valores de aplicaciones como determinados textos en una página web, y en general cualquier cosa que se pueda recolectar de forma automatizada. [34]

1.2.6.2 Zabbix



Zabbix fue iniciado como un proyecto interno de software en 1998. Luego de 3 años, en 2001, este fue lanzado al público sobre GPL. Y tomo 3 años más hasta su primera versión estable, 1.0, que fue lanzada en 2004.

⁷ **NASDAQ** (National Association of Securities Dealers Automated Quotation) es la bolsa de valores electrónica y automatizada más grande de los Estados Unidos, con más de 3.800 compañías y corporaciones.

Zabbix es un Sistema de Monitoreo de Redes creado por Alexei Vladishev. Está diseñado para monitorear y registrar el estado de varios servicios de red, Servidores, y hardware de red.

Usa MySQL, PostgreSQL, SQLite, Oracle o IBM DB2 como base de datos. Su backend está escrito en C y el frontend web está escrito en PHP. Zabbix ofrece varias opciones de monitoreo. Chequeos simples que pueden verificar la disponibilidad y el nivel de respuesta de servicios estándar como SMTP o HTTP sin necesidad de instalar ningún software sobre el host monitoreado. Un agente Zabbix puede también ser instalado sobre máquinas UNIX y Windows para monitorear estadísticas como carga de CPU, utilización de red, espacio en disco, etc. Como alternativa a instalar el agente sobre los host, Zabbix incluye soporte para monitorizar vía protocolos SNMP, TCP y ICMP, como también sobre IPMI, JMX, SSH, telnet y usando parámetros de configuración personalizados. [35]

En resumen, ofrece un control centralizado, disponibilidad de hasta 1000 nodos, multiplataforma de soporte en clientes y eficiente para Linux y Win32, autenticación de usuarios segura, sistema de notificaciones flexible para e-mail o SMS basado en cualquier evento, incluido también XMPP (Protocolo extensible de mensajería y comunicación de presencia) (anteriormente llamado Jabber), que se pone en funcionamiento tanto cuando ocurre un problema como cuando se resuelve. [33]

1.2.6.3 Zenoss



Otra plataforma de gestión de red y servidores OpenSource es Zenoss Core Versión el proyecto de creación de Zenoss comenzó en 2005 y fue iniciado por Erik Dahl y Bill Karpovich, los cuales formaron la compañía Zenoss, Inc. Esta empresa es patrocinadora del núcleo Zenoss y proporciona apoyo, mantenimiento y desarrollo de productos. Destacan que es una empresa donde tienen el código y el control de la evolución del mismo y también su indemnización, a diferencias de otras empresas como puede ser el caso de Hyperic, que viene de un fondo comercial y hace que una parte de su código sea OpenSource. Es un producto licenciado

bajo la GNU General Public License Versión 2.0 y publicada por la Free Software Foundation.

Zenoss Core es un producto de vigilancia y seguimiento para una red informática y de supervisión de infraestructuras IT. Puede gestionar la configuración, salud, rendimiento de dispositivos, servidores y aplicaciones. Todo esto a través de un único paquete de integrado de software. Ofrece monitorización de dispositivos y servicios en la red (SNMP, HTTP, POP3, etc.), recursos hardware y detecta automáticamente nuevos recursos en la red y cambios en su configuración. Realiza notificaciones y alertas basados en un conjunto de reglas. Es un producto multiplataforma para soporte en clientes, incluyendo:

- Windows Server (2000, 2003, 2008), XP, Vista, 7.
- GNU/Linux.
- Tomcat y servidores Java/JMX.

Para ser instalado como servidor soporta distribuciones:

- Linux:
 - ✓ Red Hat Enterprise Linux
 - ✓ CentOS
 - ✓ Fedora Core
 - ✓ Debian
 - ✓ Ubuntu Server
 - ✓ OpenSUSE
- Mac OS X v10.5 y v10.6
- Windows (Requiere VMWare Player y la aplicación virtual Zenoss)

Para la consola o interfaz web necesita:

- Firefox 3.6.x, 4, 5 o Internet Explorer 7, 8, 9. O superiores
- Adobe Flash Player. Actualizados

1.2.6.4 Cacti



Actualmente, la comunidad de dicho producto está trabajando en la elaboración de dos nuevas versiones 1.0.0 y 1.1.0 con

mejoras planificadas como por ejemplo: mejora de la interfaz web 2.0 basado en AJAX, plugins integrados en el núcleo de la aplicación, grupos de usuarios y permisos, etc. Está publicada bajo la licencia GPL (GNU Public Licenced).

No dispone de una versión comercial ni otra licencia privativa para la distribución del producto, tampoco de un soporte comercial o profesional. Pone a disposición un soporte gratuito mantenida por la comunidad mediante una lista de correo y un foro.

Es una aplicación enfocada para la generación de gráficos avanzados y diseñada para aprovechar el poder de almacenamiento y la funcionalidad que poseen las aplicaciones RRDtool⁸. Sirve para monitorizar redes en LAN de un tamaño pequeño o redes más amplias de hasta cientos de dispositivos. La recolección de datos en los dispositivos a monitorizar se realiza mediante el protocolo SNMP y se almacenan en la RRD (base de datos Round Robin) y luego genera gráficos en formato PNG. También puede recolectar los datos mediante scripts para consultas en XML ejecutados desde el cron de forma periódica en el caso de Linux, por ejemplo, para función de realizar ping a un host. Pueden generarse plantillas para determinados dispositivos tales como router, switch o servidores y también para gráficas, con el propósito de generalizar la monitorización de dispositivos similares, pudiendo exportarlas e importarlas posteriormente en otros equipos.

Funciona bajo una base de datos MySQL versión 4.1.x, 5.x o superior. Además, entre sus requisitos necesita PHP 4.3.6 o superior y un servidor web como Apache o IIS⁹. La versión de RRDtool 1.0.49 o 1.2.x o superior, teniendo

⁸ **RRDtool:** Es el acrónimo de *Round Robin Database Tool*. Herramienta que trabaja con una base de datos que maneja planificación. Su finalidad principal es el tratamiento de datos temporales y datos seriales como temperaturas, transferencias en redes, cargas del procesador, etc.

⁹ **IIS:** Internet Information Services, Servicios de Información de Internet por sus siglas en ingles. IIS es un servidor web.

en cuenta de que existen problemas en la versión 1.2.28 en la representación de texto y leyendas en los gráficos.

Tiene una interfaz web de usuario personalizable y desarrollada en PHP que permite el acceso mediante usuarios con diferentes privilegios, para darle permisos sobre ciertas áreas de Cacti.

1.2.6.5 Nagios



El principal software libre orientado a la monitorización y la posible solución para la administración de dispositivos de redes es desde hace mucho tiempo Nagios Core Versión 3.x. Es una herramienta Open Source y está diseñado y mantenido por Ethan Galstad, autor de dicho software, junto con un grupo de desarrolladores que mantienen varios plugins. Según su propio autor, el significado de su nombre, N.A.G.I.O.S es un acrónimo recursivo: “Nagios Ain’t Gonna Insist On Sainthood”. Es una referencia a la encarnación original del software bajo el nombre de Netsaint.

Está licenciado bajo la GNU General Public License Versión 2 publicada por Free Software Foundation. También posee una licencia comercial Nagios Powered™ la cual pone a disposición de sus clientes dos software: Nagios XI y OpMon. El primero de ellos, se puede obtener basándose en el volumen de nuestro sistema: entre 1 a 8 nodos o para nodos ilimitados, y representa la versión de Nagios comercial. El segundo, es una solución de gobierno IT y gestión de procesos empresariales y es compatible con Nagios.

En cuanto a su arquitectura y definición, es un sistema de monitorización monolítico y orientado a eventos que vigila los equipos, tanto su hardware como software, alertando cuando el comportamiento de los mismos no es el adecuado. Puede monitorizar servicios de red, recursos hosts y puede programar plugins específicos para nuevos sistemas. El control remoto es manejado a través de túneles SSH o SSL cifrado. Fue diseñado para sistemas GNU/Linux pero también funciona en variantes Unix.

Está basado en una estructura maestro-esclavo donde el maestro es el servidor dedicado para Nagios y los esclavos las máquinas a monitorizar.

En cada uno de los esclavos o clientes a monitorizar se configuran los plugins o scripts que serán ejecutados para chequear un determinado servicio. Dichos scripts pueden estar desarrollados en diferentes lenguajes o tecnologías: Perl, C/C++/C#, Expect/TCL, Bash, Ruby, Python, o PHP. Aunque Nagios posee opcionalmente un intérprete embebido de Perl que acelera la ejecución de estos scripts.

En el maestro se ejecuta una herramienta de conexión remota, la más habitual es el demonio NRPE, con la cual el servidor accede a los plugins o scripts de medición disponibles y configurados en las máquinas remotas o esclavos.

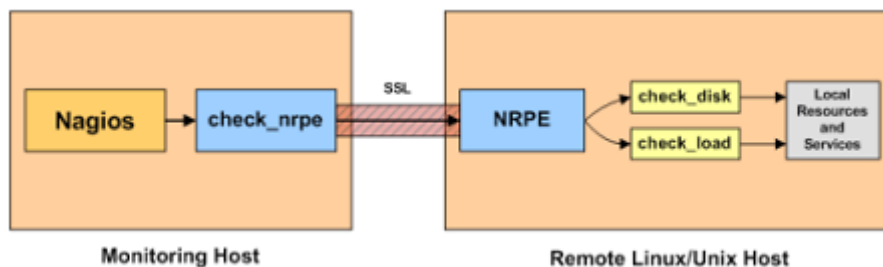


Figura 2. Esquema de ejecución entre maestro-esclavo.

- ✓ Supervisión de los servicios red (SMTP, POP3, HTTP, NNTP, PING, etc.).
- ✓ Monitorización de los recursos (carga de procesador, espacio en disco, etc.).
- ✓ Capacidad para definir una jerarquía de servidores en la red, lo que permite la detección de hosts 'down' o inalcanzables.
- ✓ Notificación de errores cuando existen problemas y cuando son resueltos mediante correo electrónico, SMS, etc.
- ✓ Interfaz web para visualizar el estado actual de la red con la posibilidad de generar informes y gráficas.

Su interfaz web nos permite la visualización de los servidores y el estado de los servicios. Podemos organizar las máquinas o esclavos monitorizados, si

realizamos la configuración oportuna, por Grupos y por Servicios. Para el primero, por ejemplo, si pertenecen a una misma familia o estación. Mientras que para el segundo, agruparlos referente a un servicio determinado, por ejemplo, para aplicaciones web el servicio HTTP.

Posee la integración de diferentes CGIs (Computer-generated imagery) que son imágenes o gráficos generados por ordenador mediante escenas estáticas o dinámicas. También utiliza la herramienta RRDtool (Round Robin Database Tool) que es una herramienta que trabaja con una base de datos para la creación de gráficas, cuyo funcionamiento es ir actualizando los valores y sobrescribiendo los antiguos, los cuales se conservan como un historial. Su finalidad principal es el tratamiento de datos temporales y datos seriales como temperaturas, transferencias en redes, cargas del procesador, etc.

Entre sus principales ventajas se encuentran:

- Es un software popularmente conocido y consolidado, ya que posee una gran cantidad de plugins de la comunidad (más de 200) para extender sus funcionalidades a través de innumerables sitios webs, que incluso son facilitados en su manual oficial. Aunque, hay etapas de su historia en la que dicha comunidad ha estado poco activa en cuanto al desarrollo de nuevos avances sobre el producto.
- Su fama ha incentivado nuevas herramientas de monitorización que contienen un núcleo basado en Nagios, como por ejemplo: Opsview o Shinkem.
- Existe buena documentación muy trabajada incluso en detalles y facilitada por la comunidad.
- Permite diferenciar entre hosts caídos o inaccesibles.
- Posee un comando que chequea y valida los ficheros de texto de configuración modificados antes de reiniciar el sistema.





Puede acoplarse con otra aplicación llamada Centreon para la gestión y control de cualquier aspecto de la herramienta desde una interfaz web, evitando las

modificaciones sobre ficheros y por línea de comandos. Aunque esta aplicación sólo funciona con todas las funcionalidades (reportes y statusmap) de Nagios en Ubuntu 9.04 o superior y conlleva una configuración y un tiempo extra para la puesta en marcha.

1.2.7 Análisis de la selección del software de monitoreo.

Para la elección de Nagios como software de monitoreo en el presente trabajo de diploma se tuvo que realizar un análisis estableciendo parámetros técnicos que se detallaran a continuación en el cuadro siguiente, con el fin de poder definir el software con las mejores características y que se adecue a las características de hardware con que cuenta en nodo central.

Defino una escala donde:

-  Muy buena: **5**
-  Buena: **3**
-  Regular: **1**
-  No Soporta: **0**

Descripción	Pandora	Zabbix	Cacti	Zenoss	Nagios
Interfaz Web	5	5	3	5	3
Alertas y Notificaciones	5	5	0	5	5
Basta información en la red	5	3	3	5	5
Plugins Flexibles	3	3	3	3	5
Escalable y Robusto	5	3	3	3	5
Complejidad en instalación y configuración	1	1	1	1	1
Graficas y estadísticas	5	5	5	5	5
Capaz de crear reportes	5	3	3	3	5
Autenticación de usuarios	5	5	5	5	5
Usados para redes locales	3	3	3	3	3
Usados para redes empresariales	3	3	0	5	5
Licencia libre	5	5	5	5	5
Versatilidad	3	3	3	3	5
Potencia	3	3	3	5	5
Fácil de usar	3	3	3	5	3
Monitoreo de entornos críticos	0	3	0	3	5
Monitoreo en tiempo real	0	5	3	3	5
Correlación y análisis de <i>logs</i> o eventos	0	3	3	5	5
Disponibilidad y Rendimiento	3	3	3	3	5

Tabla 1. Análisis de la selección del software de monitoreo.

Como se puede ilustrar en la tabla anterior Nagios cumple con todas las características y funcionalidades a desarrollarse a nuestro entorno de trabajo.

Gracias a un estudio del arte de todas las posibles herramientas de monitoreo de servicios de redes basadas en software libre se pudieron encontrar Trabajos de Diploma como “Análisis del Rendimiento de Sistemas VoIP bajo Condiciones de Red Variable”[36], “Diseño e Implementación de un Sistema de Monitoreo y Control Basado en Software Libre para la Red de Telecomunicaciones de la Dirección de Informática y Sistemas de la Gobernatura del Estado Bolívar”[7] entre otros, que permitió declarar estas descripciones antes mencionadas.

Cabe resaltar que dicha herramienta también carece de algunas funcionalidades importantes pero al ser una herramienta en constante desarrollo pues va cubriendo esas irregularidades que desde sus inicios en el 2004 traían consigo, no se puede afirmar que hay alguna herramienta que cumpla con todas las características para monitorear una red informática, cada día más hay algo nuevo que conocer en las redes y un equipo de desarrollo no para su proyecto para actualizar alguna vulnerabilidad que traiga su software sino que sacan una versión estable o empresarial para así ganar más.

1.3 Conclusiones de capítulo

Tras un análisis de los diferentes servicios prestados en el Nodo Central de la RED Uho y las necesidades de monitoreo que el mismo tiene, después de estudiadas las nuevas tendencias, se llega a la siguiente conclusión:

- Los mecanismos de monitorización hospedados actualmente para el control de los servicios que transita por la red en el Nodo Central de la Uho no satisfacen las necesidades que se tiene, corroborando a la necesidad de contar con técnicas adecuada para dicha tarea sobre la base de los fundamentos teóricos planteados en este capítulo.
- El uso de las Herramientas de Monitoreo de Código Abierto, y en especial Nagios instalado en una máquina dedicada, basado en

tecnología de Código Abierto, implementado en la red como servidor, maestro-esclavo en el Nodo Central donde se encontrarán ubicados los principales servidores y servicios, constituyen una alternativa eficiente y sostenible para la protección y monitoreo de los servicios y equipos de la red de datos Uho.

Capítulo

2

2 Descripción y Resultados de la propuesta

La configuración de la solución propuesta, su comprensión en todos los aspectos así como la evaluación de los resultados obtenidos una vez implantados son la esencia fundamental del presente capítulo.

2.1 Implementación en el nodo central del software de monitoreo Nagios

El Nodo Central de la Uho tiene entre sus particularidades la tarea de prestar a los usuarios del centro los principales servicios de red, de ahí que el uso de sistemas basados en Código Abierto (Open Source) le dan respuestas a las políticas trazados por el país al hacer uso y publicación de las mismas para poner en marcha tales servicios como el correo electrónico.

Nagios es un estable servidor de monitoreo basado en código abierto que posee formidables características como hemos visto en el capítulo anterior, la elección de este software nos permitirá conocer en tiempo real lo que está pasando con los servicios y equipos del nodo central Uho. Para su implementación se hace necesario describir cada protocolo de red, y en caso de un equipo (hardware) saber su ubicación real y que deseamos saber de dicho equipo. Para ejecutar tales pasos necesitaremos crear una maquina

virtual dedicada solamente para el servidor Nagios y luego instalar dicho servidor en cualquiera de sus formas.

A continuación describiremos los parámetros a monitorear, crearemos la maquina virtual con la Plataforma de Virtualización Promox VE e instalar Nagios.

2.1.1 Parámetros a Monitorear con Nagios

Los parámetros de monitoreo en el actual trabajo de diploma han sido seleccionados para monitorear el rendimiento de los servicios que se brindan en el nodo central Uho así como los recursos utilizados y eventos en ocurrencia.

2.1.1.1 Descripción del servicio de correo electrónico mediante (Postfix Dovecot)

El servicio de correo que brinda el nodo central para todos los usuarios de la red Uho esta implementado por medio de un software basado en software libre llamado Postfix Dovecot. Postfix es un potente servidor de correo, programa informático dedicado al enrutamiento y envío de correo electrónico, creado con la intención de que sea una alternativa más rápida, fácil de administrar y segura al ampliamente utilizado Sendmail.[8]

2.1.1.1.1 Información Cuantitativa y Cualitativa del servidor de correo

Se cuenta con un Servidor Central dedicado solamente a la transferencia de los mensajes por medio del agente *MTA Postfix*, Agente de Transferencia de Correo (del inglés *Mail Transport Agent* o *MTA*; también *Message Transport Agent*, Agente de Transporte de Mensajes) es uno de los programas que ejecutan los servidores de correo, y tiene como fin transferir un conjunto de datos de una computadora a otra [8], se cuenta con un balanceador solamente dedicado a su función para entregar de forma balanceada a otros tres servidores dedicados al recibo y envío de los mensajes, los mismo cuentan con una configuración más profunda.

Nota: Todos los servicios del nodo central están virtualizados, las características del hardware expuestas son las que presenta la maquina física.

Servidor Central con IP: **10.26.0.1**

➤ Hardware

- ❖ Intel(R) Core(TM) i3-2120 CPU 3.30GHz, 3292 MHz
- ❖ Memoria RAM de 4 GB
- ❖ Disco Duro de 1 TB
- ❖ Adaptador de red **Realtek** y 1 **TP-Link**
- ❖ Nombre del motherboard **Pegatron** IPMSB-H61

➤ Software

- ❖ Debian GNU/Linux 6.0.7 (squeeze)
- ❖ Soporte para Apache, php, gcc compiler, GD development libraries
- ❖ MTA Postfix Dovecot

Servidor de correo “BalanceadorUho” con IP: **10.26.0.75**

➤ Hardware

- ❖ Dell Poweredge 1800 Dual Xeon a 3Ghz 800FSB
- ❖ Memoria RAM 2gb ECC DDR2 (800mhz)
- ❖ 1 Disco Duro Sata de 250 GB
- ❖ Adaptador de red Ethernet Gigabit
- ❖ Nombre del motherboard Dell PowerEdge

➤ Software

- ❖ Debian GNU/Linux 6.0.7 (squeeze)
- ❖ Soporte para Apache, php, gcc compiler, GD development libraries
- ❖ MTA Postfix Dovecot

Servidor de correo “ServerEmail_1” con IP: **10.26.2.1**

➤ Hardware

- ❖ Altos g540 xeon qc e5405 2. 0ghz
- ❖ Velocidad de reloj a 2000 MHz

- ❖ Unidad de dispositivo, velocidad de transferencia a 3000 MB/s
- ❖ Características de red-Dual 10/100/1000 Ethernet
- ❖ 1TB Disco Duro Serial ATA II
- ❖ Memoria interna 2048 MB
- Software
 - ❖ Debian GNU/Linux 6.0.7 (squeeze)
 - ❖ Apache2 y sus dependencias
 - ❖ Postfix Dovecot
 - ❖ Dependencias del Postfix , Imap, Pop3, SNMP, SMTP

Servidor de correo “ServerEmail_2” con IP: **10.26.2.4**

- Hardware
 - ❖ Dell Poweredge 1800 Dual Xeon a 3Ghz 800FSB
 - ❖ Memoria RAM 2gb ECC DDR2 (800mhz)
 - ❖ 1 Disco Duro Sata de 250 GB
 - ❖ Adaptador de red Ethernet Gigabit
 - ❖ Nombre del motherboard Dell PowerEdge
- Software
 - ❖ Debian GNU/Linux 6.0.7 (squeeze)
 - ❖ Apache2 y sus dependencias
 - ❖ Postfix Dovecot
 - ❖ Dependencias del Postfix , Imap, Pop3, SNMP, SMTP

Servicio de correo “ServerEmail_3” con IP: **10.26.2.9**

- Hardware
 - ❖ Dell Poweredge 1800 Dual Xeon a 3Ghz 800FSB
 - ❖ Memoria RAM 2gb ECC DDR2 (800mhz)
 - ❖ 1 Disco Duro Sata de 250 GB
 - ❖ Adaptador de red Ethernet Gigabit
 - ❖ Nombre del motherboard Dell PowerEdge
- Software
 - ❖ Debian GNU/Linux 6.0.7 (squeeze)
 - ❖ Apache2 y sus dependencias
 - ❖ Postfix Dovecot

- ❖ Dependencias del Postfix , Imap, Pop3, SNMP, SMTP

2.1.1.1.2 Caso 1. Comprobación del servicio

Estos parámetros fueron consultados con los administradores del nodo central de la red Uho a la hora de ser redactado este documento.

A monitorear:

- ❖ Estado del servicio SMTP
- ❖ Estado ping
- ❖ Estado CPU
- ❖ Estado memoria física
- ❖ Estado memoria virtual
- ❖ Estado servicio IMAP
- ❖ Estado servicio POP3
- ❖ Estado de los procesos

2.1.1.2 Descripción del servicio web mediante (Apache)

El servicio web que se brinda a todos los usuarios de la red Uho esta implementado por medio de un software basado en código abierto llamado Apache. Apache[37] es un servidor HTTP más conocido hoy en día a nivel mundial es utilizado por muchas entidades por las características que presenta entre ellas permitir la autenticación de usuarios sobre bases de datos y negocio de contenido.

2.1.1.2.1 Información Cuantitativa y Cualitativa del servicio web

Se cuenta con un servidor central y único, en él se hospeda el software Apache2 implementando HTTP y HTTPS lo que nos permite acceder de forma segura a estos protocolos utilizados para direcciones web o las llamadas URL.

🚦 Servidor web “ServerWebUho” con IP: **10.26.0.73**

➤ Hardware

- ❖ Dell Poweredge 1800 Dual Xeon a 3Ghz 800FSB
- ❖ Memoria RAM 2gb ECC DDR2 (800mhz)

- ❖ 2 Disco Duro Sata de 250 GB
- ❖ Adaptador de red Ethernet Gigabit
- ❖ Nombre del motherboard Dell PowerEdge

➤ Software

- ❖ Debian GNU/Linux 6.0.7 (squeeze)
- ❖ Apache2 y todas sus dependencias
- ❖ Firewall

2.1.1.2.2 Caso 2. Comprobación del servicio web

Estos parámetros fueron consultados con los administradores del nodo central de la red Uho a la hora de ser redactado este documento.

A monitorear:

- ❖ Estado servicio HTTP y HTTPS
- ❖ Estado del seguimiento de redirecciones
- ❖ Estado ping
- ❖ Estado Procesos

2.1.1.3 Descripción del servicio de acceso remoto mediante (FreeRADIUS)

Catalogado como unos de los servicios más importantes por los usuarios de la red Uho, el servicio de acceso remoto está siendo implementado por medio de un software basado en código abierto, permitiéndoles así a los administradores hacer un buen uso del mismo, este software presenta potentes herramientas en cuestiones de seguridad y autenticación.

2.1.1.3.1 Información Cuantitativa y Cualitativa del servicio acceso remoto

Se cuenta con un servidor virtual dedicado solamente a esta función por medio del software FreeRADIUS, también consta de pequeños paquetes como librerías y lenguajes de escritura, dependencias que se necesitan para que el software realice de forma satisfactoria su función, es válido recordar que el FreeRADIUS es utilizado para la autenticación de los usuarios desde sus casa hacia la Uho.

✚ Servidor web “ServerWebUho” con IP: 10.26.0.0

➤ Hardware

- ❖ Dell Poweredge 1800 Dual Xeon a 3Ghz 800FSB
- ❖ Memoria RAM 2gb ECC DDR2 (800mhz)
- ❖ 2 Disco Duro Sata de 250 GB
- ❖ Adaptador de red Ethernet Gigabit
- ❖ Nombre del motherboard Dell PowerEdge

➤ Software

- ❖ Debian GNU/Linux 6.0.7 (squeeze)
- ❖ FreeRADIUS
- ❖ Firewall

2.1.1.3.2 Caso 3. Comprobación del servicio acceso remoto

Estos parámetros fueron consultados con los administradores del nodo central de la red Uho a la hora de ser redactado este documento.

A monitorear:

- ❖ Estado ping
- ❖ Estado de conexión al Radius
- ❖ Estado procesos

2.1.1.4 Descripción del servicio de FTP mediante (ProFTPD)

El servicio de transferencia de ficheros conocido como FTP que brinda el nodo central para todos los usuarios de la red Uho esta implementado por medio de un software basado en código abierto llamado ProFTPD en su versión 1.3.3. Reconocido servidor que alberga disimiles de características tales como la autenticación parámetro declarado por el admin, y reglas de seguridad para aquellos intrusos que deseen publicar información subversiva en el mismo.

2.1.1.4.1 Información Cuantitativa y Cualitativa del servicio FTP

Se cuenta con un servidor virtual donde se encuentra instalado y en perfecto funcionamiento este servicio. Además se cuenta con una serie de paquetes previamente instalados para resolver cuestiones de seguridad en dicho

servidor. Es importante resaltar que existen en la Uho otros servidores FTP dedicados cada uno a una especialidad en específico llámese FACII, FH, FACE, FACING.

✚ Servidor web “ServerWebUho” con IP: 10.26.0.130

➤ Hardware

- ❖ Dell Poweredge 1800 Dual Xeon a 3Ghz 800FSB
- ❖ Memoria RAM 2gb ECC DDR2 (800mhz)
- ❖ 1TB Disco Duro Serial ATA II
- ❖ Adaptador de red Ethernet Gigabit
- ❖ Nombre del motherboard Dell PowerEdge

➤ Software

- ❖ Debian GNU/Linux 6.0.7 (squeeze)
- ❖ ProFTPD
- ❖ Firewall
- ❖ Apache2 y dependencias

2.1.1.4.2 Caso 4. Comprobación del servicio FTP

A monitorear:

- ❖ Estado FTP
- ❖ Estado CPU
- ❖ Estado ping
- ❖ Espacio en disco

2.1.1.5 Descripción del servicio de DNS mediante (Bind9)

El servicio de nombre de dominios DNS o del inglés *Domain Name System* que brinda el nodo central para todos los usuarios de la red Uho esta implementado por medio de un software basado en código abierto llamado Bind9 en su versión 9.7.3. Reconocido servidor que alberga disimiles de características tales como la resolución de nombres de dominios permitiendo este una mejor navegación para los usuarios de la red, debido que muchos no tienen

conocimiento sobre los nombre de los sitios web que desean alcanzar con solo saber la IP del mismo podrán tener una búsqueda satisfactoria.

2.1.1.5.1 Información Cuantitativa y Cualitativa del servicio DNS

Se cuenta con dos servidores centrales virtuales donde se encuentra instalado y en perfecto funcionamiento este servicio. Además se cuenta con una serie de paquetes previamente instalados para resolver cuestiones de seguridad en dicho servidor y otro servidor DNS ubicado en la sede Celia Sánchez Manduley permitiendo este resolver las direcciones que se hospedan en la Oscar Lucero y demás instituciones del MES.

✚ Servidor DNS “ServerDNS_1” con IP: 10.26.0.52

➤ Hardware

- ❖ Intel(R) Core(TM) i3-2120 CPU 3.30GHz, 3292 MHz
- ❖ Memoria RAM de 4 GB
- ❖ Disco Duro de 1 TB
- ❖ Adaptador de red **Realtek** y 1 **TP-Link**
- ❖ Nombre del motherboard **Pegatron IPMSB-H61**

➤ Software

- ❖ Debian GNU/Linux 6.0.7 (squeeze)
- ❖ Bind9
- ❖ Firewall
- ❖ Paquetes de dependencias del DNS

✚ Servidor DNS “ServerDNS_2” con IP: 10.26.0.1

➤ Hardware

- ❖ Intel(R) Core(TM) i3-2120 CPU 3.30GHz, 3292 MHz
- ❖ Memoria RAM de 4 GB
- ❖ Disco Duro de 1 TB
- ❖ Adaptador de red **Realtek** y 1 **TP-Link**
- ❖ Nombre del motherboard **Pegatron IPMSB-H61**

➤ Software

- ❖ Debian GNU/Linux 6.0.7 (squeeze)
- ❖ Bind9
- ❖ Firewall
- ❖ Paquetes de dependencias del DNS

2.1.1.5.2 Caso 5. Comprobación del servicio DNS

Estos parámetros fueron consultados con los administradores del nodo central de la red Uho a la hora de ser redactado este documento.

A monitorear:

- ❖ Estado Total Procesos
- ❖ Estado servicio DNS
- ❖ Tiempo de respuesta DIG
- ❖ Estado servicio PING

2.2 Instalación del servidor de monitoreo Nagios

Para la instalación de Nagios en la distribución de Gnu/Linux distro Debian en su versión 6 se ha establecido un procedimiento el cual fue diseñado paso a paso durante desarrollo del trabajo de diploma.

Características de la plataforma de Virtualización y del Servidor Nagios:

🌐 Plataforma Virtual:

➤ Hardware

- ❖ Dell Poweredge 1800 Dual Xeon a 3Ghz 800FSB
- ❖ Memoria RAM 2gb ECC DDR2 (800mhz)
- ❖ 1TB Disco Duro Serial ATA II
- ❖ Adaptador de red Ethernet Gigabit
- ❖ Nombre del motherboard Dell PowerEdge

➤ Software

- ❖ Apache2 y sus dependencias
- ❖ Plataforma (Promox VE)
- ❖ Firewall

Servidor Nagios

➤ Hardware

- ❖ Dell Poweredge 1800 Dual Xeon a 3Ghz 800FSB
- ❖ Memoria RAM 2gb ECC DDR2 (800mhz)
- ❖ 1TB Disco Duro Serial ATA II
- ❖ Adaptador de red Ethernet Gigabit
- ❖ Nombre del motherboard Dell PowerEdge

➤ Software

- ❖ Apache2 y dependencias
- ❖ Server Nagios v3.2.1
- ❖ PHP5
- ❖ Herramientas RRDtool
- ❖ Perl y dependencias

2.2.1 Procedimiento de instalación Nagios

1. Instalación de un servidor web. (en mi caso Apache2)
2. Instalación de librerías y compiladores (imágenes, lenguajes de scripts)
3. Creamos grupos y usuarios para nagios
4. Instalamos Nagios
5. Configurar la interfaz web (dándole permisos con Apache2)
6. Iniciar Nagios y Apache2

Para información más detallada de cada uno de estos pasos ver el **anexo 1**. Para ingresar a la interfaz Web de Nagios lo hacemos desde nuestro navegador web predeterminado con la siguiente dirección *http://ip_server/nagios3* donde nos pedirá un usuario y contraseña y aquí pondremos los que hemos definido durante la instalación de la interfaz Web, en mi caso sería *nagiosadmin nagios*.

Ya tengo a Nagios hospedado como un servidor de monitoreo, por ahora todo lo tiene por default, Teniendo en cuenta que más adelante necesitare de alguna herramienta que me permita visualizar los datos obtenidos por nagios para

interpretados por graficas para ver el comportamiento de los parámetros seleccionados hago uso de la herramienta NagiosGrapher capaz de interpretar los datos que Nagios genera. Importante resaltar que nagios también grafica pero no trae consigo alguna opción que permita exportar sus graficas a algún tipo de extensión como PNP, PDF. Cuestión que con NagiosGrapher se solucionara.

2.2.2 Instalación de la Herramienta NagiosGrapher.

Lo primero que debemos de hacer es ver si lo tenemos en nuestro repositorio para no tener que descargarlo de otras fuentes como Internet, hacemos un ***aptitude search nagiosgrapher*** y nos devuelve:

```
root@control:~# aptitude search nagiosgrapher
pB nagiosgrapher          - Charting add-on for Nagios
```

Luego realizar algunos cambios en nagios para que el addons comience a generar las graficas. Para ver la instalación completa del addons ver el **anexo 2** donde se explica cada pasó.

2.3 Resultados obtenidos con Nagios

Se expondrán los diferentes resultados obtenidos con la implementación de Nagios en el Nodo Central de la Red Uho, es importante resaltar que las comprobaciones que se muestran a continuación fueron consultadas por los administradores del nodo y aquí solo se exponen las que se consideraron más importante teniendo en cuenta la prioridad que le dan los usuarios a los servicios que se prestan en nuestra entidad.

Cabe mencionar que cada servicio tiene su particularidad que lo hace distinto de los demás, en algunas ocasiones se repiten un mismo chequeo a varios servicios debido a que cumple con las necesidades de monitoreo de dichos parámetros tal es el caso de Uso de la CPU, Estado de los Procesos y el Ping.

2.3.1 Caso 1. Comprobación del servicio de correo electrónico

El siguiente ejemplo muestra el funcionamiento del ServerEmail_1 con los diferentes parámetros que se han implementado para su monitorización:

Host ↑↓	Service ↑↓	Status ↑↓	Last Check ↑	Duration ↑↓	Attempt ↑↓	Status Information
ServerEmail_1	Estado Imap	OK	2013-08-08 14:58:33	2d 23h 34m 34s	1/4	IMAP OK - 0.001 second response time on port 143 [* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE STARTTLS AUTH=PLAIN] Dovecot ready.]
	Estado Mailq	OK	2013-08-08 14:58:05	3d 12h 8m 28s	1/4	OK: mailq reports queue is empty
	Estado Pop3	OK	2013-08-08 14:58:37	2d 23h 34m 30s	1/4	POP OK - 0.001 second response time on port 110 [+OK Dovecot ready.]
	Estado servicio PING	OK	2013-08-08 14:58:09	0d 2h 55m 25s	1/4	PING OK - Packet loss = 0%, RTA = 0.19 ms
	Estado servicio SMTP	OK	2013-08-08 14:53:41	0d 2h 52m 53s	1/4	SMTP OK - 0.002 sec. response time

5 Matching Service Entries Displayed

Figura 3. Estado del ServerEmail_1

2.3.1.1 Estado Imap

Como se puede observar en las siguientes capturas, los datos sacados tanto del equipo físicamente de la aplicación de Nagios como por consola, realizados por el script son prácticamente iguales.

Hay que tener en cuenta que están sacados con algunos segundos de retardo entre captura y captura:

```
root@control:~# /usr/lib/nagios/plugins/check_imap -H 10.26.2.1 -w 5 -c 10 -t 5
IMAP OK - 0.001 second response time on port 143 [* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-
REFERRALS ID ENABLE STARTTLS AUTH=PLAIN] Dovecot ready.]
|time=,000943s;5.000000;10.000000;0.000000;5.000000
```

Figura 4. Captura realizada mediante scrip

Además, se puede ver en los gráficos que genera tanto Nagios como su Addons Nagiosgrapher. Observemos ahora la opción de Disponibilidad para este parámetro en nagios y luego en nagiosgrapher.

Step 3: Select Report Options

Report Period:

If Custom Report Period...

Start Date (Inclusive):

End Date (Inclusive):

Report time Period:

Assume Initial States:

Assume State Retention:

Assume States During Program Downtime:

Include Soft States:

First Assumed Service State:

Backtracked Archives (To Scan For Initial States):

Figura 5. Crear reporte de Disponibilidad ServerEmail_1. Estado Imap

Como se puede observar cada parámetro definido por nagios puede ser cambiado a las necesidades que desee visualizar en ese momento el administrador, las figuras 6 y 7 reflejan el reporte y muestra los datos obtenidos del script.

En la figura 7 se ilustra una serie de eventos de inicio y fin, duración del evento y el estado de la información que el script descargo del servicio, estos parámetros son de gran importancia para los administradores del centro; dado que les permite realizar mantenimientos a los servicios cuando estos requieran del mismo debido a la cantidad de churre (datos indeseables acumulados en cache) que no permite realizar un buen funcionamiento del servicio publicado.

Service State Breakdowns:

State	Type / Reason	Time	% Total Time	% Known Time
OK	Unscheduled	6d 23h 42m 46s	99.829%	99.829%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	6d 23h 42m 46s	99.829%	99.829%
WARNING	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%
UNKNOWN	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%
CRITICAL	Unscheduled	0d 0h 17m 14s	0.171%	0.171%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 0h 17m 14s	0.171%	0.171%
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%

Figura 6. Averías de estado de servicio ServerEmail_1 Estado Imap

Service Log Entries:
[View full log entries]

Event Start Time	Event End Time	Event Duration	Event/State Type	Event/State Information
2013-05-29 11:30:23	2013-05-29 11:30:24	0d 0h 0m 1s	SERVICE OK (HARD)	First Service State Assumed (Faked Log Entry)
2013-05-31 15:48:46	2013-05-31 16:33:38	0d 0h 44m 52s	SERVICE CRITICAL (HARD)	No route to host
2013-06-01 00:00:00	2013-06-01 17:52:27	0d 17h 52m 27s	SERVICE OK (HARD)	IMAP OK - 0.001 second response time on port 143 [* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE STARTTLS AUTH=PLAIN] Dovecot ready.]
2013-06-01 17:52:27	2013-06-01 17:57:27	0d 0h 5m 0s	SERVICE CRITICAL (HARD)	No route to host
2013-06-01 17:57:27	2013-06-02 00:00:00	0d 6h 2m 33s	SERVICE OK (HARD)	IMAP OK - 0.001 second response time on port 143 [* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE STARTTLS AUTH=PLAIN] Dovecot ready.]
2013-06-02 00:00:00	2013-06-03 00:00:00	1d 0h 0m 0s	SERVICE OK (HARD)	IMAP OK - 0.001 second response time on port 143 [* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE STARTTLS AUTH=PLAIN] Dovecot ready.]
2013-06-03 00:00:00	2013-06-03 05:51:23	0d 5h 51m 23s	SERVICE OK (HARD)	IMAP OK - 0.001 second response time on port 143 [* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE STARTTLS AUTH=PLAIN] Dovecot ready.]
2013-06-03 05:51:23	2013-06-03 05:58:13	0d 0h 4m 50s	SERVICE CRITICAL (HARD)	No route to host
2013-06-03 05:58:13	2013-06-03 13:04:18	0d 7h 8m 5s	SERVICE OK (HARD)	IMAP OK - 0.001 second response time on port 143 [* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE STARTTLS AUTH=PLAIN] Dovecot ready.]

Figura 7. Entradas del registro del servicio ServerEmail_1 Estado_Imap

Para ganar e tiempo he reservado una serie de ilustraciones en los anexo donde se exponen los privilegios de usar este servidor de monitoreo.

Ilustración obtenida del Addons NagiosGrapher:

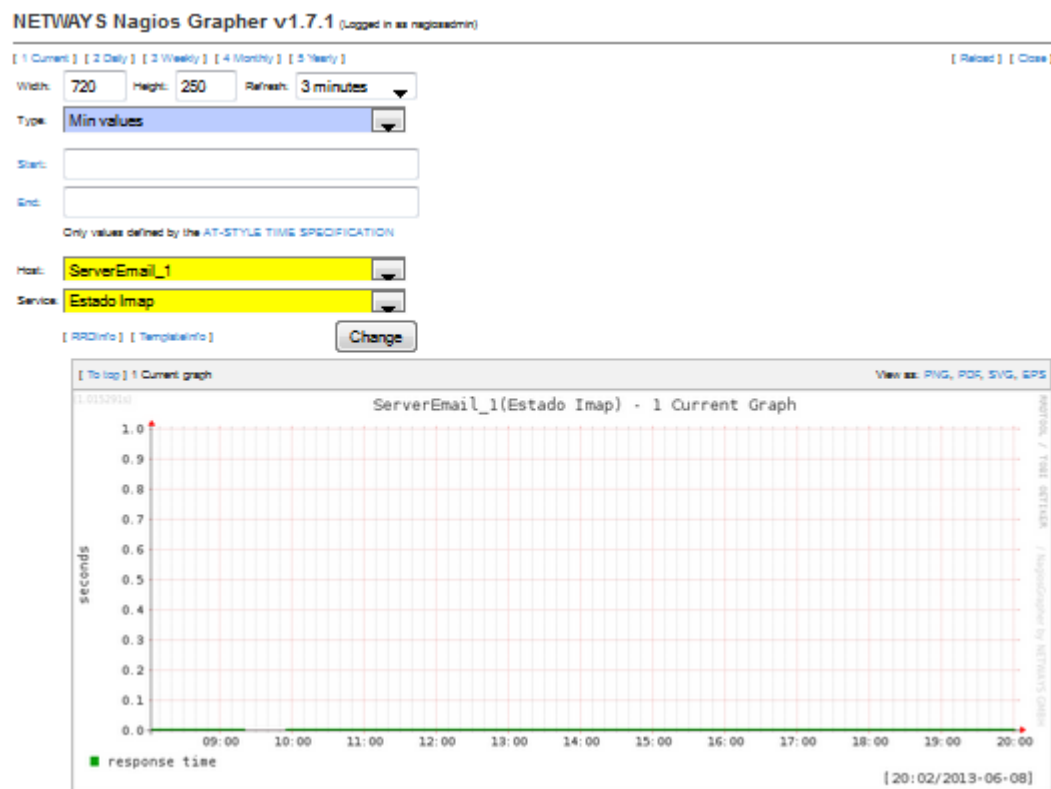


Figura 8. NagiosGrapher ServerEmail_1 Estado Imap

2.3.1.2 Estado Mailq

A continuación se detalla el estado de las posibles colas en los servidores de correos, para esto es imprescindible la función del comando Mailq que nos permite liberar la cola que exista en nuestros servidores. Aclarar que al momento de correr el script no existía cola.

```
root@control:/etc/nagios3# /usr/lib/nagios/plugins/check_mailq -w 200 -c 1000 -M postfix -t 600
OK: mailq reports queue is empty|unsent=0;200;1000;0
root@control:/etc/nagios3#
```

Figura 9. Captura realizada por el script Estado Mailq

Del mismo modo, los gráficos exponen los resultados obtenidos por el script.

Service State Breakdowns:

State	Type / Reason	Time	% Total Time	% Known Time
OK	Unscheduled	7d 0h 0m 0s	100.000%	100.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	7d 0h 0m 0s	100.000%	100.000%
WARNING	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%
UNKNOWN	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%
CRITICAL	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%

Figura 10. Averías de estado de servicio ServerEmail_1

Service Log Entries:
[View full log entries]

Event Start Time	Event End Time	Event Duration	Event/State Type	Event/State Information
2013-05-29 11:30:23	2013-05-29 11:30:24	0d 0h 0m 1s	SERVICE OK (HARD)	First Service State Assumed (Faked Log Entry)
2013-06-01 00:00:00	2013-06-02 00:00:00	1d 0h 0m 0s	SERVICE OK (HARD)	OK: mailq reports queue is empty
2013-06-02 00:00:00	2013-06-03 00:00:00	1d 0h 0m 0s	SERVICE OK (HARD)	OK: mailq reports queue is empty
2013-06-03 00:00:00	2013-06-03 13:04:18	0d 13h 4m 18s	SERVICE OK (HARD)	OK: mailq reports queue is empty
2013-06-04 00:00:00	2013-06-04 07:58:00	0d 7h 58m 0s	SERVICE OK (HARD)	OK: mailq reports queue is empty
2013-06-05 00:00:00	2013-06-05 13:17:33	0d 13h 17m 33s	SERVICE OK (HARD)	OK: mailq reports queue is empty
2013-06-06 00:00:00	2013-06-06 00:23:17	0d 0h 23m 17s	SERVICE OK (HARD)	OK: mailq reports queue is empty
2013-06-07 00:00:00	2013-06-07 20:14:58	0d 20h 14m 58s	SERVICE OK (HARD)	OK: mailq reports queue is empty

Figura 11. Entradas del registro del servicio ServerEmail_1 Mailq

Service Log Entries:
[View full log entries]

Event Start Time	Event End Time	Event Duration	Event/State Type	Event/State Information
2013-06-02 23:59:59	2013-06-03 00:00:00	0d 0h 0m 1s	SERVICE CRITICAL (HARD)	First Service State Assumed (Faked Log Entry)
2013-06-03 00:00:00	2013-06-03 13:04:18	0d 13h 4m 18s	SERVICE OK (HARD)	OK: mailq reports queue is empty
2013-06-04 00:00:00	2013-06-04 07:58:00	0d 7h 58m 0s	SERVICE OK (HARD)	OK: mailq reports queue is empty
2013-06-05 00:00:00	2013-06-05 13:17:33	0d 13h 17m 33s	SERVICE OK (HARD)	OK: mailq reports queue is empty
2013-06-06 00:00:00	2013-06-06 00:23:17	0d 0h 23m 17s	SERVICE OK (HARD)	OK: mailq reports queue is empty
2013-06-07 00:00:00	2013-06-07 20:14:58	0d 20h 14m 58s	SERVICE OK (HARD)	OK: mailq reports queue is empty

Figura 12. Entradas del registro Criticas del servicio ServerEmail_1 Mailq

Hasta ahora los datos ilustrados han sido del ServerEmail_1 teniendo en cuenta que los tres servidores poseen los mismo parámetros a monitorear expondré graficas diferentes en cuanto a servicio y servidor.

2.3.1.3 Estado POP3

A continuación mostrare imágenes del servicio pop3 en el servidor 1, 2 y 3 obtenidas con NagiosGrapher esto nos permitirá hacer comparativas entre uno u otro servidor.

ServerEmail_1:

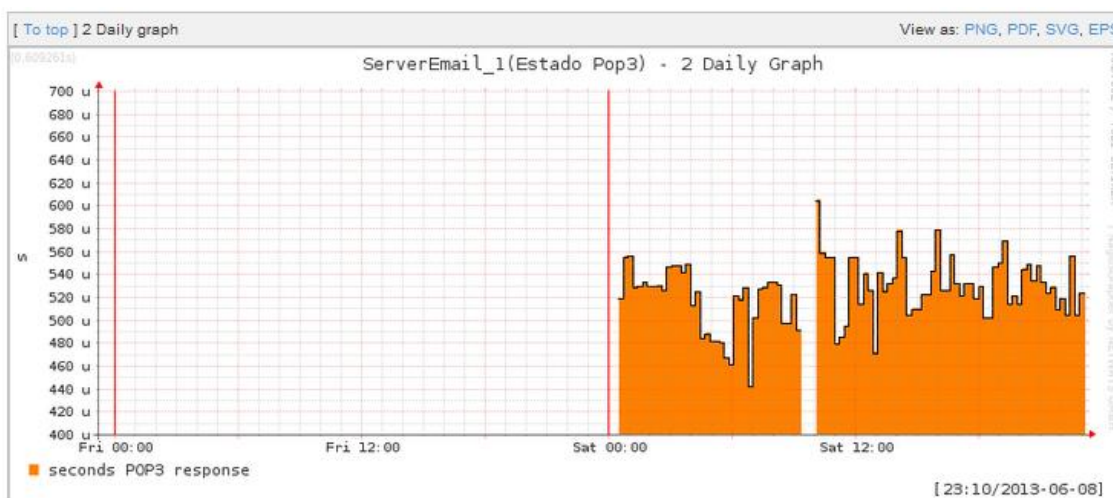


Figura 13. NagiosGrapher: ServerEmail_1 Estado Pop3

ServerEmail_2

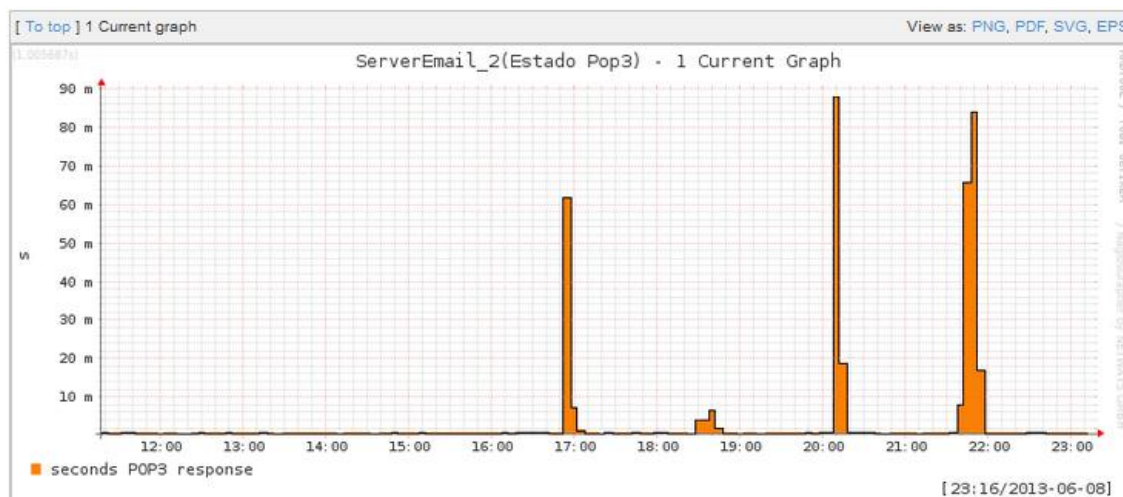


Figura 14. NagiosGrapher: ServerEmail_2 Estado Pop3

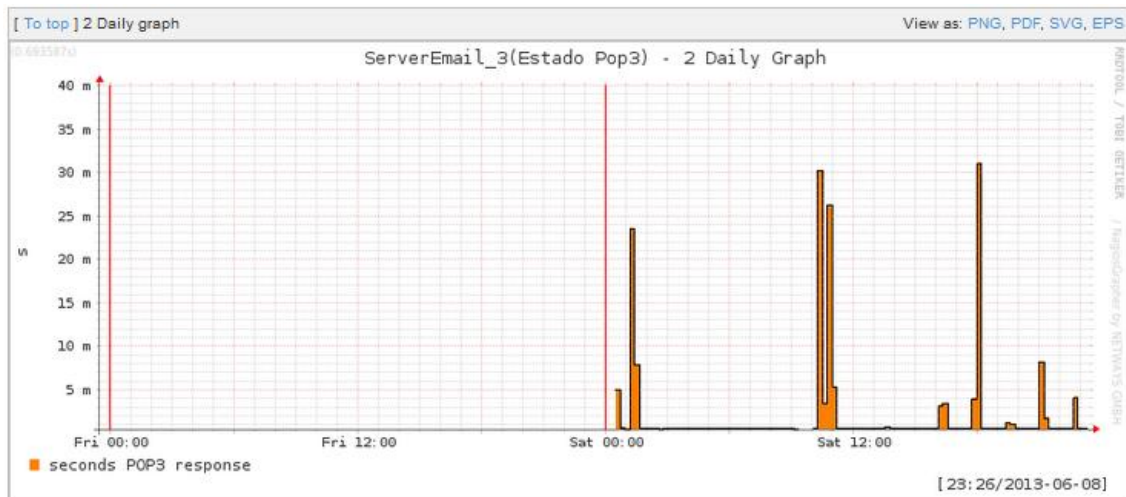


Figura 15.NagiosGrapher: ServerEmail_3 Estado Pop3

Captura realizada mediante script.

```
root@control:~# /usr/lib/nagios/plugins/check_pop -H 10.26.2.9 -p 110 -w 5 -c 10 -s 20
POP OK - 0.001 second response time on port 110 [+OK Dovecot ready.]|time=
0.000676s;5.000000;10.000000;0.000000;10.000000
root@control:~#
```

Figura 16.Captura realizada mediante script Estado Pop3.

2.3.1.4 Estado servicio PING

El servicio Ping comprueba el estado de la comunicación con el host local con uno o varios equipos remotos de una red TCP/IP por medio del envío de paquetes ICMP de solicitud y de respuesta. Mediante esta utilidad puede diagnosticarse el estado, velocidad y calidad de nuestra red. Teniendo en cuenta que es muy tedioso estar realizando ping a intervalos de tiempo es mejor tenerlo montado como servicio así solo debemos de monitorear.

Se muestra a continuación datos obtenidos por NagiosGrapher del servidor 3 "ServerEmail_3". Para ver la disponibilidad de los demás servidores ver los anexos.

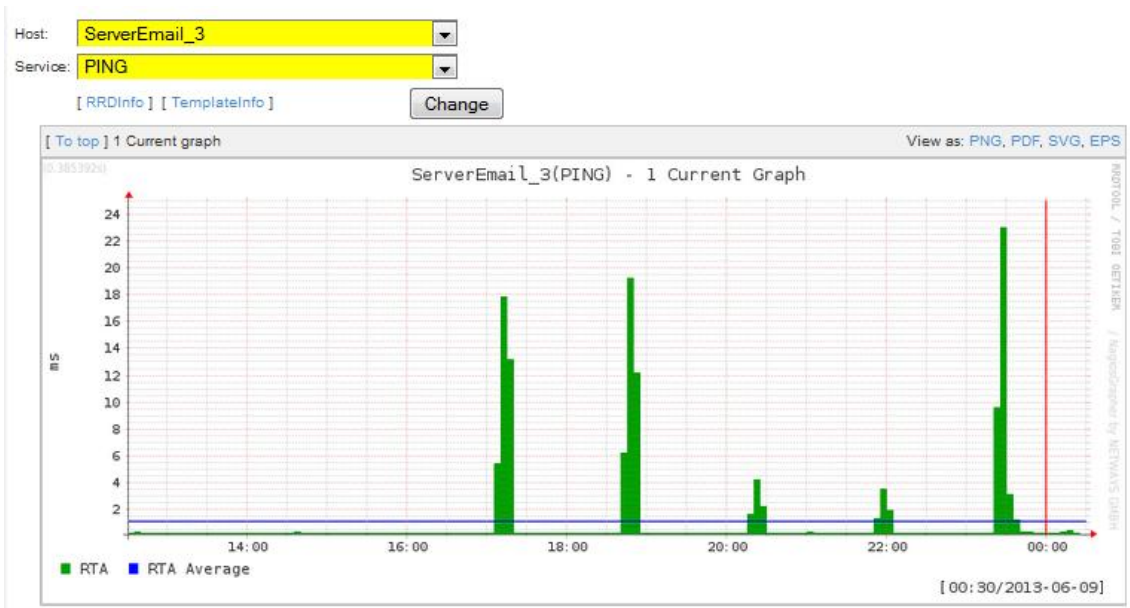


Figura 17. NagGrapher-SERVEREmail_3 Estado servicio Ping

2.3.1.5 Estado servicio SMTP

Este formidable protocolo de la capa de aplicación basado en texto, es utilizado en nuestra red para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos (PDA, teléfonos móviles, etc.). Implementado en nuestros BalanceadorUho permitiendo que se reparta la carga de los correos en nuestros servidores.

Se mostrara una interfaz del balanceador obtenida desde nagiosgrapher para visualizar los demos servidores ver anexos.

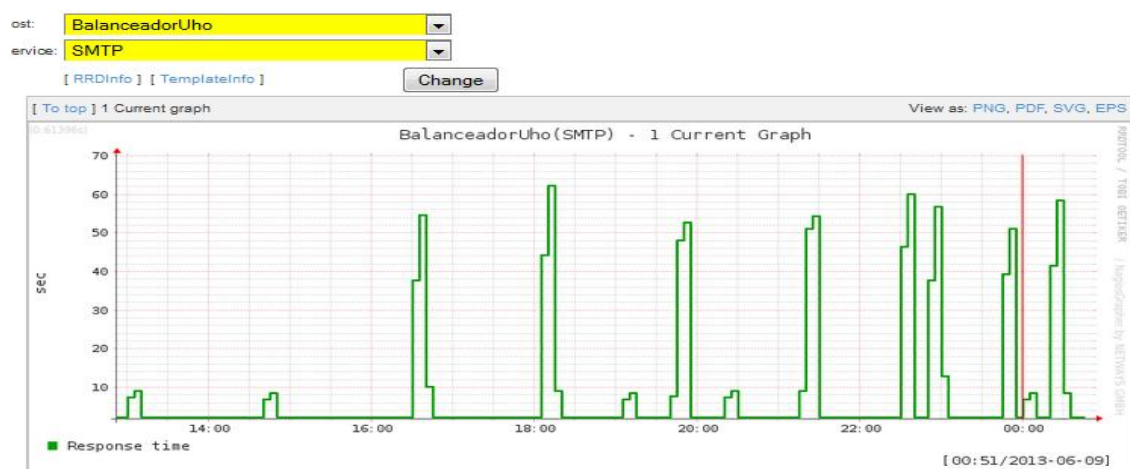


Figura 18. NagiosGrapher-BalanceadorUho Estado servicio SMTP

2.3.2 Caso 2. Comprobación del servicio web

El seguimiento de este servicio en tiempo real les permite a los administradores del nodo conocer del comportamiento del servidor Apache que es el encargado de divulgar todas páginas web hospedadas en dicho servidor, tal es el caso del servidor web Correoweb, Webmail, Plataforma de aprendizaje Moodle, y demás sitios de divulgación de la Uho. La siguiente ilustración muestra los parámetros hasta ahora monitoreando dicho servicio.

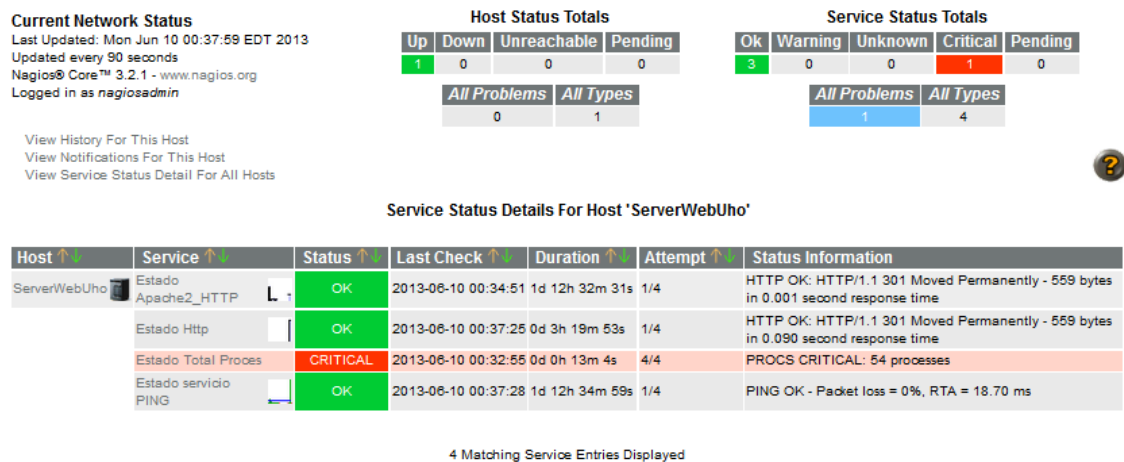


Figura 19. Estado servicios ServerWebUho

2.3.2.1 Estado servidor Apache2_HTTP

Como se puede observar en las siguientes capturas, los datos sacados tanto del equipo físicamente de la aplicación de Nagios como por consola, realizados por el script son prácticamente iguales.

Hay que tener en cuenta que están sacados con algunos segundos de retardo entre captura y captura:

```
root@control:~# /usr/lib/nagios/plugins/check_http -H correoweb.uho.edu.cu -I 10.26.0.73 -w 20 -c 40 -4
HTTP OK: HTTP/1.1 301 Moved Permanently - 569 bytes in 0.001 second response time |time=0.000971s;20.000000;40.000000;0.000000 size=569B;;0
root@control:~#
```

Figura 20. Captura realizada por script al ServerWebUho

```
root@control:~# /usr/lib/nagios/plugins/check_http -H www.facebook.com -I
10.26.0.73
HTTP OK: HTTP/1.1 301 Moved Permanently - 565 bytes in 0.001 second response time
|time=0.000950s;;;0.000000 size=565B;;;0
root@control:~# /usr/lib/nagios/plugins/check_http -H ServerWebUho -I 10.26.0.73
HTTP OK: HTTP/1.1 301 Moved Permanently - 561 bytes in 0.001 second response time
|time=0.000920s;;;0.000000 size=561B;;;0
root@control:~#
```

Figura 21. Captura realizada por script al ServerWebUho

Podemos observar que los script poseen diferentes datos, la figura 20 muestra una petición al servicio de correoweb verificando parámetros de advertencia y crítico, y la figura 21 una petición de conexión al sitio web facebook y otra al propio ServerWebUho.

Observemos ahora que arrojan las graficas en cuanto al estado del Apache2_HTTP, primero crearemos un reporte de disponibilidad desde el Nagios.

Step 3: Select Report Options

Report Period:

If Custom Report Period...

Start Date (Inclusive):

End Date (Inclusive):

Report time Period:

Assume Initial States:

Assume State Retention:

Assume States During Program Downtime:


Include Soft States:

First Assumed Service State:

Backtracked Archives (To Scan For Initial States):

Figura 22. Crear reporte de Disponibilidad ServerWebUho. Estado Apache2_HTTP

Service State Breakdowns:



State	Type / Reason	Time	% Total Time	% Known Time
OK	Unscheduled	7d 0h 0m 0s	100.000%	100.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	7d 0h 0m 0s	100.000%	100.000%
WARNING	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%
UNKNOWN	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%
CRITICAL	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%

Figura 23. Averías de estado del ServerWebUho. Estado Apache2_HTTP

Observemos que el servidor apache durante los últimos siete días se ha comportado al 100%, valido aclarar que el solo hospeda las páginas web de los servicios, si un servidor de correo presenta problemas como Webmail se resolverá en dicho servidor no en el apache. El apache seguirá corriendo y este mismo nos dirá el problema que estamos presentando.

Service Log Entries:
[View condensed log entries]

Event Start Time	Event End Time	Event Duration	Event/State Type	Event/State Information
2013-05-29 11:30:23	2013-05-29 11:30:24	0d 0h 0m 1s	SERVICE OK (HARD)	First Service State Assumed (Faked Log Entry)
2013-05-29 11:30:24	2013-05-29 11:44:49	0d 0h 14m 25s	PROGRAM END	Normal program termination
2013-05-29 11:44:49	2013-05-30 23:03:06	1d 11h 18m 17s	PROGRAM (RE)START	Program start
2013-05-30 23:03:06	2013-05-30 23:03:07	0d 0h 0m 1s	PROGRAM END	Normal program termination
2013-05-30 23:03:07	2013-05-30 23:04:35	0d 0h 1m 28s	PROGRAM (RE)START	Program start
2013-05-30 23:04:35	2013-05-30 23:04:38	0d 0h 0m 3s	PROGRAM END	Normal program termination
2013-05-30 23:04:38	2013-05-30 23:07:20	0d 0h 2m 42s	PROGRAM (RE)START	Program start
2013-05-30 23:07:20	2013-05-30 23:07:22	0d 0h 0m 2s	PROGRAM END	Normal program termination
2013-05-30 23:07:22	2013-05-30 23:13:47	0d 0h 6m 25s	PROGRAM (RE)START	Program start
2013-05-30 23:13:47	2013-05-30 23:13:49	0d 0h 0m 2s	PROGRAM END	Normal program termination
2013-05-30 23:13:49	2013-05-31 11:08:54	0d 11h 55m 5s	PROGRAM (RE)START	Program start

Figura 24. Entradas del registro del servicio ServerWebUho. Estado Apache2_HTTP

Grafica arrojada por el modulo NagiosGrapher

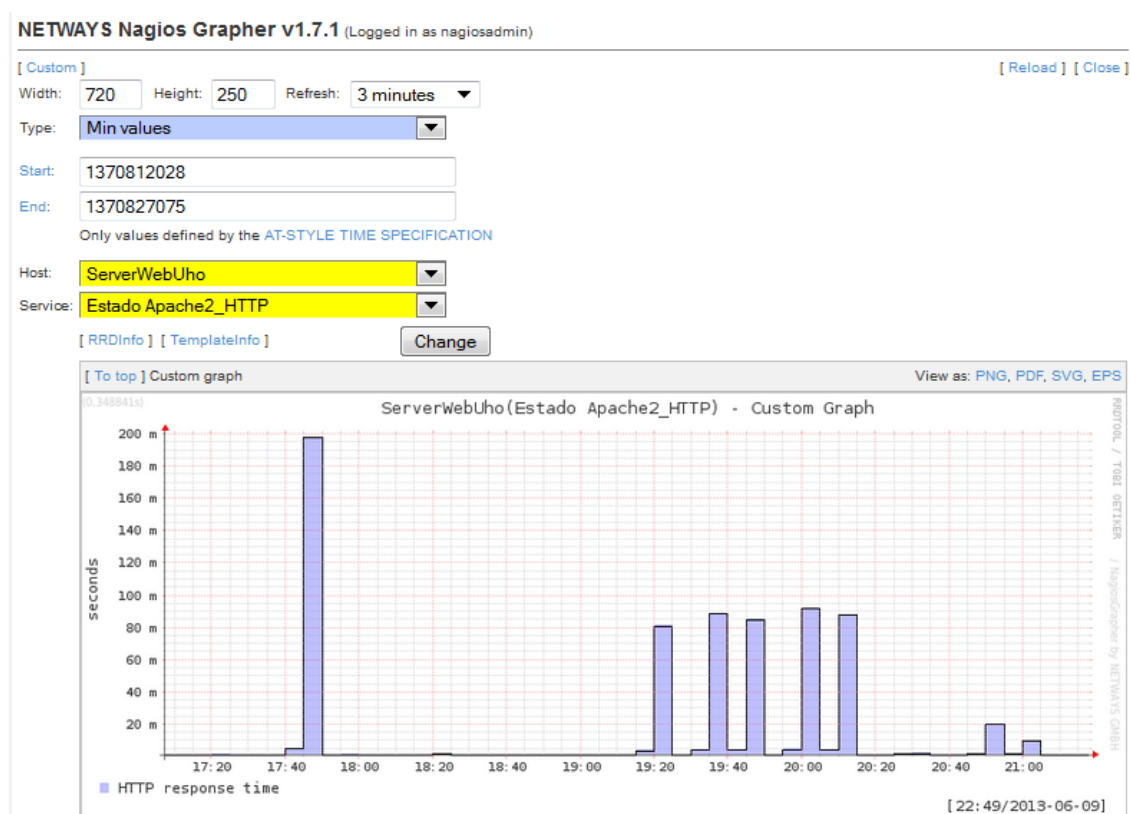


Figura 25. . NagiosGrapher-ServerWebUho. Estado Apache2_HTTP

2.3.2.2 Estado del servicio PING

El servicio Ping comprueba el estado de la comunicación con el host local con uno o varios equipos remotos de una red TCP/IP por medio del envío de paquetes ICMP de solicitud y de respuesta. Mediante esta utilidad puede diagnosticarse el estado, velocidad y calidad de nuestra red. Teniendo en cuenta lo monótono de estar realizando ping a intervalos de tiempo es mejor tenerlo montado como un servicio y así solo debemos de monitorear.

Se muestra a continuación datos obtenidos mediante pruebas realizadas por script, declarando valores como advertencias, valores críticos, cantidad de paquetes de pérdidas entre otros se sometieron al cheque los ip siguientes:

IP: 10.26.0.73—ServerWebUho

IP: 10.26.0.10—ServerProxy

IP: 10.26.2.1—ServerEmail_1

IP: 10.26.0.52—ServerDNS_1

```

root@control:~# /usr/lib/nagios/plugins/check_ping -H 10.26.0.73 -w 10.0,5% -c
20.0,10% -p 10 -t 10 -4
PING OK - Packet loss = 0%, RTA = 0.18 ms|rta=
0.176000ms;10.000000;20.000000;0.000000 pl=0%;5;10;0
root@control:~# /usr/lib/nagios/plugins/check_ping -H 10.26.0.10 -w 10.0,5% -c
20.0,10% -p 10 -t 10 -4
PING CRITICAL - Packet loss = 20%, RTA = 0.17 ms|rta=
0.172000ms;10.000000;20.000000;0.000000 pl=20%;5;10;0
root@control:~# /usr/lib/nagios/plugins/check_ping -H 10.26.2.1 -w 10.0,5% -c
20.0,10% -p 10 -t 10 -4
PING OK - Packet loss = 0%, RTA = 0.20 ms|rta=
0.199000ms;10.000000;20.000000;0.000000 pl=0%;5;10;0
root@control:~# /usr/lib/nagios/plugins/check_ping -H 10.26.0.52 -w 10.0,5% -c
20.0,10% -p 10 -t 10 -4
PING OK - Packet loss = 0%, RTA = 0.09 ms|rta=
0.086000ms;10.000000;20.000000;0.000000 pl=0%;5;10;0
root@control:~#

```

Figura 26. Captura realizada por script ServerWebUho. Estado PING

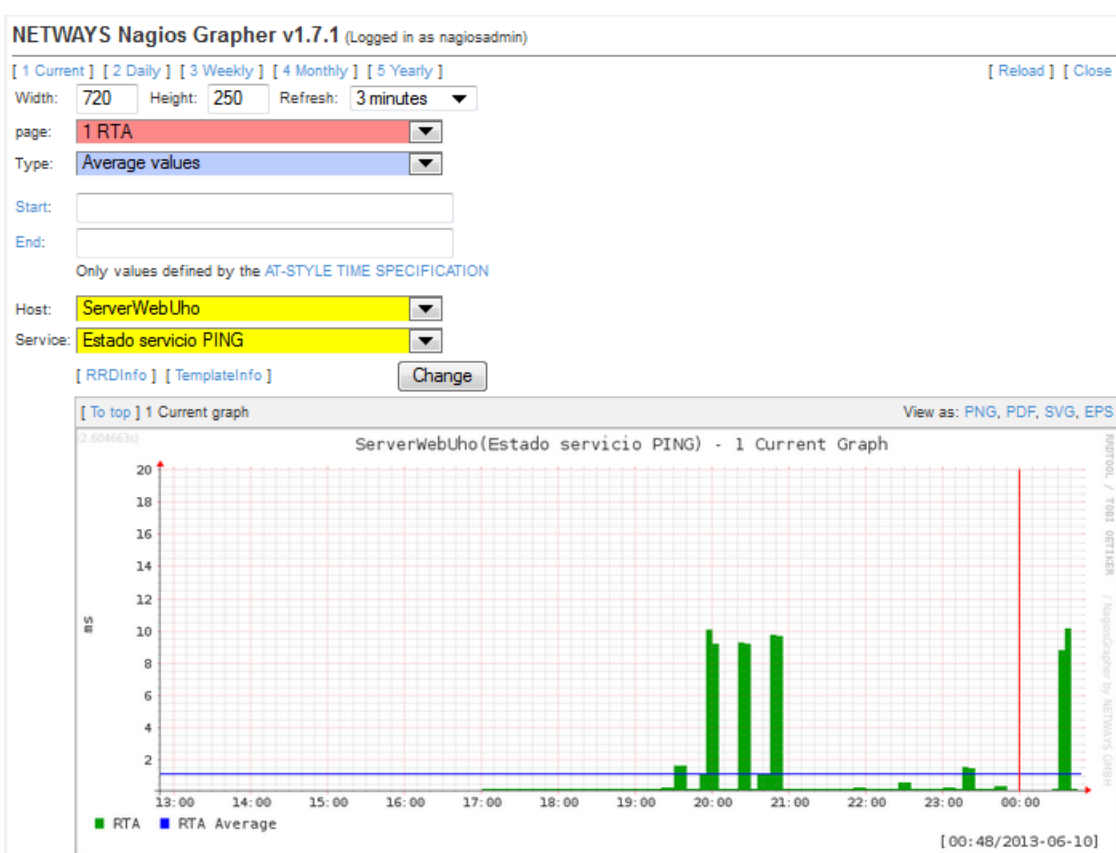


Figura 27. NagiosGrapher-ServerWebUho. Estado servicio PING

Estas capturas que no son más que los datos que envía Nagios a Nagiosgrapher son de gran importancia, le permite al administrador determinar horarios (horarios picos) donde se le realiza mayor petición o consultas al servicio y les permite a los administradores del mismo acometer mejor su trabajo y monitorizar con mucha más frecuencias dicho servidor.

2.3.3 Caso 3. Comprobación del servicio Acceso Remoto (FreeRADIUS)

El servicio de acceso remoto que es brindado para todos los usuarios de la red Uho ha alcanzado una gran importancia para los procesos sustantivos de la universidad, tal es el caso como son las conexiones de las demás sedes universitarias hacia nuestro centro. Su monitorización en tiempo real les permite a los administradores del nodo saber el comportamiento del mismo.

Nagios permite chequear a todos los usuarios que tiene la base de datos del FreeRADIUS, servidor de autenticación dedicado a este servicio, pero en este caso no es lo que se propone para ello ya esta implementado otro software en el nodo verificando la cantidad de usuarios conectados al mismo, es por ello que solo se realiza la monitorización a la posible pérdida de paquetes hacia este servidor.

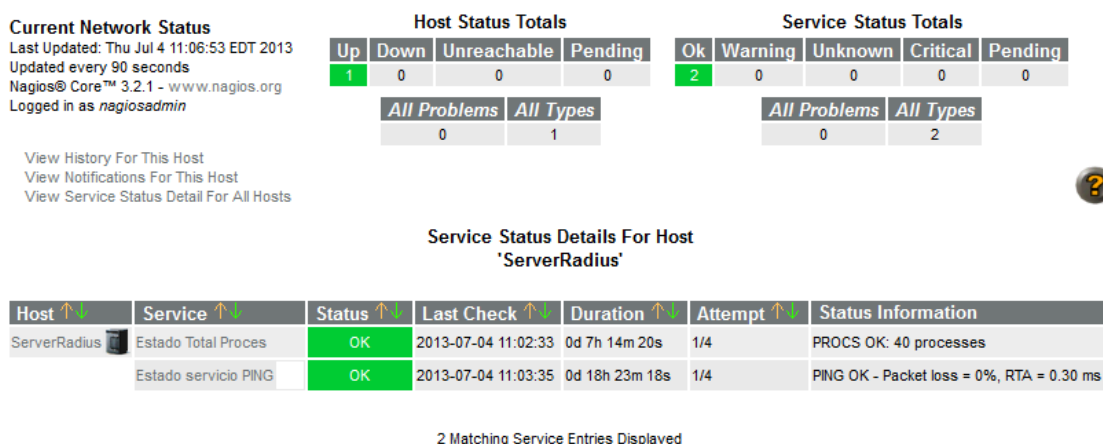


Figura 28. Estado servicio ServerRadius

Como muestra la figura 28 el estado del servidor así como los servicios a monitorear.

2.3.3.1 Estado del servicio PING

La figura 29 que se muestra a continuación contiene las Tramas de servicio PING durante un mes este le permite a los administradores ver su comportamiento, además de observar el tiempo que dura alguna perdida.

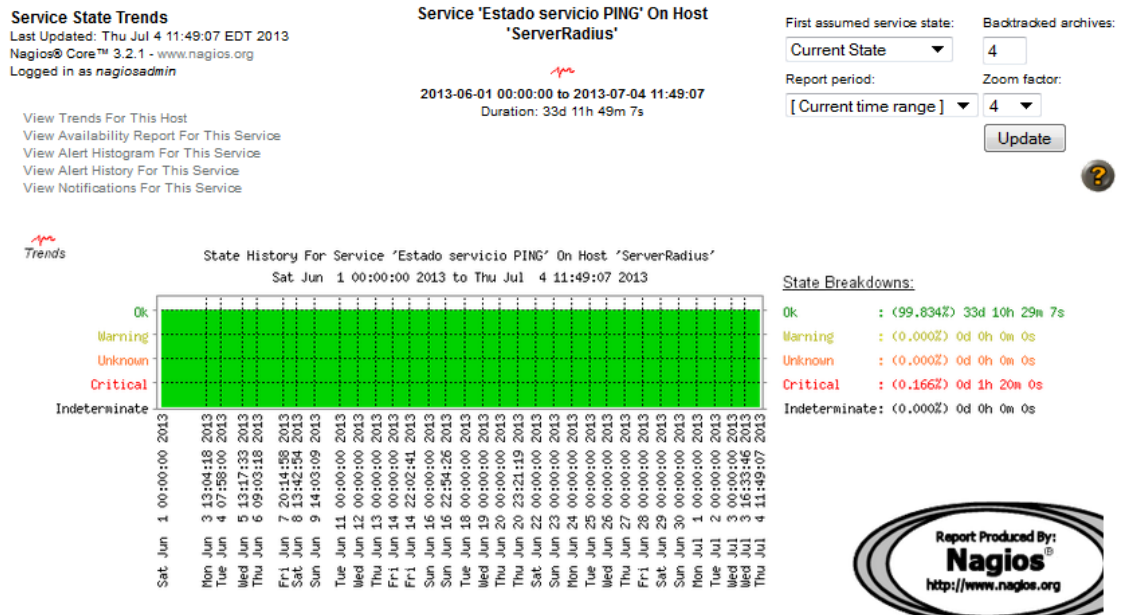


Figura 29. Trama Servicio PING: ServerRadius

De igual forma la creación de reportes en Nagios le posibilita al administrador tener un historial de todos los servicios y host, uno de los reportes más completos dentro de la gama de reportes del servidor nagios es el de Disponibilidad. Permitiendo saber qué tiempo estuvo disponible, si el servicio ha estado estable y otros parámetros que se pueden visualizar en el reporte creado.

Step 3: Select Report Options

Report Period: *** CUSTOM REPORT PERIOD ***

If Custom Report Period...

Start Date (Inclusive): June 1 2013

End Date (Inclusive): July 4 2013

Report time Period: None

Assume Initial States: Yes

Assume State Retention: Yes

Assume States During Program Downtime: Yes

Include Soft States: No

First Assumed Service State: Current State

Backtracked Archives (To Scan For Initial States): 4


Create Availability Report!

Figura 30. Crear reporte de Disponibilidad: ServerRadius-Servicio PING

Es válido aclarar que los parámetros que se observan en el reporte creado en la figura 30 pueden ser cambiados así se podrá obtener un mejor resultado de lo que se desea.

[Availability report completed in 0 min 0 sec]

Service State Breakdowns:



State	Type / Reason	Time	% Total Time	% Known Time
OK	Unscheduled	33d 13h 1m 18s	99.835%	99.835%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	33d 13h 1m 18s	99.835%	99.835%
WARNING	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%
UNKNOWN	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%
CRITICAL	Unscheduled	0d 1h 20m 0s	0.165%	0.165%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 1h 20m 0s	0.165%	0.165%
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	33d 14h 21m 18s	100.000%	100.000%

Figura 31. Averías de estado del ServerRadius: Servicio PING

Service Log Entries:

[View full log entries]

Event Start Time	Event End Time	Event Duration	Event/State Type	Event/State Information
2013-05-29 11:30:23	2013-05-29 11:30:24	0d 0h 0m 1s	SERVICE OK (HARD)	First Service State Assumed (Faked Log Entry)
2013-06-09 00:00:00	2013-06-09 00:11:50	0d 0h 11m 50s	SERVICE OK (HARD)	PING OK - Packet loss = 0%, RTA = 0.34 ms
2013-06-11 00:00:00	2013-06-11 10:20:09	0d 10h 20m 9s	SERVICE OK (HARD)	PING OK - Packet loss = 0%, RTA = 0.18 ms
2013-06-12 00:00:00	2013-06-13 00:00:00	1d 0h 0m 0s	SERVICE OK (HARD)	PING OK - Packet loss = 0%, RTA = 0.17 ms
2013-06-13 00:00:00	2013-06-14 00:00:00	1d 0h 0m 0s	SERVICE OK (HARD)	PING OK - Packet loss = 0%, RTA = 4.51 ms
2013-06-14 00:00:00	2013-06-14 08:59:59	0d 8h 59m 59s	SERVICE OK (HARD)	PING OK - Packet loss = 0%, RTA = 0.19 ms
2013-06-14 08:59:59	2013-06-14 09:04:59	0d 0h 5m 0s	SERVICE CRITICAL (HARD)	PING CRITICAL - Packet loss = 80%, RTA = 0.77 ms
2013-06-14 09:04:59	2013-06-14 10:39:59	0d 1h 35m 0s	SERVICE OK (HARD)	PING OK - Packet loss = 0%, RTA = 0.17 ms
2013-06-14 10:39:59	2013-06-14 11:09:59	0d 0h 30m 0s	SERVICE CRITICAL (HARD)	CRITICAL - Host Unreachable (10.26.0.249)
2013-06-14 11:09:59	2013-06-14 11:41:26	0d 0h 31m 27s	SERVICE OK (HARD)	PING OK - Packet loss = 0%, RTA = 0.16 ms
2013-06-15 00:00:00	2013-06-16 00:00:00	1d 0h 0m 0s	SERVICE OK (HARD)	PING OK - Packet loss = 0%, RTA = 0.17 ms
2013-06-16 00:00:00	2013-06-16 22:54:28	0d 22h 54m 28s	SERVICE OK (HARD)	PING OK - Packet loss = 0%, RTA = 0.17 ms
2013-06-17 00:00:00	2013-06-17 00:01:35	0d 0h 1m 35s	SERVICE OK (HARD)	PING OK - Packet loss = 0%, RTA = 1.75 ms
2013-06-18 00:00:00	2013-06-19 00:00:00	1d 0h 0m 0s	SERVICE OK (HARD)	PING OK - Packet loss = 0%, RTA = 0.20 ms
2013-06-19 00:00:00	2013-06-20 00:00:00	1d 0h 0m 0s	SERVICE OK (HARD)	PING OK - Packet loss = 0%, RTA = 0.18 ms
2013-06-20 00:00:00	2013-06-20 23:21:19	0d 23h 21m 19s	SERVICE OK (HARD)	PING OK - Packet loss = 0%, RTA = 0.16 ms
2013-06-21 00:00:00	2013-06-22 00:00:00	1d 0h 0m 0s	SERVICE OK (HARD)	PING OK - Packet loss = 0%, RTA = 0.16 ms
2013-06-22 00:00:00	2013-06-23 00:00:00	1d 0h 0m 0s	SERVICE OK (HARD)	PING OK - Packet loss = 0%, RTA = 0.34 ms
2013-06-23 00:00:00	2013-06-24 00:00:00	1d 0h 0m 0s	SERVICE OK (HARD)	PING OK - Packet loss = 0%, RTA = 0.17 ms
2013-06-24 00:00:00	2013-06-25 00:00:00	1d 0h 0m 0s	SERVICE OK (HARD)	PING OK - Packet loss = 0%, RTA = 0.15 ms
2013-06-25 00:00:00	2013-06-25 14:49:45	0d 14h 49m 45s	SERVICE OK (HARD)	PING OK - Packet loss = 0%, RTA = 0.18 ms
2013-06-26 00:00:00	2013-06-27 00:00:00	1d 0h 0m 0s	SERVICE OK (HARD)	PING OK - Packet loss = 0%, RTA = 0.18 ms

Figura 32. Entradas del registro del servicio ServerRadius: Servicio PING

La monitorización de servicios de red, equipos físicos (host, router, switch) son hoy en día un eslabón de gran importancia en cualquier institución, de ahí que cada día existan personas que trabajen minuciosamente hacia este fin. Exponer todos los gráficos y datos adquiridos con la implementación del servidor nagios no es el motivo de esta investigación, pero si es importante saber que gracias al mismo se han podido acometer medidas de chequeos con un tiempo de periodo más cortos y una vista en tiempo real de lo que está pasando en los servidores del nodo central gracias a esta implementación se pudo llegar a conclusiones.

Conclusiones

La Informatización de la Sociedad es el proceso de utilización ordenada y masiva de las Tecnologías de la Información y las Comunicaciones en la vida cotidiana, para satisfacer las necesidades de todas las esferas de la sociedad, en su esfuerzo por lograr cada vez más eficacia y eficiencia en todos los procesos y por consiguiente mayor generación de riqueza y aumento en la calidad de vida de los ciudadanos.

Actualmente la Universidad de Holguín, y dentro de esta el Nodo Central RED Uho, se encuentra en un proceso de continua mejora de los servicios que se prestan a los usuarios de la red. Identificar la situación problemática de cada uno de estos servicios, brinda la posibilidad de trabajar más concretamente en las dificultades que aún existen. La supervisión de algunos servicios ha sido solucionada aquí, pero para otras serán necesarios nuevos procesos investigativos que inmiscuyan tanto al personal que labora en el grupo de red, así como a los usuarios que se benefician de estos servicios.

El Servidor Nagios implementado ha de permitir desarrollar una administración y monitoreo más completa de los Servicios a los Administradores del Nodo Central de la Red Uho.

El Servidor de Monitoreo que se ha implementado y se ha puesto a punto en el Nodo de la Red Uho posibilita la vigilancias de todos los servicios declarados en el mismo así como equipos físicos ubicados en distintas áreas de la Uho. Este permite a su vez que los administradores puedan realizar mantenimientos programados y no bajar los servicios por esta causa.

En estos momentos el servidor Nagios se encuentra funcionando en el Nodo Central de la Red Uho con más de 50 chequeos implementados de diversas formas hacia los Servidores de correo electrónico, acceso remoto y demás servidores hospedados en el nodo, se encuentran también 21 equipos físicos

entre switch y routers y de forma general 59 servidores repartido entre las sedes municipales y la sede Celia Sánchez Manduley.

Los argumentos obtenidos permiten afirmar que se cumple la hipótesis y se logró el objetivo para resolver el problema que dio lugar a esta investigación.

Recomendaciones

El Servidor Nagios que se ha implementado es un eslabón de la cadena de transformaciones en que se encuentra inmerso el Nodo Central RED Uho. Muchas son las expectativas de mejoras de los diferentes servidores y servicios de red que se brindan a los usuarios. El estudio de la situación problemática arrojó otras dificultades que por diferentes aspectos no fueron posibles culminar, y las que se reflejan a continuación como parte de las recomendaciones de este trabajo de diploma:

- Estudiar la posibilidad de incorporarle a Nagios algún método para exportar sus reportes en algún tipo de extensión ejemplo PDF.
- Incorporar la herramienta PNP4Nagios para vista de mejores graficas.
- Incorporar la herramienta NagiosQL que nos permite trabajar desde una interfaz web los datos de Nagios.
- Estudiar la posibilidad de enviar notificaciones vía Jabber.

Se recomienda a los administradores de los diferentes nodos aprovechar las potencialidades de este servidor ya sea para elevar su cultura informática en temas de redes, seguridad y monitoreo, así como el de fieles guardianes de los servicios que prestan en dicha entidad.

Referencias Bibliográficas:

- [1] "Tecnología_informática," 22 de Abril, 2013. [Online]. Available: http://es.wikipedia.org/wiki/Tecnologia_informática.
- [2] "Telemática," 18 de Abril, 2013. [Online]. Available: <http://es.wikipedia.org/wiki/Telemática>.
- [3] Dayamí Proenza Pupo and F. L. F. Castillo, "SISTEMA INFORMÁTICO PARA LA SEGURIDAD EN LAS CONEXIONES Y COMUNICACIONES DE LA RED DE DATOS EN EL NODO CENTRAL DE LA UNIVERSIDAD DE HOLGUÍN 'OSCAR LUCERO MOYA'," 2009.
- [4] "Redes," 1 de Mayo, 2013. [Online]. Available: <http://vgg.sci.uma.es/redes/servicio.html>.
- [5] "Red de computadoras - Wikipedia, la enciclopedia libre," 8 de Abril, 2013. [Online]. Available: http://es.wikipedia.org/wiki/Red_de_computadoras.
- [6] J. J. G. MEJIA, "Tesis de grado en Nagios," Septiembre, 2010. [Online]. Available: <http://www.buenastareas.com/ensayos/Tesis-De-Monitoreo-De-Redes-Con/712649.html>.
- [7] Luis G. Menegón R, "Diseño e Implementación de un Sistema de Monitoreo y Control Basado en Software Libre para La Red de Telecomunicaciones en la Dirección de Informática y Sistemas de la Gobernación del Estado Bolívar," 2011.
- [8] J. J. Esteve, *Administración avanzada de GNU / Linux*. 2010.
- [9] "Grupo de Traducción al Castellano de RFCs," Abril, 2013. [Online]. Available: <http://www.rfc-es.org>.
- [10] "World Wide Web - Wikipedia," 24 de Febrero, 2013. [Online]. Available: http://es.wikipedia.org/wiki/World_Wide_Web.
- [11] "Hypertext Transfer Protocol," 2013. [Online]. Available: http://es.wikipedia.org/wiki/Hypertext_Transfer_Protocol.
- [12] "¿Qué es un servidor FTP (FTP Servers)." [Online]. Available: <http://www.masadelante.com/faqs/servidores-ftp>.
- [13] "Acceso Remoto," 2013. [Online]. Available: <http://www.abartiateam.com/>.
- [14] J. B. Dueñas, "Configuración básica de Freeradius con soporte de LDAP," 30 de Mayo, 2012.

- [15] "Wi-Fi," 26 de Mayo, 2013. [Online]. Available: <http://es.wikipedia.org/wiki/Wi-Fi>.
- [16] "IEEE 802," 26 de Mayo, 2013. [Online]. Available: http://es.wikipedia.org/wiki/IEEE_802.11.
- [17] "REGLAMENTO DE SEGURIDAD PARA LAS TECNOLOGAS DE LA INFORMACION."
- [18] R. Stallman, "Linux y GNU - Proyecto GNU - Free Software Foundation," 20 de Abril, 2013. [Online]. Available: <http://www.gnu.org/gnu/linux-and-gnu.html>.
- [19] "Sobre Linux El rincón de Linux," 25 de Abril, 2013. [Online]. Available: http://www.linux-es.org/sobre_linux.
- [20] "Linux," 2013. [Online]. Available: <http://www.linux.org/>.
- [21] "Linux Standard Base (LSB) _ The Linux Foundation," 27 de febrero, 2013. [Online]. Available: <http://www.linuxfoundation.org/collaborate/workgroups/lsb>.
- [22] Andrew S. Tanenbaum, *Redes de computadoras*, Cuarta edi. 2003.
- [23] "Catedrático, Científico de la computación Andrew S. Tanenbaum," 30 de Abril, 2013. [Online]. Available: http://es.wikipedia.org/wiki/Andrew_S._Tanenbaum.
- [24] "El modelo OSI y los Protocolos de Red." 2012.
- [25] "Nagios Open Source Network Monitoring System." 2010.
- [26] Mario Zaizar, "Resumen Protocolos de Monitorizacion," 2003, pp. 1–7.
- [27] "Modelo OSI," 27 de Abril, 2013. [Online]. Available: http://es.wikipedia.org/wiki/Modelo_OSI.
- [28] "Organización Internacional de Normalización," 15 de Abril, 2013. [Online]. Available: http://es.wikipedia.org/wiki/Organizaci%C3%B3n_Internacional_de_Normalizaci%C3%B3n.
- [29] "Virtualización - Wikipedia, la enciclopedia libre," 26 de Mayo, 2013. [Online]. Available: http://es.wikipedia.org/wiki/Virtualizaci%C3%B3n#M.C3.A1quina_virtual.
- [30] "Virtualización SO," 26 de Mayo, 2013. [Online]. Available: <http://www.tecnologiapyme.com/software/que-es-la-virtualizacion>.

- [31] Marisa López-Vallejo, Eduardo Huedo Cuesta, and Juan Garbajosa Sopeña, *Tecnologías para la eficiencia energética en los sistemas TI*. Madrid: , 2010.
- [32] M. C. Juárez, W. G. G. Herrera, and S. T. Sánchez, “Software libre vs software propietario Ventajas y desventajas,” 2006.
- [33] Luis Caballero Cruz, “Estado del Arte,” in *Sistema de Monitorización*, 2013, pp. 4, 15.
- [34] “Pandora FMS - Wikipedia, la enciclopedia libre,” 7 de Marzo, 2013. [Online]. Available: http://es.wikipedia.org/wiki/Pandora_FMS.
- [35] “Zabbix - Wikipedia, la enciclopedia libre,” 11 de Marzo, 2013. [Online]. Available: <http://es.wikipedia.org/wiki/Zabbix>.
- [36] E. G. S. Cruz, “Análisis del Rendimiento de Sistemas VoIP bajo Condiciones de Red Variable,” 2011.
- [37] “Servidor HTTP Apache - Wikipedia, la enciclopedia libre,” 29 de Mayo, 2013. [Online]. Available: http://es.wikipedia.org/wiki/Servidor_apache.

Anexos

Anexo 1 Procedimiento detallado para la instalación de Nagios	83
Anexo 2 Instalación del Addons NagiosGrapher	87
Anexo 3 Resultados de la Monitorización del FTP	88
Anexo 4 Servido Nagios	91
Anexo 5 Reporte obtenido con NagiosGrapher Balanceador	93
Anexo 6 Reporte obtenido con NagiosGrapher WIFIUHO-1	94
Anexo 7 Reporte obtenido con NagiosGrapher DNS-FH	94

Anexo 1 Procedimiento detallado para la instalación de Nagios

1. Soporte necesario

Partimos de una instalación limpia de nuestro sistema operativo Debian *squeese* en su versión 6.0.7 en una maquina virtual ejecutada desde una plataforma de virtualización llamada Promox VE. Lo primero que necesitamos es instalar nuestro entorno de compilación. Hay un paquete en Debian con todo lo que necesitas para ello.

Nota: Toda esta documentación fue realizada utilizando el Repositorio del Sistema Operativo ubicado en nuestro servidor por lo que no fue necesario invocar comandos externos para la instalación de addons.

```
root@control # apt-get install apache2 #damos enter y nos  
pedirá instalar una serie de librerías aceptamos
```

```
root@control # apt-get install build-essential # damos enter
```

2. Librerías

El segundo paso es instalar las librerías necesarias para, posteriormente, instalar Nagios. Necesitamos las jpeg, png y gd2. Estas librerías vienen con la distribución estable y son las que permiten visualizar los iconos en Nagios.

```
root@control # apt-get install libjpeg62 libjpeg62-dev  
libpng12-0 libpng12-dev libgd2 libgd2-dev
```

3. Grupos

Lo siguiente es crear los grupos y usuarios necesarios para Nagios:

```
root@control# useradd nagios
root@control# passwd nagios
root@control# groupadd nagios
root@control# groupadd nagcmd
root@control# usermod -G nagios nagios
root@control# usermod -G nagcmd nagios
root@control# usermod -G nagcmd www-data
```

Con esto hemos creado un nuevo usuario (nagios), le asignamos una contraseña, creamos dos grupos (nagios y nagcmd). Añadimos nagios a ambos grupos, el usuario www-data (el que usa Apache2) al grupo nagcmd y, por comodidad aunque no es indispensable, nuestro usuario común al grupo nagios para que la edición de ficheros de configuración nos resulte más cómoda.

Ya lo tenemos todo listo ahora solo falta instalar nagios y aquellos paquetes que nos pida durante el proceso de instalación, para ver que versión está disponible en nuestro servidor, con tan solo escribir *# aptitude search nagios* nos devolverá la versión de nuestro repo.

```
root@control # apt-get install nagios3
```

Creamos una contraseña para el acceso web del usuario nagiosadmin y reiniciamos apache:

```
root@control# htpasswd -c /etc/nagios3/htpasswd.users
nagiosadmin
root@control# /etc/init.d/apache2 reload
```

Y por último arrancamos nagios y, si no presenta ningún error, creamos un enlace para que de ahora en adelante arranque de forma automática al iniciar el servidor:

```
root@control# /etc/init.d/nagios3 start

root@control# ln -s /etc/init.d/nagios3
/etc/rcS.d/S99nagios3
```

Con esto nagios está totalmente funcional y accesible vía web a través de la URL “http://10.26.0.31/nagios3”. La configuración por defecto monitoriza algunos servicios en la propia máquina dónde se instala y nos debe de bastar para saber que funciona correctamente.

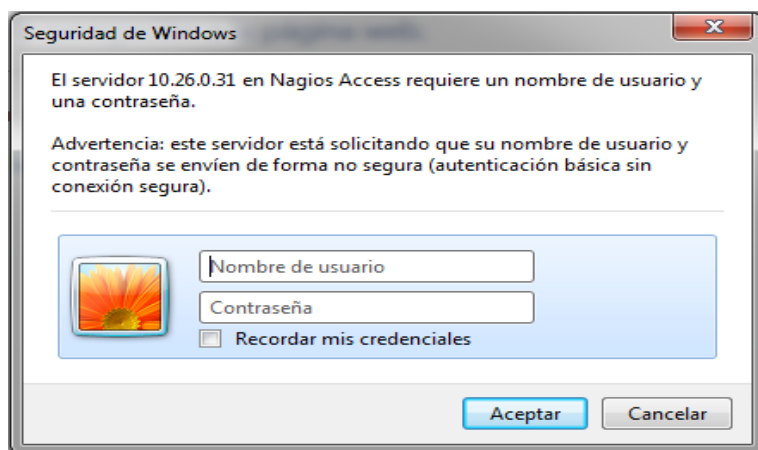


Figura 33. Autenticación de Nagios Interfaz Web

La siguiente imagen muestra la interfaz grafica de Nagios en funcionamiento.

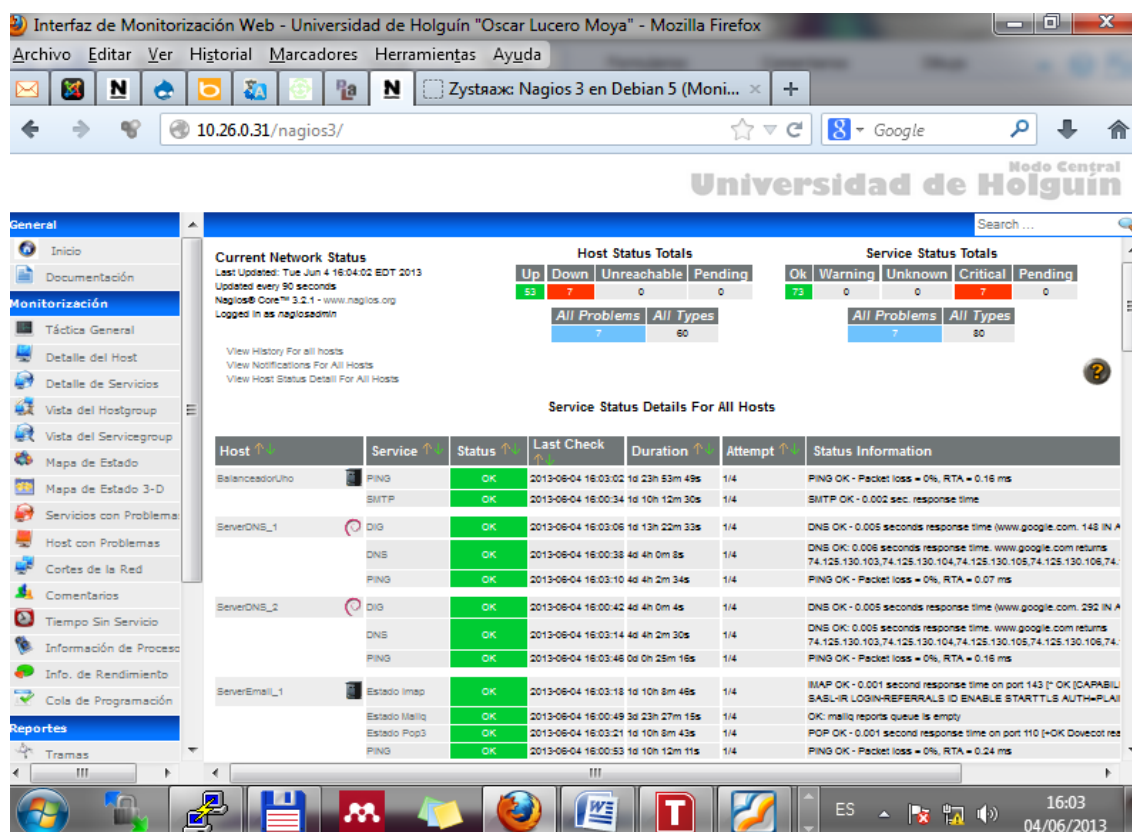


Figura 34. Interfaz Web de Nagios

Anexo 2 Instalación del Addons NagiosGrapher

Al igual que en anexo anterior se parte de una instalación limpia, es importante aclarar que como ya tenemos nuestro Nagios funcionando es preciso realizar alguna salva del mismo esto nos garantizara que si mientras estamos trabajando sobre Nagios y NagiosGrapher ocurra algún problema tendremos nuestro respaldo. Empezamos:

Nagiosgrapher (no confundir con Nagiosgraph que es otro diferente) es un programa que construye gráficas a partir de los datos que Nagios le da.

Instalación:

Esta herramienta se encuentra en los repositorios de Debian y para instalarla solo debemos llamar a instalar el paquete **nagiosgrapher**. Para instalarlo desde consola tendremos que ejecutar el siguiente comando:

```
root@control#: aptitude install nagiosgrapher
```

Editamos el fichero **/etc/nagios3/nagios.cfg** y añadimos las siguientes líneas:

```
process_performance_data=1
service_perfddata_command=ngraph-process-service-perfddata-pipe
```

Reiniciamos Nagios:

```
root@control#: /etc/init.d/nagios3 restart
```

Entonces Nagios ya enviará datos a NagiosGrapher.

Pasado un tiempo veremos cómo se han creado ficheros en la carpeta **/etc/nagiosgrapher/nagios3/serviceext**. Entonces volvemos a reiniciar Nagios para que coja estos ficheros:

```
root@control#: /etc/init.d/nagios3 restart
```

Ahora ya podremos ver en la página *Service Detail* unos iconos en la columna *Service* al lado del nombre de cada servicio.

Anexo 3 Resultados de la Monitorización del FTP

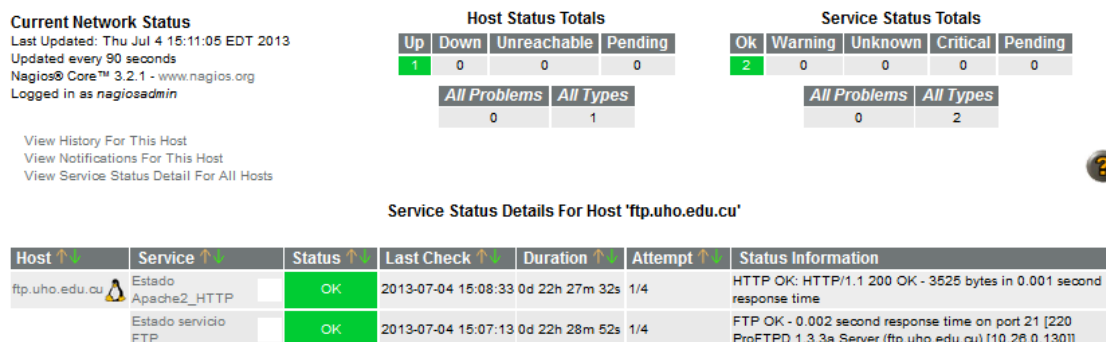


Figura 35.Estado servicios FTP

Disponibilidad del servicio: Reportes obtenidos. Estado Apache2_HTTP

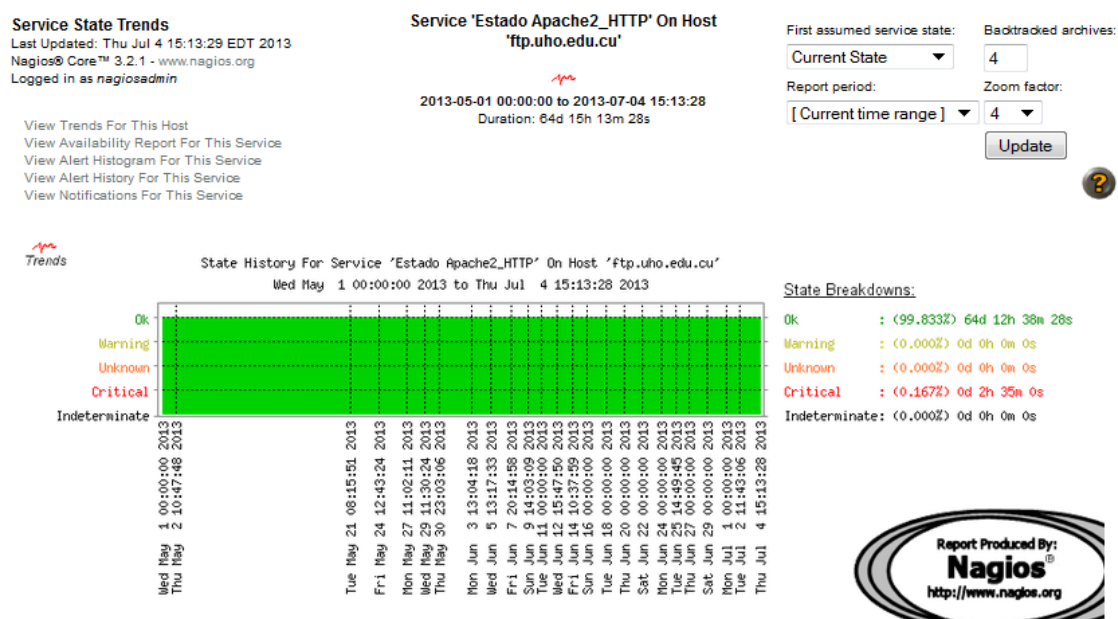


Figura 36. Trama Servicio Apache_HTTP. FTP-Uho

Service State Breakdowns:

State	Type / Reason	Time	% Total Time	% Known Time
OK	Unscheduled	64d 12h 40m 56s	99.833%	99.833%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	64d 12h 40m 56s	99.833%	99.833%
WARNING	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%
UNKNOWN	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%
CRITICAL	Unscheduled	0d 2h 35m 0s	0.167%	0.167%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 2h 35m 0s	0.167%	0.167%
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	64d 15h 15m 56s	100.000%	100.000%

Figura 37. Averías Servicio Apache_HTTP: FTP-Uho

Service Log Entries:

[View full log entries]

Event Start Time	Event End Time	Event Duration	Event/State Type	Event/State Information
2013-05-01 00:00:00	2013-05-02 10:47:48	1d 10h 47m 48s	SERVICE OK (HARD)	First Service State Assumed (Faked Log Entry)
2013-06-09 00:00:00	2013-06-09 00:11:50	0d 0h 11m 50s	SERVICE OK (HARD)	HTTP OK: HTTP/1.1 200 OK - 3525 bytes in 0.001 second response time
2013-06-11 00:00:00	2013-06-11 10:20:09	0d 10h 20m 9s	SERVICE OK (HARD)	HTTP OK: HTTP/1.1 200 OK - 3525 bytes in 0.001 second response time
2013-06-12 00:00:00	2013-06-12 15:47:50	0d 15h 47m 50s	SERVICE OK (HARD)	HTTP OK: HTTP/1.1 200 OK - 3525 bytes in 0.002 second response time
2013-06-12 15:47:50	2013-06-12 17:02:50	0d 1h 15m 0s	SERVICE CRITICAL (HARD)	No route to host
2013-06-12 17:02:50	2013-06-13 00:00:00	0d 6h 57m 10s	SERVICE OK (HARD)	HTTP OK: HTTP/1.1 200 OK - 3525 bytes in 0.108 second response time
2013-06-13 00:00:00	2013-06-14 00:00:00	1d 0h 0m 0s	SERVICE OK (HARD)	HTTP OK: HTTP/1.1 200 OK - 3525 bytes in 0.085 second response time
2013-06-14 00:00:00	2013-06-14 10:37:59	0d 10h 37m 59s	SERVICE OK (HARD)	HTTP OK: HTTP/1.1 200 OK - 3525 bytes in 0.001 second response time
2013-06-14 10:37:59	2013-06-14 11:07:59	0d 0h 30m 0s	SERVICE CRITICAL (HARD)	No route to host
2013-06-14 11:07:59	2013-06-14 11:41:26	0d 0h 33m 27s	SERVICE OK (HARD)	HTTP OK: HTTP/1.1 200 OK - 3525 bytes in 0.002 second response time
2013-06-15 00:00:00	2013-06-16 00:00:00	1d 0h 0m 0s	SERVICE OK (HARD)	HTTP OK: HTTP/1.1 200 OK - 3525 bytes in 0.008 second response time
2013-06-16 00:00:00	2013-06-16 22:54:26	0d 22h 54m 26s	SERVICE OK (HARD)	HTTP OK: HTTP/1.1 200 OK - 3525 bytes in 0.001 second response time
2013-06-17 00:00:00	2013-06-17 00:01:35	0d 0h 1m 35s	SERVICE OK (HARD)	HTTP OK: HTTP/1.1 200 OK - 3525 bytes in 0.091 second response time
2013-06-18 00:00:00	2013-06-19 00:00:00	1d 0h 0m 0s	SERVICE OK (HARD)	HTTP OK: HTTP/1.1 200 OK - 3525 bytes in 0.001 second response time
2013-06-19 00:00:00	2013-06-20 00:00:00	1d 0h 0m 0s	SERVICE OK (HARD)	HTTP OK: HTTP/1.1 200 OK - 3525 bytes in 0.001 second response time
2013-06-20 00:00:00	2013-06-20 23:21:19	0d 23h 21m 19s	SERVICE OK (HARD)	HTTP OK: HTTP/1.1 200 OK - 3525 bytes in 0.001 second response time
2013-06-21 00:00:00	2013-06-22 00:00:00	1d 0h 0m 0s	SERVICE OK (HARD)	HTTP OK: HTTP/1.1 200 OK - 3525 bytes in 0.083 second response time
2013-06-22 00:00:00	2013-06-23 00:00:00	1d 0h 0m 0s	SERVICE OK (HARD)	HTTP OK: HTTP/1.1 200 OK - 3525 bytes in 0.001 second response time
2013-06-23 00:00:00	2013-06-24 00:00:00	1d 0h 0m 0s	SERVICE OK (HARD)	HTTP OK: HTTP/1.1 200 OK - 3525 bytes in 0.001 second response time
2013-06-24 00:00:00	2013-06-25 00:00:00	1d 0h 0m 0s	SERVICE OK (HARD)	HTTP OK: HTTP/1.1 200 OK - 3525 bytes in 0.001 second response time
2013-06-25 00:00:00	2013-06-25 14:49:45	0d 14h 49m 45s	SERVICE OK (HARD)	HTTP OK: HTTP/1.1 200 OK - 3525 bytes in 0.001 second response time
2013-06-26 00:00:00	2013-06-27 00:00:00	1d 0h 0m 0s	SERVICE OK (HARD)	HTTP OK: HTTP/1.1 200 OK - 3525 bytes in 0.001 second response time
2013-06-27 00:00:00	2013-06-28 00:00:00	1d 0h 0m 0s	SERVICE OK (HARD)	HTTP OK: HTTP/1.1 200 OK - 3525 bytes in 0.001 second response time

Figura 38. Entradas del registro del servicio Apache2_HTTP: FTP-Uho

Disponibilidad del servicio: Reportes obtenidos. Estado Servicio FTP

Service State Breakdowns:

State	Type / Reason	Time	% Total Time	% Known Time
OK	Unscheduled	64d 12h 31m 21s	99.813%	99.813%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	64d 12h 31m 21s	99.813%	99.813%
WARNING	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%
UNKNOWN	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%
CRITICAL	Unscheduled	0d 2h 54m 20s	0.187%	0.187%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 2h 54m 20s	0.187%	0.187%
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	64d 15h 25m 41s	100.000%	100.000%

Figura 39. Averías Servicio FTP

Service Log Entries:

[View full log entries]

Event Start Time	Event End Time	Event Duration	Event/State Type	Event/State Information
2013-05-01 00:00:00	2013-05-02 10:47:48	1d 10h 47m 48s	SERVICE OK (HARD)	First Service State Assumed (Faked Log Entry)
2013-06-09 00:00:00	2013-06-09 00:11:50	0d 0h 11m 50s	SERVICE OK (HARD)	FTP OK - 0.002 second response time on port 21 [220 ProFTPD 1.3.3a Server (ftp.uho.edu.cu) [10.26.0.130]]
2013-06-11 00:00:00	2013-06-11 10:20:09	0d 10h 20m 9s	SERVICE OK (HARD)	FTP OK - 0.002 second response time on port 21 [220 ProFTPD 1.3.3a Server (ftp.uho.edu.cu) [10.26.0.130]]
2013-06-12 00:00:00	2013-06-12 02:05:12	0d 2h 5m 12s	SERVICE OK (HARD)	FTP OK - 0.002 second response time on port 21 [220 ProFTPD 1.3.3a Server (ftp.uho.edu.cu) [10.26.0.130]]
2013-06-12 02:05:12	2013-06-12 02:10:03	0d 0h 4m 51s	SERVICE CRITICAL (HARD)	CRITICAL - Socket timeout after 10 seconds
2013-06-12 02:10:03	2013-06-12 15:49:40	0d 13h 39m 37s	SERVICE OK (HARD)	FTP OK - 0.002 second response time on port 21 [220 ProFTPD 1.3.3a Server (ftp.uho.edu.cu) [10.26.0.130]]
2013-06-12 15:49:40	2013-06-12 17:04:40	0d 1h 15m 0s	SERVICE CRITICAL (HARD)	No route to host
2013-06-12 17:04:40	2013-06-13 00:00:00	0d 6h 55m 20s	SERVICE OK (HARD)	FTP OK - 0.002 second response time on port 21 [220 ProFTPD 1.3.3a Server (ftp.uho.edu.cu) [10.26.0.130]]
2013-06-13 00:00:00	2013-06-14 00:00:00	1d 0h 0m 0s	SERVICE OK (HARD)	FTP OK - 0.004 second response time on port 21 [220 ProFTPD 1.3.3a Server (ftp.uho.edu.cu) [10.26.0.130]]
2013-06-14 00:00:00	2013-06-14 10:38:39	0d 10h 38m 39s	SERVICE OK (HARD)	FTP OK - 0.002 second response time on port 21 [220 ProFTPD 1.3.3a Server (ftp.uho.edu.cu) [10.26.0.130]]
2013-06-14 10:38:39	2013-06-14 11:08:39	0d 0h 30m 0s	SERVICE CRITICAL (HARD)	No route to host
2013-06-14 11:08:39	2013-06-14 11:41:26	0d 0h 32m 47s	SERVICE OK (HARD)	FTP OK - 0.003 second response time on port 21 [220 ProFTPD 1.3.3a Server (ftp.uho.edu.cu) [10.26.0.130]]
2013-06-15 00:00:00	2013-06-16 00:00:00	1d 0h 0m 0s	SERVICE OK (HARD)	FTP OK - 0.002 second response time on port 21 [220 ProFTPD 1.3.3a Server (ftp.uho.edu.cu) [10.26.0.130]]

Figura 40. Entradas del registro del servicio FTP: FTP-Uho

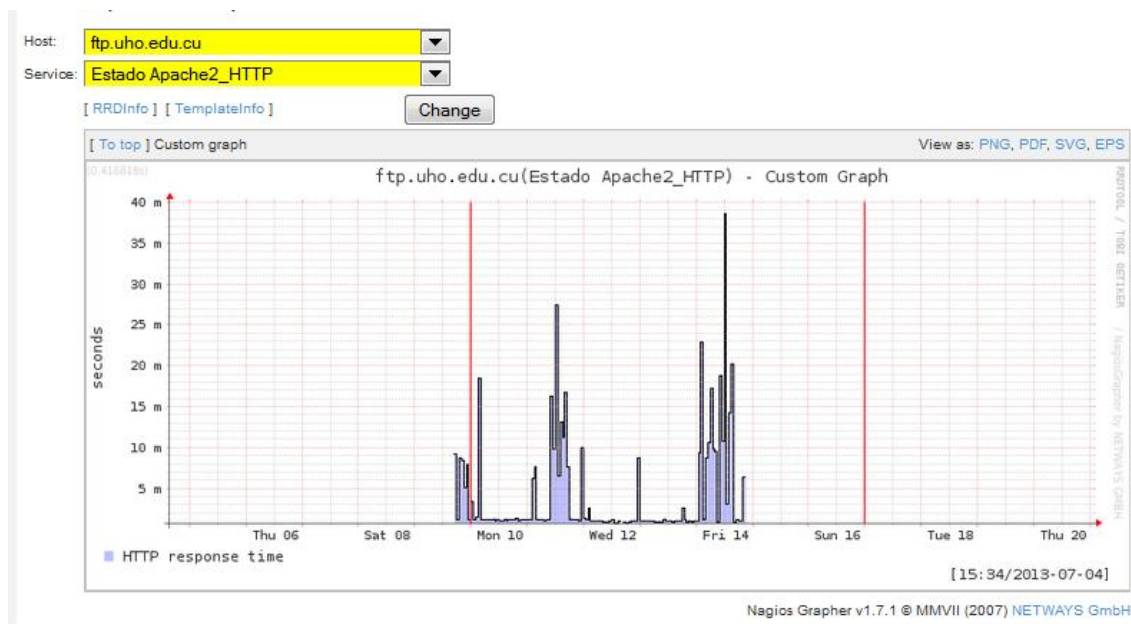


Figura 41.NagiosGrapher: Servicio Apache2_HTTP: FTP-Uho

Anexo 4 Servido Nagios

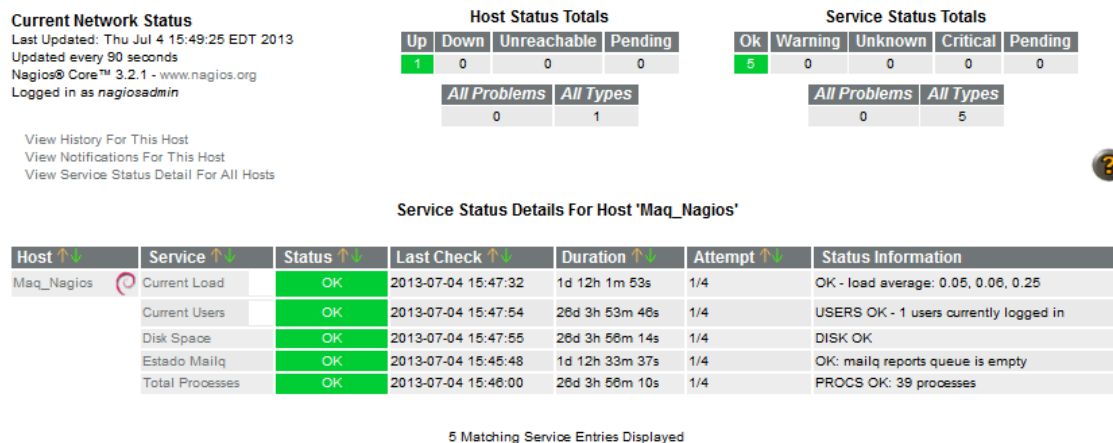


Figura 42. Estado de los servicio en el Servidor Nagios

Trama de Nagios desde Enero 2013

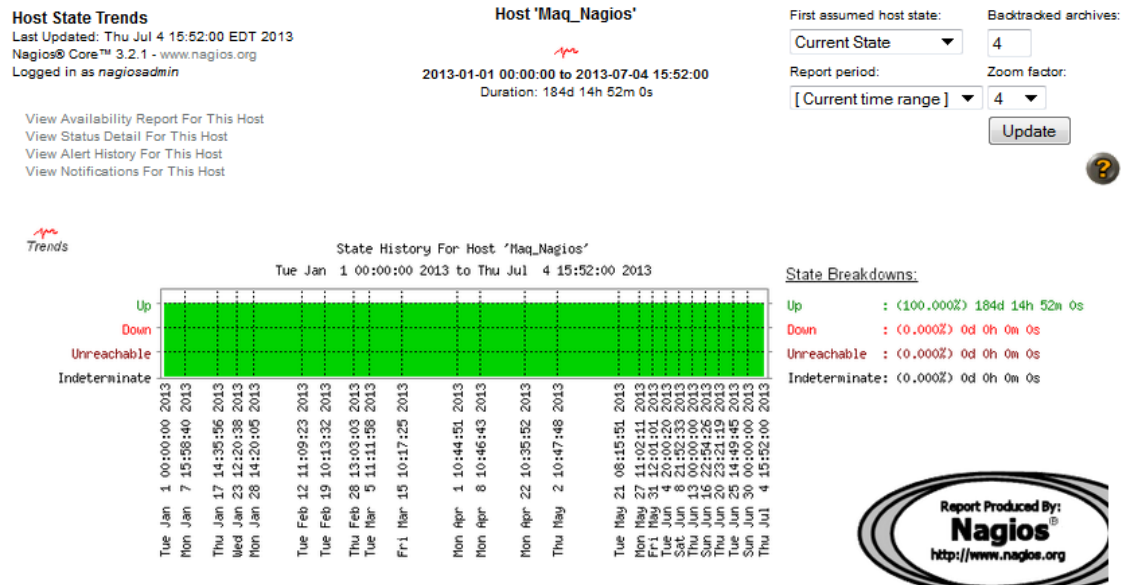


Figura 43. Trama Servidor Nagios

Disponibilidad Servidor Nagios

[Availability report completed in 0 min 1 sec]

Host State Breakdowns:

State	Type / Reason	Time	% Total Time	% Known Time
UP	Unscheduled	184d 14h 54m 3s	100.000%	100.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	184d 14h 54m 3s	100.000%	100.000%
DOWN	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%
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	184d 14h 54m 3s	100.000%	100.000%

Figura 44. Averías Servidor Nagios

State Breakdowns For Host Services:

Service	% Time OK	% Time Warning	% Time Unknown	% Time Critical	% Time Undetermined
Current Load	99.857% (99.857%)	0.055% (0.055%)	0.000% (0.000%)	0.089% (0.089%)	0.000%
Current Users	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
Disk Space	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
Estado Mailq	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
Total Processes	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
Average	99.971% (99.971%)	0.011% (0.011%)	0.000% (0.000%)	0.018% (0.018%)	0.000%

Host Log Entries:
[View full log entries]

Event Start Time	Event End Time	Event Duration	Event/State Type	Event/State Information
2013-01-01 00:00:00	2013-01-07 15:58:40	6d 15h 58m 40s	HOST UP (HARD)	First Host State Assumed (Faked Log Entry)
2013-06-09 00:00:00	2013-06-09 00:11:50	0d 0h 11m 50s	HOST UP (HARD)	PING OK - Packet loss = 0%, RTA = 0.04 ms
2013-06-11 00:00:00	2013-06-11 10:20:09	0d 10h 20m 9s	HOST UP (HARD)	PING OK - Packet loss = 0%, RTA = 0.05 ms
2013-06-12 00:00:00	2013-06-13 00:00:00	1d 0h 0m 0s	HOST UP (HARD)	PING OK - Packet loss = 0%, RTA = 0.05 ms
2013-06-13 00:00:00	2013-06-14 00:00:00	1d 0h 0m 0s	HOST UP (HARD)	PING OK - Packet loss = 0%, RTA = 0.06 ms
2013-06-14 00:00:00	2013-06-14 11:41:26	0d 11h 41m 26s	HOST UP (HARD)	PING OK - Packet loss = 0%, RTA = 0.05 ms
2013-06-15 00:00:00	2013-06-16 00:00:00	1d 0h 0m 0s	HOST UP (HARD)	PING OK - Packet loss = 0%, RTA = 0.06 ms
2013-06-16 00:00:00	2013-06-16 22:54:26	0d 22h 54m 26s	HOST UP (HARD)	PING OK - Packet loss = 0%, RTA = 0.05 ms
2013-06-17 00:00:00	2013-06-17 00:01:35	0d 0h 1m 35s	HOST UP (HARD)	PING OK - Packet loss = 0%, RTA = 0.06 ms
2013-06-18 00:00:00	2013-06-19 00:00:00	1d 0h 0m 0s	HOST UP (HARD)	PING OK - Packet loss = 0%, RTA = 0.04 ms
2013-06-19 00:00:00	2013-06-20 00:00:00	1d 0h 0m 0s	HOST UP (HARD)	PING OK - Packet loss = 0%, RTA = 0.06 ms
2013-06-20 00:00:00	2013-06-20 23:21:19	0d 23h 21m 19s	HOST UP (HARD)	PING OK - Packet loss = 0%, RTA = 0.06 ms
2013-06-21 00:00:00	2013-06-22 00:00:00	1d 0h 0m 0s	HOST UP (HARD)	PING OK - Packet loss = 0%, RTA = 0.05 ms
2013-06-22 00:00:00	2013-06-23 00:00:00	1d 0h 0m 0s	HOST UP (HARD)	PING OK - Packet loss = 0%, RTA = 0.06 ms
2013-06-23 00:00:00	2013-06-24 00:00:00	1d 0h 0m 0s	HOST UP (HARD)	PING OK - Packet loss = 0%, RTA = 0.05 ms

Figura 45.Entradas del registro del Servidor Nagios.

Anexo 5 Reporte obtenido con NagiosGrapher Balanceador

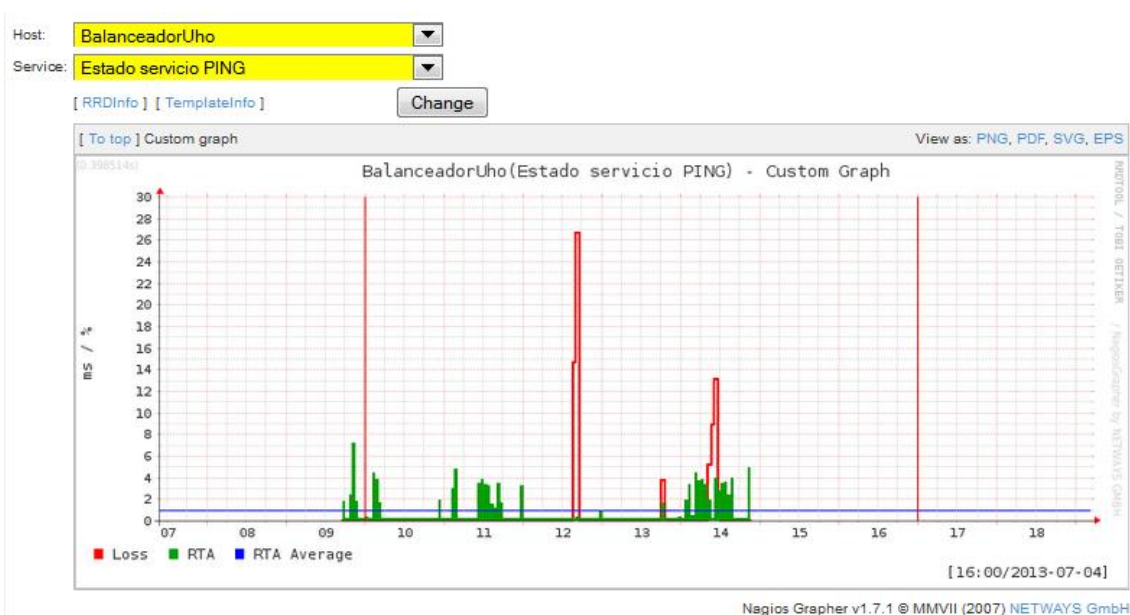


Figura 46. NagiosGrapher Balanceador Servicio PING

Anexo 6 Reporte obtenido con NagiosGrapher WIFIUHO-1

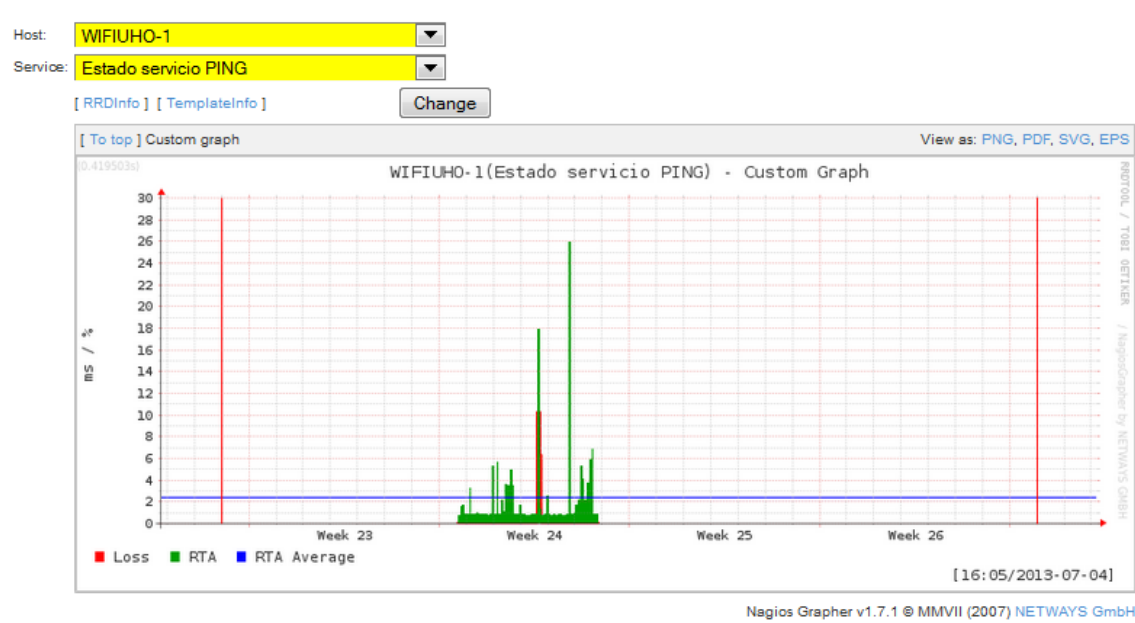


Figura 47.NagiosGrapher WIFIUHO-1 Servicio PING

Anexo 7 Reporte obtenido con NagiosGrapher DNS-FH

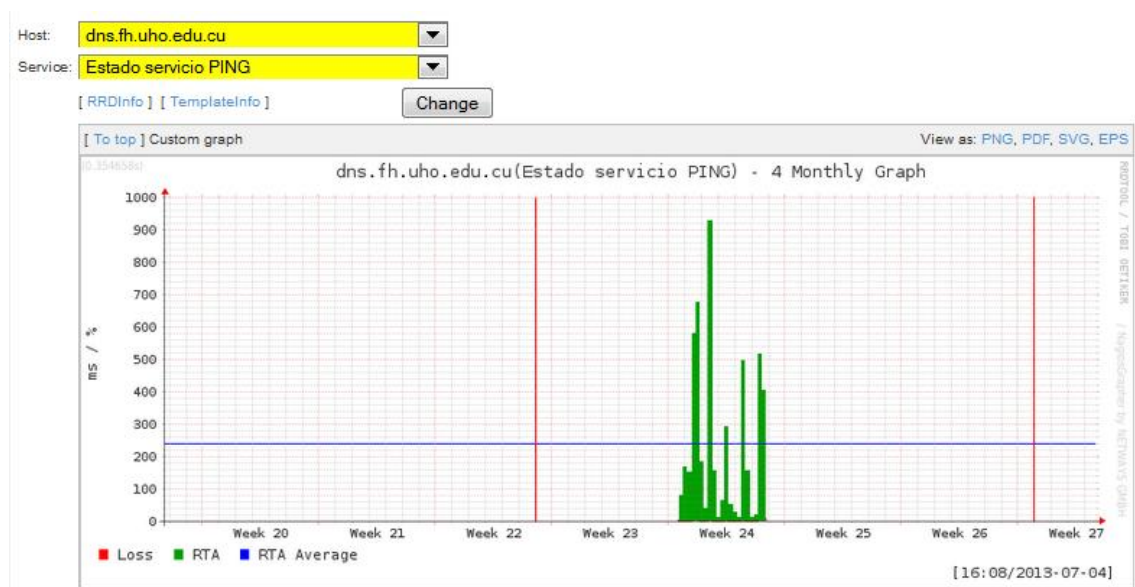


Figura 48.NagiosGrapher DNS-FH Servicio PING