ISSN 1390 – 9770

Rev. SINAPSIS, Edición Nº 11, Vol. 2, Diciembre 2017

Implementación de los sistemas de gestión de la red en dos universidades americanas.

Implementation of network management systems in two American universities.

Implementación de un Sistema de Gestión de Red.

Autores: Manuel José Linares Alvaro, MSc.(1)

Ing. Ligia Sánchez Parrales(2)

Ing. Kleber Germiniano Marcillo Parrales.(3)

(1) Universidad de Granma, Cuba. Departamento de Redes. (cheche@udg.co.cu)

(2) Instituto Tecnológico Superior "Portoviejo", Manabí, Ecuador (ligia1980@live.com)

(3) Universidad Estatal del Sur de Manabí, Ecuador.

Contacto: cheche@udg.co.cu

Receptado: 20/09/2017 Aceptado: 13/11/2017

Resumen.

En este trabajo se describen tanto los diferentes pasos que se siguieron como las aplicaciones que se seleccionaron y emplearon para la implementación del sistema de gestión de la red, primero en Universidad de Granma, y luego en el Instituto Tecnológico Superior "Portoviejo" (ITSUP), empleando para ello software libre, también tiene el propósito de demostrar la factibilidad de la implementación de un sistema de gestión en cualquier institución. Actualmente, como resultado de este trabajo, Tanto la Universidad de Granma como en ITSUP, cuentan con un sistema para monitorear la red que ha contribuido a la disminución significativa de los tiempos de interrupciones por fallas en los servicios, detección de ataques, intrusos y programas malignos en la red y una optimización en el empleo de las Tecnologías de la Información, sobre todo, en el uso de los canales de transmisión de datos. Se demuestra que aunque a primera vista, un sistema de gestión puede resultar costoso, la inversión puede reducirse notablemente, empleando software libre, pues existe una amplísima gama de aplicaciones muy eficaces y completas, que se pueden utilizar sin pagar por su empleo, modificación o distribución.

Palabras clave: Gestión de Redes, Sistemas de Gestión de Redes, Monitoreo de redes, Modelos de Gestión de Redes

Abstract.

This work describes the steps followed and the applications that were selected and applied for the implementation of the network management system, first at the University of Granma and then at the ITSUP, using free software, is also intended to demonstrate the feasibility of implementing a management system in any institution. Currently, as a result of this work, both the University of Granma and ITSUP, have a system to monitor the network that has contributed to a significant decrease in interruption times due to service failure, detection of attacks, intruders and programs malignancies in the network and an optimization in the use of Information Technologies, especially in the use of data transmission channels. It is shown that, although at first glance, a management system can be expensive, investment can be significantly reduced, using free software, since there is a very wide range of very efficient and complete applications that can be used without paying for their use, modification or distribution.

Key words: Network Management, Network Management Systems, Network Monitoring, Network Management Models.

Introducción

Autores como Marrero y Hernández (2016), señalan que la importancia adquirida por las tecnologías de la información para el crecimiento y desarrollo de las organizaciones ha impulsado la evolución del concepto de gestión de infraestructuras al concepto de implantación de procesos para la gestión de servicios de estas tecnologías; con respecto a esto, otros autores, son del criterio que en el mundo actual, las organizaciones dependen cada vez más de las TI, con el propósito de apoyar los procesos que en ellas se desarrollan y cumplir con las necesidades de los clientes, por ello, los servicios de TI están siendo cada vez más utilizados para apoyar y automatizar las actividades de una organización, con el fin de conseguir aumentar la competitividad de ésta y mejorar su funcionamiento a través de la generación de valores y la reducción de costes. De esta manera, un correcto funcionamiento de estos servicios es fundamental para la organización y por esta razón, es preciso llevar a cabo una adecuada gestión de los mismos. (Pastor, 2015).

Los principales problemas relacionados con la expansión de las redes son la gestión de su correcto funcionamiento día a día y la planificación estratégica de su crecimiento. De hecho se estima que más del 70 % del coste de una red corporativa se atribuye a su gestión y operación. Por todo ello, la gestión de redes, como conjunto de actividades dedicadas al control y vigilancia de recursos de telecomunicación, se ha convertido en un aspecto de enorme importancia en el mundo de las telecomunicaciones. (Pérez, 2013)

Desafortunadamente, en la actualidad, el procedimiento de gestión y monitoreo de redes, resulta una actividad que se descuida con frecuencia, sobre todo en entidades medianas y pequeñas.

La Universidad de Granma (UdG), ubicada en la provincia que lleva este mismo nombre, abarca desde hace algunos años toda la región, pues tiene presencia en cada uno de los municipios que forman la provincia, de ahí que su red de ordenadores, sea una de las más grandes a nivel provincial, tanto en extensión como en cantidad de ordenadores y servicios y llegue a todas las extensiones, sedes y dependencias de la institución. La red y sus servicios comenzaron a funcionar en diciembre de 1996, sin embargo, no fue hasta el 2005, que se comenzaron a implementar algunas herramientas para monitorear el funcionamiento de la red pues antes de esta fecha no existían sistemas que garantizaran tanto la calidad y estabilidad de los servicios suministrados como la seguridad de la información que en sus servidores se almacenaba. Por su parte, el ITSUP, es una entidad ubicada en Portoviejo, Provincia de Manabí, el cual tiene ya más de 20 años de fundado, funciona como unidad educativa durante las mañanas y parte de la tarde, mientras que durante las noches, se desempeña como instituto.

Partiendo de lo antes expuesto, puede señalarse como **problema** existente, la carencia de un sistema de gestión que permita tener una visión global del estado de la red de las instituciones antes señaladas (UdG e ITSUP), y conocer en tiempo real o diferido, la situación de los servicios de sus principales nodos o centros de datos, su infraestructura y seguridad, el estado de los enlaces y equipos que componen la estructura fundamental de la red y la disponibilidad de los servicios brindados.

Esta investigación tuvo como **objetivo**, implementar un sistema de gestión y monitoreo para la red de la Universidad de Granma. Luego, la experiencia acumulada, se utilizó con la misma finalidad para el ITSUP.

Se establecieron como objetivos específicos:

- Seleccionar un modelo de gestión adecuado para la red de la Universidad de Granma.
- Implementar las herramientas de gestión que complementen el modelo.
- Demostrar la factibilidad del uso de herramientas de gestión basadas en software libre.

Se definieron, como **objeto de estudio** la gestión de redes y como **campo de acción** los modelos de referencia y herramientas de gestión de redes que se emplean actualmente a nivel internacional.

Materiales y métodos.

El proceso de implementación del sistema de gestión de redes de la Universidad de Granma, comenzó en 2005, y se caracterizaba por el empleo de herramientas aisladas, como el MRTG y el Nagios, sin embargo, no fue hasta 2012 que la gestión de la red en la mencionada entidad, comenzó a diseñarse como un sistema organizado e integrador, basado en la aplicación de modelos respaldados por normas internacionales, para lo cual se establecieron pautas en la selección de las herramientas o software a emplear y cuyo perfeccionamiento, mejoras, actualizaciones e introducción de nuevas aplicaciones se ha extendido hasta la fecha actual.

Por otra parte, en el ITSUP la situación era similar, y hasta el año 2015, no existía en este instituto un sistema que permitiera gestionar y monitorear la red, el cual se implementó de acuerdo a la experiencia acumulada en la Universidad de Granma, a partir de los convenios de trabajo y colaboración existente entre ambas entidades.

Esta investigación contó de varias etapas: Revisión del estado del arte sobre los procesos de gestión de red, elección del modelo de gestión a seguir, la elección de las herramientas para implementar el modelo y la implementación de éstas.

Modelos de gestión de redes.

Los modelos de gestión se ocupan de normalizar la información gestionada, y el modo en que se deben llevar a cabo las comunicaciones en cuanto a protocolo y servicios de gestión, con el propósito de conseguir interoperabilidad entre gestor y agentes. (Pérez, 2013). En este sentido es preciso destacar que los modelos solo definen *qué* se puede gestionar y *cómo* se puede hacer. (Marrero & Hernández, 2016). Por otra parte, hay que señalar que para cada problema en cuestión, puede existir más de un modelo a aplicar, por lo que es importante conocer el ámbito de actuación en la organización, además resulta imprescindible el comprometimiento e implicación absolutos de la dirección de la entidad con el proceso, de manera tal que se logre una implantación en toda la organización y no solo en las áreas claves de ésta. (Ibáñez, 2012)

Los modelos de referencia constituyen marcos conceptuales introducidos con la finalidad de organizar las tareas y funciones que forman parte de la gestión de redes y proveen numerosos beneficios a las organizaciones, entre los que se destacan competitividad, eficiencia en infraestructura de TI y un alineamiento de estas tecnologías que contempla las metas de la organización en la que se implementan. (Clemm, 2007)

Selección del modelo para el sistema de gestión de la red.

Durante el desarrollo del proyecto, se analizaron varios modelos de gestión tales como el modelo TMN (Telecommunications Management Network), FCAPS (Fault, Configuration, Accounting, Performance and Security, modelo de la ISO para la interconexión de sistemas abiertos), eTOM (modelo de gestión que se inició en el TeleManagement Forum en el 2001), COBIT (desarrollado por la Asociación de Auditoría y Control de Sistemas de Información o Information Systems Audit and Control Association, ISACA) e ITIL (Information Technology Infrastructure Library o Librería de Infraestructura de Tecnologías de Información, conjunto de buenas prácticas de gestión de servicios, desarrollado por el "Office of Government Commerce" del Reino Unido y aceptado en todo el mundo como estándar de facto).

Luego de valorar las ventajas, desventajas, complejidad para su implementación y características que ofrecía cada uno de los modelos, se optó por emplear el FCAPS, por sus facilidades para establecer de manera sencilla, rápida y eficiente los diferentes procesos necesarios para implementar un adecuado sistema de gestión de red. Este modelo, constituye uno de los que tiene mayor aceptación y uso. (Gómez & González, 2013)

Como se ha mencionado, FCAPS, es el modelo de gestión recomendado por la ISO (International Organization for Standardization) para la interconexión de sistemas abiertos, y expresa cinco categorías en las que el modelo divide las funciones de la gestión de redes: fallos, configuración, contabilidad, desempeño y seguridad: (Ding, 2009), (ISO, 1997), (Gómez & González, 2013).

Selección e implementación de las herramientas de gestión.
Para la selección de las herramientas a utilizar, se establecieron cuatro requisitos específicos, que todo el software seleccionado debería cumplir incondicionalmente:

- Herramientas basadas Software libre y código abierto.
- Todas las aplicaciones deberían tener una Interface Web.
- Preferencia por software diseñado para sistemas operativos de tipo Linux.
- El software seleccionado deberían contar con un amplio respaldo bibliográfico, una extensa experiencia en su utilización y aplicación.

Luego siguieron varios años de ensayos, pruebas, actualizaciones, tentativas y selección de sistemas, de hecho se trata de un proceso que está en constante perfeccionamiento y evolución. Cabe señalar que siempre se partió de criterios de "monitorear todo lo que fuera monitoreable", pues en el campo de las redes, es imposible predecir qué tipo de información puede ser útil, necesaria o decisiva en una situación determinada, así en la actualidad, se ha logrado chequear en todo momento, desde el tamaño de las colas de correos en los servidores de email, el nivel de actualización de los sistemas antivirus, el espacio en sus discos, hasta la entrada y autenticación de usuarios en éstos.

Resultados y discusión.

En la tabla 1, se muestran las aplicaciones que han sido seleccionadas y se emplean en este momento, asociadas con la categoría del proceso de gestión de la red de acuerdo al modelo FCAPS, con un resumen de su función o empleo.

Categorías	Software o Aplicación empleado	Función (resumida)
Gestión de la configuración	NetDot	Documentación de la red, gestión de inventarios y activos, etc.
	Bacula	Gestión de los resguardos de las configuraciones
	Nagios	Registros de topología dinámicos
	OCS Inventory	Gestión de Inventarios.
	Rancid	Control de versiones y configuraciones en routers y switchs
Gestión de Fallos	Nagios	Este software es capaz de detectar servicios detenidos e intentar arrancar el mismo, notificando el evento.
	LightSquid	Herramienta para analizar en tiempo diferido, el acceso a internet por parte de los usuarios de la UdG

Gestión de los registros y contabilidad	SARG	Similar al anterior.
	SQStat	Herramienta para analizar en tiempo real, el acceso a internet por parte de los usuarios de la UdG
	FreeSA	Similar al LightSquid y SARG.
	Webalizer	Similar al LightSquid, SARG y FreeSA, pero más orientado a resúmenes estadísticos generales que al análisis por usuario.
	Sendmail Analyzer	Análisis del comportamiento del tráfico de correos y todos lo relacionado con éste.
	OCS Inventory	Inventarios de los activos de TI.
Gestión del desempeño	MRTG	Herramientas muy usadas en la gestión del tráfico y el rendimiento. Utilizado para tener una idea rápida del comportamiento del ancho de banda en las diferentes interfaces de los dispositivos de la red, canales de enlaces, interfaces de red en los servidores, etc. El Cacti es similar al MRTG, pero más moderno y configurable.
	Cacti	
	FlowViewer	Herramientas similares al NetFlow de Cisco. Determinantes tanto para gestionar desempeño por protocolo de alto nivel, como la seguridad.
	NFsen+NFsight+SSHCUre	
	SmokePing	Magnifico software para monitorear los tiempos de retardo de la red y los servicios.
	LibreNMS	Aplicación para chequear la disponibilidad de los recursos de la red.
	Nagios	Completísima herramienta para monitorear disponibilidad de hardware y servicios.
Gestión de Seguridad	NFsen+NFsight+SSHCUre	Herramientas similares al NetFlow de Cisco. Determinantes tanto para gestionar desempeños por protocolos de alto nivel, como la seguridad.
	Flow Viewer	
	OSSIM	Sistema de detección de intrusos y eventos de seguridad.
	Bacula	Muy completo sistema de resguardos.
	SmokePing	Magnifico software para monitorear los tiempos de retardo de la red y los servicios.
	MRTG	Utilizado para tener una idea rápida del comportamiento del ancho de banda en los diferentes routers, canales de enlaces, interfaces de red en los servidores, etc.
	Cacti	

Tabla 1. Categorías en el sistema de gestión implementado, asociadas al software que se emplea para su implementación.

Caracterización general de las principales aplicaciones seleccionadas para desarrollar el sistema de gestión de la red universitaria.

MRTG (Multi Router Transfer Grapher - http://oss.oetiker.ch/mrtg/). Empleado para supervisar en tiempo real, una gran cantidad de dispositivos, servicios y aplicaciones, principalmente ruteadores y switchs. (Oetiker, 2012). También se pueden implementar otras funcionalidades utilizando las tablas MIBS de los diferentes equipos y el protocolo SNMP. Por ejemplo, en esta experiencia se empleó con mucho éxito tanto en el chequeo del consumo de ancho de banda en las diferentes interfaces de red de los dispositivos, como en la supervisión de las temperaturas y voltajes de routers, switchs y otros; a modo de ejemplo, en la figura 1 se muestran gráficos generados con MRTG, sobre las temperaturas del local del nodo central de la red de la Universidad y la carga del procesador de su router principal.

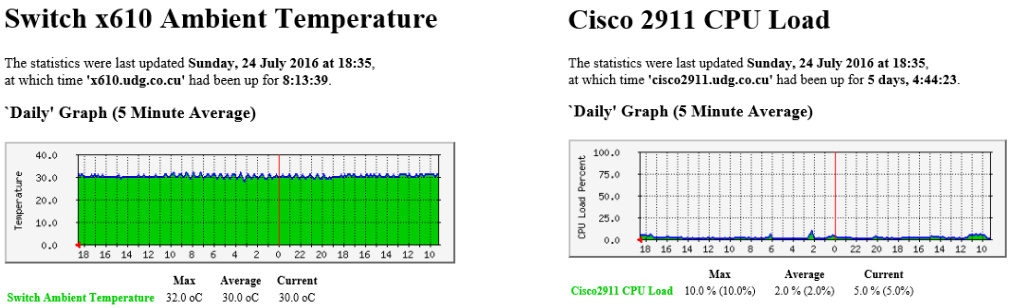

Figura 1. Graficos generados por MRTG. Izquierda: temperaturas promedio del local donde se encuentran los servidores principales de la UdG. Derecha: Carga del procesador o CPU del router – Firewall principal.

Esta herramienta también se utiliza para graficar en el transcurso del tiempo, el comportamiento de las colas en los servidores de correos, la cantidad de mensajes rechazados, la cantidad de correos contaminados con virus y aquellos clasificados como SPAM. Actualmente se está tratando de reemplazar el MRTG por el Cacti, sin embargo, el grupo de especialistas de la red, afirman que aunque el segundo tiene mejor aspecto gráfico, y mayores facilidades para agregar dispositivos, MRTG es más fácil y simple de utilizar, pues no requiere contraseñas ni procesos de autenticación para visualizar la información que genera.

NFSEN, NFSight y SSHCure. (http://nfsen.sourceforge.net/). Se trata de un sensor para NetFlow. De acuerdo a su sitio web oficial, constituye de una interfaz gráfica basada en web para las herramientas Netflow de Cisco y Nfdump (colector de datos de flujos). Entre sus prestaciones más sobresalientes se encuentran (Haag, N.A), la visualización de los datos de NetFlow: flujos, paquetes y bytes utilizando RRD, navegación simple a través de la web y datos de NetFlow, procesamiento y filtrado de datos netflow por períodos de tiempo, creación secuencias históricas, así como perfiles continuos, sistema condicional para el establecimiento de avisos o alertas y la capacidad para la instalación de plugins que aumenten sus potencialidades y facilidades.

Gracias a esta poderosa herramienta, se puede conocer de manera real o diferida, datos específicos sobre el tráfico generado desde o hacia un host, servicio, puerto o protocolo determinado. También constituye una herramienta de seguridad, pues podría permitir al personal encargado investigar, (por solo citar un ejemplo), si ha tenido lugar algún tipo de tráfico desde una dirección IP, para un protocolo y un destino determinados.

El gráfico 2, muestra el ancho de banda consumido por los usuarios navegando en redes públicas (Internet), a través de los dos proveedores de servicios con que cuenta la UdG (InfoCom y RedUniv). Cabe mencionar que las curvas muestran valores relativamente bajos debido a que el momento en

que se tomó esta imagen la entidad está cerrada por estar todo su personal de vacaciones y son muy pocos los usuarios que utilizan los servicios de la red, por lo que el tráfico que se consume, es mínimo. En el esquema se aprecian 3 curvas: una roja para el ancho de banda que se consume a través del proveedor RedUniv, otra verde representando el consumido a través de InfoCom y una curva azul que representa el ancho de banda total.

Gráfico 2. Ancho de banda consumido por la Universidad de Granma en acceso a redes públicas.

Es importante mencionar que este software posee además un rápido y poderoso motor de filtros, que permite que todos los flujos sean depurados antes de que se traten con posterioridad. (Haag, N.A). Tan poderosos resultan los filtros, que podrían considerarse un pseudolenguaje que permite obtener información aún más detallada de los diferentes flujos que representa. Ejemplo de ello lo constituye el propio gráfico 2, el cual es generado filtrando todos los flujos con la condición de que no provengan de redes cubanas universitarias y cuya entrada de datos sea a través de las interfaces de conexión para el enlace con los proveedores de servicios y los puertos de origen de los datos de los flujos sean el 80 o el 443.

A esta poderosa herramienta, se le han instalado plugins como el SSHcure, que muestra procesos de reconocimientos hechos a la red en busca de servicios SSH abiertos, en períodos previos de 24 horas o más. Otro “plugin” que ha resultado extremadamente útil en el proceso de gestión de la red

universitaria, lo constituye el NFSight. (https://sourceforge.net/p/nfsight/home/Nfsight/). Es conocido que la detección de procesos de reconocimiento o "scaneos" hechos a los servicios y activos de una red, es fundamental para tener una idea de posibles ataques y del estado general del sistema, pero se requiere de un conjunto de complejas herramientas para recoger, procesar, y representar los datos, de manera práctica y eficiente. NFSight brinda una solución flexible y práctica para la visualización de la actividad de la red, y suministra de manera rápida y gráfica puntos de vista sobre el estado de los activos de ésta, además construye flujos bidireccionales y los aprovecha para la detección e identificación de actividad cliente/servidor y la detección de intentos de intrusión. (Berthier et al., 2010).

La Figura 3, muestra como el host con dirección IP 5.254.66.144, ha estado realizando un reconocimiento de la red, en busca de servidores web, en el período de tiempo comprendido entre las 13:20 y las 16:30 horas del día 24 de julio de 2016, apreciándose, por el color de los puntos, que no obtuvo ninguna respuesta por parte de los servidores de la red de la entidad tratada, por lo tanto, no hay posibilidad de que se haya comprometido la seguridad de los sistemas.

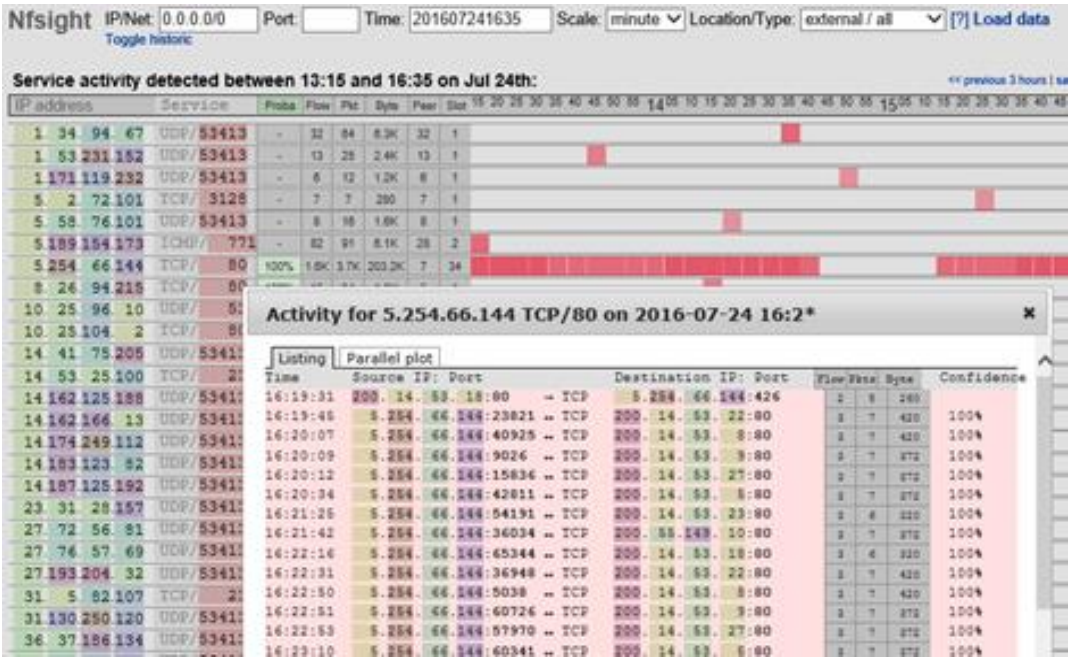

Figura 3. Interfaz de NFSigh que muestra la actividad de la red desde hosts externos, en un rango de tiempo determinado.

Nagios. (http://www.nagios.org). Una de las principales utilidades para gestionar la red de la UdG. Según su equipo de desarrollo, se trata de una aplicación libre y de código abierto, muy ampliamente utilizada, capaz de vigilar tanto equipos o hardware como y servicios o software, cuenta con una interfaz web para la monitorización y manejo y chequea tanto servicios de red (SMTP, POP3, HTTP,

SNMP, etc) como recursos de hardware en ordenadores o dispositivos (carga del procesador, uso de los discos, memoria, estado de los puertos, etc). Es independiente al sistema operativo, brinda la posibilidad de monitorización remota mediante túneles SSL cifrados o SSH o utilizando el servicio NRPE. La cantidad de plugins existentes es enorme, de hecho, se puede plantear que existen plugins para monitorear casi, cualquier proceso. Ofrece varias maneras de informar la ocurrencia de fallas de servicios o hosts: por teléfono, SMS, mensajería instantánea, pager o email. Otro aspecto importante del Nagios es la posibilidad de restablecer un servicio, después de detectada una falla, e informar al administrador. (Nagios_Development_Team, 2013)

Cuando se proyectó la instalación del Nagios como parte del sistema de gestión, se establecieron parámetros comunes a monitorear en los principales hosts que alojaban servicios en la entidad: espacio disponible los dispositivos de almacenamiento, particiones y archivos de intercambio; carga de trabajo en cada host, uso del procesador, usuarios conectados por SSH, total de procesos en ejecución, estado de la sincronía con los servidores de tiempo de la UdG, etc. (figura 4)

Host	Service	Status	Last Check	Duration	Attempt	Status Information
mail	/ Partition	OK	25-07-2016 10:16:24	0d 22h 58m 14s	1/4	DISK OK - free space: / 17624 MB (92% inode=99%):
	/boot Partition	OK	25-07-2016 10:17:16	0d 22h 57m 22s	1/4	DISK OK - free space: /boot 4515 MB (97% inode=99%):
	/home Partition	OK	25-07-2016 10:17:16	0d 22h 57m 22s	1/4	DISK OK - free space: /home 16845 MB (80% inode=99%):
	/opt Partition	OK	25-07-2016 10:18:57	0d 23h 0m 41s	1/4	DISK OK - free space: / 17624 MB (92% inode=99%):
	/tmp Partition	OK	25-07-2016 10:18:58	0d 23h 0m 40s	1/4	DISK OK - free space: /tmp 38068 MB (99% inode=99%):
	/usr/local Partition	OK	25-07-2016 10:18:58	0d 23h 0m 40s	1/4	DISK OK - free space: /usr 12799 MB (90% inode=94%):
	/var Partition	OK	25-07-2016 10:18:58	0d 23h 0m 40s	1/4	DISK OK - free space: /var 7820 MB (82% inode=99%):
	/var/log/ Partition	OK	25-07-2016 10:16:22	0d 22h 58m 16s	1/4	DISK OK - free space: /var/log 33159 MB (86% inode=99%):
	/var/spool/amavisd Partition	OK	25-07-2016 10:16:23	0d 22h 58m 16s	1/4	DISK OK - free space: /var/spool/amavisd 17494 MB (92% inode=99%):
	/var/spool/postfix Partition	OK	25-07-2016 10:16:23	0d 22h 58m 15s	1/4	DISK OK - free space: /var/spool/postfix 18946 MB (99% inode=99%):
	Bacula-fd Status	OK	25-07-2016 10:16:24	0d 22h 58m 14s	1/4	PROCS OK: 1 process with command name 'bacula-fd'
	Clamav Update	OK	25-07-2016 10:16:24	0d 22h 58m 14s	1/4	ClamAV OK: daily.cvd 21967 (Mon Jul 25 07:06:08 2016) is up to date
	Current Load	OK	25-07-2016 10:18:57	0d 23h 0m 41s	1/4	OK - load average: 0.03, 0.12, 0.13
	Current Users	OK	25-07-2016 10:17:16	0d 22h 57m 22s	1/4	USERS OK - 0 users currently logged in
	HTTP	OK	25-07-2016 10:17:23	0d 22h 57m 15s	1/4	HTTP OK: HTTP/1.1 200 OK - 259 bytes in 0.003 second response time
	NTP Syncronization	OK	25-07-2016 10:17:16	0d 22h 57m 22s	1/4	Synchronized with the server: 200.14.53.29 offset: -1.045
	Postfix Queue	OK	25-07-2016 10:17:16	0d 22h 57m 22s	1/4	OK: Mail queue is empty
	Running Amavisd	OK	25-07-2016 10:18:58	0d 22h 55m 40s	1/4	PROCS OK: 3 processes with command name 'amavi'
	Running Apolicy	OK	25-07-2016 10:18:58	0d 23h 0m 40s	1/4	PROCS OK: 1 process with command name 'twistd'
	Running Clamd	OK	25-07-2016 10:18:58	0d 23h 0m 40s	1/4	PROCS OK: 1 process with command name 'clamd'
	Running Postfix	OK	25-07-2016 10:18:58	0d 22h 55m 40s	1/4	PROCS OK: 1 process with command name 'master'
	Running Spamassassin	OK	25-07-2016 10:16:23	0d 22h 58m 16s	1/4	PROCS OK: 3 processes with command name 'spamd'
	SMTP	OK	25-07-2016 10:16:22	0d 22h 58m 16s	1/4	SMTP OK - 0.010 sec. response time
	SSH	OK	25-07-2016 10:16:24	0d 22h 58m 15s	1/4	SSH OK - OpenSSH_6.6.1 (protocol 2.0)
	Swap Usage	OK	25-07-2016 10:16:23	0d 22h 58m 15s	1/4	SWAP OK - 100% free (8191 MB out of 8191 MB)
	Total Processes	OK	25-07-2016 10:17:16	0d 22h 57m 22s	1/4	PROCS OK: 190 processes with STATE = RSZDT

Figura 4. Diferentes parámetros chequeados para el host que aloja el sistema de correos entrantes de la UdG.

También se establecieron parámetros específicos a chequear en función de los servicios que aloja cada servidor o host, por ejemplo, en la figura 4 se muestran los parámetros que se vigilan para un host que hospeda uno de los sistemas de correo entrante: se monitorean, además de los parámetros comunes, el estado del cliente del sistema de resguardos, el nivel de actualización del antivirus (Clamav), el tamaño de la cola de correos, el estado de procesos propios del sistema de correos como son el sistema antispam, el antivirus y el programa de transporte de correos.

El sistema se diseñó para que emitiera las alarmas se enviaran tanto por el mensajero instantáneo local (OpenFire) como por correo electrónico.

En cada servidor existe un grupo de servicios fundamentales que en caso de que estos se detuvieran por cualquier causa, el Nagios se encarga de intentar ponerlos en funcionamiento nuevamente, por ejemplo, el Squid en el servidor proxy, el Postfix en los servidores de correos o el Apache en los servidores web.

Bacula (http://blog.bacula.org/) y Webacula (http://webacula.sourceforge.net/). Bacula es el sistema instalado en los diferentes centros de datos de institución encargado de realizar copias de resguardo: una colección de herramientas de respaldo, capaces de cubrir las necesidades de respaldo de equipos bajo redes IP. Este potente sistema se basa en una arquitectura cliente-servidor que resulta eficaz y fácil de manejar, dada la amplia gama de funciones y características que brinda. Se adapta tanto al uso personal como profesional, para parques de ordenadores muy grandes. Licencia de Software libre y código abierto y resulta independiente al Sistema Operativo. (Bacula.org, 2016). Webacula, es la herramienta que facilita la gestión y empleo de los resguardos de este sistema a través de una interface web.

El sistema fue configurado de manera que se realizaran resguardos automáticos y diarios de tipo incremental a todos los servidores existentes en los nodos o centros de datos de la UdG. También se realizan resguardos diferenciales durante los fines de semanas y resguardos completos, un fin de semana de cada mes. La gestión y control de este sistema se facilita utilizando el Webacula.

SmokePing (http://oss.oetiker.ch/smokeping/). Diseñado para mantener un registro histórico de los tiempos de retardo en una red, de hecho, es considerada una de las mejores herramientas existentes para la visualización de éstos y cuenta con un elevado número de plugins. Posee además un sistema de alertas sumamente configurable y una ventana gráfica en tiempo real con el retardo y medidas de pérdidas de paquetes. No se limita a medir y graficar solo retardos de ICMP, sino también es capaz de generar gráficos a partir de tiempos de demoras para otros servicios (HTTP, DNS, SMTP, SSH, LDAP, etc). Otra característica importante de este sistema es que permite definir rangos estadísticos para generar alarmas enviadas vía correo electrónico. (Oetiker, 2007).

Este software se configuró enfocado principalmente al chequeo de los tiempos de respuestas en los enlaces a redes remotas que forman la red de la Universidad de Granma, pero también se configuraron chequeos a los principales servicios, servidores y dispositivos de red, por ejemplo, la figura 5 describe los tiempos de respuestas promedios para la interfaz del router del proveedor de servicios principal

de la UdG para el acceso a redes públicas, brindando de este modo una idea de las condiciones, estado y nivel de saturación de ese canal de comunicaciones.

LibreNMS. Sofware basado en el uso del protocolo SNMP, diseñado para descubrir la red y chequear el hardware de los diferentes dispositivos que la forman. Derivado de Observium y escrito en PHP como una aplicación de Web. No solo brinda apoyo a un gran rango de fabricantes de hardware (Cisco, Linux, FreeBSD, Juniper, rocade, Foundry, HP y muchos más), sino también a una enorme variedad de dispositivos: CPU, memoria, sistemas de almacenamiento, tráfico de interfaces, estadísticas de paquetes y errores muy detallados. (Figura 6).

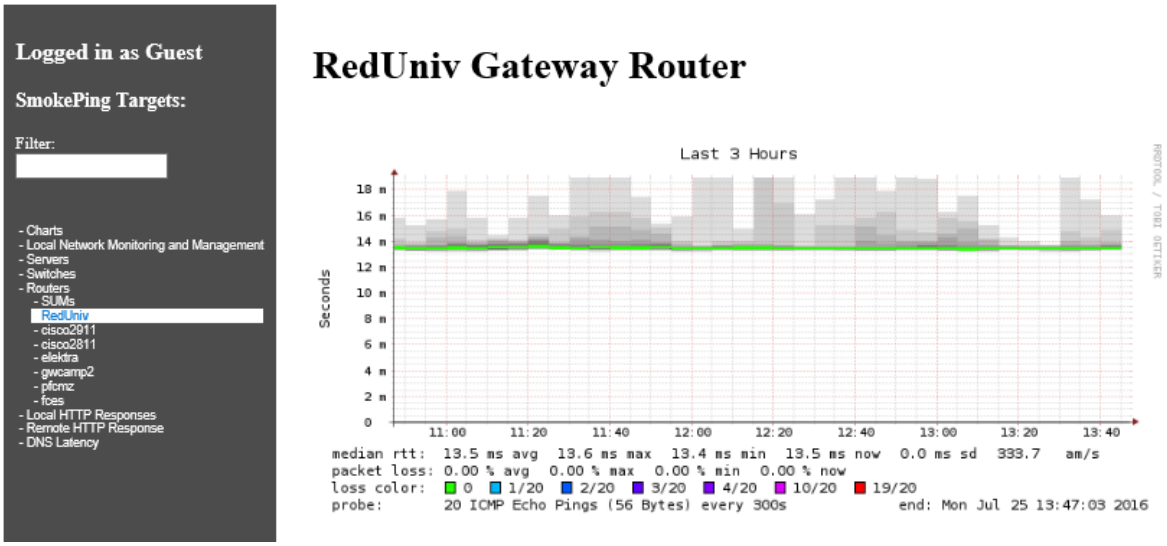

Figura 5. Tiempos de retardo registrados para el router del principal proveedor de acceso a redes externas.

LibreNMS es capaz de registrar valores de temperaturas, frecuencias de rotación de los ventiladores, voltaje, amperaje, electricidad, frecuencia de Sensores, procesos, carga promedio y estadísticas de tiempo de disponibilidad. Detecta además versiones de sistemas operativos y brinda estadísticas detalladas de las pilas IPv4, Ipv6, TCP y UDP, etc. (NSRC, 2015b).

LightSquid (http://lightsquid.sourceforge.net/), SARG, (https://sourceforge.net/projects/sarg/) SQStat (http://samm.kiev.ua/sqstat/), Webalizer (http://www.webalizer.org/) y Free-SA (https://sourceforge.net/projects/free-sa/). Aplicaciones instaladas en los proxys con finalidad de coleccionar informaciones estadísticas sobre el uso y accesos a redes externas y públicas a través de los proxys de la institución. Funcionan, procesando los registros que generan los estos programas, específicamente el Squid, a partir de los cuales se crean páginas web con valiosa información, ayudando de este modo a la interpretación de los registros. Todos poseen un ambiente de trabajo a

través de una interface Web. Mientras que el LightSquid, Sarg, Webalizer y FreeSA, muestran la información indizada de períodos de tiempo anteriores al día en curso, el SQStat es capaz de mostrar los accesos a redes externas a través del proxy en tiempo real.

Hoy por hoy, el hardware de todos los dispositivos del centro de datos principal de la red de la UdG, es monitoreado por medio de este sistema. Por ejemplo, en la figura 6 se aprecia una pequeña fracción del reporte para el router principal de la entidad.

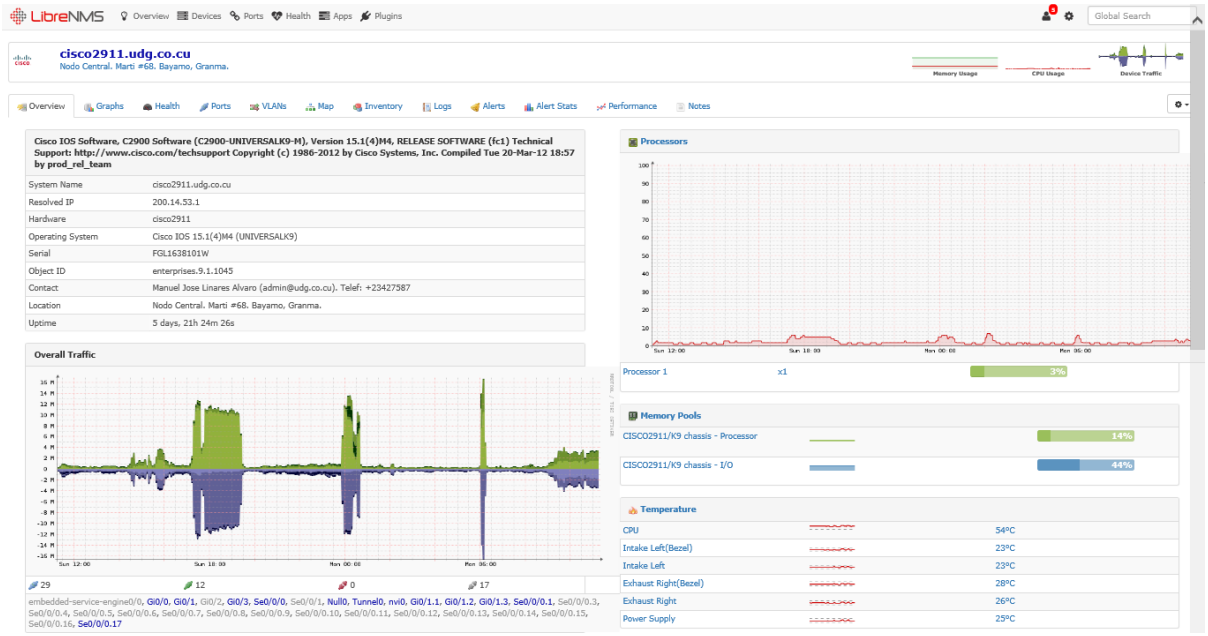

Figura 6. Vista parcial del reporte de los principales componentes de hardware para uno de los ruteadores principales de la entidad tratada.

OCS Inventory NG. (Open Computer and Software Inventory Next Generation - http://www.ocsinventory-ng.org/en/). Herramienta basada en software libre y arquitectura cliente - servidor, útil en la gestión de los registros y contabilidad, pues permite generar un inventario de los activos de TI en cualquier institución, recopilando información sobre el hardware y software de equipos existentes en la red que ejecutan el programa de cliente OCS, luego es capaz de visualizar la información colectada través de una interfaz web. Actualmente, todos los activos de IT, de todos los centros de datos de la red de la UdG y el ITSUP, están registrados en las bases de datos de esta aplicación y se ha logrado configurar el sistema de manera tal que envíe alarmas por correo electrónico en caso de cambios de dispositivos de hardware (procesadores, discos duros, memorias, etc).

Rancid (http://www.shrubbery.net/rancid/) y WebSVN (http://subversion.apache.org/). Rancid se encarga de mantener un archivo histórico de los cambios en la configuración y otros componentes de

los equipos (Cisco, HP, Juniper, Foundry, etc.). Funciona con enrutadores y conmutadores (Switchs) mediante la automatización de la recolección y resguardo de los archivos de configuraciones. Entre las principales funciones de Rancid, se destacan tanto el resguardo de las configuraciones de algunos equipos de hardware, como las auditorías de los usuarios que accedieron e hicieron cambios en éstos. (NSRC, 2015a), (Kilmer, N.A).

En estos momentos, se resguarda con ayuda de estas herramientas, las configuraciones de tres ruteadores Cisco y algunos switch de capa 3 que poseen un IOS muy similar al de Cisco, facilitando no solo el control de versiones y los procesos de resguardo, sino también el análisis de la configuración actual para la realización de cambios y mejoras. Se envían notificaciones por correo electrónico, cuando se detectan cambios en las configuraciones de los diferentes dispositivos.

AlienVault OSSIM. (Open Source Security Information Management – http://www.alienvault.com). Aunque este sistema no forma parte directamente de esta investigación, si es un componente importante del sistema de gestión implementado, por lo que se aborda en este documento.

Se trata de una colección de software bajo la licencia GPL, agrupadas con el objetivo de ofrecer una herramienta que ayude al manejo de eventos de seguridad mediante un motor de correlación y una colección detallada de aplicaciones útiles al administrador para tener una vista de todos los aspectos relativos a la seguridad en su infraestructura. OSSIM se ha diseñado para ayudar a los administradores de red en la seguridad de las computadoras, detección de intrusos y vulnerabilidades. Entre las aplicaciones más conocidas que lo forman, podrían mencionarse Arpwatch, Pads, para la detección de anomalías en servicios, el Openvas para detectar de intrusos utilizando un escaner de vulnerablidades, el Snort o Suricata para los eventos de la red, entre otros. En estos momentos existe un host en la UdG que aloja el OSSIM, con varios sensores distribuidos en los diferentes campus que de la Universidad de Granma.

Se utilizan otras aplicaciones en los procesos de gestión, como son el NetDot, para documentar la red, la cual contiene valiosas informaciones relacionadas con el inventario de dispositivos y activos, el esquema de direccionamiento de la red, las zonas de dominio, los principales contactos de sus administradores y proveedores, los diagramas y planos topológicos, licencias de la red, contratos, etc.

Sendmail analyzer (http://sendmailanalyzer.darold.net/features.html). Software empleado para monitorear el funcionamiento de sistemas de correos basados en sendmail o postfix y el tráfico de correos generado por éstos. Es libre y está programado para procesar archivos de registros de Postfix

o Sendmail y generar, en tiempo real, estadísticas dinámicas en HTML con salida gráfica. En estos momentos, todos los servidores de correos se gestionan con esta aplicación.

Conclusiones.

Ciertamente, en la medida que se aumente la complejidad de una red, serán cada vez más costosos y complejos los sistemas de gestión de la misma, pero en las condiciones actuales, donde la información es un valor de elevadísimo costo, la preservación confiable y segura de ésta, es una necesidad imperiosa, por lo que se justifican completamente todas las inversiones que se hagan para preservarla, por ello, es importante la creación de una consciencia que implique tanto a administradores de sistemas, como a directivos, en la necesidad de la implementación de un sistema de gestión que permita conocer a los especialistas, lo que sucede en la red que controlan.

Se hace imprescindible la mejora de los sistemas de gestión de red en las instituciones de la región.

Aunque a primera vista, un sistema de gestión puede resultar costoso, la inversión puede reducirse considerablemente, empleando software libre, pues existe una amplísima gama de aplicaciones muy eficaces y completas, que se pueden utilizar sin pagar por su empleo, modificación o distribución.

Referencias.

Bacula.org. (2016). Bacula Documentation. from http://blog.bacula.org/documentation/

Berthier, R., Cukier, M., Hiltunen, M., Kormann, D., Vesonder, G., & Sheleheda, D. (2010). *Nfsight: NetFlow-based Network Awareness Tool*.

Clemm, A. (2007). *Network Management Fundamentals* M. B. Ray (Ed.) Retrieved from http://lib.agu.edu.vn:8180/collection/bitstream/123456789/4424/1/Network%20management%20fundamentals.pdf

Ding, J. (2009). *Advances in Network Management*: CRC Press.

Gómez, D., & González, A. (2013). *ARQUITECTURA PARA LA GESTIÓN DE SERVICIOS ADMINISTRADOS DE TECNOLOGÍA.* (MAESTRÍA EN GESTIÓN INFORMÁTICA Y TELECOMUNICACIONES SANTIAGO DE CALI). Retrieved from https://www.google.com.cu/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjQ0Ma-tYzOAhWsyoMKHapCCbcQFggaMAA&url=https%3A%2F%2Fcore.ac.uk%2Fdownload%2Fpdf%2F41976485.pdf&usg=AFQjCNG10CEOGyucfCAewHnT26tAAtrTfA&bvm=bv.127984354,d.cWw

Haag, P. (N.A). User Documentation nfdump & NfSen.

Ibáñez, D. H. (2012). *Implantación de directrices ITIL en un Departamento de Soporte y Operaciones de una empresa.* (Proyecto de fin de carrera), Universidad Carlos III de Madrid.

ISO. (1997). International Organization for Standardarization, Information technology - Open Systems Interconnecions.

Kilmer, H. (N.A). *Tracking Device Configuration Changes witth RANCID*.

Marrero, D., & Hernández, H. (2016). *IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN PARA LA RED NACIONAL UNIVERSITARIA.* (Trabajo de diploma para optar por el Título de Ingeniero en Telecomunicaciones y Electrónica), Instituto Superior Politécnico "José Antonio Echeverría".

Nagios_Development_Team. (2013). Nagios, The Industry Standard In IT Infrastructure Monitoring. Nagios Documentation., from https://www.nagios.org/documentation/

NSRC. (2015a). Gestión de Redes. Gestión de configuraciones con RANCID.

NSRC. (2015b). *LibreNMS*. Paper presented at the LibreNMS, "Todo en Uno", Monitoreo y Gráficos, El Dragón de Muchas Cabezas. Walk. Track de Gesitón y Monitoreo de Redes, Tecnológico de San Carlos.

Oetiker, T. (2007). SmokePing Documentation. from http://oss.oetiker.ch/smokeping/doc/index.en.html

Oetiker, T. (2012). MRTG Documentation. from http://oss.oetiker.ch/mrtg/doc/index.en.html

Pastor, F. (2015). Propuesta de política de gestión de capacidad para una compañía de tecnologías de la información de acuerdo con los requerimientos de ITIL. *3 Ciencias, 4*.

Pérez, L. (2013). *ESTUDIO COMPARATIVO DE LOS SISTEMAS GESTIÓN Y MONITOREO BASADOS EN LOS REQUERIMIENTOS GENERALES DE LA RED DE UN CAMPUS UNIVERSITARIO.* (Master en Redes de Comunicaciones), Pontificia Universidad Católica del Ecuador.