ESCUELA TÉCNICA SUPERIOR DE INGENIEROS INDUSTRIALES Y DE TELECOMUNICACIÓN

UNIVERSIDAD DE CANTABRIA

Trabajo Fin de Grado

EVALUACIÓN DE HERRAMIENTAS DE MONITORIZACIÓN DE REDES SOBRE PLATAFORMA EMBEBIDA

(Evaluation of network monitoring tools on embedded platform)

Para acceder al Título de

Graduado en

Ingeniería de Tecnologías de Telecomunicación

Autor: Marina Cabezón Rodríguez **10 - 2017**

E.T.S. DE INGENIEROS INDUSTRIALES Y DE TELECOMUNICACION

GRADUADO EN INGENIERÍA DE TECNOLOGÍAS DE TELECOMUNICACIÓN

CALIFICACIÓN DEL TRABAJO FIN DE GRADO

Realizado por: Marina Cabezón Rodríguez
Director del TFG: Roberto Sanz Gil
Título: "Herramientas de monitorización de redes sobre plataforma embebida"
Title: "Evaluation of network monitoring tools on embedded platform"

Presentado a examen el día: 17 de octubre de 2017

para acceder al Título de

GRADUADO EN INGENIERÍA DE TECNOLOGÍAS DE TELECOMUNICACIÓN

Composición del Tribunal:
Presidente (Apellidos, Nombre): Sanz Gil, Roberto
Secretario (Apellidos, Nombre): Irastorza Teja, José Ángel
Vocal (Apellidos, Nombre): Pérez Arriaga, Jesús

Este Tribunal ha resuelto otorgar la calificación de: .....

Fdo.: El Presidente

Fdo.: El Secretario

Fdo.: El Vocal

Fdo.: El Director del TFG
(sólo si es distinto del Secretario)

Vº Bº del Subdirector

Trabajo Fin de Grado Nº
(a asignar por Secretaría)

Resumen

El avance de la tecnología y el aumento de las infraestructuras de redes ha creado una necesidad de buscar herramientas capaces de monitorizar en tiempo real y gestionar los posibles problemas que puedan aparecer en dichas redes.

En este trabajo se estudian tres herramientas que actualmente son ampliamente utilizadas y que se han adaptado para funcionar sobre una plataforma embebida. La plataforma embebida, en este caso, la Raspberry Pi está diseñada para cumplir necesidades específicas, que podría realizar un ordenador, pero a un bajo coste.

La herramienta Nagios Enterprise Monitoring Tool (NEMS) permite monitorizar grandes redes, tanto equipos como servicios. Permite crear informes, para mantener un control sobre los datos recogidos por la herramienta, y alertas, que avisen al administrador de la herramienta cuando el funcionamiento de algún dispositivo o servicio no sea el esperado.

Multi Router Traffic Grapher (MRTG) es una herramienta cuyo punto fuerte es la creación de gráficas a partir del tráfico recogido en una red a lo largo del tiempo.

Por último, Netflow es un protocolo que genera flujos de datos a partir del tráfico que pasa a través de una red. Permite aplicar filtros a dichos flujos para que la gestión y control sea más específica.

Palabras Clave

Monitorización, red, dispositivo, servicio, Nagios, MRTG, Netflow, router, SNMP, notificación, informe, interfaz web, grafico, Pandora FMS, servidor.

Abstract

Technology development and the increment of network infrastructures has required to look for tools able to monitor in real time and manage the future problems that can appear in these networks.

This work analysed three different monitoring tools that are used worldwide and that have been adapted to work on an embedded platform. This platform, which in this case is the Raspberry Pi, is designed to fulfil specific requirements, that can achieve a computer, but with low cost.

Nagios Entreprise Monitoring Tool can monitor large networks, both hosts and services. It creates reports, to control the data collected by the tool, and alerts, to notify de administrator when the system failed or does not work at it is expected.

Multi Router Traffic Grapher (MRTG) is a tool which strong point is the creation of graphics about network traffic collected over time.

Finally, Netflow is a protocol that generates data flows from the traffic passing through a network. It is possible to filter the flows for more specific management and control.

Keywords

Monitoring, network, host, service, Nagios, Netflow, router, SNMP, notification, report, web interface, graphic, Pandora FMS, server.

Agradecimientos

En primer lugar, a mi familia y a mis amigas de toda la vida por su apoyo durante estos cuatro años de grado. Gracias por alegraros siempre de mis logros y ayudarme sin tener que pedirlo.

A mi tutor, Roberto, cuya ayuda y dedicación han hecho posible este Trabajo de Fin de Grado. Gracias por enseñarme con paciencia cuando surgían problemas, y con cercanía.

Por último, a mis compañeros de carrera y sobre todo a aquellos que se han convertido en grandes amigos. Gracias por los descansos de una hora en la biblioteca, las risas en las épocas más duras y los buenos momentos tanto dentro como fuera de la Universidad.

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

LISTA DE ACRÓNIMOS

Wi-Fi	Wireless Fidelity
RAM	Random Access Memory
USB	Universal Serial Bus
HDMI	High Definition Multimedia Interface
CSI	Camera Serial Interface
NEMS	Nagios Entreprise Monitoring Server
MRTG	Multi Router Traffic Grapher
SNMP	Simple Network Management Protocol
POP3	Post Office Protocol
HTTP	Hypertext Transfer Protocol
PING	Packet Internet Groper
SSH	Secure Shell
IMAP	Internet Message Access Protocol
FTP	File Transfer Protocol
OS	Operating System
CPU	Central Processing Unit
MIB	Management Information Base
HTML	HyperText Markup Language
IP	Internet Protocol
MTU	Maximum Transmission Unit
FMS	Flexible Monitoring System
TCP	Transmission control protocol
UDP	User Datagram Protocol
LAN	Local Area Network
PHP	Hypertext Preprocessor
DB	Database
WMI	Windows Management Instrumentation
SLA	Service Level Agreement
ICMP	Internet Control Message Protocol)

1 INTRODUCCIÓN

1.1 MOTIVACIÓN

En la actualidad, debido a la gran evolución de la tecnología en los últimos años, cualquier empresa o negocio cuenta con una red de datos con la que ofrecen o gestionan un determinado servicio. Ante un fallo o caída en dicha red, la empresa puede sufrir grandes problemas, así como el descontento de los clientes, que finalmente acabarán cambiando de compañía.

En definitiva, la competencia entre empresas en gran parte reside en la manera en que gestionan sus recursos y cómo reaccionan ante los posibles problemas que puedan surgir. La implementación de procedimientos para una administración efectiva y control de la red será lo que marque la diferencia entre unas empresas y otras.

Un sistema de monitorización está continuamente testeando la red con el fin de encontrar problemas causados por cualquier tipo de componentes; si encuentra algún tipo de problema o fallo, el sistema notificará al administrador, de tal manera que se pueda actuar eficazmente ante el evento. [1]

Por todo esto, en los últimos años se han implementado múltiples herramientas de monitorización de redes de software libre flexibles, efectivas y que produzcan datos abiertos para los analistas y gestores de red es una tarea crucial para sacar el máximo de las redes actuales. [2]

Además, con los progresos en el ámbito de la electrónica, nació la Raspberry Pi. Según sus creadores, la Raspberry Pi es una computadora de tamaño de tarjeta de crédito que se conecta a su televisor y un teclado. Es un pequeño ordenador capaz de ser utilizado en proyectos de electrónica, y para muchas de las cosas que hace su PC de escritorio, como hojas de cálculo, procesamiento de textos, navegación por Internet y juegos. Fue creado para enseñar programación y creación digital. [3]

El software de la Raspberry Pi llamado Raspbian es open source; el sistema operativo es una versión adaptada de Debian.

Con la evolución de la Raspberry Pi llegamos a su última versión, la Raspberry Pi 3 model B que incluye conectividad Wi-Fi inalámbrica y Bluetooth, 1 GB de RAM, cuarto puertos USB, puerto de Ethernet y HDMI, Micro SD, cámara CSI, etc. [3]

Las grandes ventajas de una Raspberry Pi como arquitectura hardware son: su reducido tamaño, su alta capacidad de proceso en relación a su tamaño y su escaso coste. Estas son las características ideales para usar este hardware para utilidades de redes, monitorización y gestión, y seguridad informática. [4]

1.2 OBJETIVOS

En este trabajo se van a estudiar tres herramientas de monitorización open source que son de las más utilizadas actualmente por empresas a nivel mundial. Estas herramientas son: NEMS, MRTG y Netflow.

Se va a ver las funcionalidades que ofrecen cada una de ellas al usuario a la hora de analizar una red y las posibilidades que ofrece: gráficos, informes, alertas, gestión de recursos físicos, monitorización de servicios, etc.

La novedad de este trabajo es que estas herramientas se van a implementar sobre una Raspberry Pi 3 modelo B, ya sea instalándolas propiamente en la placa o utilizándola como agente enviando información a la herramienta.

Debido a los beneficios que tiene este dispositivo, las herramientas de monitorización actuales se están adaptando para su funcionamiento en la Raspberry Pi y en el sistema operativo Raspbian. Se estudiará también la instalación y configuración de las tres herramientas en la placa.

Además, como la monitorización de redes y el uso de Raspberry Pi cada día va a más, no solo es interesante su combinación para el ámbito empresarial, sino también para el ámbito académico.

Por este motivo, se han diseñado tres guiones de prácticas correspondientes a las tres herramientas estudiadas; las cuales se podrían introducir en el temario de alguna asignatura del grado en Ingeniería de Tecnologías de Telecomunicación. En este caso, los guiones han sido adaptados para que las prácticas sean realizadas en el laboratorio de Telemática de la Universidad de Cantabria.

Por último, se hará una pequeña comparación entre las herramientas de monitorización tanto de las funcionalidades que ofrecen a los usuarios como de su facilidad de implementación en la Raspberry Pi.

1.3 CONTENIDO DE LA MEMORIA

Esta memoria está dividida en varios capítulos. Los tres primeros capítulos hacen referencia a tres herramientas de monitorización que existen en el mercado: NEMS (Nagios Enterprise Monitoring Server), MRTG (Multi Router Traffic Grapher) y Netflow.

Dentro de estos tres capítulos se hará una breve introducción a las herramientas, cuál es su funcionamiento básico y cuál es la función de la Raspberry con respecto a la herramienta; la instalación o configuración tanto de la Raspberry como de la herramienta, y de todos los dispositivos necesarios para que se puedan obtener unos resultados; y por último, se explicará cómo la herramienta muestra los resultados al usuario, qué tipo de información es capaz de analizar y se pondrán ejemplos visuales de resultados obtenidos experimentalmente.

Se incluirá un capítulo de “CONCLUSIONES” en el que se realizará una pequeña comparación entre las tres herramientas analizadas, tanto a nivel de utilidad y facilidad de uso por parte de un usuario como de su implementación en la Raspberry Pi. Y se haga una pequeña valoración en cuanto a las líneas futuras que se podría seguir en este ámbito de trabajo.

Después de este análisis, en los ANEXOS I, II, y III, se incluirán tres guiones de prácticas implementando las anteriores herramientas en un entorno de laboratorio para el ámbito académico. El contenido de estas prácticas plasma los contenidos teóricos, vistos en los capítulos anteriores, en un entorno real; con una serie de cuestiones que se podrían plantear al alumno a lo largo de las mismas.

2 NAGIOS ENTERPRISE MONITORING SERVER (NEMS)

2.1 INTRODUCCIÓN

NEMS es una imagen de Nagios 4 que permite monitorizar redes y que está específicamente diseñada para funcionar sobre la RaspberryPi versión 3. El objetivo de Nagios es detectar cualquier equipo, servicio o sistema que no esté funcionando correctamente para que la solución del problema se haga lo más rápido posible y los usuarios del sistema sean lo menos partícipes posibles del problema detectado.

Entre sus múltiples funciones destacan: [5]

- Supervisión de servicios de red (SMTP, POP3, HTTP, PING, etc.)
- Supervisión de los recursos del host (carga del procesador, uso del disco, etc.)
- Plugin de diseño simple que permite a los usuarios desarrollar fácilmente sus propios controles de servicio.
- Controles de servicios y hosts paralelos. Se pueden supervisar diferentes servicios, tanto del mismo dispositivo como de dispositivos diferentes, al mismo tiempo.
- Capacidad para definir la jerarquía de host de red utilizando hosts "principales", permitiendo la detección y distinción entre hosts que están inactivos y aquellos que son inaccesibles.
- Notificaciones de contacto cuando se producen problemas de servicio o de host y se resuelven (mediante correo electrónico u otro método definido por el usuario).
- Interfaz web opcional para ver el estado actual de la red, la notificación y el historial de problemas, el archivo de registro, etc.

Para la monitorización de hosts y servicios, NEMS utiliza plugins. Estos son componentes externos a los que Nagios les pasa información sobre lo que debe comprobarse y los límites críticos y de advertencia; una vez transmitida esta información, los plugins harán las respectivas comprobaciones y analizarán los resultados.

El resultado del chequeo de estos plugins es el estado del servicio o host monitorizado (NEMS solo recoge cuatro estados: Ok, Warning, Critical y Unknown) e información más detallada sobre los mismos. Esto significa que además de encontrar problemas, Nagios previene a la empresa que lo implemente, de tenerlos en un futuro.

Una de las ventajas de este sistema es que se pueden monitorizar a la vez múltiples máquinas de diferentes localizaciones. La información de esas máquinas se va a recoger en un único servidor Nagios y de esta manera se podrá acceder a toda la información de la infraestructura desde una única máquina.

Este servidor engloba varias interfaces web de monitorización, entre ellas:

- Nagios Core, en el que se puede hacer un seguimiento de los hosts y servicios a monitorizar en la red, acceder a alarmas y notificaciones, acceder a información específica de la Raspberry,etc.
- Nagios Nconf, a través de la cual se puede hacer cambios en la configuración adecuándola a nuestra infraestructura.
- NagVis es un complemento de visualización para una mejor gestión de la red a través de Nagios. Crea mapas de acuerdo a las relaciones padre/hijo entre hosts de la red monitorizada por Nagios. [6]
- Check_MK es una extensión del sistema de monitorización de Nagios que permite crear una configuración usando Python y descargar el trabajo desde Nagios Core permitiendo que más sistemas sean supervisados desde un solo servidor Nagios.

2.2 PRIMEROS PASOS CON NEMS

Una vez grabada la imagen de la herramienta NEMS en una tarjeta de memoria mayor de 8GB, se iniciará el programa en una Raspberry, en mi caso la Raspberry versión 3 model B. [7]

Cuando se haya cargado la imagen el primer comando que se deberá escribir será **sudo nems-init**. Con este comando haremos las primeras configuraciones, entre ellas, elegir un nombre de usuario y una password para las interfaces web nConf, Nagios Core y Check_MK. Para la interfaz Nagvis el usuario/contraseña será por defecto *admin/admin* (deberá ser cambiado tras la primera entrada en el sistema).

Ya se podrá acceder al servidor Nagios desde el navegador a través del enlace **http://IPADDRESS** donde IPADDRESS es la dirección IP asociada a la Raspberry y donde se ha configurado el servidor Nagios. Dicha configuración del servidor (añadir hosts, servicios) se hará a través de nConf, http://IPADDRESS/nconf . Bajo la pestaña Reporting se podrán encontrar las demás interfaces web que aportan los resultados en tiempo real de monitorización, Nagios Core http://IPADDRESS/nagios3, Nagvis y Check_MK. Por último, bajo la pestaña System se podrá acceder a información específica de la Raspberry. [7]

2.3 CONFIGURACIÓN NEMS

La configuración de los equipos y servicios a monitorizar se puede realizar de manera muy intuitiva a través de la interfaz web Nagios nConf. Esta interfaz permite, no solo añadir equipos a la red, sino que ofrece múltiples opciones para hacer que la configuración se realice de mejor manera y para una mejor gestión de toda la red. A continuación, se explican los objetos más interesantes que ofrece esta interfaz.

2.3.1 HOSTS

Desde la interfaz nConf se pueden añadir equipos a la configuración. Para ello, solo hay que conocer la dirección IP del dispositivo, el tipo de dispositivo (equipo Linux, Windows server, impresora, router o switch), sus ajustes preestablecidos, establecer los periodos de chequeo y de notificación.

A parte de esto se pueden definir relaciones entre hosts mediante el objeto parent hosts que permite definir la topología de la infraestructura. Los equipos padres suelen ser routers, switches, firewalls, etc. que se encuentran entre el equipo de monitorización y un host remoto y que se encargan de transmitir tráfico de paquetes entre ambos. Si el estado de una máquina es inaccesible puede deberse a que su parent host se haya caído.

Además, se pueden crear grupos que engloben a varios dispositivos que por ejemplo vayan a utilizar los mismos servicios o tengan características similares para facilitar así su monitorización y organización. El host se guardará en una base de datos.

Uno de los principales beneficios es que nConf permite a los usuarios definir plantillas y ajustes preestablecidos que pueden aplicarse al agregar hosts. Un host preestablecido contiene todos los servicios que se deben agregar a un host con todos los comandos vinculados y todos los valores predeterminados establecidos. También contiene el comando host-alive-check que se aplicará al nuevo host. Al añadir un host, el usuario debe ajustar algunos parámetros para adecuar la monitorización del host a su caso específico. [8]

NEMS viene por defecto con unas plantillas predefinidas que hacen referencia a varios posibles tipos de máquinas (OS): Linux, Windows Server, Router, Switch, HP Printer, HP Unix, Free BSD y Sun Solaris. En cualquier caso, y como bien se ha dicho antes, el usuario puede añadir más sistemas desde Nconf en la parte de additional items y advanced items.

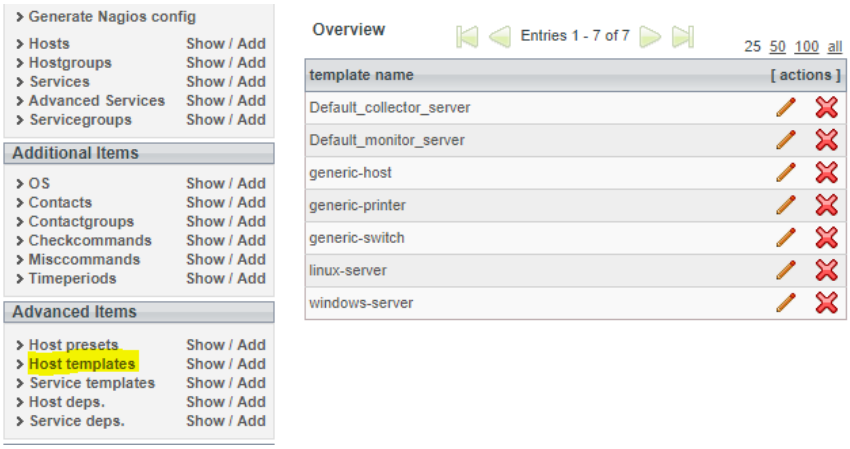


Figura 2.1. *Plantillas de dispositivos predefinidas en Nagios nConf*

Los periodos de chequeo y notificación se establecen a partir de los siguientes objetos: [9]

Check period	Hace referencia al nombre de un time period (objeto definido en Nagios definido más adelante) que determina cuándo se pueden hacer los chequeos de la máquina.
Max check attemps	Especifica el número de veces que un test tiene que informar de que una máquina ha caído antes de que se asuma que realmente lo ha hecho.
Check Interval	Especifica cada cuánto tiempo (en minutos) se chequea una máquina.
Retry Interval	Especifica el tiempo (en minutos) que hay que esperar antes de volver a chequear si la máquina está activa.
Notification period	Especifica el periodo de tiempo en el que se pueden enviar notificaciones. Hace referencia a un objeto time period. Las notificaciones tendrán opciones que explicaremos más adelante.
First notification delay	Especifica el tiempo (en minutos) que se tarda en enviar la primera notificación desde que la máquina ha caído.
Notification Interval	Especifica el tiempo (en minutos) que se espera entre notificaciones de que una máquina ha caído.

Tabla 2.1. *Opciones de chequeo y notificación configurables en Nagios nConf*

El estado de una máquina puede ser UP o DOWN. En el apartado he hecho referencia a "máquinas caídas", esto significa que su estado es DOWN.

En la siguiente imagen se puede ver un ejemplo de cómo se ha añadido un router configurado en un servidor Nagios:

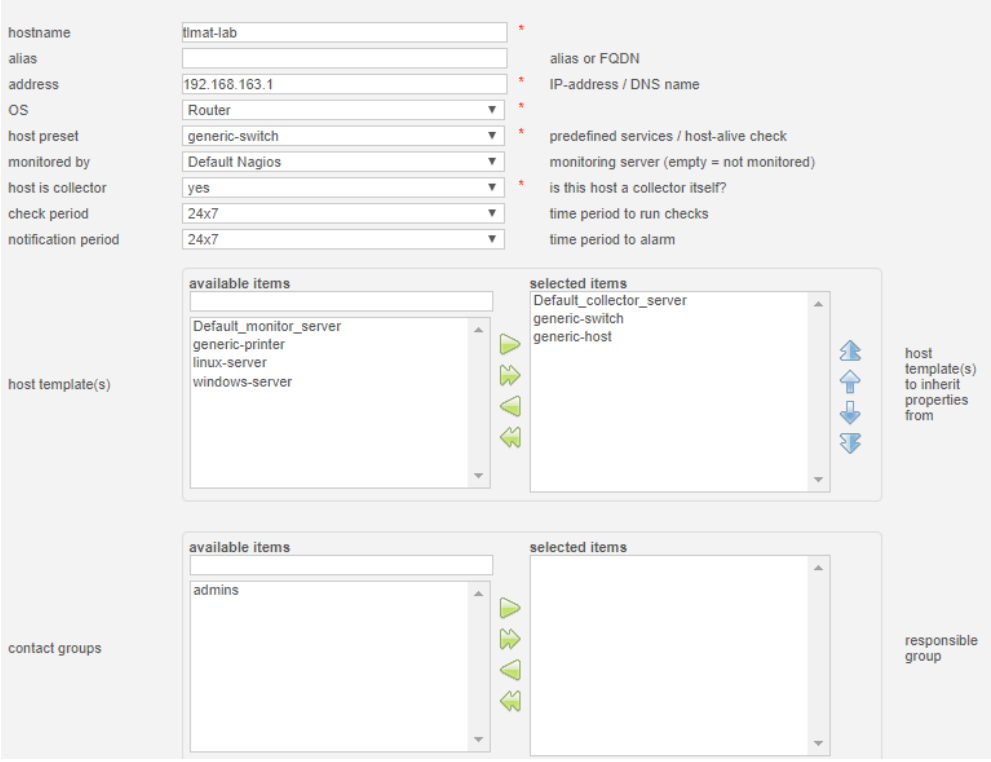


Figura 2.2. *Plantilla de Nagios nConf para añadir un equipo al servidor Nagios (1)*

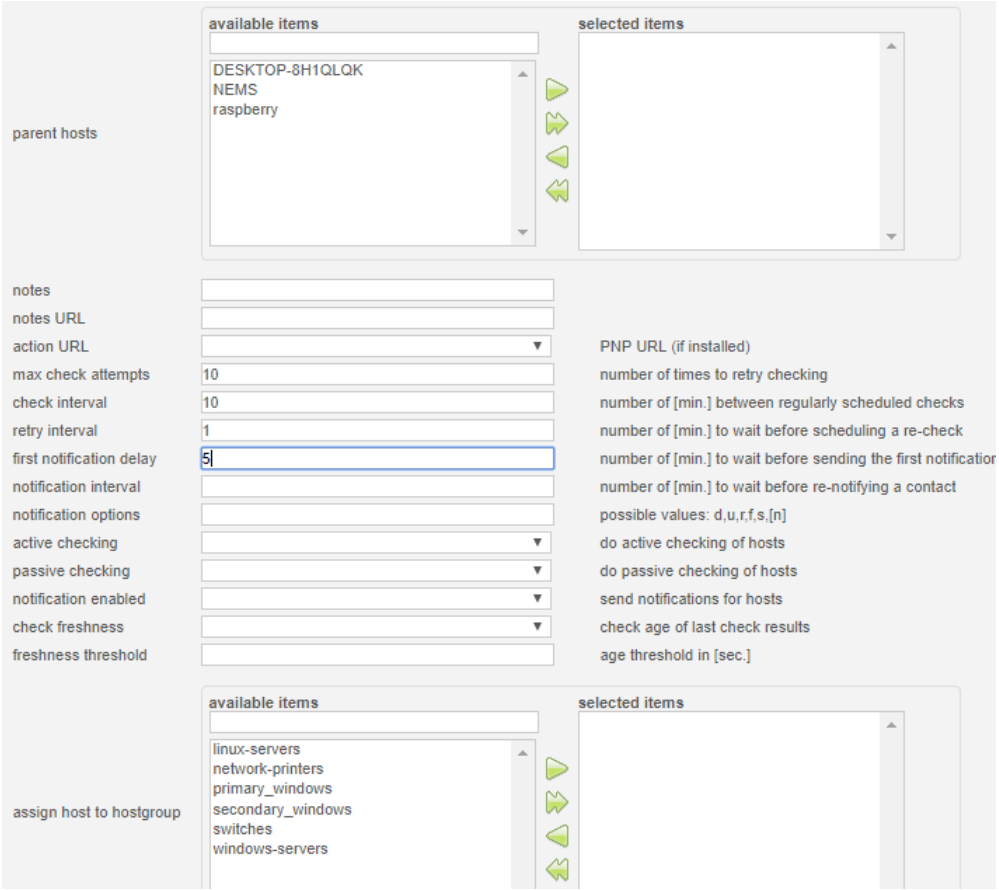


Figura 2.3. *Plantilla de Nagios nConf para añadir un equipo al servidor Nagios (2)*

En este ejemplo se chequeará un router durante todo el día y todos los días de la semana. Este router se ha definido como un generic-switch que incluye el comando host-alive-check que se encargará de mirar si la máquina está activa y funcionando. Se chequeará cada 10 minutos y a los 10 intentos fallidos se asumirá que el router ha caído y se pondrá su estado a DOWN. La primera notificación de que el router está DOWN será a los 5 minutos.

A la hora de añadir una máquina, no todos los objetos explicados anteriormente es obligatorio definirlos. Solamente son obligatorios los siguientes campos: host_name, address, OS, host-preset, host-collector.

Cada vez que se añada o modifique un host, servicio, plantilla o ajuste a través de nConf se deberá activar un proceso que exportará el contenido de la base de datos en que se guardan todos estos ajustes al formato de configuración de Nagios. Esto se realiza a través del Generate Nagios config en Nagios nConf. Una vez que se ha generado la configuración, nConf hará una comprobación de sintaxis obligatoria de los archivos. [8]

Figura 2.4. *Generate Nagios config deployment*

Una vez añadido el host, en la interfaz web Nagios Core podremos visualizar inmediatamente dicha máquina y su estado en tiempo real. Uno de los inconvenientes de esta herramienta es que no permite el autodescubrimiento de hosts sino que hay que añadirlos manualmente uno a uno.

Trabajando sobre la red del laboratorio, he configurado NEMS para monitorizar un ordenador con sistema operativo Windows, el servidor NEMS con sistema operativo Linux, el router del laboratorio y la propia Raspberry configurada como si fuera un switch.

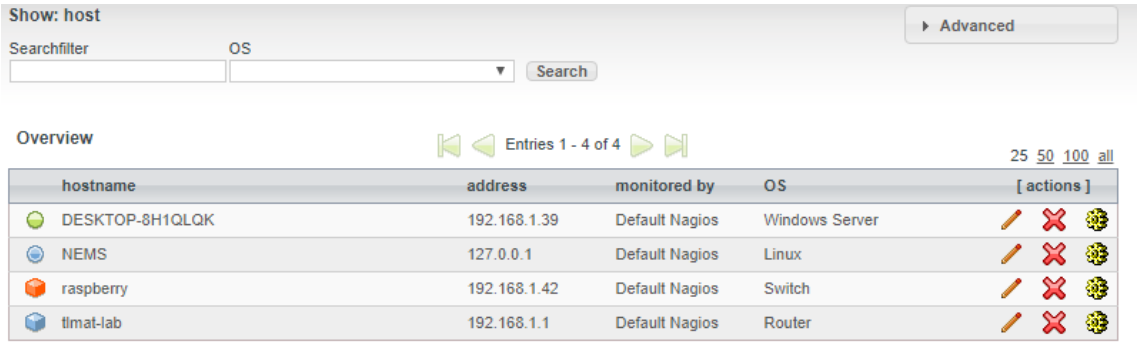


Figura 2.5. *Equipos configurados en la interfaz Nagios nConf*

Para una mejor gestión de la red, Nagios permite agrupar las máquinas en grupos. Con el objeto host-group se pueden agrupar máquinas por su tipo, su sistema operativo, su localización, etc.

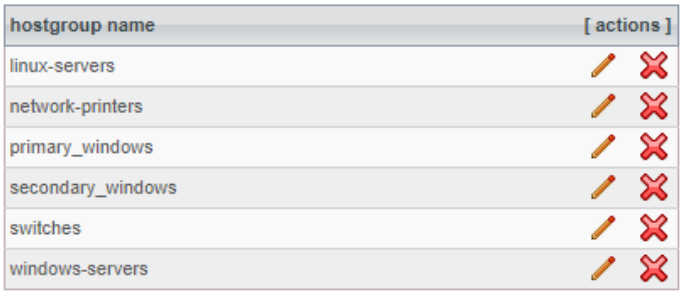


Figura 2.6. *Host groups configurados*

Una de las ventajas que tiene formar un grupo es que se puede definir un servicio que podrá ser monitorizado en todas las máquinas que pertenezcan a ese grupo sin necesidad de tener que ir una a una estableciendo dicho servicio.

Por ejemplo, en la siguiente imagen se puede observar un grupo que engloba dos servidores Linux (NEMS y Raspberry) y que por estar en dicho grupo en esos servidores se van a monitorizar una serie de servicios como HTTP, SSH, PING, etc.

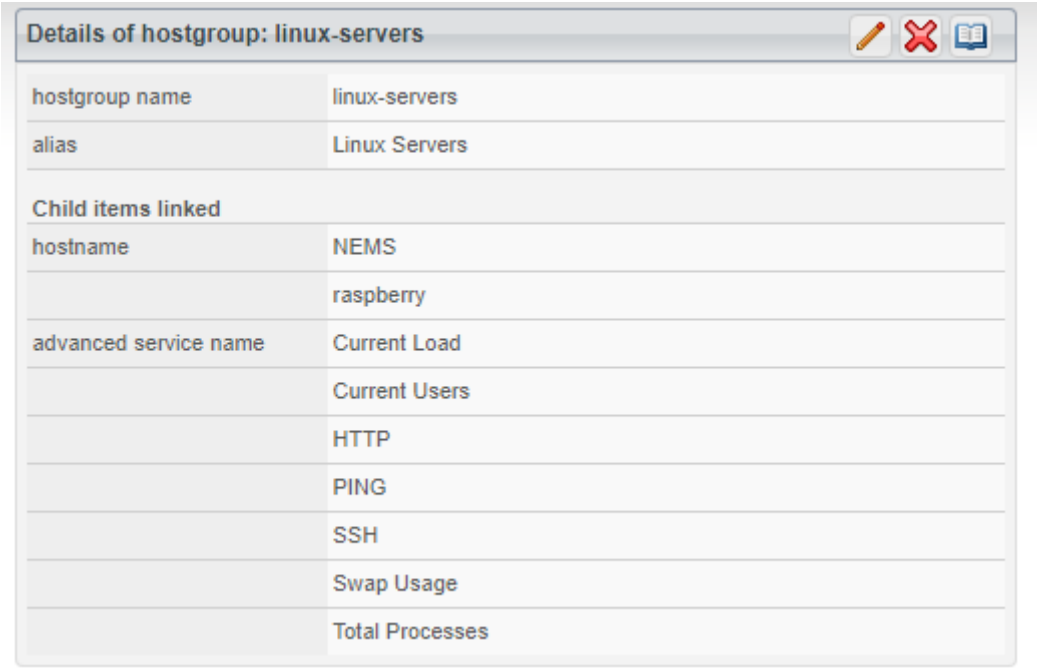


Figura 2.7. *Ejemplo de host group*

2.3.2 SERVICIOS

El poder de esta herramienta de monitorización reside en los servicios que se pueden monitorizar. Estos pueden ser tanto servicios públicos como privados.

Un servicio es “público” cuando es accesible a través de la red - ya sea en la red local o por Internet como HTTP, POP3, IMAP, FTP y SSH. Estos servicios y aplicaciones, así como sus protocolos, pueden ser monitorizados por Nagios sin necesidad de requerimientos de acceso especiales. [10]

En cambio, los servicios “privados” no pueden ser monitorizados con Nagios sin la intervención de algún agente. Ejemplos de servicios privados asociados con los equipos son la carga de CPU, uso de memoria, uso en disco, cuentas de usuarios activos, información de procesos, etc. Estos servicios privados o atributos de los equipos usualmente no son expuestos a clientes externos. Esta situación requiere que un agente intermediario sea instalado en el equipo que se desea monitorizar esa información. [10]

Sobre los dispositivos que hemos configurado anteriormente podemos añadir diferentes servicios de monitorización. Para ver la disponibilidad de dichas máquinas es

conveniente añadir a todos ellos el servicio PING que nos hará saber si ese ordenador está configurado en la red y nos notificará si alguno de ellos cae en un momento dado.

A la hora de definir servicios es obligatorio fijar unos intervalos de chequeo del servicio y de notificación de los mismos por si alguno de ellos da algún problema a la hora de ser monitorizado. Los parámetros que definen estos periodos son los mismos que en los hosts.

En los servicios también se pueden definir plantillas con una serie de servicios a monitorizar definidos para una mayor facilidad, por ejemplo, si se quieren definir dichos servicios en múltiples equipos (en vez de tener que añadir cada servicio uno a uno, se añadirían todos los servicios de una vez).

Como en el caso de las máquinas, los servicios también se pueden agrupar. Estas agrupaciones sirven para manejar de una manera más efectiva los servicios, que sea más organizado a la hora de ver la información de los mismo en las interfaces web y para configurar dependencias entre equipos.

Por ejemplo, en la siguiente figura podemos observar que se ha creado un group llamado web-services que va a englobar a todos los servicios web que se vayan a monitorizar, como el servicio HTTP.

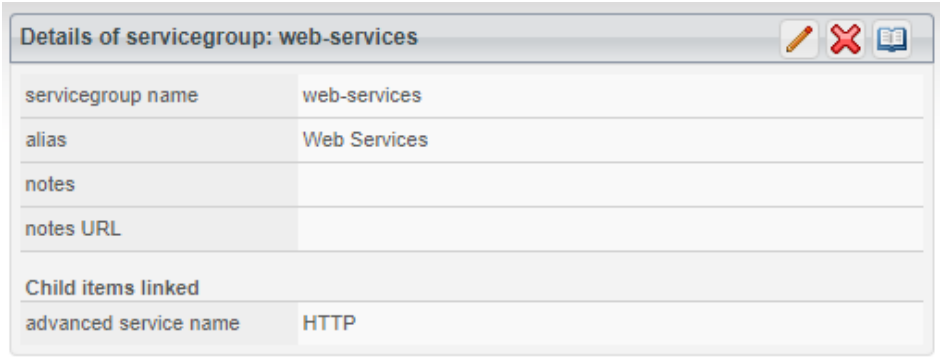


Figura 2.8. *Ejemplo de service group*

2.3.3 COMANDOS

Los comandos definen cómo se deben hacer los chequeos de hosts y servicios, y cómo deben funcionar las notificaciones. Otra de sus funciones es reestablecer el sistema automáticamente si es posible. [9]

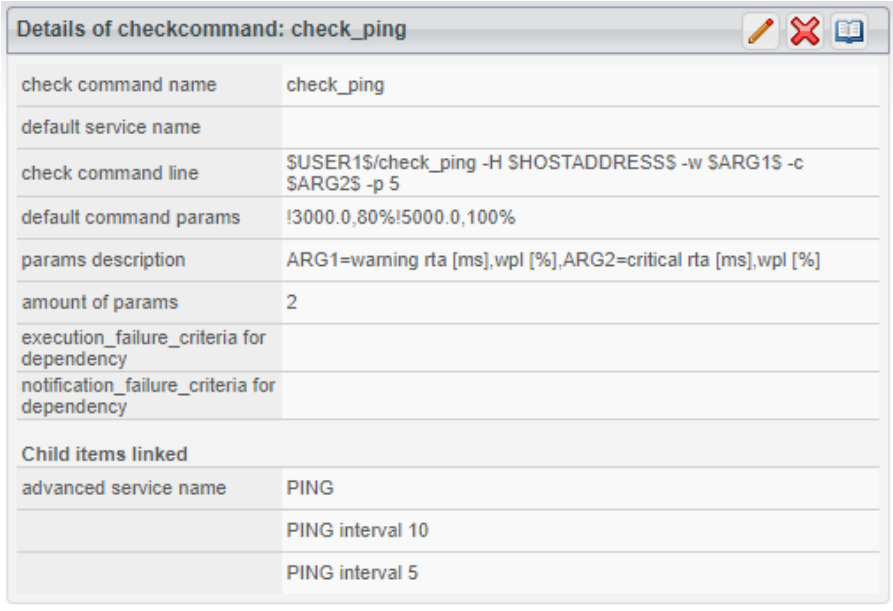
La propia imagen de NEMS incluye una serie de comandos preestablecidos basados en plugins que son los que chequean los distintos servicios (SSH, HTTP, etc.) pero también el usuario puede añadir sus propios comandos.

En la siguiente figura podemos ver los comandos que vienen predefinidos por Nagios y que hacen referencia a los servicios que se pueden monitorizar con dicho servidor.

check command name	[actions]
check_ad	
check_dhcp	
check_exchange	
check_ftp	
check_hpjd	
check_http	
check_iis	
check_imap	
check_local_disk	
check_local_load	
check_local_mrtgtraf	
check_local_procs	
check_local_swap	
check_local_users	
check_nrpe (Linux Monitoring)	
check_nt	
check_ping	
check_pop	
check_smtp	
check_snmp	
check_sql	
check_ssh	
check_tcp	
check_ts	
check_udp	

Figura 2.9. *Comandos configurados en Nagios*

Los comandos se definen con dos parámetros: un nombre único que puede ser el mismo o no al plugin al que hace referencia y una línea de comandos que contiene una serie de argumentos que permite que se le pasen para que el chequeo sea más flexible.



Details of checkcommand: check_ping

check command name	check_ping
default service name	
check command line	$USER1$/check_ping -H $HOSTADDRESS$ -w $ARG1$ -c $ARG2$ -p 5
default command params	!3000.0,80%!5000.0,100%
params description	ARG1=warning rta [ms],wpl [%],ARG2=critical rta [ms],wpl [%]
amount of params	2
execution_failure_criteria for dependency	
notification_failure_criteria for dependency	
Child items linked	
advanced service name	PING
	PING interval 10
	PING interval 5

Figura 2.10. *Ejemplo de comando para monitorizar servicio PING*

2.3.4 TIME PERIODS

Los time periods son definiciones de periodos de tiempo en los que se pueden realizar los chequeos o se pueden enviar notificaciones de equipos y servicios. Estas definiciones se aplican a la hora de definir equipos y servicios en los parámentros check period y notification period.[9]

Nagios trae predefinidos algún time period pero el usuario puede añadir los suyos propios. Solo hace falta un nombre único, un alias y el tiempo que se quiera definir. Por ejemplo, en la siguiente imagen podemos ver cómo se ha añadido un periodo de tiempo que engloba todos los días de la semana y todas las horas del día.

Figura 2.11. *Plantilla para añadir un time period*

2.3.5 CONTACTOS

Los contactos hacen referencia a diferentes personas que pueden ser los propietarios de diferentes máquinas, encargados de gestionar y solucionar problemas que pueden surgir en los dispositivos, destinatarios de notificaciones, etc.

A la hora de crear un contacto solo es obligatorio un nombre, un alias y una dirección de email. También se pueden definir los periodos de notificación de equipos y servicios y que tipo de notificaciones han de ser enviadas al contacto (estas opciones de notificación serán explicadas en el apartado NOTIFICACIONES).

Los contactos se asignan a los usuarios que inician sesión en una de las interfaces web y todas las operaciones que se realicen a través de esa interfaz quedarán registradas como ese usuario y se permitirán dependiendo del acceso que tenga dicho usuario a determinados servicios. [9]

Los contactos también pueden ser agrupados en contact groups para dividir tareas y responsabilidades entre, por ejemplo, los empleados de una empresa. Así, por ejemplo, las notificaciones de los servicios irán destinadas a un grupo de trabajo y las de los dispositivos a otro.

2.3.6 PLANTILLAS

Como ya se ha mencionado anteriormente, Nagios permite crear plantillas para definir parámetros comunes que puedan ser aplicados a la hora de definir nuevos equipos y servicios.

Cuando se aplica una plantilla a un host o servicio, éste adquiere todas las propiedades definidas en la plantilla. Es posible aplicar varias plantillas a un único equipo. Si las plantillas especifican un mismo parámetro, predominará el valor del parámetro de la primera plantilla. [9]

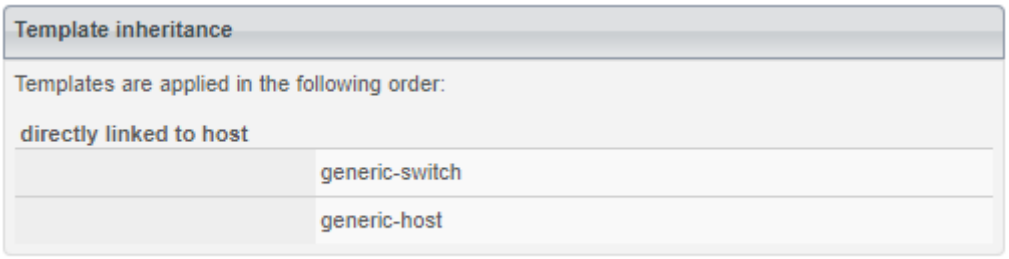


Figura 2.12. *Plantillas utilizadas por un host para su definición*

La anterior figura es una captura de la definición del equipo Raspberry que hemos añadido anteriormente. Dicho equipo hereda parámetros de dos plantillas definidas, generic-switch y generic-host.

2.4 NAGIOS CORE

Nagios Core es la interfaz web que muestra los resultados de la monitorización de hosts y servicios. Ofrece tanto una visión global del sistema como una información más detallada y precisa de cada elemento. También recoge alertas y notificaciones que automáticamente aparecen publicadas en la interfaz.

La visión global de red configurada se puede ver en la pestaña Tactical Overview. Esta da información sobre los estados de dispositivos y servicios, y cuántos tienen las notificaciones y los chequeos habilitados o deshabilitados. En la web se puede ver toda esta información mediante barras gráficas o con una lista más detallada de la información. [9]

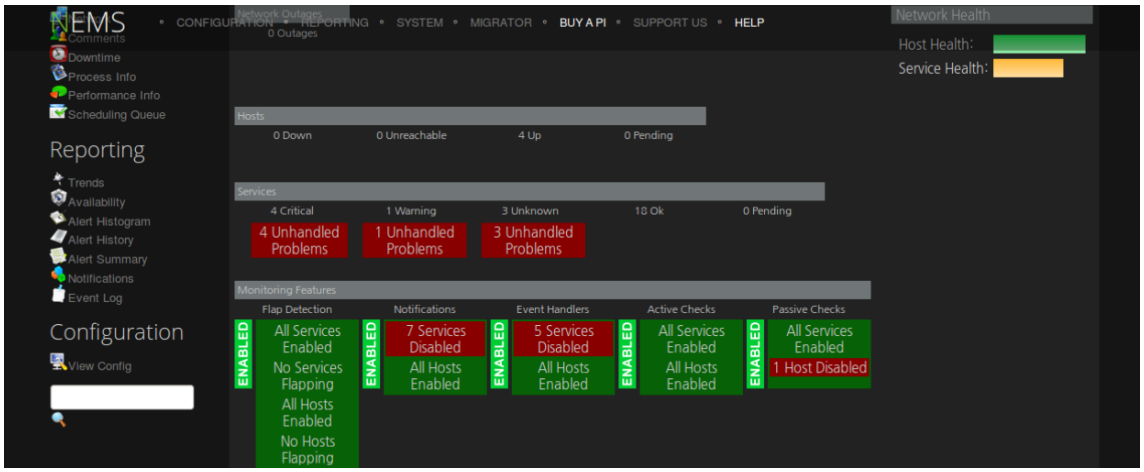


Figura 2.13. *Tactical Overview*

Se puede clicar sobre los servicios deshabilitados para saber en qué dispositivo se obtiene ese servicio erróneo y más detalles acerca del problema.

2.4.1 VISUALIZACIÓN DE HOSTS

En el apartado de Host Detail, se puede ver una lista de todos los dispositivos configurados junto con sus estados e información sobre el último chequeo.

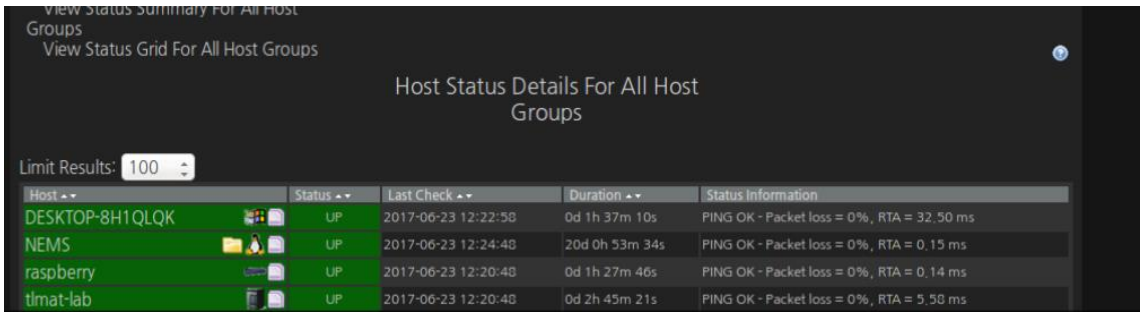


Figura 2.14. *Visualización de los hosts configurados en Nagios Core*

Clicando en cada uno de los dispositivos podemos obtener información más detallada de cada uno.

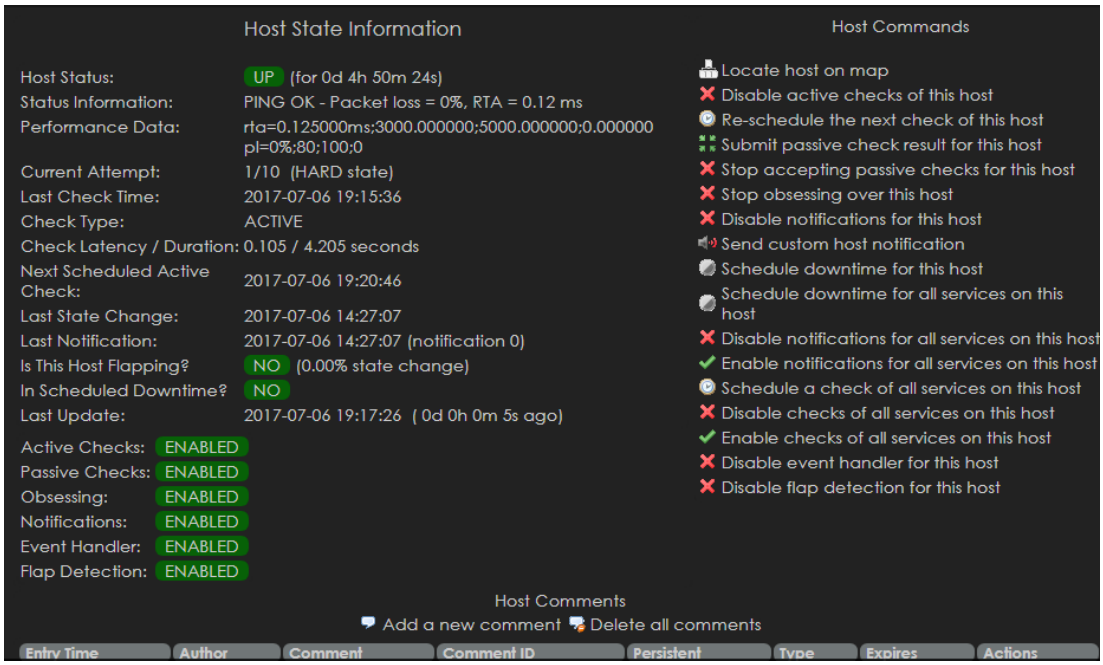


Figura 2.15. *Información específica sobre un dispositivo*

La imagen muestra información detallada sobre el host Raspberry como su estado, información sobre el último chequeo y algunas funcionalidades que pueden estar habilitadas o no en cada host como las notificaciones. También, muestra si el dispositivo está en un estado de flapping; esto se produce cuando una máquina o servicio cambia de estado muy rápidamente.

En la pestaña Hostgroups, aparecen los hosts divididos en los diferentes grupos que se hayan configurado desde Nagios nConf. Por ejemplo, durante la configuración se creó un grupo llamado Linux-server al que pertenecía dos equipos, NEMS y Raspberry.

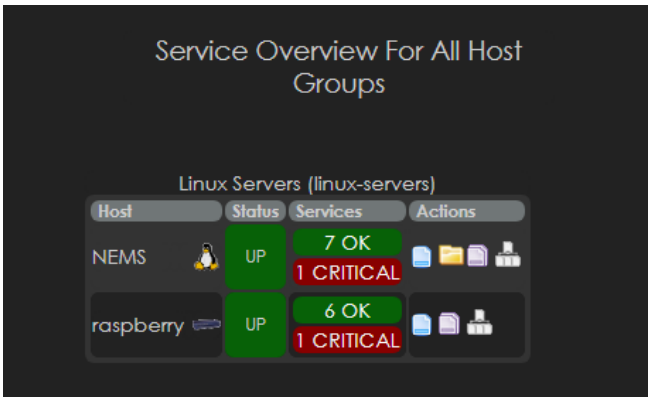


Figura 2.16. *Visualización de grupos de dispositivos*

También existe una pestaña llamada Host problem en la que aparecen los dispositivos cuyo estado es DOWN con información adicional sobre el porqué de dicho estado.

La interfaz web Nagvis también ofrece una visión de la red configurada anteriormente similar a la que se puede ver en el Status map de Nagios Core. Aparece un mapa en el que se recogen todos los hosts; y si pones el ratón sobre cada host te aparece una pestaña con información más detallada y los servicios que cada host tiene asociado.

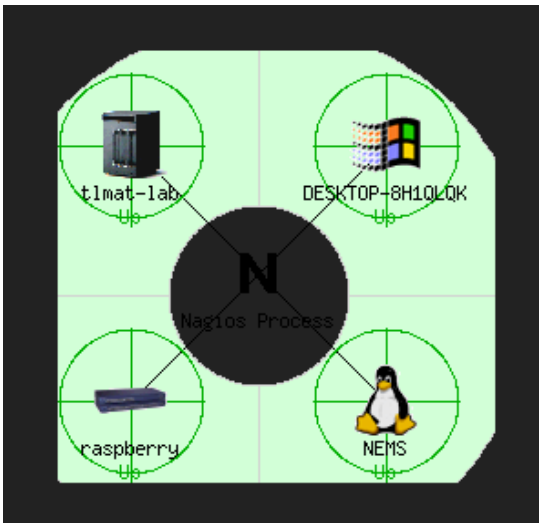


Figura 2.17. *Status map*

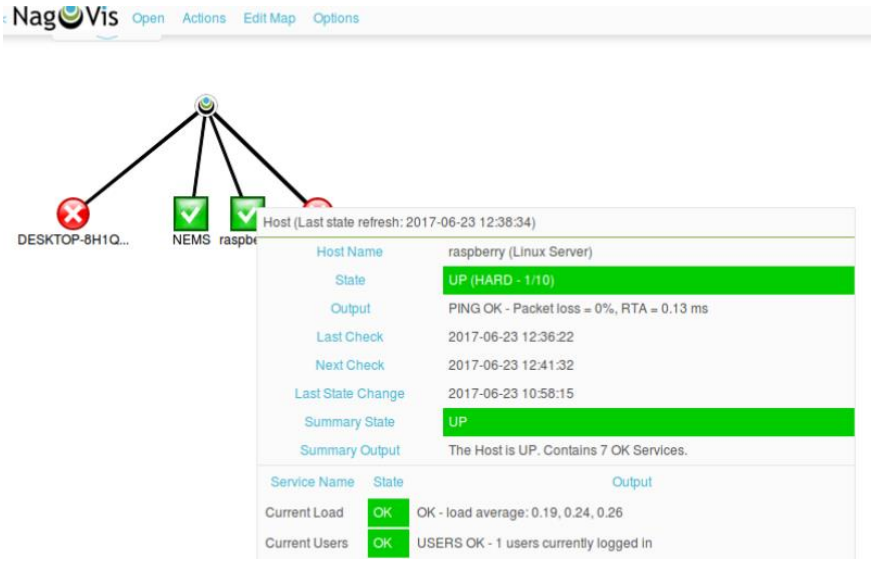


Figura 2.18. *Mapa en la interfaz web NagVis*

En la interfaz web Nagvis los dispositivos aparecerán en verde tanto si su estado es UP como si todos los servicios configurados son monitorizados correctamente; sino aparecerán en rojo.

2.4.2 VISUALIZACIÓN DE SERVICIOS

En la siguiente figura podemos observar una captura de pantalla de Nagios Core en el apartado de Service Detail que muestra una serie de servicios añadidos al router del laboratorio y a la Raspberry: da información del estado de dichos servicios, de la fecha de chequeo e información del chequeo y, en caso de error, el motivo del fallo.

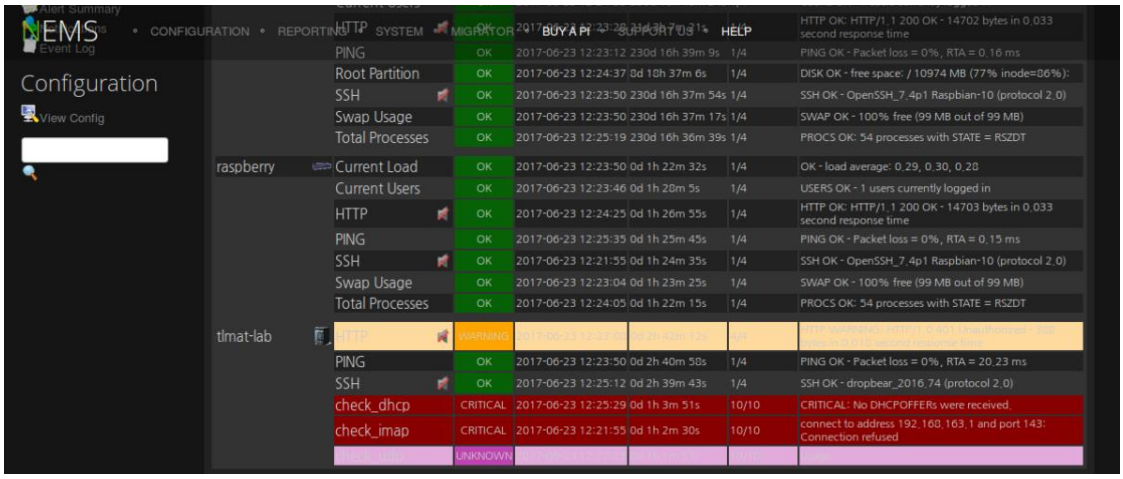


Figura 2.19. Visualización de los servicios monitorizados en tiempo real en Nagios Core

Para ver más información sobre el estado de cada servicio podemos clicar en cada uno de ellos. Por ejemplo, en la siguiente figura vemos el servicio HTTP monitorizado en la Raspberry con más detalle.

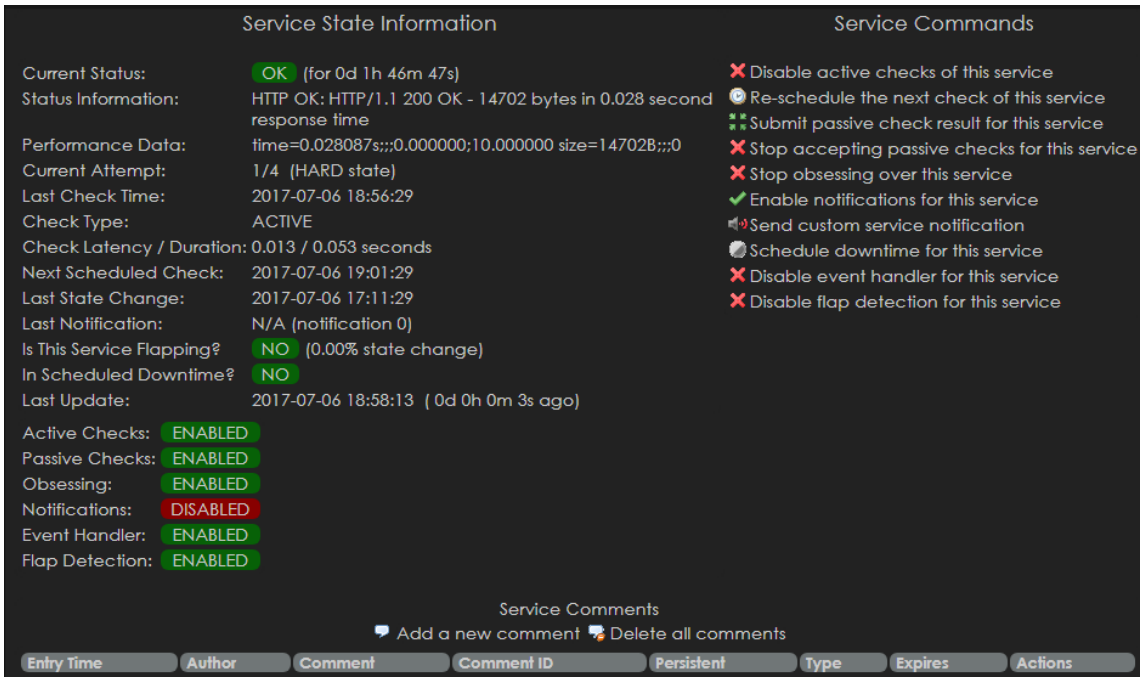


Figura 2.20. Información específica sobre un servicio

Se puede ver una tabla con información detallada del servicio como su estado actual, los resultados del chequeo e información sobre el último y el siguiente chequeo que se pretende realizar. La página también muestra información sobre las notificaciones, que en este caso están deshabilitadas y si el servicio está en un estado de flapping (el servicio cambia muy rápido de estado).

Por último, pueden aparecer comentarios sobre el servicio que haya escrito el administrador, es usual que cuando un servicio falle en este apartado de comentarios aparezca la explicación del fallo.

Como en el caso de los dispositivos, en la pestaña Servicegroups aparecen los dispositivos que monitorizan los servicios incluidos en un grupo. Por ejemplo, en la configuración de NEMS creamos un grupo llamado Web services que solo recogía el servicio HTTP; así aparecerán en este grupo los equipos en los que se esté monitorizando HTTP.

Por último, los problemas sobre servicios se recogerán en un apartado llamado Service Problems.

2.4.3 DOWNTIMES Y SCHEDULING QUEUE

Al configurar una red en NEMS se pueden programar paradas cuando se quiera dejar de monitorizar tanto un dispositivo como un servicio. Esto aparece reflejado en la pestaña Downtime. [9]

Se pueden ver dos listas, una para dispositivos y otra para servicios, en las que aparece el intervalo de tiempo en el que el chequeo está parado y el usuario que ha programado dicha parada.

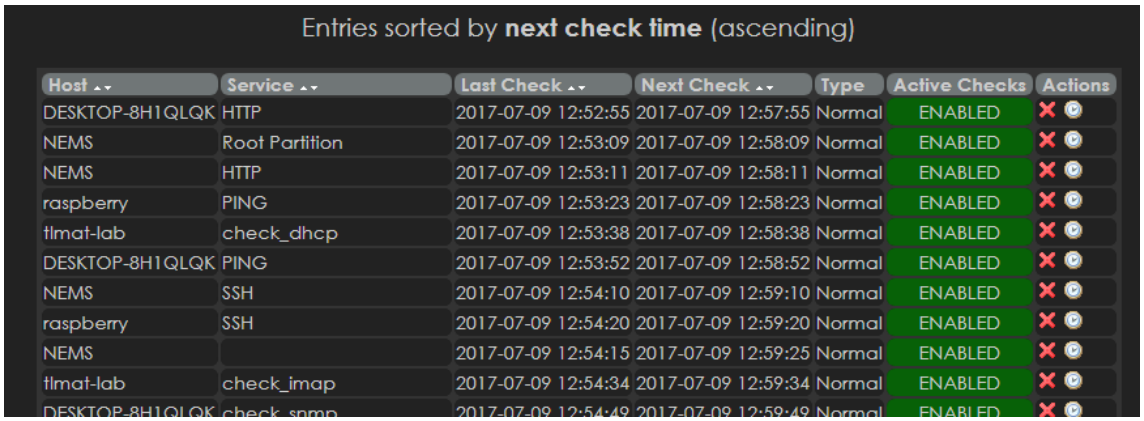


Figura 2.21. *Scheduling queue*

En cuanto a programación de chequeos, en la pestaña Scheduling queue se pueden ver los servicios y los dispositivos que van a ser chequeados ordenados de manera ascendente por proximidad entre la fecha actual y la fecha del siguiente chequeo.

2.4.4 REPORTING

Una de las mejores utilidades de Nagios Core es que se pueden generar informes y alertas. Esta interfaz web ofrece tres tipos de informes:

1. Trends: este informe muestra un historial de los cambios de estado que ha sufrido un dispositivo o servicio junto con la información que se ha ido obteniendo de los respectivos chequeos. [9]

En la siguiente figura se puede ver un informe del dispositivo Raspberry en el que se ha recogido el historial de cambios de estado del dispositivo en los últimos 7 días.

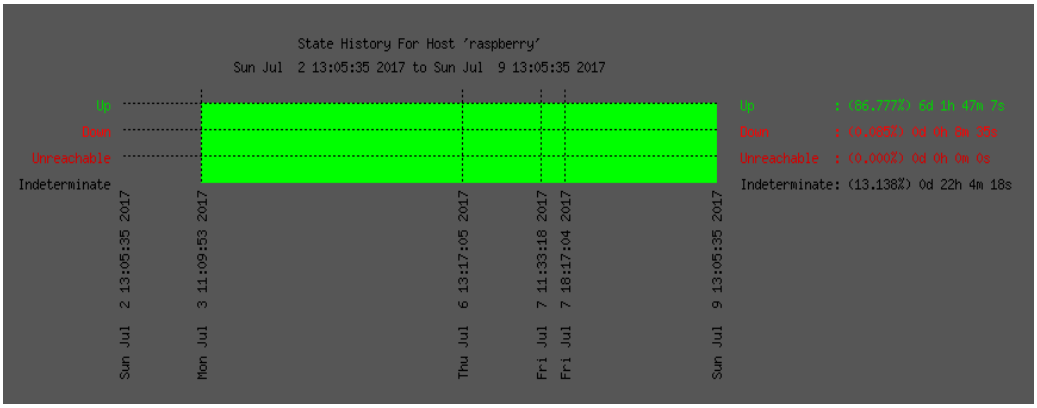


Figura 2.22. *Trend report*

2. Availability: este informe muestra un historial de cuánto tiempo ha estado un dispositivo en un estado determinado. Puede informar sobre un objeto o sobre varios incluyendo grupos de dispositivos o servicios. [9]

   En la siguiente figura podemos observar el informe del grupo de equipos linux-servers con la información de estado en los últimos 7 días.

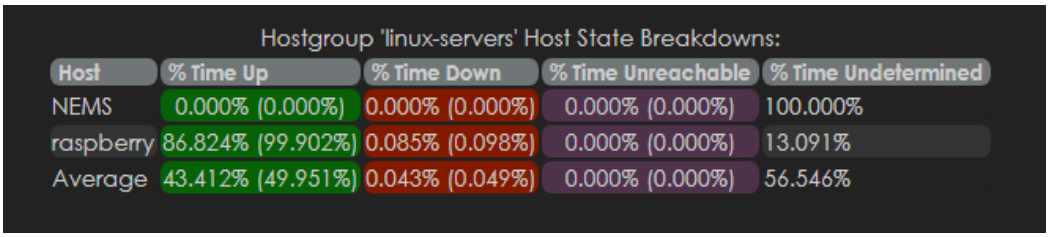


Figura 2.23. *Availability report*

3. Alert: este informa muestra el número de alertas que se han producido para un dispositivo o servicio en un periodo de tiempo. Este informe aparece en modo de histograma. También se puede obtener una lista completa con todas las alertas que se han ido registrando en el sistema. [9]

   En la siguiente imagen se puede ver un histograma con información sobre las alertas que se han producido en el dispositivo DESKTOP durante los últimos 7 días.

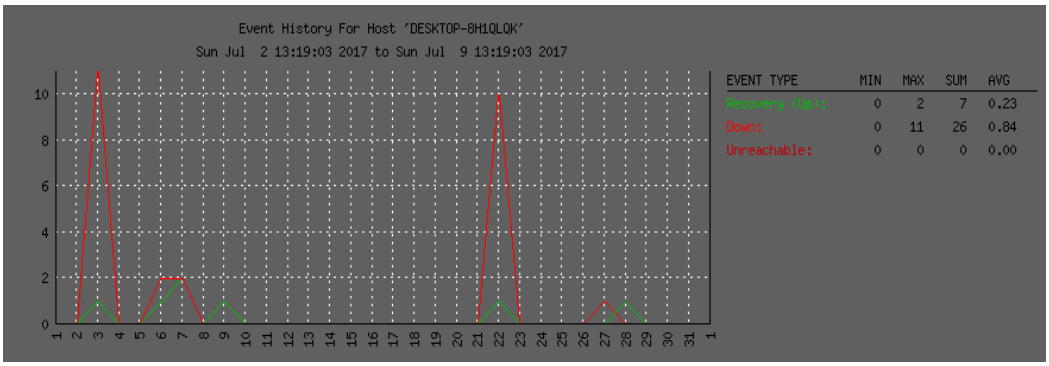


Figura 2.24. *Alert Histogram*

A la hora de generar informes hay que especificar sobre qué dispositivo o servicio se quiere realizar, el periodo de tiempo sobre el que se quiere recoger información y otros parámetros que se quieran o no incluir en los informes.

2.5 NOTIFICACIONES

Las alertas y notificaciones sobre elementos de la red configurados en el servidor se pueden ver en línea sobre Nagios Core dentro del apartado REPORTING o se puede configurar el sistema para que las notificaciones se envíen por correo electrónico para su mejor control.

Host	Service	Type	Time	Contact	Notification Command	Information
DESKTOP-8H1QLQK	CPU Load	UNKNOWN	2017-06-23 12:24:42	admind	notify-service-by-email	NSClient - ERROR: Invalid password.
tlmat-lab	check_udp	UNKNOWN	2017-06-23 12:17:28	admind	notify-service-by-email	Usage:
tlmat-lab	check_imap	CRITICAL	2017-06-23 12:11:58	admind	notify-service-by-email	connect to address 192.168.163.1 and port 143: Connection refused
tlmat-lab	check_dhcp	CRITICAL	2017-06-23 12:05:36	admind	notify-service-by-email	CRITICAL: No DHCPOFFERs were received.
DESKTOP-8H1QLQK	check_snmp	UNKNOWN	2017-06-23 11:58:15	admind	notify-service-by-email	No OIDs specified
DESKTOP-8H1QLQK	Check disk space of /var	CRITICAL	2017-06-23 11:51:24	admind	notify-service-by-email	(Return code of 139 is out of bounds)
tlmat-lab	check_udp	UNKNOWN	2017-06-23 11:42:33	admind	notify-service-by-email	Usage:
tlmat-lab	check_imap	CRITICAL	2017-06-23 11:41:52	admind	notify-service-by-email	connect to address 192.168.163.1 and port 143: Connection refused
tlmat-lab	check_dhcp	CRITICAL	2017-06-23 11:40:41	admind	notify-service-by-email	CRITICAL: No DHCPOFFERs were received.
DESKTOP-8H1QLQK	CPU Load	UNKNOWN	2017-06-23 11:24:40	admind	notify-service-by-email	NSClient - ERROR: Invalid password.
DESKTOP-8H1QLQK	check_snmp	UNKNOWN	2017-06-23 11:23:19	admind	notify-service-by-email	No OIDs specified
DESKTOP-8H1QLQK	check_snmp	UNKNOWN	2017-06-22 12:43:34	admind	notify-service-by-email	No OIDs specified
DESKTOP-8H1QLQK	check_snmp	UNKNOWN	2017-06-22 12:13:30	admind	notify-service-by-email	No OIDs specified
DESKTOP-8H1QLQK	N/A	HOST UP	2017-06-22 12:09:08	admind	notify-host-by-email	PING OK - Packet loss = 0%, RTA = 55,99 ms
DESKTOP-8H1QLQK	N/A	HOST DOWN	2017-06-22 11:45:55	admind	notify-host-by-email	(Host Check Timed Out)

Figura 2.25. *Notificaciones en la interfaz web Nagios Core*

2.5.1 NOTIFICACIONES POR CORREO ELECTRÓNICO

Primero hay que cambiar el fichero de configuración **resource.cfg**. En este fichero se especifica un archivo de recursos opcional que puede contener macros $USERn$. Estas macros pueden almacenar nombres de usuario, contraseñas, rutas de directorio, etc. [11]

En este caso tendremos que configurar una dirección de email desde la cual donde se enviarán las notificaciones, la dirección del servidor SMTP (si se utiliza otro puerto que no sea el 25 para el servidor SMTP, se deberá especificar también de la siguiente manera: smtp.gmail.com:port) y por último el usuario y password para la autenticación del servidor SMTP. [5]

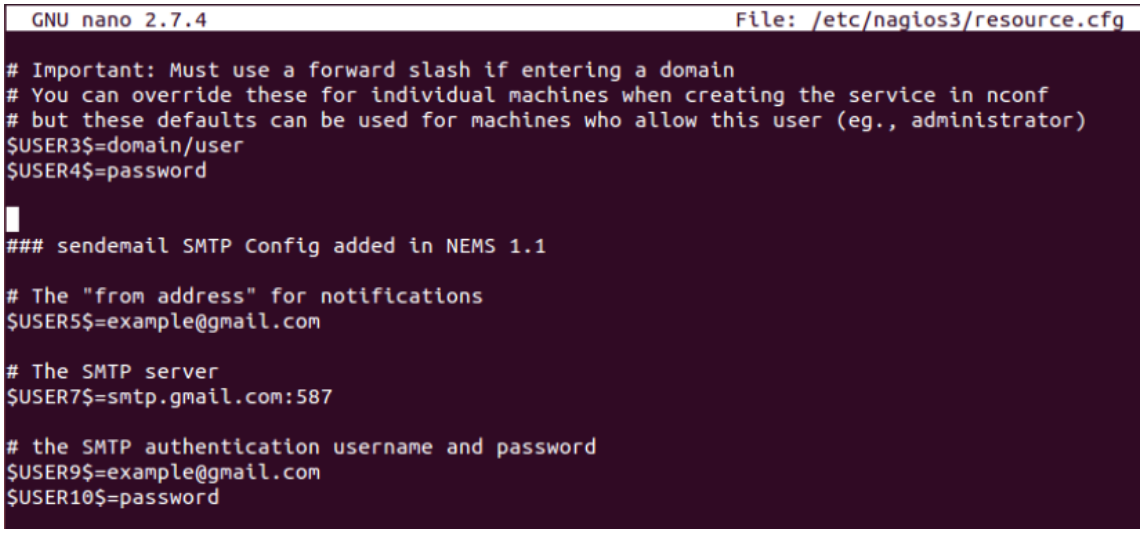


Figura 2.26. Fichero de configuración de notificaciones resource.cfg

Para que se puedan enviar las notificaciones de manera correcta, si se trata de una cuenta Gmail hay que habilitar el acceso a aplicaciones menos seguras a través de este enlace https://myaccount.google.com/lesssecureapps. [5]

Después de esto hay que configurar la dirección de correo de destino. Esto se realiza desde NEMS-nConf dentro de la sección Contacts. En el usuario se podrá configurar la dirección; si hubiera más de un usuario se podrían mandar las notificaciones a diferentes correos dependiendo del usuario que esté utilizando la herramienta.

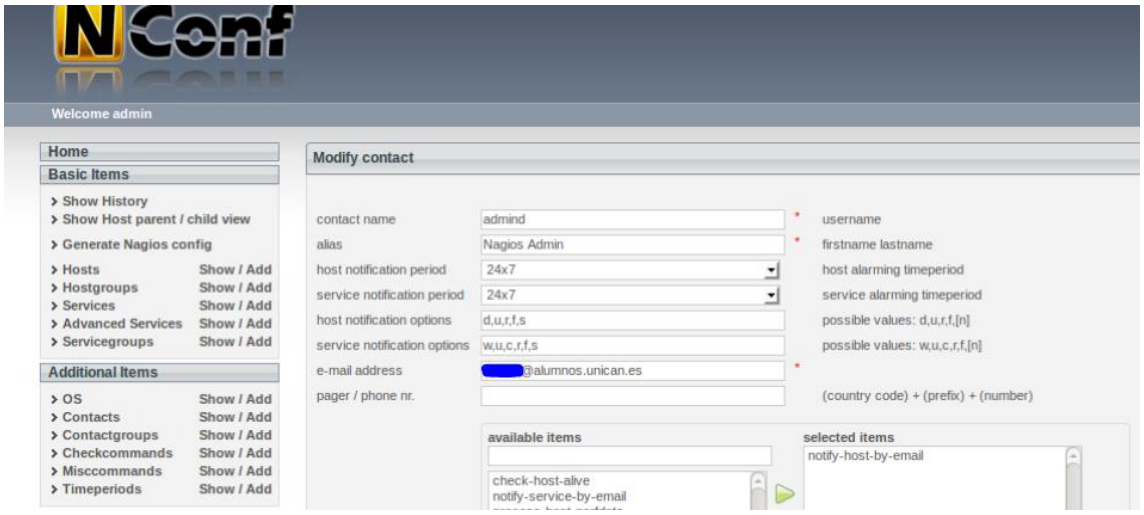


Figura 2.27. Configuración del correo de destino de las notificaciones desde Nagios nConf

Tipos de notificaciones: las notificaciones pueden ser de varios tipos dependiendo si hacen referencia a un dispositivo de la red o a un servicio. [5]

EQUIPOS	SERVICIOS
D – el equipo ha caído	W – Estado de warning
U – el equipo es inalcanzable	U – Estado desconocido
R – notificar al recuperar	C – Estado crítico
F – notificar si está oscilando entre on off	F – El servicio está oscilando entre on off
S – notificar si un tiempo de inactividad de un servicio programado empieza o termina	N – No se notifica
N – no se notifica	

Tabla 2.2. *Tipos de notificaciones en NEMS*

Una vez configurado correctamente, las notificaciones van apareciendo en la bandeja de correo que se haya establecido para recibir dichas alertas.

A modo de ejemplo, en el apartado de servicios la monitorización del protocolo de aplicación IMAP en el router del laboratorio (dispositivo tlmat-lab) aparecía en estado crítico. Tras la configuración de las notificaciones, llegará el siguiente correo que nos informará del dispositivo al que hace referencia la alerta, el servicio afectado e información más detallada sobre el fallo.

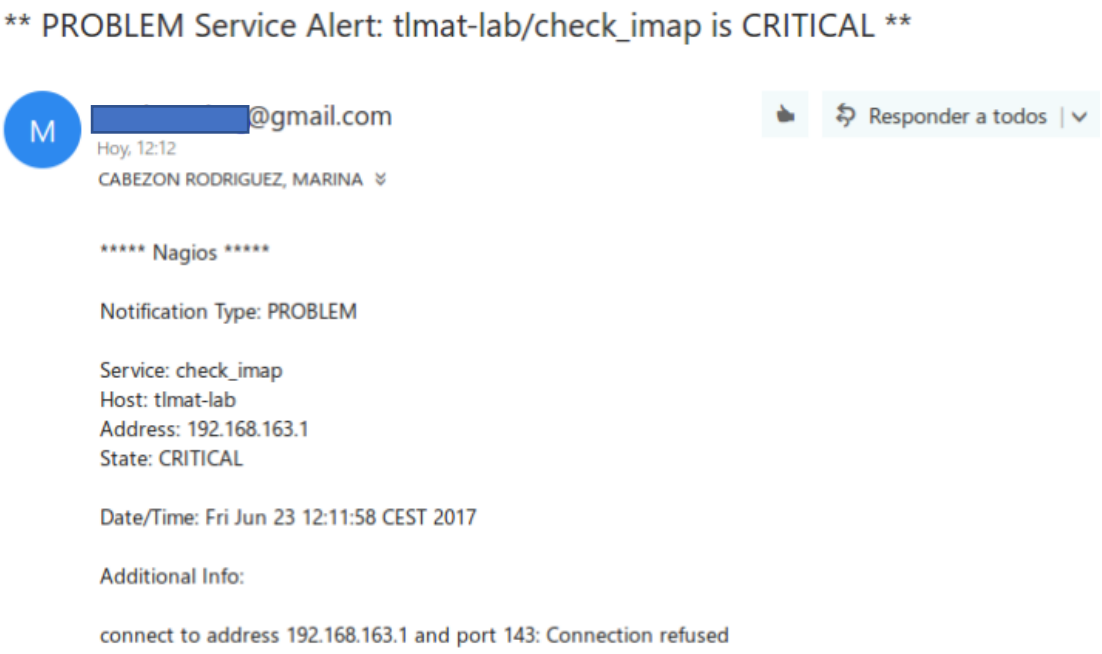


Figura 2.28. *Ejemplo de correo de notificación*

3 MULTI ROUTER TRAFFIC GRAPHER (MRTG)

3.1 INTRODUCCIÓN

MRTG está escrito en Perl y se puede obtener de manera gratuita a través de Internet. Esta herramienta surgió en 1994 en la universidad de Leicester, UK; la universidad disponía de solo un enlace de Internet de 64kbit que durante las horas de trabajo era casi inutilizable debido a la gran cantidad de personas que lo estaban usando a la vez. A través de esta herramienta, se daba información a los usuarios de la ocupación del enlace. [12]

Su funcionamiento es bastante sencillo: cada 5 minutos la herramienta lee el contador de octetos entrantes y salientes del router gateway de Internet. Mediante la diferencia de dos lecturas consecutivas y dividiendo el resultado por el tiempo transcurrido, se determina la velocidad de datos o tráfico promedio en el enlace durante los últimos 5 minutos.[12] Una vez obtenidos estos datos, se muestran en gráficos embebidos en páginas web que pueden ser visualizados desde cualquier navegador.

Además de una visión diaria detallada, MRTG también crea gráficos del tráfico durante los últimos siete días, el último mes y el último año. Esto es posible porque MRTG mantiene un registro de todos los datos obtenidos del router. Este registro se va consolidando automáticamente para que no crezca durante el tiempo, pero sigue guardando la información relevante de todo el tráfico registrado durante los dos últimos años.

Sin embargo, MRTG no está limitado al registro de datos de tráfico. Es posible supervisar cualquier variable SNMP que se elija como monitorizar cargas de sistemas, sesiones de inicio de sesión, disponibilidad de modems, etc.; se puede utilizar un programa externo para recopilar los datos que se quieran supervisar con la herramienta; pero esto queda fuera de este proyecto. MRTG incluso permite acumular dos o más fuentes de datos en un solo gráfico. [12]

Experimentalmente vamos a trabajar con esta herramienta sobre la Raspberry Pi 3, que como también hemos visto anteriormente, a pesar de su reducido tamaño, tiene la suficiente potencia para realizar tareas de gestión de red utilizando las herramientas de software apropiadas.

3.1.1 SNMP

Simple Network Management Protocol es el protocolo de gestión de red a través del cual MRTG es capaz de monitorizar los distintos dispositivos configurados. SNMP está especificado en la RFC 1157. [13]

Los tres conceptos fundamentales de SNMP son MIB, agente y gestor. El gestor y el agente se comunican mediante dicho protocolo. La estación gestora sirve como interfaz entre el gestor humano y el sistema de gestión de red, envía peticiones a los agentes para que estos les manden información. Los dispositivos de red (routers, hosts, switchs, etc.) pueden tener instalados agentes SNMP y éstos responden a las órdenes de las estaciones gestoras y de forma asíncrona las envían información importante no solicitada. [14]

La información de gestión SNMP se recoge en bases de datos llamadas MIBs. Las MIBs se encuentran en los dispositivos gestionados y forman un conjunto de puntos de acceso a los dispositivos desde la estación gestora. Los recursos a monitorizar en la red se encuentran representados en la MIB como objetos y estos objetos están ordenados de forma jerárquica sobre una estructura de árbol. Cada objeto lleva asociado un identificador de objeto único (OID). [14]

Las operaciones SNMP se realizan sobre los objetos de la MIB. Hay tres tipos de operaciones:

1. Get: la estación gestora extrae el valor de un objeto del agente.
2. Set: la estación gestora fija el valor de un objeto del agente.
3. Trap: el agente notifica a la estación gestora eventos significativos.

3.2 ENTORNO DE TRABAJO

Para poder monitorizar routers o dispositivos tenemos que asegurarnos que estos tienen configurado SNMP. Sino se puede configurar de una manera muy básica:

Para entrar en la configuración del router, se hace a través de una sesión telnet:

telnet 192.168.110.1

RI> enable

RI# configure terminal

RI(config)#snmp-server community public ro

RI(config)#end

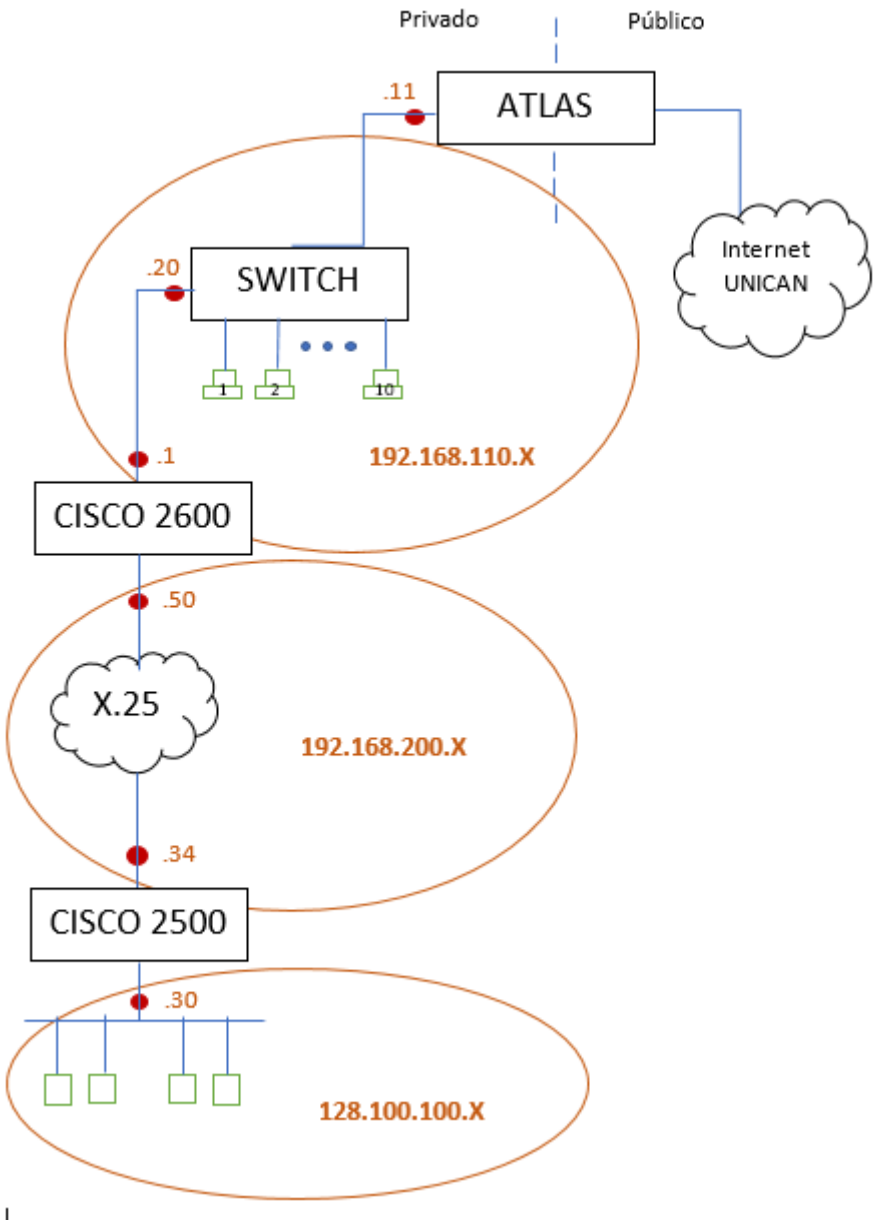


Figura 3.1. *Topología del laboratorio*

Para comprobar el funcionamiento de la herramienta sobre diferentes dispositivos vamos a monitorizar dos routers y un switch.

En la figura podemos observar la topología del laboratorio docente de Telemática. Existen 3 subredes IP: 192.168.110.X en la que se encuentra el switch y atlas, que es el servidor que nos da salida al internet que proporciona la universidad; una subred X.25 entre los routers Cisco; y la subred 128.100.100.X con topología en bus.

Tanto el switch, los routers como atlas son agentes SNMP, por lo tanto, podremos monitorizar el tráfico que pasa por ellos.

3.3 INSTALACIÓN DE SNMP EN LA RASPBERRY PI

Si no tenemos el servicio SNMP instalado previamente, deberemos hacerlo antes de instalar cualquier servicio de MRTG. [15]

sudo apt-get update

sudo apt-get upgrade

sudo apt-get install snmpd snmp

Para que nuestra Raspberry sea accesible desde cualquier otro equipo de la red necesitaremos abrir el fichero de configuración snmpd.conf:

sudo nano /etc/snmp/snmpd.conf

Sustituiremos la línea *agentAddress udp:127.0.0.1:161* por *agentAddress 161*; y en la línea siguiente a '#rocommunity public localhost' insertaremos: *recommunity public.*

Reiniciaremos el servicio:

service snmpd restart

3.4 INSTALACIÓN Y CONFIGURACIÓN DE MRTG EN RASPBERRY PI

Instalaremos la herramienta a través de la ventana de comandos:

sudo apr-get install mrtg

Como hemos dicho anteriormente se necesita tener un servidor web instalado, si no lo tenemos previamente, podremos instalar uno cualquiera en mi caso, he optado por Apache. A parte de ser el servidor web más utilizado, se descarga fácilmente del paquete APT (Advanced Packing Tool). [16]

sudo apt-get install apache2

Para comprobar si Apache está instalado y funcionando:

sudo service apache2 status

Si no está funcionando se activará de la siguiente manera: **sudo service apache2 start**.

Una vez instalado el servidor web y comprobar que funciona, debemos crear la carpeta donde se van a crear los datos MRTG que observaremos desde el navegador.

mkdir /var/www/html/mrtg

En cuanto a la configuración del sistema, a la hora de añadir equipos a monitorizar lo más sencillo es utilizar una herramienta que ya viene incluida con el paquete de MRTG, cfgmaker. Trabajando primeramente sobre el router Cisco 2600, se configuraría desde la ventana de comandos de la siguiente manera:

sudo cfgmaker public@192.168.110.1 >> /etc/mrtg.cfg

Cfgmaker crea en el fichero de configuración mrtg.cfg código a partir de la información snmp específica que obtenga del dispositivo.

Para acceder al router se utilizar la notación community@router. Community o comunidad es como la contraseña del dispositivo al que quieres acceder y que se especificó a la hora de configurar snmp en el router. Si no se especifica la comunidad, por defecto será *public*. Si la comunidad no es correcta, no se obtendrá respuesta del dispositivo.[12]

Router hace referencia a la dirección IP del dispositivo SNMP o su DNS. A continuación del nombre se pueden especificar hasta 6 opciones más de SNMP: router[:[prt][:[tmout][:[retr][:[backoff][:vers]]]]] [12]

De especial interés es la opción *vers* ya que hace referencia a la versión de SNMP que se requiere que tenga el dispositivo a monitorizar. Cfgmaker soporta SNMPv3; a la hora de ejecutar el cfgmaker hay que añadir la opción **--enablesnmpv3** antes de community@router para habilitar dicha versión.

Además de esa opción, y con la misma sintaxis que ésta, existen muchas más para hacer más específica y fácil la búsqueda de interfaces. [12] Algunas de ellas son:

--version	Imprime la versión de MRTG.
--ifref *nr|ip|eth|descr|name*	Permite seleccionar el método de búsqueda de interfaces. Si no se selecciona ninguno, por defecto es nr que significa que identifica las interfaces por su índice en la MIB (hay que tener que este índice puede cambiar por ejemplo si el router añade más interfaces; ya que SNMP las ordena léxico-gráficamente). Las otras opciones de búsqueda son: por su dirección IP (ip), por la dirección ethernet (eth), por la descripción de la interfaz (descr) o por su nombre (name).
--ifdesc *nr|ip|eth|descr|name|type|alias*	Permite seleccionar qué quieres utilizar para describir la interfaz. Esta descripción aparecerá en el código HTML que crea la herramienta en el fichero de configuración.
--enable-ipv6	Para soportar dirección IP versión 6.
--no-down	Cfgmaker solo incluye en el fichero de configuración las interfaces que operativamente están UP (las demás si que las incluye, pero comentadas). Con esta opción, aparecerían todas las interfaces.

--output *file*	Crea un fichero llamado file con la información recibida del cfgmaker (que aparece de todas maneras en la ventana de comandos).
--nointerfaces	No genera líneas de configuración para las interfaces; simplemente las muestra por pantalla. Cfgmaker no hay ningún sondeo del router para recuperar la información de las interfaces lo que hace que la ejecución de la herramienta sea más rápida. Con esta opción no se crearían las gráficas de tráfico en el servidor web que es lo que estamos buscando de esta herramienta.

Tabla 3.1. *Opciones de la herramienta cfgmaker*

Al ejecutar la herramienta cfgmaker, hace un recorrido por la MIB del router dando información sobre las interfaces de este y, entre otras cosas, los índices que estos tienen en la MIB; esto último es importante porque el índice es lo que va a utilizar para diferenciar el tráfico entre interfaces de un mismo router. [16]

```
pi@NEMS:~ $ sudo cfgmaker  public@192.168.110.1
--base: Get Device Info on public@192.168.110.1:
--base: Vendor Id: cisco
--base: Populating confcache
--base: Get Interface Info
--base: Walking ifIndex
--snpd:   public@192.168.110.1: -> 1 -> ifIndex = 1
--snpd:   public@192.168.110.1: -> 2 -> ifIndex = 2
--snpd:   public@192.168.110.1: -> 3 -> ifIndex = 3
--snpd:   public@192.168.110.1: -> 4 -> ifIndex = 4
--snpd:   public@192.168.110.1: -> 5 -> ifIndex = 5
--base: Walking ifType
--snpd:   public@192.168.110.1: -> 1 -> ifType = 6
--snpd:   public@192.168.110.1: -> 2 -> ifType = 5
--snpd:   public@192.168.110.1: -> 3 -> ifType = 6
--snpd:   public@192.168.110.1: -> 4 -> ifType = 22
--snpd:   public@192.168.110.1: -> 5 -> ifType = 1
--base: Walking ifAdminStatus
--snpd:   public@192.168.110.1: -> 1 -> ifAdminStatus = 1
--snpd:   public@192.168.110.1: -> 2 -> ifAdminStatus = 1
--snpd:   public@192.168.110.1: -> 3 -> ifAdminStatus = 1
--snpd:   public@192.168.110.1: -> 4 -> ifAdminStatus = 2
--snpd:   public@192.168.110.1: -> 5 -> ifAdminStatus = 1
--base: Walking ifOperStatus
--snpd:   public@192.168.110.1: -> 1 -> ifOperStatus = 1
--snpd:   public@192.168.110.1: -> 2 -> ifOperStatus = 2
--snpd:   public@192.168.110.1: -> 3 -> ifOperStatus = 1
--snpd:   public@192.168.110.1: -> 4 -> ifOperStatus = 2
--snpd:   public@192.168.110.1: -> 5 -> ifOperStatus = 1
--base: Walking ifMtu
--snpd:   public@192.168.110.1: -> 1 -> ifMtu = 1500
--snpd:   public@192.168.110.1: -> 2 -> ifMtu = 1500
--snpd:   public@192.168.110.1: -> 3 -> ifMtu = 1500
--snpd:   public@192.168.110.1: -> 4 -> ifMtu = 1500
--snpd:   public@192.168.110.1: -> 5 -> ifMtu = 1500
--base: Walking ifAlias
--snpd:   public@192.168.110.1: -> 1 -> ifAlias =
--snpd:   public@192.168.110.1: -> 2 -> ifAlias =
--snpd:   public@192.168.110.1: -> 3 -> ifAlias =
--snpd:   public@192.168.110.1: -> 4 -> ifAlias =
--snpd:   public@192.168.110.1: -> 5 -> ifAlias =
--base: Walking vmVlan
--base: Walking vlanTrunkPortDynamicStatus
--base: Walking ifSpeed
--snpd:   public@192.168.110.1: -> 1 -> ifSpeed = 100000000
--snpd:   public@192.168.110.1: -> 2 -> ifSpeed = 1544000
--snpd:   public@192.168.110.1: -> 3 -> ifSpeed = 100000000
--snpd:   public@192.168.110.1: -> 4 -> ifSpeed = 1544000
--snpd:   public@192.168.110.1: -> 5 -> ifSpeed = 4294967295
# Created by
# /usr/bin/cfgmaker public@192.168.110.1
```

Figura 3.2. *Cfgmaker sobre el router cisco 2600*

Como podemos observar en la captura de pantalla, al ejecutar el cfgmaker sobre el router cisco 2600, sabemos que este tiene 5 interfaces: 2 ethernet, 2 serial y una de consola. También se ve más información sobre estas interfaces como su velocidad, su MTU, …

A parte de dicha información, la utilidad de la herramienta es que crea un fichero de configuración de código Perl que contiene variables que recogen la información SNMP de cada interfaz de los dispositivos y que luego se utilizan en un código HTML (que también crea la propia herramienta) para que el usuario pueda ver la información desde el navegador web. [12]

```
##################################################################
# Multi Router Traffic Grapher -- Sample Configuration File
##################################################################
# This file is for use with mrtg-2.5.4c

# Global configuration
WorkDir: /var/www/html/mrtg
RunAsDaemon: Yes
WriteExpires: Yes

Title[^]: Traffic Analysis for

# 128K leased line
# ---------------
#Title[leased]: a 128K leased line
#PageTop[leased]: <H1>Our 128K link to the outside world</H1>
#Target[leased]: 1:public@router.localnet
#MaxBytes[leased]: 16000

#Title[cisco2600_if]: Traffic Analysis for FastEthernet0/0 of cisco2600
#PageTop[cisco2600_if]:
#Target[cisco2600_if]: if:public@192.168.110.1
#MaxBytes[cisco2600_if]: 12500000



# Created by
# /usr/bin/cfgmaker public@192.168.110.1


### Global Config Options

#  for UNIX
# WorkDir: /home/http/mrtg

#  for Debian
WorkDir: /var/www/html/mrtg

#  or for NT
# WorkDir: c:\mrtgdata

### Global Defaults

#  to get bits instead of bytes and graphs growing to the right
# Options[_]: growright, bits

EnableIPv6: no

##################################################################
# System: c2600
# Description: Cisco Internetwork Operating System Software
#          IOS (tm) C2600 Software (C2600-I-M), Version 12.0(7)T,  RELEASE SOFTWARE (fc2)
#          Copyright (c) 1986-1999 by cisco Systems, Inc.
```

Figura 3.3. *Fichero configuración mrtg.cfg que resulta del cfgmaker*

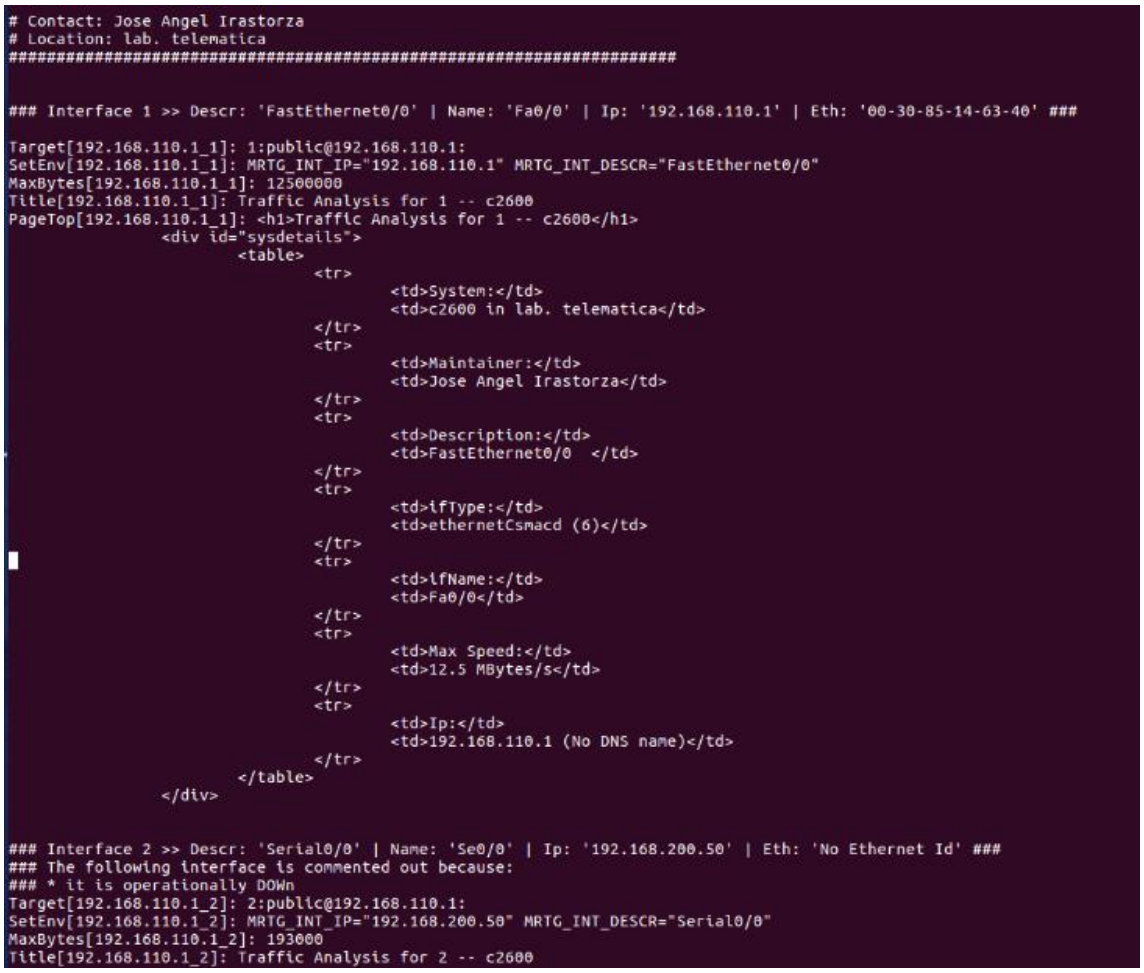


Figura 3.4. *Continuación del fichero de configuración mrtg.cfg*

En la primera imagen podemos ver las líneas de configuración que se han creado para el dispositivo Cisco 2600. Por defecto toma el directorio de trabajo, el directorio donde se van a crear todos los archivos web, como **/var/www/mrtg** pero Apache no coge la información de esa ruta sino de **/var/www/html/mrtg**.

Por lo tanto, cada vez que se vaya a incluir un nuevo dispositivo hay que cambiar la línea *WorkDir: /var/www/mrtg* por *WorkDir: /var/www/html/mrtg* o a la hora de ejercutar el cfgmaker desde la ventana de comandos, añadir la opción **--global "workdir: /var/www/html/mrtg"**.

En la segunda imagen, aparece un ejemplo del código html para una de las interfaces del router.

Una vez creado el fichero de configuración hay que generar un index.html, que es la página web principal donde vamos a poder ver los datos de los dispositivos configurados. Esto se realiza con la herramienta indexmaker.

indexmaker /etc/mrtg.cfg > /var/www/html/mrtg/index.html

Esta herramienta, como la anterior, ofrece varias opciones: [12]

--title *text*	Añadir un título a la página web index.html.
--bodyopt *text*	Permite cambiar los colores de lo referente a la etiqueta <BODY> del código HTML.
--columns *number*	Distribuye los gráficos en tantas columnas como se especifique. Por defecto crea 2 columnas.
--sort *title|name|descr|original*	Ordena los gráficos en la página web por el título, el nombre, la descripción de la interfaz o lo deja como está.
--enumerate	Enumera los gráficos para generar un orden.
--width *number*	Establece un ancho de gráfico.
--height *number*	Establece una altura de gráfico.
--section *h1|title|name|description|portname*	Permite elegir que se quiere como título de cada gráfico.
--show *day|week|month|year|none*	Se puede elegir que gráficos se muestran en la página index.html. Se crean gráficos diarios, mensuales y anuales y por defecto aparecen los diarios en el index.html (aunque cuando pinchas en ellos te aparecen los tres).

Tabla 3.2. *Opciones de la herramienta indexmaker*

Ya solo queda iniciar el servicio para poder ver los resultados en el navegador web. Se puede hacer con **sudo service mrtg start** pero es mejor reiniciar la Raspberry Pi (**sudo reboot**).

Cada vez que reiniciásemos el sistema tendríamos que ejecutar MRTG manualmente, por lo que es mejor crear un servicio que lo inicie automáticamente cada vez que encendamos la Raspberry Pi.

Inicio automático: [15]

Los servicios de Linux pueden ser iniciados o parados con scripts alojados en la carpeta /etc/init.d. Para que el servicio MRTG se inicie automáticamente deberemos crear el siguiente script en la carpeta **/etc/init.d/mrtg** :

```
#! /bin/sh
PATH=/sbin:/usr/sbin:/bin:/usr/bin
DESC="MRTG"
NAME="mrtg"
DAEMON=/usr/bin/$NAME
DAEMON_ARGS="/etc/mrtg.cfg –user root --logging /var/log/mrtg.log"
case "$1" in
  start)
        echo "Starting $DESC..."
        env LANG=C $DAEMON $DAEMON_ARGS
        echo "$NAME started."
        ;;
  stop)
        echo "Stopping $DESC..."
        pkill $NAME &> /dev/null
        echo "$NAME stopped."
        ;;
  *)
        FULL_NAME=/etc/init.d/$NAME
        echo "Usage: $FULL_NAME {start|stop}." >&2
        ;;
esac
exit
```

Figura 3.5. *Script para inicio del servicio MRTG automático*

Este archivo debe ser ejecutable por lo que tenemos que darle permisos:

sudo chmod +x /etc/init.d/mrtg

Por último, programamos su ejecución automática instalando el archivo en la secuencia de reinicio de la Raspberry Pi:

sudo update-rc.d mrtg defaults

Reiniciamos el sistema para que los cambios queden guardados:

sudo shutdown -r now

3.5 RESULTADOS DE MONITORIZACIÓN

Tras la correcta instalación de todos los archivos, comprobaremos que todo funciona desde la siguiente URL http://direcciónIPdelaraspberry/mrtg.

Aparece la página index.html creada en la configuración de MRTG con los gráficos diarios del tráfico de las interfaces de los dispositivos configurados.

Figura 3.6. *Index.html que muestra los gráficos de datos de tráfico*

La línea azul de los gráficos hace referencia al tráfico de salida y la línea verde índica el nivel de tráfico de entrada.

En las imágenes se muestra el tráfico que hay en 3 interfaces del router cisco 2600; de las gráficas c2600, la 1 y la 3 hacen referencia a interfaces ethernet y la 2 a una interfaz serie.

El switch tiene 24 interfaces y cada interfaz está conectada a un ordenador del laboratorio. Monitorizándolas 24 observamos que solo hay tráfico de entrada en la interfaz 7 ya que es el ordenador desde el que se está trabajando.

Y por último, he monitorizado dos interfaces del router cisco 2500 y desde uno de los ordenadores de la red x.25 se han estado enviando PINGs y por lo tanto en la última gráfica se puede observar que el tráfico de entrada es igual que el tráfico de salida.

Si queremos más información sobre cada una de las interfaces, se puede pinchar en los gráficos y aparece una página como la de la siguiente imagen:

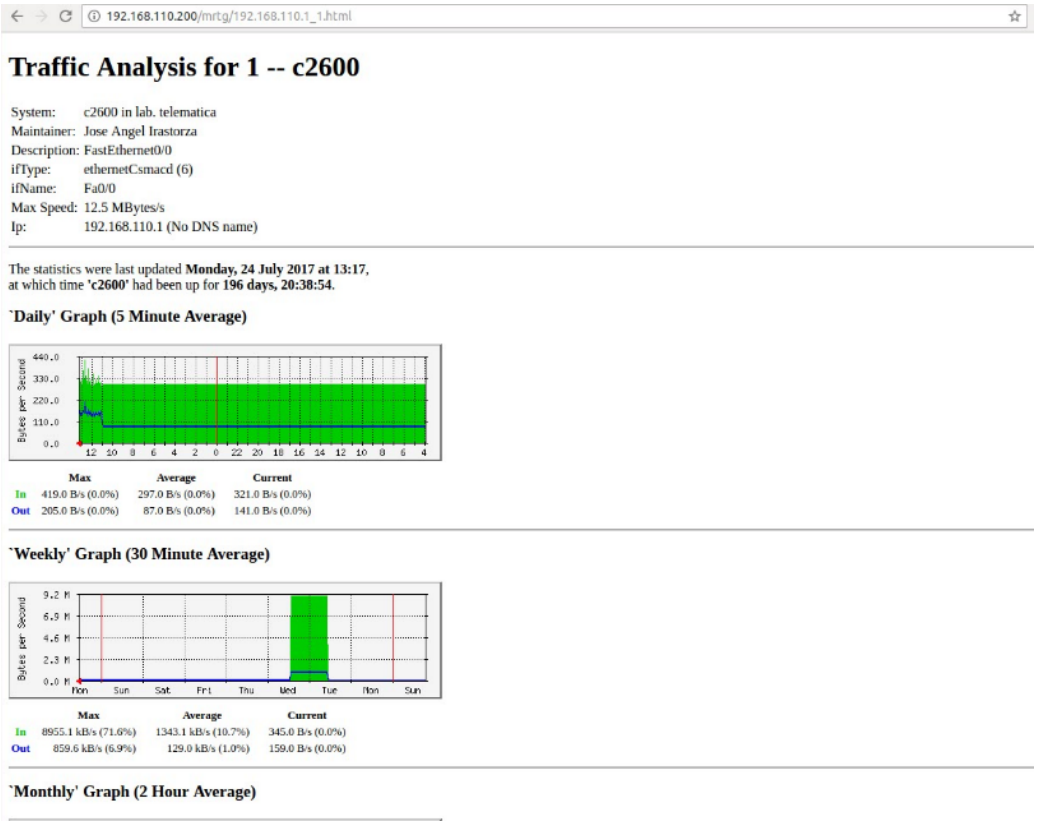


Figura 3.7. *Gráficos diarios y semanales de datos de tráfico*

Te aparece información como el nombre de la interfaz, su descripción, la velocidad, su dirección IP, cuando ha sido la última vez que se han actualizado los datos de los gráficos, etc.

Además, se incluyen cuatro gráficas con los datos promedio de tráfico diario, semanal, mensual y anual. Los datos se van actualizando en tiempo real: los datos diarios se actualizan cada 5 minutos, los semanales cada 30 minutos, los mensuales cada dos horas y los anuales cada día.

Debajo de cada gráfica aparece la tasa máxima, media y actual de tráfico tanto de entrada como de salida.

3.5.1 VERACIDAD DE LOS DATOS

Una vez obtenidos los gráficos confiamos en que los datos que muestran son correctos, pero como todo, no hay que confiar ciegamente. Por ejemplo, puede que, debido a un error, el router deje de enviar los datos de tráfico correctamente y los gráficos muestren que no existe tráfico en dicho router, lo cual sería una interpretación errónea de los datos. Por ello para comprobar la exactitud de la información de MRTG no viene mal utilizar herramientas como la interfaz de comandos del router.

Cuando MRTG no puede recopilar o almacenar todos los datos de un router, repite el valor del intervalo anterior en vez de bajar la tasa de tráfico a 0. [17] Por ello, hay que tener cuidado al ver secciones de tráfico completamente planas porque puede ser que en ese periodo de tiempo no haya sido posible recoger los datos de tráfico.

MRTG necesita bastante mantenimiento ya que cada que vez que se mueva una red o las interfaces de un router habrá que comprobar que dichos cambios se vean reflejados dentro de la configuración del servicio. [17]

4 NETFLOW

4.1 INTRODUCCIÓN

Netflow es un protocolo de red desarrollado por Cisco que permite recopilar información de tráfico IP y supervisarlo. A diferencia de la monitorización de redes activa, como la implementada por las herramientas PING o Traceroute, en la cual se inyecta tráfico adicional para realizar las diferentes medidas; esta tecnología agrega los paquetes de información en flujos, los cuales se exportan para ser almacenados y analizados.

Un flujo se define como "un conjunto de paquetes IP que pasan un punto de observación en la red durante un cierto intervalo de tiempo, de manera que todos los paquetes pertenecientes a un flujo particular tienen un conjunto de propiedades comunes". [18] Estos atributos comunes son: dirección IP origen, dirección IP destino, puerto origen, puerto destino, tipo de protocolo IP, interfaz del router o switch y tipo de servicio IP.

La monitorización de redes mediante flujos de datos se puede dividir en varias fases: [19]

1. Observación de paquetes: los paquetes de datos que pasan por un punto de observación, por ejemplo, interfaces de routers o switches, son capturados.
2. Medición y exportación del flujo: los paquetes se introducen en flujos que son registrados en una base de datos llamada Flow cache. Cuando el flujo ha terminado, un registro del mismo se exporta a dispositivos para su almacenamiento y procesado, llamados Colectores Netflow.
3. Recopilación de datos: los datos recibidos se almacenan y pre-procesan. Alguna de las tareas de pre-procesado son la compresión de datos, agregación, anonimización de datos, filtrado y generación de resúmenes.
4. Análisis de datos: correlación y agregación, clasificación y caracterización del tráfico, detección de anomalías, búsqueda de datos, informes y alertas, etc.

Integraremos la Raspberry Pi en el proceso de recogida de datos y exportación de flujos Netflow al colector. Cuando estas funciones se hacen en un dispositivo dedicado nos referimos a él como sonda Netflow.

Además, para el proceso de análisis de datos se va a usar Pandora Flexible Monitoring System (Pandora FMS). Es un software de monitorización flexible desarrollado por Ártica, una compañía española fundada en 2005, que se utiliza para gestionar infraestructuras TI como equipos de red, servidores Windows y Unix, infraestructura virtualizada y todo tipo de aplicaciones. [20] En este documento dejaremos de lado las múltiples opciones de monitorización que tiene, y nos centraremos en las posibilidades en cuanto al estudio del tráfico Netflow.

4.2 ENTORNO DE TRABAJO

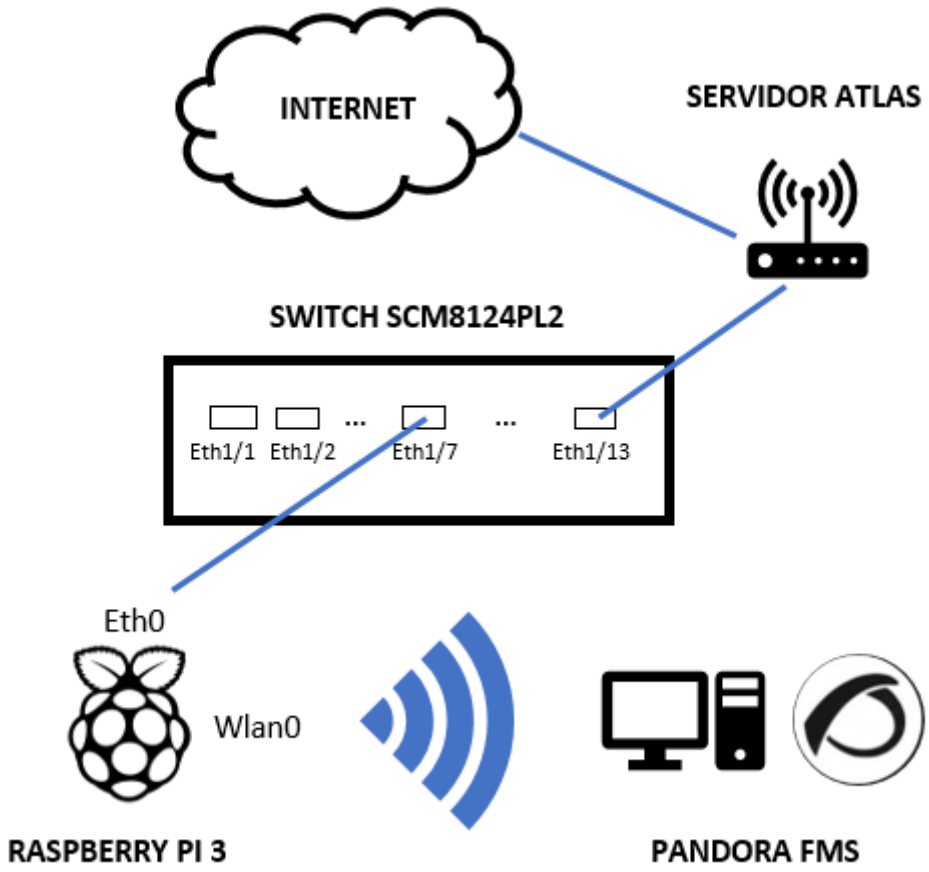


Figura 4.1. *Entorno de trabajo para la herramienta Netflow*

Se va a trabajar sobre la subred 192.168.110.X del laboratorio de docencia del Departamento de Telemática de la Universidad de Cantabria para monitorizar el tráfico de datos que entra o sale hacía Internet. Esta información pasará por el servidor atlas del laboratorio que hace de proxy.

Tanto el servidor atlas como los dispositivos de la red local del laboratorio (ordenadores, routers, etc.) están conectados a un switch.

La observación de paquetes, su introducción en flujos y su exportación hacia el colector, se hará a través de una sonda Netflow o "flow probe" que en este caso será la Raspberry Pi 3. Hay que configurar la Raspberry para que a partir de la información recogida de la subred se generen los datos Netflow que serán analizados posteriormente.

Para que la sonda pueda observar todo el tráfico de la subred, el switch tendrá que reflejar los paquetes de la interfaz a la que está conectado el servidor atlas (Eth1/13) a la interfaz donde está conectado la sonda (Eth1/7). Esto es lo que normalmente se conoce como 'Port mirroring', lo que requiere un cambio en la configuración del switch.

Como la conexión Ethernet de la Raspberry se encargar de escuchar y recolectar los datos de tráfico, tendremos que utilizar la interfaz Wi-Fi para enviar los datos Netflow al servidor de Pandora FMS, que hará la función de colector. Para ello, necesitaremos otro router (dirección IP 192.168.110.11), al cual conectaremos la Raspberry y el colector. Los datos Netflow se enviarán a través del protocolo UDP.

Una vez recibida la información en el colector, a través de la consola que lleva implementada Pandora FMS, se podrá analizar la información de monitorización. Esta consola consiste en una interfaz web que muestra los datos recolectados mediante gráficos y permite aplicar filtros para un mejor estudio de la información.

4.3 CONFIGURACIÓN DE LA RED Y EL ENTORNO

4.3.1 PORT MIRRORING

Hay que configurar el switch del laboratorio para que todo el tráfico de datos que haya en la red LAN, y que pasa a través del servidor atlas, pueda ser observado por la sonda Netflow.

Para ello, establecemos una sesión telnet con el switch cuya dirección IP es 192.168.110.20:

telnet 192.168.110.20

Realizaremos el port mirroring desde la interfaz ethernet 1/13, que es donde está conectado el proxy, a la interfaz ethernet 1/7, donde conectaremos la Raspberry Pi. De este modo todo el tráfico que pase por la interfaz 13 del switch será reenviado a la interfaz 7. En la siguiente imagen se muestran los comandos para establecer dicha configuración

```
Vty-0#config
Vty-0(config)#interface ethernet 1/7
Vty-0(config-if)#port monitor ethernet 1/13 both
```

Figura 4.2. *Configuración del port mirroring en un switch SMC*

El comando **port monitor** configura una sesión espejo o “mirror session” El puerto destino se establece especificando una interfaz Ethernet. Si a la hora de establecer una sesión espejo añadimos la palabra “both”, se reflejarán tanto los paquetes recibidos como los transmitidos por dicha interfaz. [21]

El comando **show port** muestra la configuración de un puerto espejo o “mirror port”.

```
Vty-0#show port monitor ethernet 1/7
Port Mirroring
-------------------------------------
 Destination Port (listen port) : Eth1/ 7
 Source Port (monitored port)   : Eth1/13
 Mode                           : RX/TX
```

Figura 4.3. *Port mirroring en la interfaz ethernet 1/7 del switch*

La velocidad del puerto origen y del puerto destino deben coincidir, de lo contrario el tráfico podría desbordar y se produciría un fallo.

4.3.2 NETFLOW PROBE

Antes de configurar la Raspberry Pi para que funcione como una sonda Netflow, deberemos instalar la imagen del sistema operativo Raspbian en ella. Para ello descargaremos la imagen de la página web oficial www.raspberrypi.org, así nos aseguramos de poder descargar la última versión de la imagen.

Una vez grabado e instalado en la Raspberry Pi y con acceso a internet, trabajaremos en ella remotamente mediante ssh.

ssh pi@dirección_IP_Raspberry

Una vez conectados, actualizaremos los repositorios y paquetes:

sudo apt-get update && sudo apt-get upgrade

Ahora sí, hay que instalar las herramientas necesarias para que la Raspberry Pi pueda actuar como una sonda Netflow.

Para recolectar los datos de tráfico utilizaremos la herramienta fprobe, que se puede descargar del paquete apt-get. Esta herramienta los recopila y lo exporta en flujos Netflow al dispositivo colector. Para ello, hay que especificar la interfaz desde la que se quieren recoger los datos de tráfico y la dirección IP y puerto del colector a la que queremos redirigir la información recolectada por la sonda. [22]

En el laboratorio, utilizamos la interfaz ethernet de la Raspberry Pi para escuchar y recoger los datos de tráfico, y la interfaz wlan0 para enviar los flujos al servidor de Pandora FMS.

Para facilitar la gestión y el acceso a la Raspberry Pi es conveniente poner una IP estática a la interfaz Wi-Fi del dispositivo. En el laboratorio, conectaremos la Raspberry Pi a otro router vía Wi-Fi para que pueda enviar los datos al colector que también estará conectado a esa red.

Editamos el fichero wpa_supplicant.conf estableciendo el usuario y contraseña de la red Wi-Fi a la que nos queremos conectar:

sudo nano /etc/wpa_supplicant/wpa_supplicant.conf

```
  GNU nano 2.2.6                File: /etc/wpa_supplicant/wpa_supplicant.conf

country=GB
ctrl_interface=DIR=/var/run/wpa_supplicant GROUP=netdev
update_config=1

network={
        ssid="LABTLMAT"
        psk="[redacted]"
}
```

Figura 4.4. *Fichero wpa_supplicant.conf*

Y editamos el fichero /network/interfaces estableciendo la dirección IP fija que vamos a asignar a la interfaz Wi-Fi de la Raspberry Pi.

sudo nano /etc/network/interfaces

```
  GNU nano 2.2.6                          File: /etc/network/interfaces

# interfaces(5) file used by ifup(8) and ifdown(8)

# Please note that this file is written to be used with dhcpcd
# For static IP, consult /etc/dhcpcd.conf and 'man dhcpcd.conf'

# Include files from /etc/network/interfaces.d:
source-directory /etc/network/interfaces.d

auto lo
iface lo inet loopback

iface eth0 inet manual

auto wlan0
allow-hotplug wlan0
iface wlan0 inet static
    wpa-conf /etc/wpa_supplicant/wpa_supplicant.conf
    address 192.168.110.92
    netmask 255.255.255.0
    broadcast 192.168.110.255
    gateway 192.168.110.90

iface default inet dhcp
```

Figura 4.5. *Fichero /etc/network/interfaces*

Deshabilitamos la interfaz ethernet con el siguiente comando:

sudo ip addr flush dev eth0

Con las dos conexiones preparadas, habilitaremos el ip_forwarding entre ambas interfaces. Esto quiere decir que los paquetes que se reciben por una interfaz del dispositivo se retransmitirán por otra interfaz hacia el nodo colector.

Cuando un paquete IP se recibe por una interfaz física, el módulo IP de entrada (IPinput) procesa el paquete. Si la dirección IP destino del paquete se corresponde con la del dispositivo se procesa el paquete y se pasa al módulo TCPinput. En el caso de que la dirección IP destino no se corresponda con la del dispositivo y el módulo IP forwarding esté activado, se pasa el paquete al módulo IP de salida (IPoutput), se consulta la tabla de encaminamiento y el paquete se retransmite por la interfaz correspondiente. [23]

sudo /sbin/sysctl -w net/ipv4/ip_forward=1

sudo sysctl -p para guardar cambios

Comprobamos si el IP forwarding está bien activado:

cat /proc/sys/net/ipv4/ip_forward

Si devuelve un 1 es que está activado, sino tendremos que activarlo.

Cada vez que se reinicia la Raspberry, el IP forwarding se desactiva y la interfaz ethernet, que antes hemos borrado, se reactiva. Por lo tanto, tendremos que volver a hacer estos pasos cada vez que encendamos la Raspberry o configurarlos en el inicio.

Una vez realizada esta configuración adicional, instalamos y ejecutamos la herramienta fprobe para convertir la Raspberry Pi en una sonda Netflow.

sudo apt-get install fprobe

Durante el proceso de instalación se tendrán que elegir la interfaz desde la que se recoge la información de la red, y la dirección IP y el puerto destino del colector donde se quieren exportar los datos Netflow. En el caso de estudio, la interfaz será eth0 y la dirección y puerto destino será la dirección IP del servidor de Pandora FMS (192.168.110.96) y el puerto por donde está escuchando; como los flujos de datos se exportan sobre el protocolo UDP, y el colector por defecto escuchará en el puerto 9995, es aconsejable elegir dicho puerto. Si más tarde se desean cambiar alguno de los datos anteriores, tan solo hará falta realizar los cambios en el fichero **/etc/default/fprobe**.

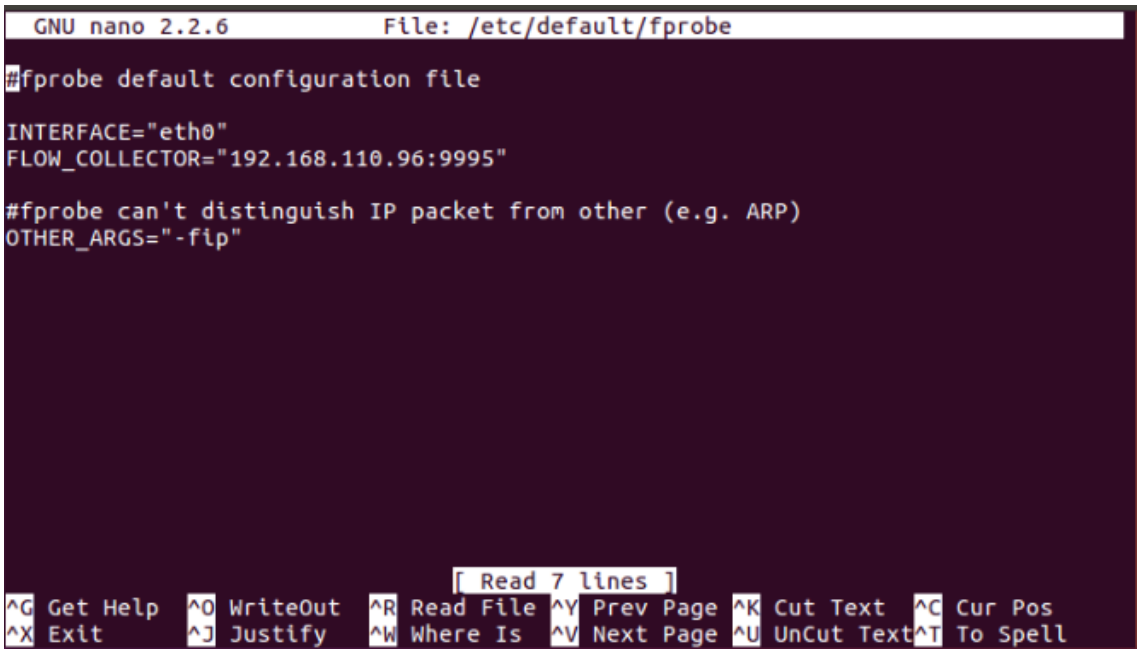


Figura 4.6. Configuración del fichero fprobe

Con esto ya tendríamos implementada la sonda Netflow, pero para asegurarnos de que funciona en todo momento, sobre todo ante reinicios y fallos de procesos, en el arranque del dispositivo haremos que se ejecute un script que comprobará que el servicio fprobe está funcionando y si no lo está, lo ejecuta de nuevo. [22]

Este es el script **netflow.sh**:

```
#!/bin/bash
check=`ps aux | grep fprobe | grep -v grep | wc -l`
if [ $check -eq 0 ]; then
/usr/sbin/fprobe -ieth0 -fip 192.168.110.96:9995
fi
```

Editar fichero **/etc/rc.local** añadiendo "**sh /home/pi/netflow.sh**" para que se ejecute en el arranque del dispositivo.

4.3.3 PANDORA FMS SOBRE UBUNTU

Pandora FMS es capaz de monitorizar el tráfico IP haciendo uso del protocolo Netflow. Permite mostrar patrones y datos generales del tráfico que resultan de gran utilidad.

Existen imágenes que instalan Pandora FMS y se pueden descargar de la página web oficial https://pandorafms.org/es/. Aunque en este apartado se va a explicar cómo instalar y configurar Pandora FMS sobre Ubuntu 16.04 LTS.

Abrir la terminal de Ubuntu y actualizar lista de repositorios e instalar actualizaciones:

sudo apt-get update && sudo apt-get upgrade

Modificamos la lista de repositorios que se encuentra en el fichero /etc/apt/sources.list, agregándole el repositorio de Ártica que son necesarios para la instalación de Pandora. Como no hay unos repositorios específicos para Ubuntu, descargaremos los correspondientes a Debian Wheezy. [24]

sudo nano /etc/apt/sources.list

Añadimos: **deb http://firefly.artica.es/debian/wheezy**

Actualizamos la base de datos de repositorios para guardar los cambios.

sudo apt-get update

Hay que descargar e instalar el cliente WMI

cd ~/Downloads

wget http://ufpr.dl.sourceforge.net/project/pandora/Tools%20and%20dependencies%20%28All%20versions%29/DEB%20Debian%2C%20Ubuntu/wmi-client_0112-1_amd64.deb

sudo dpkg -i wmi-client_0112-1_amd64.deb

Partiendo de un sistema operativo recién instalado, tendremos que descargar algunas dependencias necesarias como apache, mysql, PHP, etc. Pandora FMS requiere de PHP en una versión 5 asique si el sistema operativo que se está utilizando es Ubuntu 14.04 se deberá instalar dicha versión; en el caso de Ubuntu 16.04 se deberá descargar la versión 5.6 de PHP.

En algunos casos para poder descargar e instalar la versión PHP 5.6 es necesario realizar lo siguiente:

sudo apt-get install software-properties-common

sudo add-apt-repository -y ppa:ondrej/php

sudo apt-get update

Instalamos las dependencias necesarias para instalar el servidor y la consola de Pandora: [25]

sudo apt-get install snmp snmpd libtime-format-perl libxml-simple-perl libxml-twig-perl libdbi-perl libnetaddr-ip-perl libhtml-parser-perl wmi-client xprobe2 nmap libmail-sendmail-perl traceroute libio-socket-inet6-perl libhtml-tree-perl libsnmp-perl snmp-mibs-downloader libio-socket-multicast-perl libsnmp-perl libjson-perl php5.6 libapache2-mod php5.6 apache2 mysql-server php5.6-gd php5.6-mysql php-pear php5.6-snmp php-db php-gettext graphviz mysql-client php5.6-curl php5.6-xmlrpc php5.6-ldap dbconfig-common php5.6-mbstring php5.6-zip

Entre estas herramientas, se encuentra mysql que es un servidor en el que se va a crear una base de datos para guardar los datos de Pandora FMS. Al instalarlo pide un usuario y contraseña; por defecto, el usuario será **root**. Esto será relevante para un proceso de instalación que veremos más adelante.

Ubuntu 16.04 LTS utiliza la versión 7.0 de PHP, por lo tanto, es posible que sea necesario desactivar esta versión y activar PHP 5.6.

sudo a2dismod php7.0

sudo a2enmod php5.6

sudo service apache2 restart

Ahora instalamos los paquetes de Pandora FMS: servidor, consola y agente.

sudo apt-get install pandorafms-console pandorafms-server pandorafms-agent-unix

Una vez instalado todo desde la terminal de Ubuntu, tendremos que terminar la instalación de la consola desde la siguiente URL: http://dirección_IP_servidor_Pandora/pandora_console/install.php en nuestro caso dirección_IP_servidor_Pandora = 192.168.110.96 (esta es la dirección que tendremos que configurar en la sonda para que le envíe los datos Netflow).

Ahora solo habrá que seguir los pasos indicados para crear la base de datos de Pandora. Se hará una revisión de las dependencias instaladas anteriormente.

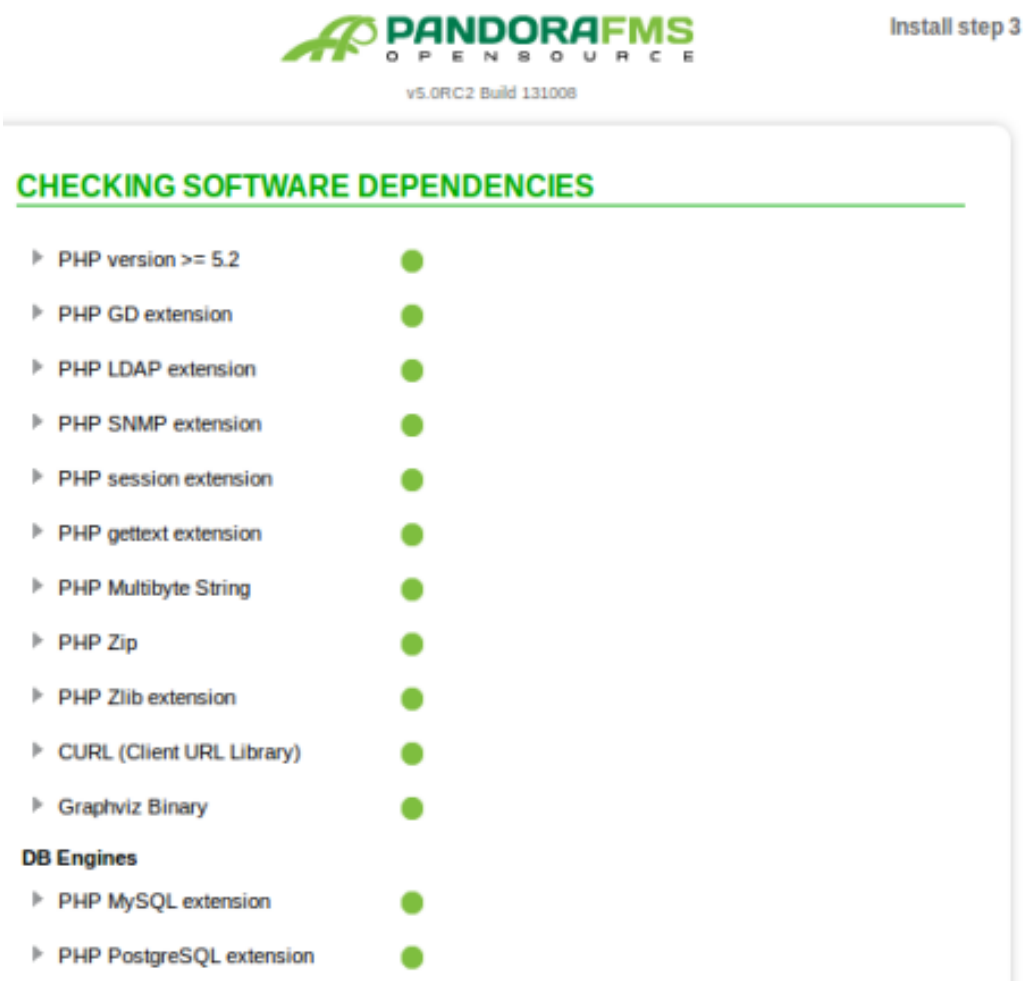


Figura 4.7. *Comprobación de dependencias de Pandora FMS*

Si alguno de los círculos estuviera en rojo significaría que falta esa dependencia y no se podría continuar. Es posible que con el comando **sudo apt-get -f install** se instalen las dependencias que faltan o sino habría que instalarlas independientemente.

Una vez corregido esto, se pasará a crear la base datos a partir de los datos de acceso al servidor mysql, que se configuraron durante su instalación.

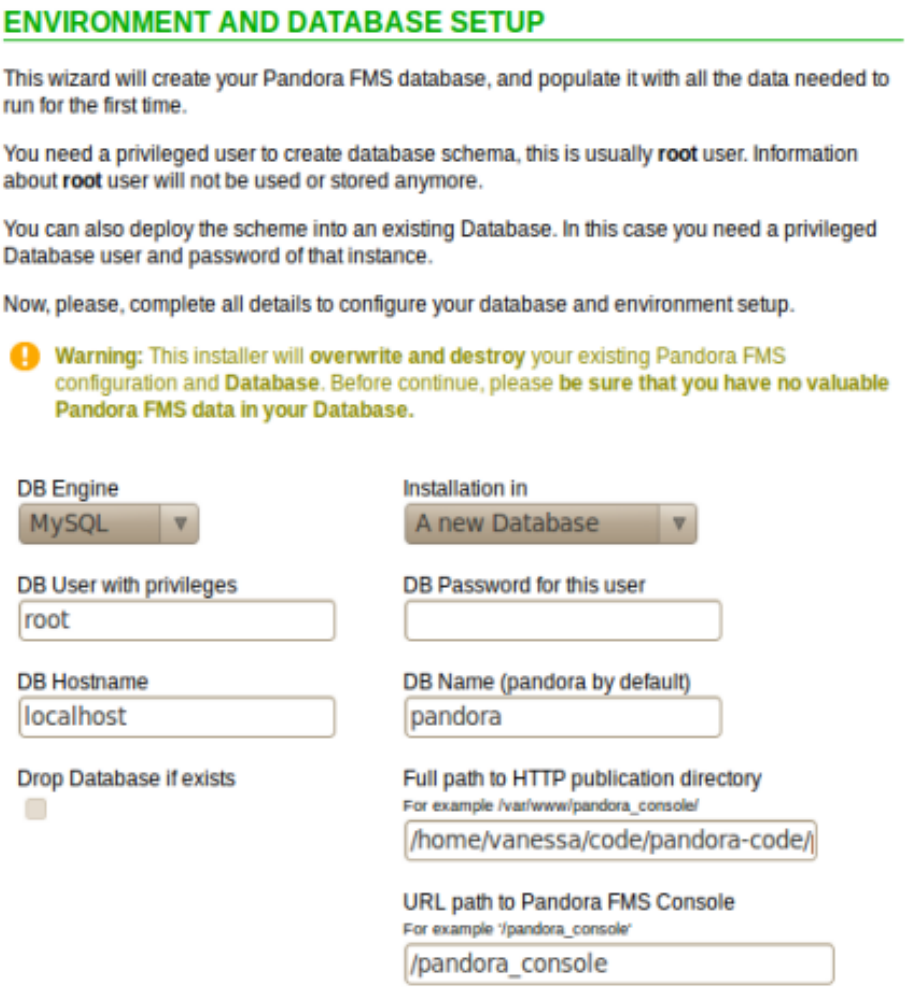


Figura 4.8. *Creación de base de datos de Pandora FMS*

En *DB User with privileges* se debe escribir el usuario del servidor de mysql, en este caso **root**, y en *DB Password for this user*, la contraseña elegida al instalar mysql.

Es posible que, a la hora de crear el esquema de la base de datos, aparezca este error en la pantalla:

Figura 4.9. *Error al crear la base de datos de Pandora FMS*

En tal caso, el error se soluciona buscando el fichero **my.cnf**:

sudo find / -name "*.cnf"

Y editar este fichero añadiendo:

[mysqld]

sql-mode="NO_AUTO_CREATE_USER,NO_ENGINE_SUBSTITUTION"

Así se quitaría el error y crearía la base de datos de Pandora.

Es importante que una vez creada, en la pantalla te aparece una contraseña aleatoria para la base de datos. Hay que configurar el fichero **/etc/pandora/pandora_server.conf** añadiendo dicha contraseña donde ponga “dbpass”.

Aquí finalizaría la instalación del servidor y consola de pandora.

Se puede accerder a la consola desde el navegador URL: http://dirección_IP_servidorPandora/pandora_console/ . El usuario será admin y la contraseña pandora.

Y tendremos que iniciar el servidor desde la terminal:

sudo /etc/init.d/pandora_server start

Cuando entremos en la consola veremos unos mensajes de alerta que indican que hay que cambiar algunos valores del fichero de configuración de Pandora. [7]

sudo nano /etc/php5/apache2/php.ini

En la sentencia **disable_functions** borrar **pctnl_exec**

Cambiar los valores de las siguientes sentencias a los que se indican a continuación:

max_execution_time = 0

max_input_time = -1

upload_max_filesize = 900M

memory_limit = 600M

4.3.4 COLECTOR NETFLOW

En realidad, el colector no es el servidor de Pandora FMS sino que este hace uso de una herramienta open-source llamada nfcapd que se encarga de almacenar la información Netflow en ficheros binarios en una ubicación determinada. Pandora FMS leerá dichos archivos, conocida la ubicación, procesándola y representándola al usuario mediante gráficos.

La herramienta nfcapd se encuentra dentro del paquete nfdump que contiene, a parte de la mencionada, una serie de herramientas que recopilan y procesan los datos Netflow. Nfdump almacena los flujos de datos en ficheros divididos en tiempo. [26]

Programas pertenecientes al paquete nfdump: [26]

nfcapd	Netflow capture Daemon	Lee los datos netflow de la red y los almacena en ficheros. Estos archivos se rotan automáticamente cada 5 minutos (lo que hace más simple la consulta al ser ficheros más pequeños) y se crean en forma de árbol, un año, debajo de éste los meses y más abajo

		los días y las horas y sobre cada uno de éstos, cuelga a su vez los ficheros de dicha hora. (Se necesita sincronización horaria entre el emisor netflow y el receptor).
nfdump	Netflow dump	Lee los datos netflow almacenados por nfcapd. Muestra los datos de flujo y puede crear estadísticas de direcciones IP, puertos, … Su sintaxis es similar a tcpdump.
nfprofile	Netflow profiler	Lee los datos netflow almacenados por nfcapd y los filtra de acuerdo a unos filtros especificados (profile). Almacena estos datos filtrados en archivos.
nfreply	Netflow reply	Lee los datos netflow almacenados por nfcapd y los envía a través de la red a otro host.
nfclean.pf	Clean up all data	Script que limpia todos los datos.
ft2nfdump	Read and convert flow-tools data	Lee ficheros de datos y los convierte en formato nfdump para que puedan ser procesados.

Tabla 4.1. *Herramientas del paquete nfdump*

Por lo tanto, teniendo instalado el servidor de Pandora en un host, conectado a la misma red que la sonda Netflow para que le envíe los flujos Netflow vía Wi-Fi. Estos datos se enviarán sobre el protocolo UDP.

En la siguiente captura del programa Wireshark, se pueden ver un conjunto de tramas que están llegando al colector (dirección IP 192.168.110.96) de la sonda Raspberry. El puerto de destino se comprueba que es el 9995, el que utiliza la herramienta nfcapd para escuchar por defecto; y el que hemos configurado en la sonda como receptor de los datos Netflow.

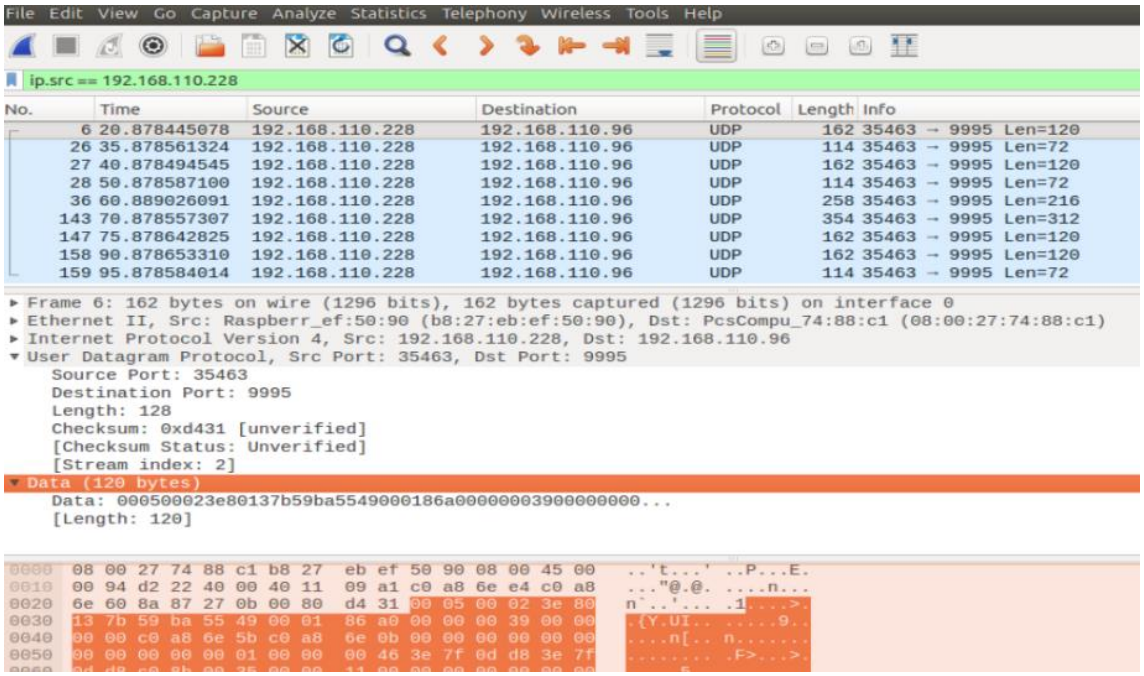


Figura 4.10. Captura Wireshark del tráfico Netflow

Primero hay que instalar el paquete nfdump.

sudo apt-get install nfdump

Una vez instalado, con la herramienta nfcapd se abrirá una vía de escucha y se recibirá la información enviada por la sonda Raspberry:

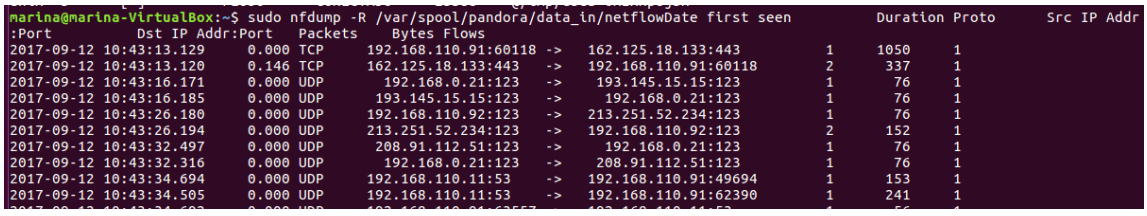
nfcapd -l /var/spool/pandora/data_in/netflow -D

En la opción -l del comando se indica la ruta donde se almacenará la información y de la que Pandora FMS leerá los datos para mostrárselos al usuario. [22] Esta ruta deberá coincidir con la que más tarde configuraremos en la consola de Pandora ya que Pandora FMS leerá los datos que muestre al usuario de dicho fichero.

La opción -D del comando hace que se ejecute en segundo plano, para que siempre permanezca a la escucha de información Netflow recibida desde la sonda. [22]

Comprobaremos que se empiezan a recibir datos en el servidor de Pandora ejecutando el siguiente comando:

nfdump –R /var/spool/pandora/data_in/netflow



```
2017-09-12 10:58:20.444    330.253 UDP     192.168.110.91:57621 ->  192.168.110.255:57621        22      1584     1
2017-09-12 11:02:38.385     15.044 UDP     192.168.110.91:49265 ->   216.58.214.174:443           8      4252     1
2017-09-12 11:02:38.424     15.049 UDP     216.58.214.174:443   ->   192.168.110.91:49265         7      2325     1
2017-09-12 11:02:39.212     15.042 UDP      192.168.110.8:57311 ->   216.58.210.174:443           7      3359     1
2017-09-12 11:02:39.252     15.045 UDP     216.58.210.174:443   ->    192.168.110.8:57311         5      1614     1
2017-09-12 11:02:57.043      0.000 UDP     192.168.110.11:138   ->  192.168.110.255:138           3       748     1
Summary: total flows: 767, total bytes: 4030014, total packets: 8426, avg bps: 22902, avg pps: 5, avg bpp: 478
Time window: 2017-09-07 11:42:34 - 2017-09-12 11:03:50
Total flows processed: 767, Blocks skipped: 0, Bytes read: 43432
Sys: 0.020s flows/second: 38350.0    Wall: 0.178s flows/second: 4304.0
```

Figura 4.11. *Visualización del tráfico Netflow con nfdump*

Además, para poder observar los gráficos de datos en la consola de Pandora deberemos habilitar Netflow en el apartado de Ajustes.

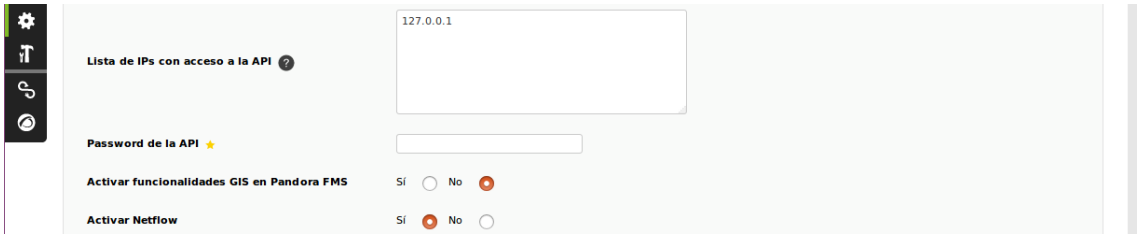


Figura 4.12. *Habilitar Netflow en la consola de Pandora FMS*

Y en la configuración correspondiente a Netflow tendremos que comprobar que el fichero de la opción "Data storage path", coincide con la ruta establecida al ejecutar nfcapd.

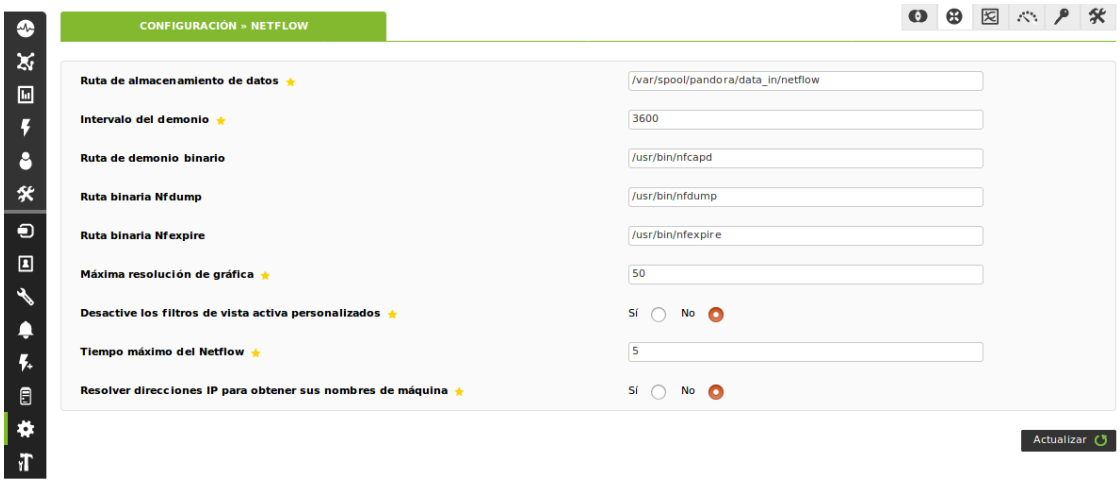


Figura 4.13. *Configuración de Netflow en la consola de Pandora FMS*

4.4 RESULTADOS DE MONITORIZACIÓN

Los resultados de monitorización serán mostrados a través de la consola de Pandora FMS. Como se ha explicado en el proceso de instalación del colector Netflow, la consola obtendrá los datos de monitorización del fichero generado por la herramienta nfcapd con la información Netflow recogida de la sonda.

Pandora FMS, no solo muestra la información Netflow sino que, tiene múltiples utilidades de monitorización como: realizar consultas tipo SNMP o WMI a agentes remotos, verificaciones de red, generación de alertas e informes SLA, verificar el rendimiento de red, control remoto de equipos, gestión de errores y eventos,

geolocalización y mapas interactivos que muestren la posición de los agentes, autodescubrimiento de hosts, monitorización de traps SNMP, etc. Pero esto queda fuera de este trabajo. [20]

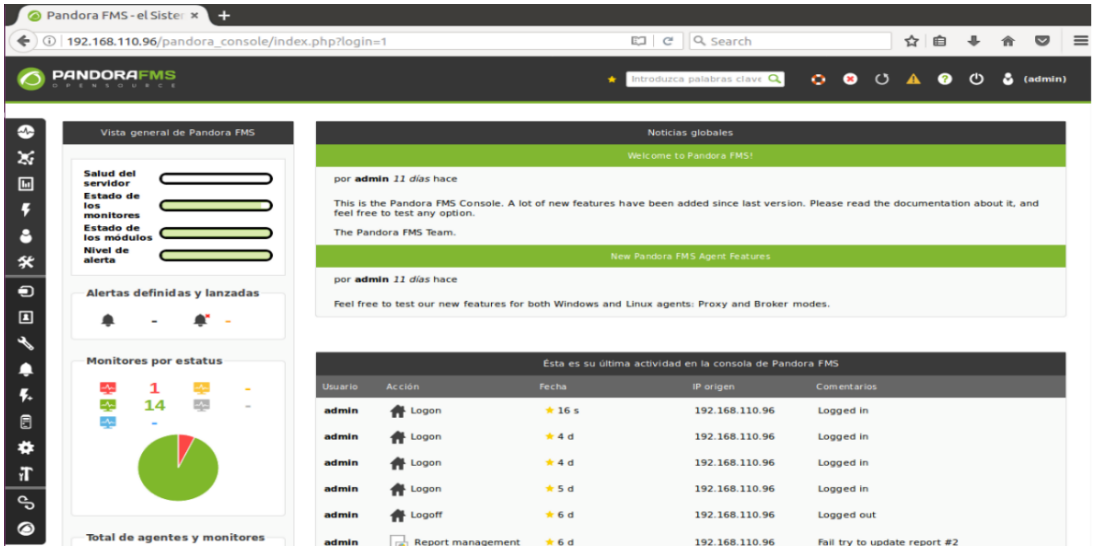


Figura 4.14. *Página principal de la consola de Pandora FMS*

4.4.1 VISUALIZACIÓN EN TIEMPO REAL

En el menú de Vistas, hay una pestaña llamada “Netflow en tiempo real” donde se podrá observar el tráfico recibido por la sonda; tanto en tiempo real como en el pasado.

Figura 4.15. *Visualización en tiempo real del tráfico Netflow*

Antes de mostrar la información, puedes filtrarla de múltiples opciones para que la búsqueda sea más personalizada. Esto es muy útil para encontrar errores en la red.

Fecha: puedes elegir tanto la fecha y hora actuales para observar el tráfico que hay actualmente o bien se puede elegir cualquier fecha pasada y hora. Esto es una ventaja a la hora de realizar búsquedas rápidas y eficientes.

Intervalo: hace referencia a que se mostrará el tráfico durante ese intervalo de tiempo elegido; es decir, si se pone de intervalo 2 horas, se mostrará la información recogida desde dos horas antes de la hora elegida. Hay muchas opciones de intervalos desde 15 minutos hasta 30 días.

Resolución: los datos se leen en bloques de un tamaño igual a la resolución. Si Periodo / Resolución es mayor que la máxima resolución configurada la resolución se ajustará de forma dinámica. Por ejemplo, para un periodo de 1 día y una resolución de 1 hora se dibujarán 24 puntos en la gráfica. [27]

Tipo: Hay 6 formas de mostrar los datos al usuario. Estos son:

1. Gráfico del área: Crea una gráfica en la que el eje X se representa el intervalo de tiempo seleccionado y en el eje Y, el formato de salida de datos elegido (bytes, bytes por segundos, etc.). [27] Si dejas el cursor en un punto de la gráfica, te da el valor exacto de tráfico, en este caso, para cada dirección IP dibujada.

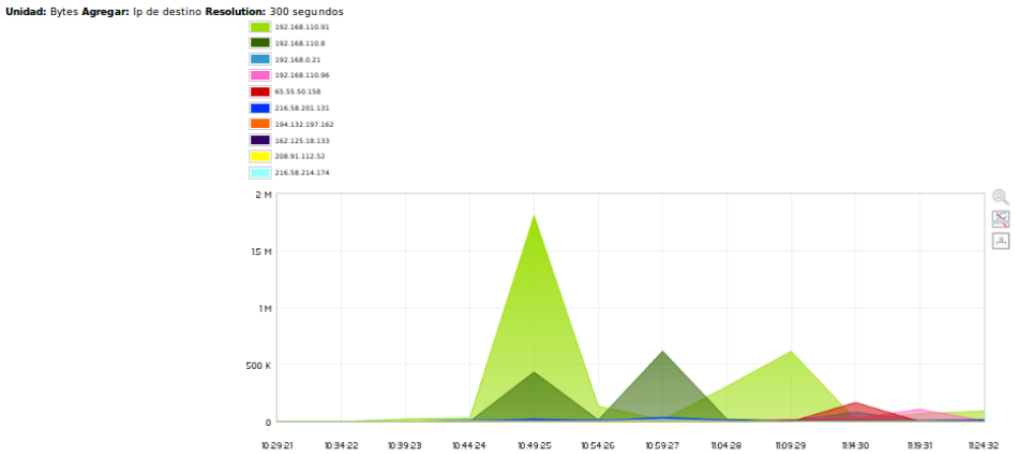


Figura 4.16. Gráfico del área

2. Gráfico de tarta y tabla resumen: muestra en un gráfico tipo pie el porcentaje de tráfico que tiene como origen una dirección IP origen específica sobre el total de tráfico. Por ejemplo, en la siguiente imagen se puede observar que, sobre el total de tráfico recogido, un 43,96% del tráfico tiene como dirección IP origen la 192.121.140.65. Además, te da información adicional sobre los datos recogidos.

Figura 4.17. Gráfico de tarta y tabla resumen

3. Tabla de datos: Representación en texto de la gráfica de área.

Unidad: Bytes **Agregar:** Ip de destino **Resolution:** 300 segundos

Fecha/Hora	192.168.110.96	192.168.0.21	192.168.110.8	192.168.110.91	192.168.110.255
10:59:21	2,732 Bytes	0 Bytes	13,052 Bytes	1,778 Bytes	748 Bytes
11:04:22	842 Bytes	0 Bytes	5,861 Bytes	3,749 Bytes	0 Bytes
11:09:23	9,490 Bytes	357 Bytes	726 Bytes	3,191 Bytes	0 Bytes
11:14:24	7,242 Bytes	1,377 Bytes	241 Bytes	2,051 Bytes	748 Bytes
11:19:25	2,898 Bytes	0 Bytes	153 Bytes	3,719 Bytes	0 Bytes
11:24:26	7,825 Bytes	357 Bytes	153 Bytes	3,280 Bytes	748 Bytes

Figura 4.18. *Tabla de datos*

4. Tabla de estadísticas: Representación en texto del gráfico de tarta.

Ip de destino	Bytes
192.168.0.21	57,936 Bytes
192.168.110.96	41,576 Bytes
192.168.110.8	30,784 Bytes
192.168.110.91	27,396 Bytes
192.168.110.228	3,280 Bytes
192.168.110.255	2,992 Bytes
192.168.110.5	1,036 Bytes
224.0.0.251	146 Bytes

Figura 4.19. *Tabla de estadísticas*

5. Malla circular: Representación de los datos en forma de malla. Cuando se quiere representar un número elevado de datos, este tipo de gráfico no es el más adecuado.

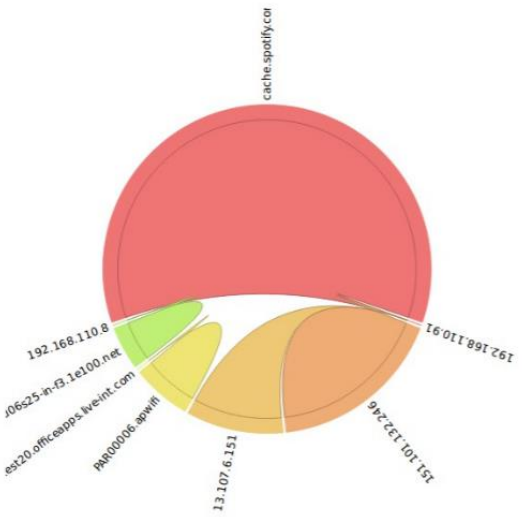


Figura 4.20. *Malla circular*

6. Tráfico detallado de la máquina: puede representar el tráfico enviado o recibido. Si se lleva el cursor sobre los elementos del gráfico, muestra información adicional sobre el tráfico. Los colores cambian dependiendo del número de puerto del protocolo correspondiente.

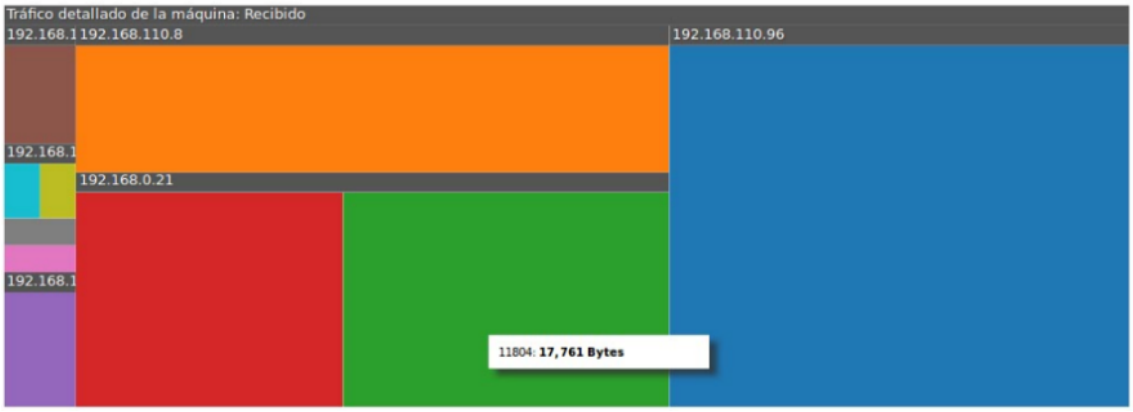


Figura 4.21. *Tráfico detallado de la máquina*

Valores máximos: número máximo de elementos que se incluyen en los gráficos. Por ejemplo, si queremos una gráfica del tráfico agregado por la dirección IP origen y con 2 valores máximos, se mostrarán solo 2 direcciones IP.

Resolución de dirección IP: se pueden resolver direcciones IP para obtener sus hostnames. [27]

Filtro: esta opción hace referencia a que además de visualizar el tráfico en tiempo real; desde esta pestaña también se pueden crear filtros. Esto se explicará en el siguiente apartado.

Cargar filtro: se pueden aplicar filtros ya creados anteriormente.

Se puede filtrar el tráfico haciendo referencia a una o varias direcciones IP o puertos destino u origen específicos e incluso por la dirección IP del router o mediante expresiones pcap si quieres filtrar la información de manera más avanzada. Esto hace la búsqueda más específica y personalizada.

Agregado por: este campo hace referencia a la manera en la que se agrupa la información del tráfico mostrada al usuario. Los gráficos se pueden agregar por la dirección IP destino, la dirección IP origen, el puerto de destino, el puerto de origen o los protocolos (TCP, UDP, etc). [27] Por ejemplo, si elegimos que sea agregado por la dirección IP destino, los flujos se agruparán para mostrar el tráfico para cada dirección IP destino diferente.

Por ejemplo, en la siguiente figura se puede observar el tráfico recogido agregado por protocolos. El tráfico total se agrupa en tres protocolos: TCP, UDP e ICMP.

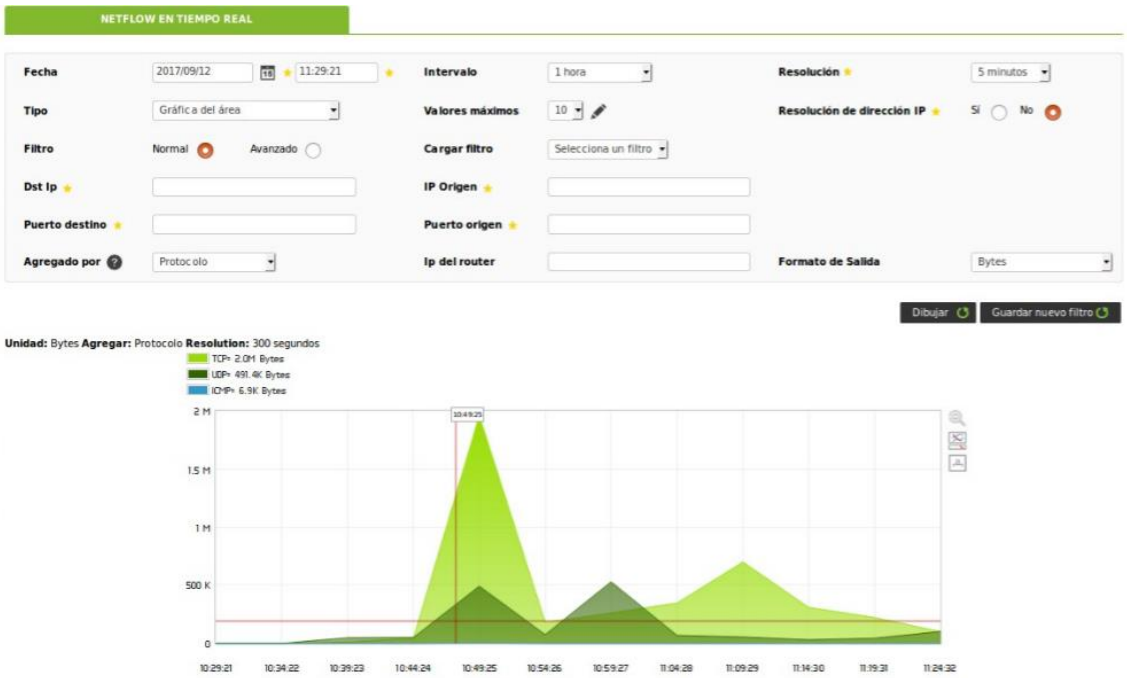


Figura 4.22. *Visualización de tráfico agregado por protocolos*

Formato de salida: los resultados se pueden mostrar en bytes, bytes por segundo, kilobytes, kilobytes por segundo, megabytes o megabytes por segundo.

En la siguiente imagen, podemos ver un ejemplo de una búsqueda realizada en la que se muestra el tráfico con dirección IP origen el servidor atlas durante una hora. Se ha filtrado de tal manera que solo aparecen 5 direcciones IP destino.

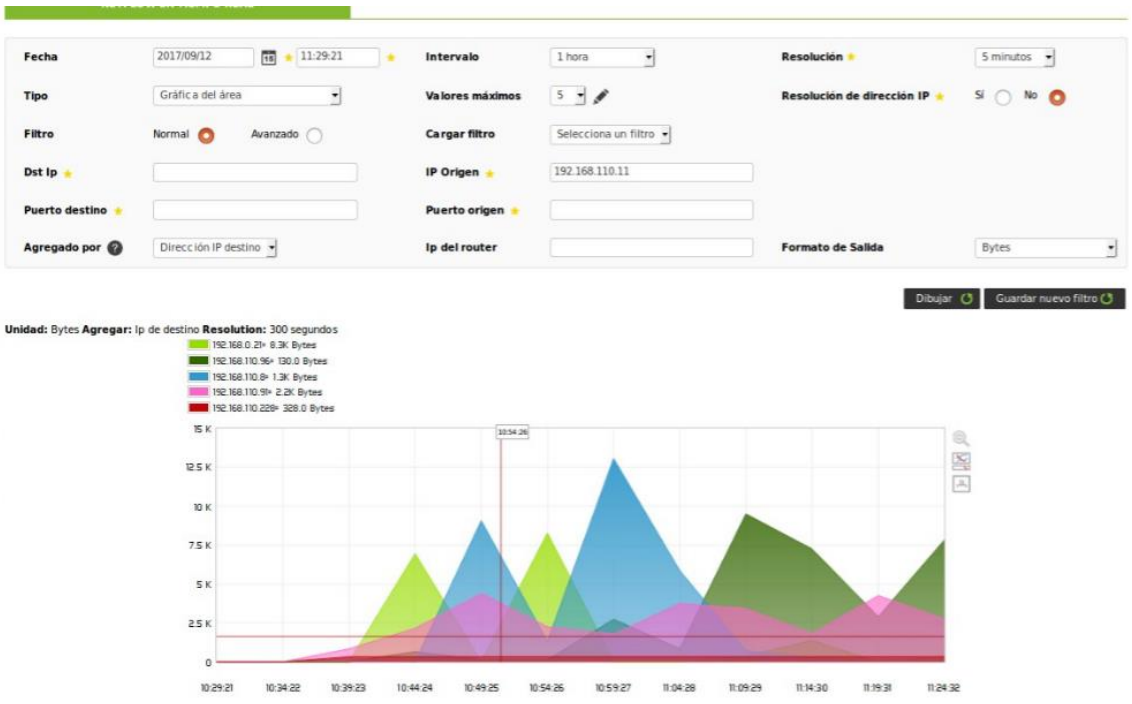


Figura 4.23. *Ejemplo visualización de datos Netflow en tiempo real*

4.4.2 FILTROS

Pandora enfoca el análisis de tráfico mediante el concepto de filtro. Define filtro como "un conjunto de reglas para especificar un tráfico determinado". [27]

Crear filtros específicos hace que las búsquedas sean más rápidas ya que cada vez que quieras, por ejemplo, saber el tráfico que sale del proxy hacia Internet con aplicar el filtro guardado anteriormente valdría.

Desde la pestaña de "Netflow en tiempo real" se pueden guardar las búsquedas como filtros. Si en vez de dibujar, se pincha en guardar filtro, te pedirá un nombre para dicho filtro y se guardará.

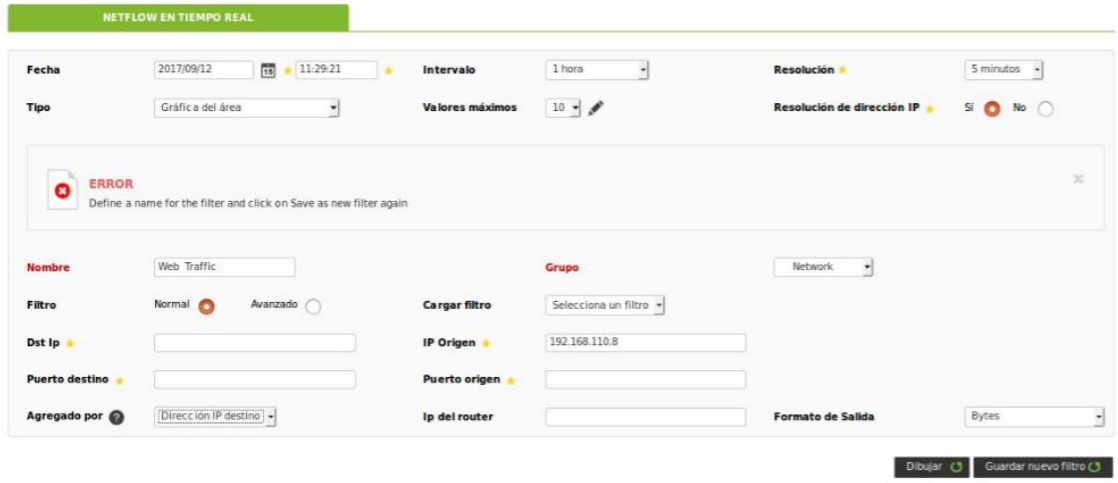


Figura 4.24. *Creación de filtro a través de la pestaña de Visualización en tiempo real*

Aunque existe una pestaña específica para la administración de filtros que se encuentra en Resources/Filtros Netflow. En dicha página se puede ver una lista de todos los filtros que se han creado y te ofrece la posibilidad de crear un filtro.

Figura 4.25. *Visualización de lista de filtros*

En la imagen anterior se puede observar como existen dos filtros llamados Prot y Web Traffic. Pinchando en cada uno de ellos se puede ver qué tipo de tráfico filtra y además se pueden editar.

A la hora de crear un filtro se pueden definir una serie de características: [27]

Nombre: es aconsejable que sea descriptivo.

Grupo: un usuario solo podrá crear o editar un filtro de un grupo al que tenga acceso. En Pandora FMS se utilizan grupos para agrupar agentes y un usuario puede tener diferentes permisos de acceso para cada grupo. [27] En el ejemplo, como hemos accedido a Pandora FMS como administrador se tiene acceso a todos los grupos, que son Aplications, Databases, Firewalls, Network, Servers, Unknown, Web, Workstations o Todo.

Filtro: los filtros pueden ser de dos tipos normal o avanzado. En el filtro normal se puede filtrar por dirección IP y puerto destino y origen, y en el filtro avanzado hay que utilizar expresiones pcap. [27] Un ejemplo de un filtro avanzado podría ser: (src net 192.168.110.0/24) or (dst net 192.168.110.0/24) que filtra el tráfico que entra o sale de la red 192.168.110.0.

Agregado por: agrupa el tráfico por la dirección IP origen, la dirección IP destino, el puerto origen, el puerto destino, el protocolo o muestra todo el tráfico sin restricciones.

Formato de Salida: los resultados se pueden mostrar en bytes, bytes por segundo, kilobytes, kilobytes por segundo, megabytes o megabytes por segundo.

En la siguiente figura se está creando un filtro normal llamado Web Traffic del grupo Network que agrupa el tráfico que sale del servidor atlas a Internet por su dirección IP destino.

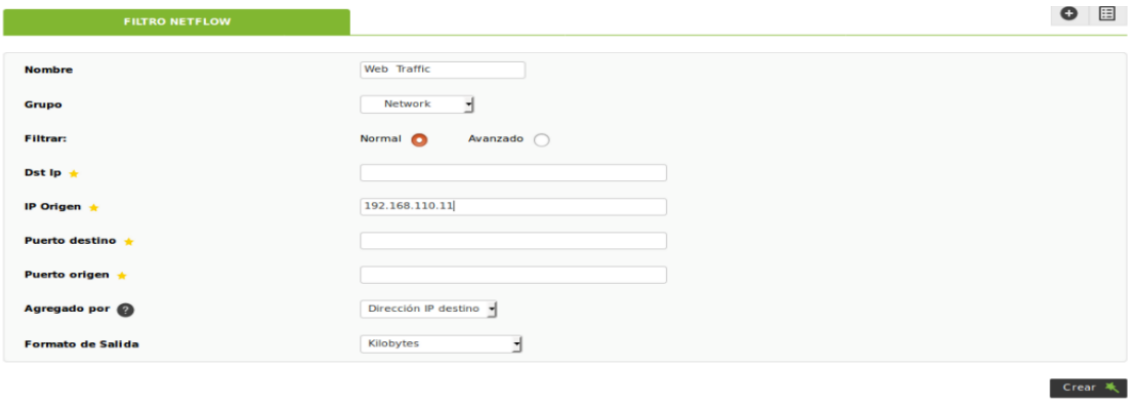


Figura 4.26. Creación de un filtro

4.4.3 INFORMES

Los informes Netflow están integrados con los informes de Pandora FMS en la pestaña Reporting/Informes Personalizados.

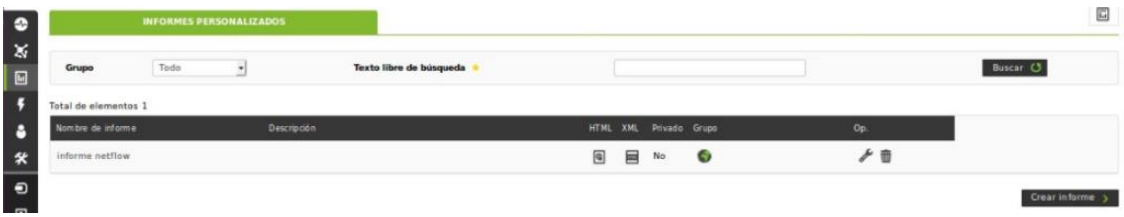


Figura 4.27. Visualización de lista de informes

Para crear un informe primero habrá que rellenar un formulario con el nombre que se quiera poner, el grupo al que pertenece, si el informe es privado o no y una descripción del mismo.

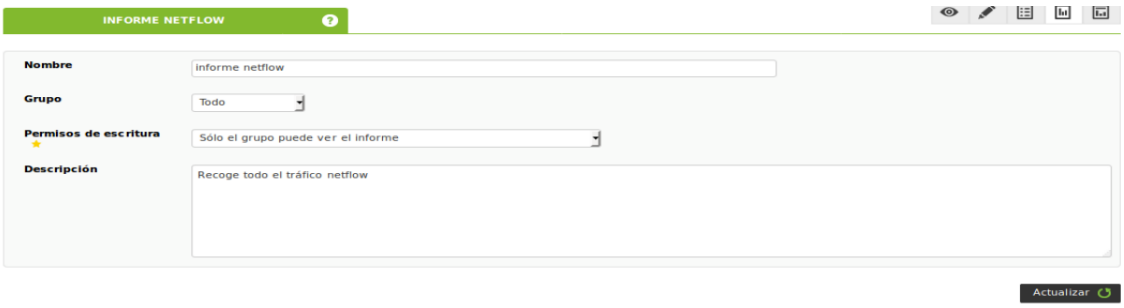


Figura 4.28. *Creación de un informe*

Una vez creado el informe, se podrá editar y añadir ítems que son los que van a incluir la información del tráfico Netflow. A la hora de añadir un ítem, habrá que elegir uno de los tipos de informe Netflow disponible. Estos tipos de informes hacen referencia a los tipos de gráficos que se explicaron en el apartado Visualización en Tiempo Real.

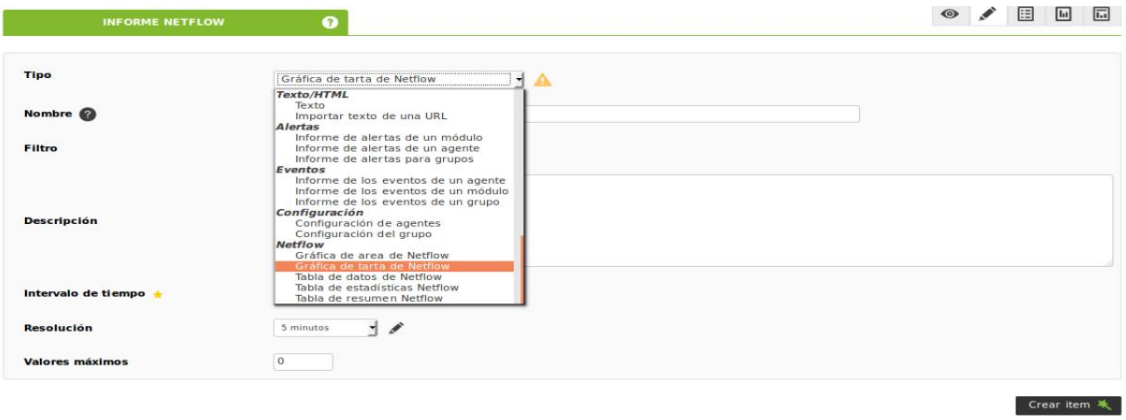


Figura 4.29. *Tipos de informes Netflow*

Además, habrá que elegir un nombre, el filtro que se va a usar, una descripción del elemento, el intervalo de tiempo en el que se van a mostrar los datos, la resolución (los datos se leerán en bloques de un tamaño igual a la resolución) y el valor máximo de puntos que se van a representar en la gráfica.

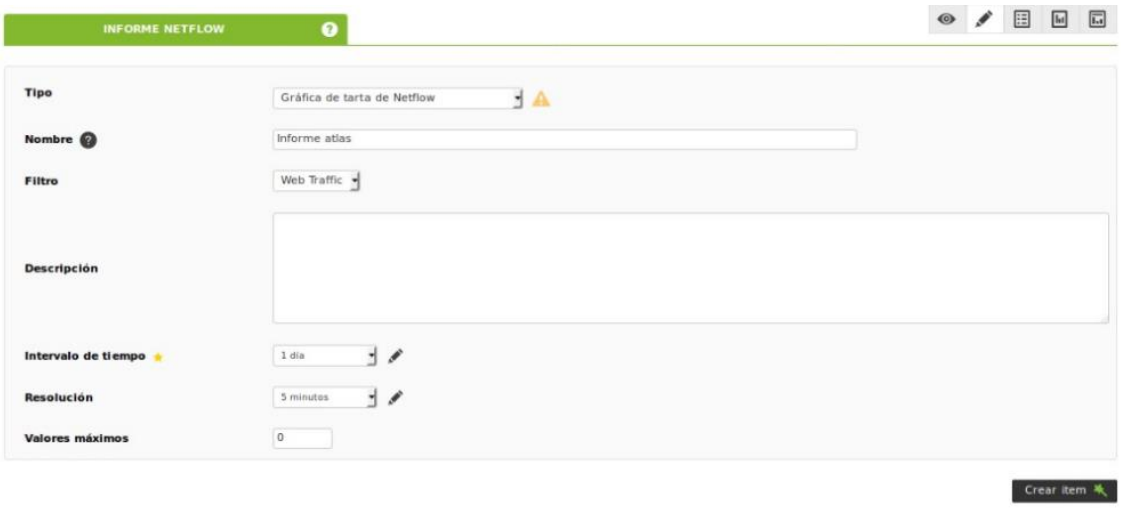


Figura 4.30. *Creación de elemento en un informe*

En la figura anterior se puede observar cómo se va a crear el elemento Informe Atlas del informe Netflow. Este elemento será una gráfica de tarta en la cual el tráfico ha sido filtrado por el filtro Web Traffic creado en el apartado Filtros y se visualizará la información recogida en un día.

Una vez creado el elemento, cuando se vaya a ver el informe, aparecerá la gráfica correspondiente al tráfico generado. Un informe puede tener más de un elemento.

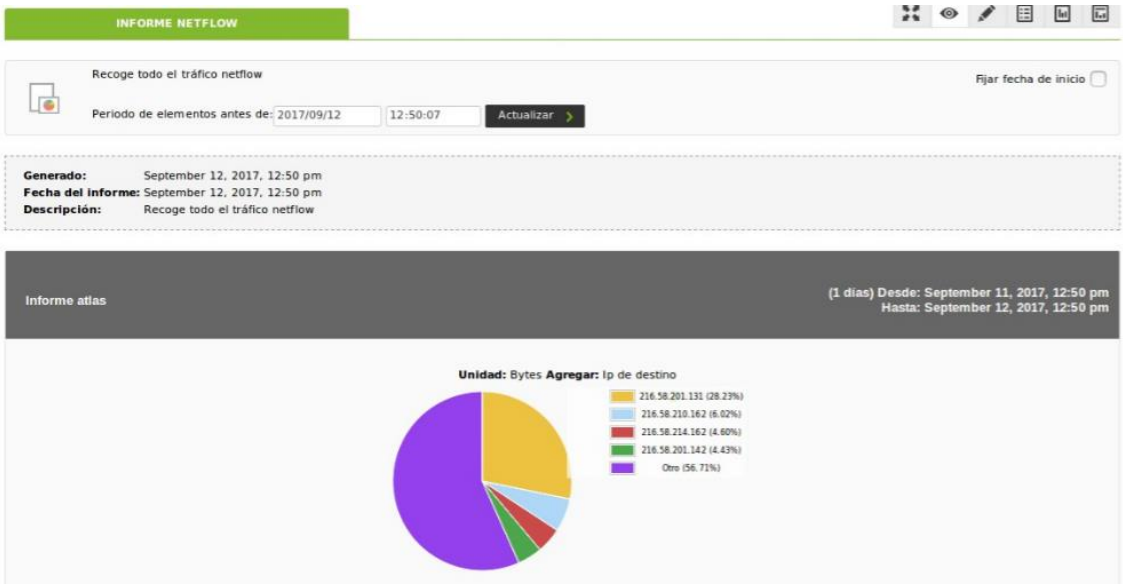


Figura 4.31. *Ejemplo informe Netflow*

5 CONCLUSIONES

En este trabajo se han estudiado tres herramientas de monitorización muy diferentes entre sí en cuanto a la forma de recoger la información de la red a monitorizar, qué tipo de información se puede analizar o cómo se muestran los resultados al usuario.

También, la función de la Raspberry en cada una de ellas era diferente:

- En NEMS se instala directamente la imagen de Nagios en la placa, lo que facilita mucho el proceso de instalación y configuración.

- En MRTG, debido al uso de SNMP, la configuración de la herramienta era un poco más específica obligando a habilitar este protocolo tanto en el router de la red a monitorizar como en la Raspberry.

- Y por último Netflow, la más compleja de todas, ya que hay que disponer de un switch configurable y de un software adicional, Pandora FMS, a través del cual mostrar los datos recogidos. La función de la Raspberry es simplemente recoger datos, transformarlos en flujos y exportarlos al colector.

En cuanto a la información de la red recogida y mostrada al usuario:

- NEMS o Nagios monitoriza tanto dispositivos como servicios los cuales tienen que ser introducidos en la interfaz web manualmente; necesita una configuración previa antes de la visualización de resultados.
  Se pueden establecer jerarquías entre los dispositivos, establecer períodos diferentes de monitorización según las necesidades existentes, diferentes plantillas para controlar un mismo recurso, según sea la naturaleza del dispositivo o servicio a controlar. Otra ventaja es que se permite las notificaciones y alertas por correo.

- MRTG es una herramienta que muestra detalladamente el tráfico de datos que circula por una red. Lo hace en forma de gráficas, y aunque no se puedan enviar alertas o realizar informes, se puede ver la evolución del tráfico a lo largo del tiempo.
  Es una herramienta menos completa que Nagios o Netflow, ya que la interfaz web de esta herramienta solo muestra la información al usuario y no es configurable. MRTG se suele utilizar como elemento adicional a Nagios, ya que una desventaja de esta última herramienta es que no muestra gráficas de estado de calidad.

- Netflow recopila el tráfico de datos que entra o sale de una red y que necesita de un software adicional para su visualización. Pandora FMS es la única, de las

tres herramientas estudiadas en este trabajo, que permite analizar y representar, la información Netflow. En general, Pandora FMS y Nagios ofrecen funcionalidades muy parecidas al usuario, aunque en cuanto a gráficos y generación de informes, Pandora FMS es mucho más completo.

En general, las tres herramientas se utilizan para gestionar grandes redes y ofrecen flexibilidad en cuanto a su gestión.

5.1 LÍNEAS FUTURAS

Poco a poco, todas las herramientas de monitorización se irán adaptando para ser implementadas en la Raspberry Pi, ya que se ahorra dinero y espacio; y aunque todavía no tenga todas las funcionalidades de un ordenador, la tecnología avanza a pasos agigantados y no tardará mucho en ponerse a la par.

De esta manera, se podrá hacer un futuro una comparativa más completa entre todas las herramientas de monitorización más utilizadas para saber cuál es la mejor o cuál se ajusta más específicamente a las necesidades de una empresa.

REFERENCIAS

[1] A. D. C. C. De and M. Magaña, “La Importancia del Monitoreo,” vol. 3, no. 2, pp. 1–28, 2016.

[2] M. T. Pegado Boureghida, “Desarrollo de un sistema de monitorización para SDNs (Software Defined Networks),” p. 20, 2015.

[3] The Raspberry Pi Foundation, “Raspberry Pi FAQs - Frequently Asked Questions.” 2015.

[4] Á. Paz, “Aplicaciones de seguridad informática de Raspberry Pi. - Gurú de la informática,” 2015. [Online]. Available: http://www.gurudelainformatica.es/2015/10/aplicaciones-de-seguridad-informatica.html. [Accessed: 02-Oct-2017].

[5] R. Ferguson, “NEMS | Bald Nerd.” [Online]. Available: http://www.baldnerd.com/category/raspberry-pi/nems/. [Accessed: 02-Oct-2017].

[6] “Welcome to NagVis Home! - NagVis.org.” [Online]. Available: http://www.nagvis.org/. [Accessed: 02-Oct-2017].

[7] R. Ferguson, “NEMS Linux – Nagios Enterprise Monitoring Server for Raspberry Pi 3 | Bald Nerd,” 2016. [Online]. Available: http://www.baldnerd.com/nems/. [Accessed: 02-Oct-2017].

[8] B. W. (Sunrise C. A. Fabian Gander, Angelo Gargiulo, “What is NConf?” [Online]. Available: http://www.nconf.org/dokuwiki/doku.php?id=nconf:about:introduction:nconf. [Accessed: 02-Oct-2017].

[9] W. Kocjan, *Learning Nagios 4*. Birmingham-Mumbai: Packt Publishing, 2014.

[10] “Nagios en Español: Monitoreando Servicios publicamente disponibles,” 2009. [Online]. Available: http://nagioses.blogspot.com.es/2009/03/monitoreando-servicios.html. [Accessed: 02-Oct-2017].

[11] NagiosConfig, “Main Configuration File Options.” [Online]. Available: https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/3/en/configmain.html. [Accessed: 02-Oct-2017].

[12] T. Oetiker, “MRTG - What is MRTG ?,” 2011. [Online]. Available: https://oss.oetiker.ch/mrtg/doc/mrtg.en.html. [Accessed: 02-Oct-2017].

[13] J. Case, M. Fedor, M. Schoffstall, and J. Davin, “RFC 1157 SNMP.” p. 36, 1990.

[14] José Ángel Irastorza, “Gestión SNMPv1,v2,v3,” 2017.

[15] S. Crespo, “Instalar MRTG y Snmp en Raspberry | Alteageek, tutoriales, raspberry pi y cisco, en español,” 2017. [Online]. Available: https://alteageek.com/2017/02/03/instalar-mrtg-y-snmp-en-raspberry/.

[Accessed: 02-Oct-2017].

[16] M. Furqan, “Network Monitoring with MRTG on Raspberry Pi - Intense School,” 2014. [Online]. Available: http://resources.intenseschool.com/network-monitoring-with-mrtg-on-raspberry-pi/. [Accessed: 02-Oct-2017].

[17] J. M. Kretchmar, “MRTG | Open Source Network Administration,” 2003, pp. 51–64.

[18] G. Sadasivan, J. Brownlee, B. Claise, and J. Quittek, *Architecture for IP flow information export*. RFC Editor.

[19] R. Hofstede *et al.*, “Flow monitoring explained: From packet capture to data analysis with NetFlow and IPFIX,” *IEEE Commun. Surv. Tutorials*, vol. 16, no. 4, pp. 2037–2064, 2014.

[20] (Ártica), “Pandora FMS: el software de monitorización flexible.,” 2002. [Online]. Available: https://pandorafms.com/es/. [Accessed: 02-Oct-2017].

[21] S. Networks, *Management Guide*. 2010.

[22] C. Andres, “Sonda netflow con Raspberry -,” 2016. [Online]. Available: https://blog.pandorafms.org/es/sonda-netflow-con-raspberry/. [Accessed: 02-Oct-2017].

[23] E. Díaz, “EiTheL Inside: IP Forwarding con Linux,” 2011. [Online]. Available: http://eithel-inside.blogspot.com.es/2011/03/ip-forwarding-con-linux.html. [Accessed: 02-Oct-2017].

[24] E. Latorres, “Servicio de Informática de Facultad de Ciencias: Instalar Pandora FMS Server en Debian 8.5,” 2016. [Online]. Available: http://informatica-fcien.blogspot.com.es/2016/10/instalar-pandora-fms-server-en-debian-85.html. [Accessed: 02-Oct-2017].

[25] (Ártica), “Pandora:Documentation en:Recon Server - Pandora FMS Wiki.” [Online]. Available: https://wiki.pandorafms.com/index.php?title=Pandora:Documentation_es:Instalacion. [Accessed: 02-Oct-2017].

[26] “NFDUMP.” [Online]. Available: http://nfdump.sourceforge.net/. [Accessed: 02-Oct-2017].

[27] (Ártica), “Pandora:Documentation es:Netflow - Pandora FMS Wiki.” [Online]. Available: https://wiki.pandorafms.com/index.php?title=Pandora:Documentation_es:Netflow#Como_operar_con_Netflow_en_Pandora. [Accessed: 03-Oct-2017].

ANEXO I. GUIÓN DE PRÁCTICAS DE LA HERRAMIENTA NEMS

Grado en Ingeniería de Tecnologías de Telecomunicación
Universidad de Cantabria
Curso 2016/2017

Práctica 1. Estudio de la herramienta de monitorización NEMS

OBJETIVOS DE LA PRÁCTICA

Los principales objetivos de esta práctica son:

- Familiarizarse con el manejo y configuración de una Raspberry Pi.
- Instalación de una imagen en la Raspberry Pi.
- Configurar dispositivos y servicios que puedan ser monitorizados desde la interfaz web nConf.
- Visualizar los resultados de monitorización en las diferentes interfaces web que ofrece NEMS.
- Generar informes y alertas desde la interfaz web Nagios Core.
- Configurar notificaciones vía correo electrónico.

INTRODUCCIÓN

NEMS es una imagen de Nagios 4 que permite monitorizar redes y que está específicamente diseñada para funcionar sobre la Raspberry Pi versión 3. El objetivo de Nagios es detectar cualquier equipo, servicio o sistema que no esté funcionando correctamente para que la solución del problema se haga lo más rápido posible y los usuarios del sistema sean lo menos partícipes posibles del problema detectado.

Entre sus múltiples funciones destacan:

- Supervisión de servicios de red (SMTP, POP3, HTTP, PING, etc.)
- Supervisión de los recursos del host (carga del procesador, uso del disco, etc.)

- Plugin de diseño simple que permite a los usuarios desarrollar fácilmente sus propios controles de servicio.
- Controles de servicios y hosts paralelos. Se pueden supervisar diferentes servicios, tanto del mismo dispositivo como de dispositivos diferentes, al mismo tiempo.
- Capacidad para definir la jerarquía de host de red utilizando hosts "principales", permitiendo la detección y distinción entre hosts que están inactivos y aquellos que son inaccesibles.
- Notificaciones de contacto cuando se producen problemas de servicio o de host y se resuelven (mediante correo electrónico u otro método definido por el usuario).
- Interfaz web opcional para ver el estado actual de la red, la notificación y el historial de problemas, el archivo de registro, etc.

DESARROLLO DE LA PRÁCTICA

1. Instalación de la imagen de NEMS en la Raspberry Pi

La herramienta se puede descargar de la página web: http://www.baldnerd.com/nems y se grabará en una tarjeta micro SD mayor de 8GB. Existen múltiples programas para grabar imágenes; para el sistema operativo Windows, el más utilizado es Win32-Disk-Imager.

Una vez seguidos estos pasos, se introducirá la tarjeta con la imagen en la Raspberry Pi y se encenderá. Esta imagen no tiene interfaz gráfica; por lo tanto, todo lo tanto la configuración inicial se deberá hacer mediante comandos.

Una vez cargada la imagen se deberá escribir **sudo nems-init** (se deberá escribir sudo cuando se escriba un comando ya que le da permisos de administrador). Con este comando haremos las primeras configuraciones, entre ellas, elegir un nombre de usuario y una password para las interfaces web nConf.

1) Elige como nombre de usuario tu nombre y como contraseña tu número de puesto.

2. Configuración de la herramienta

La configuración de NEMS se hará a partir de la interfaz web nConf. Para acceder a ella habrá que abrir el navegador y escribir http://direcciónIPdelaraspberry/nconf.

2.1. Añadir hosts

Esta herramienta no tiene una opción de autodescubrimiento de equipos, por lo tanto, tendremos que añadir cada host manualmente.

A la hora de agregar los equipos, hay dos campos obligatorios que son host-preset y OS que hacen referencia a algunos ajustes preestablecidos y plantillas para definir el dispositivo dependiendo si es un router, un equipo con sistemas operativo Windows o Linux, una impresora, etc. Estas plantillas vienen ya definidas por la propia herramienta, asique el alumno no tendrá más que seleccionar la más adecuada.

Además, se deben establecer los periodos de chequeo y notificación para hacer la monitorización más personalizada (check period y notification period). En la siguiente tabla vienen explicados más campos que se pueden rellenar para definir la monitorización:

Max check attemps	Especifica el número de veces que un test tiene que informar de que una máquina ha caído antes de que se asuma que realmente lo ha hecho.
Check Interval	Especifica cada cuánto tiempo (en minutos) se chequea una máquina.
Retry Interval	Especifica el tiempo (en minutos) que hay que esperar antes de volver a chequear si la máquina está activa.
First notification delay	Especifica el tiempo (en minutos) que se tarda en enviar la primera notificación desde que la máquina ha caído.
Notification Interval	Especifica el tiempo (en minutos) que se espera entre notificaciones de que una máquina ha caído.

2) Desde la pestaña hosts se podrán añadir los dispositivos que se quieran monitorizar. Cada alumno deberá añadir como mínimo el router cisco 2600 del laboratorio (dirección IP: 192.168.110.1).

   El dispositivo se monitorizará durante todo el día y todos los días de la semana (check period y check Interval = 24x7). Se chequeará cada 10 minutos (check Interval) y a los 10 intentos fallidos (max check attemps) se asumirá que el router ha caído y se pondrá su estado a DOWN. La primera notificación de que el router está DOWN será a los 5 minutos (first notification delay).

*Cada vez que se haga un cambio en la configuración del servidor Nagios, se deberá activar un proceso que exportará el contenido de la base de datos en que se guardan todos estos ajustes al formato de configuración de Nagios. Esto se realiza a través del Generate Nagios config -> Deploy.

2.2 Servicios a monitorizar

NEMS puede monitorizar tanto servicios “públicos”, como HTTP, POP3, IMAP, FTP y SSH, como “privados”, a carga de CPU, uso de memoria, uso en disco, etc.

Cuando se crean los hosts, se pueden asociar directamente los servicios que se quieren supervisar. Algunos de estos servicios no será posible monitorizarlos debido a la configuración del router del laboratorio por motivos de seguridad; aun así, los configuraremos para observar más adelante las notificaciones de error.

A la hora de relacionar los servicios con los dispositivos se pueden establecer también los periodos e intervalos de chequeo y de notificación igual que en el caso de los dispositivos.

3) Desde la pestaña hosts, editar el dispositivo añadido anteriormente para monitorizar los servicios HTTP, PING, SSH Y check_imap. Configurar los servicios con los mismos intervalos de chequeo y notificación que en el apartado 2.
   Una vez añadidos, guardar los cambios con Generate Nagios config -> Deploy.

3. Visualización de los resultados de monitorización

Para ver los datos obtenidos de los dispositivos y servicios configurados desde la interfaz de nConf, deberemos ir a la siguiente URL: http://direcciónIPdelaraspberry/nagios3. Accedemos a la interfaz Nagios Core que ofrece tanto una visión global del sistema, como información más detallada de cada elemento. También recoge alertas y notificaciones que automáticamente aparecen publicadas.

3.1. Hosts y servicios

En la pestaña Tactical Overview se recoge una visión general de los dispositivos configurados, tanto de los propios equipos como de los servicios monitorizados. Se pueden ver los estados de dispositivos y servicios, y cuántos tienen las notificaciones y los chequeos habilitados o deshabilitados.

También en la pestaña Status Map, aparece un mapa con los dispositivos y poniendo el ratón encima de cada uno aparece más información como por ejemplo los servicios que se están monitorizando.

Para obtener más detalle de los equipos monitorizados, en la pestaña Host Detail aparece información sobre el estado y el último chequeo. Clicando en cada host, la información aparece desglosada.

4) Hacer click sobre el router configurado, ¿qué servicio se utiliza para saber si el dispositivo está en un estado UP o DOWN? ¿Cuándo se ha realizado el último chequeo? ¿Cuándo se va a realizar el siguiente chequeo? ¿Están las notificaciones habilitadas para dicho dispositivo?

En cuanto a los servicios, en la pestaña Service Detail aparecen los equipos configurados con cada uno de los servicios que se están monitorizando en dicho dispositivo. Clicando sobre cada uno de ellos, igual que en el caso de los hosts, se ve información del estado de dichos servicios, la fecha de chequeo e información del chequeo y, en caso de error, el motivo del fallo.

5) De los 4 servicios monitorizados en el router del laboratorio, ¿cuál es el estado de cada servicio? Si alguno de dichos servicios falla, ¿cuál es el motivo del fallo? ¿Hay algún servicio en estado de flapping?

En la pestaña Scheduling Queue, aparecen los dispositivos y servicios que van a ser chequeados, ordenados de manera ascendente por proximidad entre la fecha actual y la fecha del siguiente chequeo.

3.2. Informes y Alertas

Bajo la pestaña Reporting, aparecen 3 tipos de informes que se pueden generar sobre los resultados obtenidos de la monitorización.

Trends	historial de los cambios de estado que ha sufrido un dispositivo o servicio
Availability	historial de cuánto tiempo ha estado un dispositivo en un estado determinado
Alert	histograma que muestra el número de alertas que se han producido para un dispositivo o servicio en un periodo de tiempo

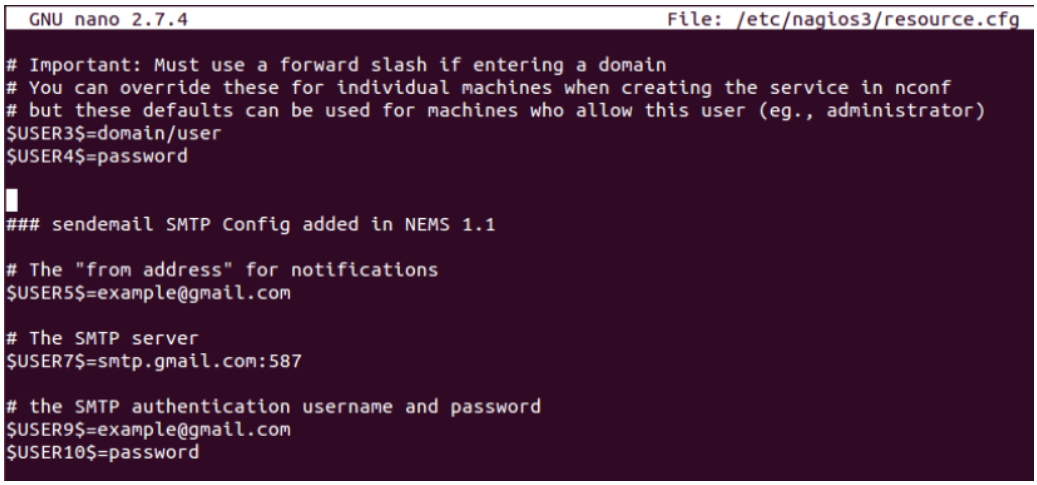
A la hora de generar informes hay que especificar sobre qué dispositivo o servicio se quiere realizar, el periodo de tiempo sobre el que se quiere recoger información y otros parámetros que se quieran o no incluir en los informes.

6) Generar los tres tipos de informes para el router del laboratorio y para el servicio HTTP monitorizado. Analizar los resultados.

4. Notificaciones vía correo electrónico

Por último, aunque las notificaciones se pueden ver bajo el apartado Reporting de la interfaz web Nagios Core, vamos a configurar la herramienta para que éstas nos lleguen al correo electrónico de la universidad.

1. Accedemos al fichero de configuración resource.cfg:
   #sudo nano /etc/nagios3/resource.cfg



Escribir en $USER5$ una dirección de Gmail desde donde se enviarán las notificaciones, en $USER7$ la dirección del servidor SNMP y el puerto (poner el mismo que en la captura anterior) y, por último, en $USER9$ y $USER10$ la dirección de correo electrónico de la universidad de cada alumno y una contraseña, donde recibirá las notificaciones.

Guardamos la configuración con **CRTL+X**.

2. Al utilizar una cuenta de Gmail, hay que habilitar el acceso a aplicaciones menos seguras a través de este enlace https://myaccount.google.com/lesssecureapps.
3. En la interfaz web nConf, dentro de la sección Contacts, aparece el nombre de usuario que utilizamos para entrar a la interfaz. Le damos a editar y en el apartado e-mail address escribimos la dirección de correo electrónico donde queremos recibir las notificaciones; en este caso la cuenta de correo de la universidad.
4. En host notification options y service notification options se pueden elegir que tipo de notificaciones se quieren recibir por correo. Además, cuando añades un host o servicio nuevo a la configuración también se puede especificar individualmente de cada uno.

   En la siguiente tabla se muestran los tipos de notificaciones que se pueden configurar tanto para equipos como para servicios:

EQUIPOS	SERVICIOS
D – el equipo ha caído	W – Estado de warning
U – el equipo es inalcanzable	U – Estado desconocido
R – notificar al recuperar	C – Estado crítico
F – notificar si está oscilando entre on off	F – El servicio está oscilando entre on off
S – notificar si un tiempo de inactividad de un servicio programado empieza o termina	N – No se notifica
N – no se notifica	

7) Configurar las notificaciones por correo para recibirlas en tu correo personal de la universidad. Se pide que al menos se reciban las notificaciones de que el router ha caído y cuando el servicio HTTP esté en estado de warning.

ANEXO II. GUIÓN DE PRÁCTICAS DE LA HERRAMIENTA MRTG

Grado en Ingeniería de Tecnologías de Telecomunicación
Universidad de Cantabria
Curso 2016/2017

Práctica 2. Estudio de la herramienta de monitorización MRTG

OBJETIVOS DE LA PRÁCTICA

Los principales objetivos de esta práctica son:

- Familiarizarse con el manejo y configuración de una Raspberry Pi.
- Conocer el funcionamiento del protocolo SNMP sobre el que se basa la herramienta.
- Configuración de SNMP en un router y en la Raspberry Pi.
- Configuración e instalación de MRTG en la Raspberry Pi.
- Visualizar y analizar los datos recogidos por la herramienta en una interfaz web

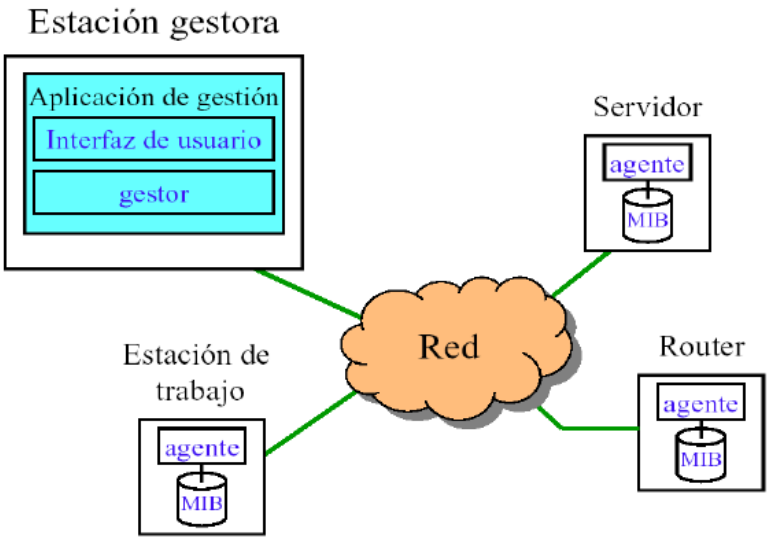
INTRODUCCIÓN

MRTG es una herramienta de monitorización de redes cuyo funcionamiento es bastante sencillo: cada 5 minutos la herramienta lee el contador de octetos entrantes y salientes del router gateway de Internet. Mediante la diferencia de dos lecturas consecutivas y dividiendo el resultado por el tiempo transcurrido, se determina la velocidad de datos o tráfico promedio en el enlace durante los últimos 5 minutos.

Una vez obtenidos estos datos, se muestran en gráficos embebidos en páginas web que pueden ser visualizados desde cualquier navegador. MRTG también crea gráficos del tráfico medio durante los últimos siete días, el último mes y el último año.

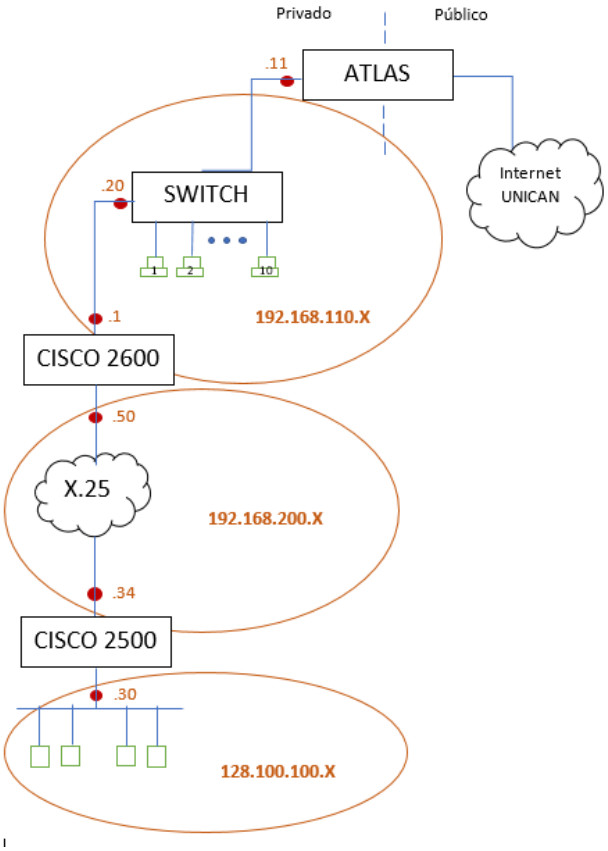
Esta herramienta obtiene información de los dispositivos a monitorizar mediante SNMP (Simple Network Management Protocol). La información de gestión SNMP se recoge en bases de datos llamadas MIBs, las cuales se encuentran en los dispositivos gestionados. Los recursos a monitorizar en la red se encuentran representados en la MIB como

objetos y estos objetos están ordenados de forma jerárquica sobre una estructura de árbol.



ENTORNO DE TRABAJO

Se va a monitorizar el tráfico que entra y sale del router Cisco 2600 del laboratorio. Dicho router comunica dos subredes: una con dirección IP 192.168.110.0 y otra SUBRED x.25 con dirección IP 192.168.200.0.



El servidor MRTG lo instalaremos en la Raspberry Pi 3 que irá conectada mediante un cable Ethernet al switch. Accederemos remotamente a la Raspberry vía SSH desde un ordenador del laboratorio. Conociendo la dirección Ip de la Raspberry, escribiremos en la ventana de comandos:

ssh pi@direcciónIPdelaRaspberry

DESARROLLO DE LA PRÁCTICA

1. Configuración de SNMP en el router

Para poder monitorizar routers o dispositivos tenemos que asegurarnos que estos tienen configurado SNMP. Entramos en la configuración del router a través de una sesión telnet:

telnet 192.168.110.1
contraseña: *git*
c2600> enable
contraseña: *telematica*
c2600# configure terminal
c2600(config)# snmp-server community public ro
c2600(config)# end

Podemos verificar la configuración SNMP con el comando show.

c2600#show snmp
Chassis: JAD050407HZ (1210873882)
Contact: Jose Angel Irastorza
Location: lab. telematica
106264 SNMP packets input
0 Bad SNMP version errors
22 Unknown community name
0 Illegal operation for community name supplied
0 Encoding errors
0 Number of requested variables
0 Number of altered variables
306 Get-request PDUs
105336 Get-next PDUs
0 Set-request PDUs
106242 SNMP packets output
0 Too big errors (Maximum packet size 1500)
23 No such name errors
0 Bad values errors
0 General errors
106242 Response PDUs
0 Trap PDUs

SNMP logging: disabled

2. Instalación de SNMP en la Raspberry Pi

Si no tenemos el servicio SNMP instalado previamente, deberemos hacerlo antes de instalar cualquier servicio de MRTG. Escribimos en la ventana de comandos:

sudo apt-get update
sudo apt-get upgrade
sudo apt-get install snmpd snmp

Para que nuestra Raspberry sea accesible desde cualquier otro equipo de la red necesitaremos
abrir el fichero de configuración snmpd.conf:

sudo nano /etc/snmp/snmpd.conf

Sustituiremos la línea *agentAddress udp:127.0.0.1:161* por *agentAddress 161*; y en la línea siguiente a '#rocommunity public localhost' insertaremos: *recommunity public.*

Reiniciaremos el servicio:

service snmpd restart

3. Instalación y configuración de MRTG

Instalaremos la herramienta a través de la ventana de comandos:

sudo apr-get install mrtg

Se necesita tener un servidor web instalado para poder ver los resultados de monitorización. En este caso intalaremos Apache.

sudo apt-get install apache2

Para comprobar si Apache está instalado y funcionando:

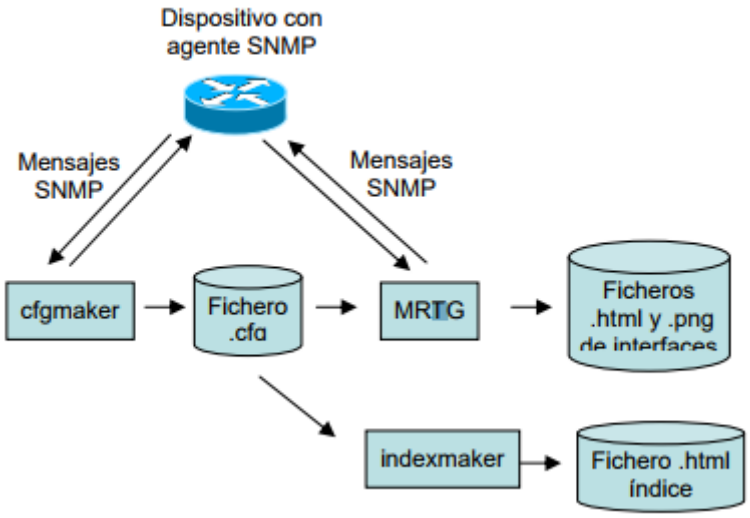
sudo service apache2 status

Si no está funcionando se activará de la siguiente manera: **sudo service apache2 start**.

Una vez instalado el servidor web y comprobar que funciona, debemos crear la carpeta donde se van a crear los datos MRTG que observaremos desde el navegador.

mkdir /var/www/html/mrtg

En cuanto a la configuración del sistema, vamos a utilizar dos herramientas que ya vienen incluidas en el paquete de MRTG, cfgmaker e indexmaker.



Cfgmaker explora mediante mensajes SNMP el dispositivo a monitorizar para averiguar que interfaces tiene y cuáles de ellas están operativas. A continuación, genera un fichero de configuración adecuado para representar gráficamente el tráfico a lo largo del tiempo en las interfaces que estaban operativas en ese momento. En el fichero de configuración se incluye también la información relativa a las interfaces que no están operativas, pero estas aparecen comentadas.

Indexmaker consolida en una página web de índice la información recopilada por MRTG para ello se basa en la información del fichero .cfg creado por cfgmaker.

sudo cfgmaker public@192.168.110.1 >> /etc/mrtg.cfg

Por defecto cfgmaker toma el directorio de trabajo como /var/www/mrtg pero Apache no coge la información de esa ruta sino de /var/www/html/mrtg. Por lo tanto, deberemos editar el fichero de configuración:

sudo nano /etc/mrtg.cfg

Y cambiar la línea WorkDir: /var/www/mrtg por WorkDir: /var/www/html/mrtg.

Ahora vamos a crear la página index con la utilidad indexmaker:

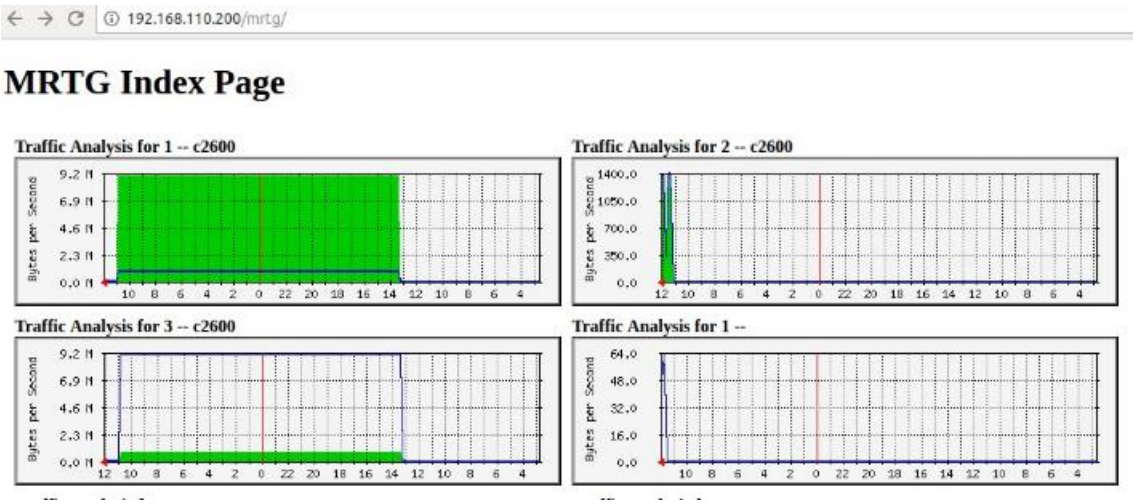
indexmaker /etc/mrtg.cfg > /var/www/html/mrtg/index.html

Y reiniciamos el servicio (cada vez que se reinicie la raspberry se deberá iniciar el servicio, se puede programar que esto se haga automáticamente, mirar ANEXO):

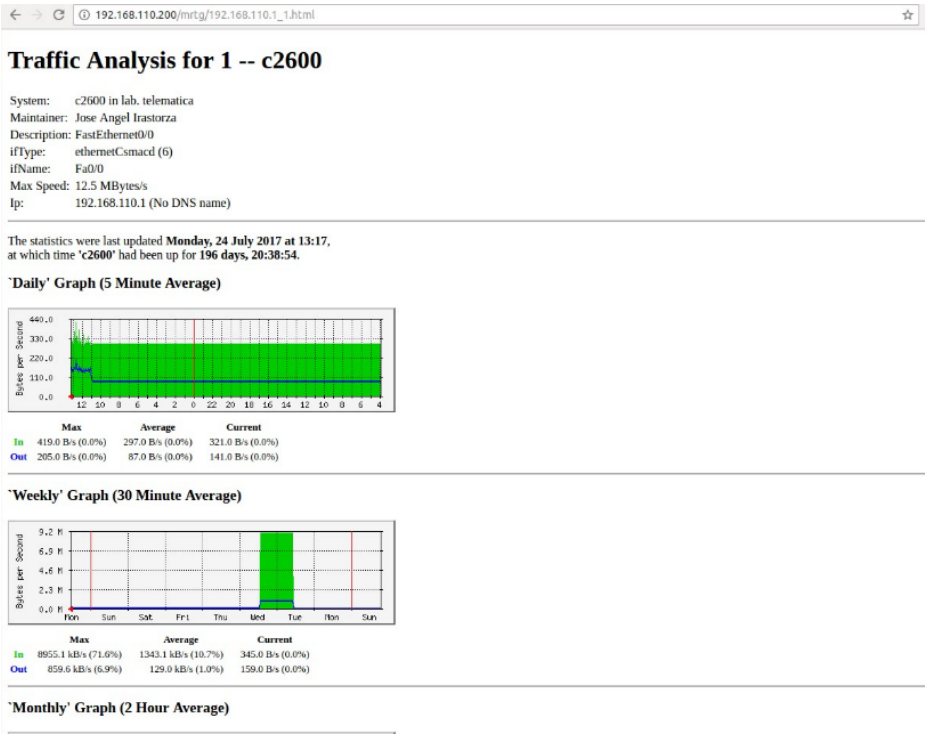
sudo service mrtg start

4. Visualización de los resultados de monitorización

Una vez instalado todo correctamente se accederá, desde cada ordenador, a la URL http://direcciónIPdelaraspberry/mrtg ; donde aparecerá una página con tres gráficas que recogen el tráfico que atraviesan las tres interfaces activas del router cisco 2600. En azul está representado el tráfico saliente y en verde, el tráfico entrante.



Si pinchamos en cada una de las gráficas, obtendremos más información acerca del tráfico en cada interfaz y se añaden gráficas con el tráfico semanal, mensual y anual recogido por la herramienta.



ANEXO

Inicio automático del servicio

Los servicios de Linux pueden ser iniciados o parados con scripts alojados en la carpeta /etc/init.d. Para que el servicio MRTG se inicie automáticamente deberemos crear el siguiente script en la carpeta /etc/init.d/mrtg :

sudo nano /etc/init.d/mrtg

Copiar:

```
#! /bin/sh
PATH=/sbin:/usr/sbin:/bin:/usr/bin
DESC="MRTG"
NAME="mrtg"
DAEMON=/usr/bin/$NAME
DAEMON_ARGS="/etc/mrtg.cfg –user root --logging /var/log/mrtg.log"
case "$1" in
  start)
        echo "Starting $DESC..."
        env LANG=C $DAEMON $DAEMON_ARGS
        echo "$NAME started."
        ;;
  stop)
        echo "Stopping $DESC..."
        pkill $NAME &> /dev/null
        echo "$NAME stopped."
        ;;
  *)
        FULL_NAME=/etc/init.d/$NAME
        echo "Usage: $FULL_NAME {start|stop}." >&2
        ;;
esac
exit
```

Escribir **CRTL+X** para guardar los cambios y salir.

Este archivo debe ser ejecutable por lo que tenemos que darle permisos:

sudo chmod +x /etc/init.d/mrtg

Por último, programamos su ejecución automática instalando el archivo en la secuencia de reinicio de la Raspberry Pi:

sudo update-rc.d mrtg defaults

Reiniciamos el sistema para que los cambios queden guardados:

sudo shutdown -r now

ANEXO III. GUIÓN DE PRÁCTICAS DE LA HERRAMIENTA NETFLOW

Grado en Ingeniería de Tecnologías de Telecomunicación
Universidad de Cantabria
Curso 2016/2017

Práctica 3. Estudio de la herramienta de monitorización Netflow

OBJETIVOS DE LA PRÁCTICA

Los principales objetivos de esta práctica son:

- Familiarizarse con el manejo y configuración de una Raspberry Pi.
- Conocer el funcionamiento del protocolo Netflow.
- Configuración de los parámetros básicos para el análisis de tráfico Netflow.
- Conocimiento de herramientas como fprobe o nfdump necesarias para la creación de flujos, su exportación y su almacenamiento.
- Visualizar y analizar los datos recogidos por la herramienta en la interfaz web de Pandora FMS.

INTRODUCCIÓN

Netflow es un protocolo de red desarrollado por Cisco que permite recopilar información de tráfico IP y supervisarlo. Se encarga de agregar los paquetes de información recogidos de una red en flujos, los cuales se exportan para ser almacenados y analizados.

Un flujo se define como "un conjunto de paquetes IP que pasan un punto de observación en la red durante un cierto intervalo de tiempo, de manera que todos los paquetes pertenecientes a un flujo particular tienen un conjunto de propiedades comunes". Estos atributos comunes son: dirección IP origen, dirección IP destino, puerto origen, puerto destino, tipo de protocolo IP, interfaz del router o switch y tipo de servicio IP.

La monitorización de redes mediante flujos de datos se puede dividir en varias fases:

5. Observación de paquetes: los paquetes de datos que pasan por un punto de observación, por ejemplo, interfaces de routers o switches, son capturados.
6. Medición y exportación del flujo: los paquetes se introducen en flujos que son registrados en una base de datos llamada Flow cache. Cuando el flujo ha

terminado, un registro del mismo se exporta a dispositivos para su almacenamiento y procesado, llamados Colectores Netflow.
Estos dos primeros pasos los realizará la Raspberry Pi, la cual hará la función de sonda Netflow.

7. Recopilación de datos: los datos recibidos se almacenan y pre-procesan. Esto se hará a través de la herramienta nfdump instalada en el colector (ordenador con sistema operativo Linux).
8. Análisis de datos: correlación y agregación, clasificación y caracterización del tráfico, detección de anomalías, búsqueda de datos, informes y alertas, etc. Para ello utilizaremos el software de monitorización libre Pandora FMS, instalado en el colector. Pandora FMS leerá los datos Netflow recogidos por el colector y los mostrará al usuario en forma de tablas, gráficos, informes, etc.

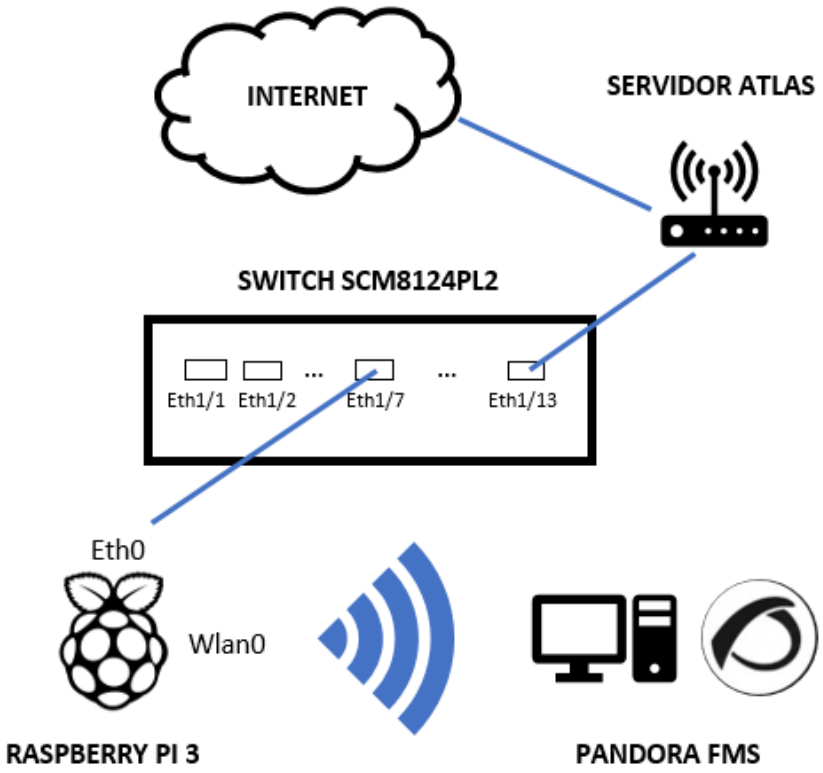
La práctica estará dividida en dos fases:

En la primera, el alumno deberá configurar los dispositivos necesarios para que el colector Netflow reciba los flujos de datos de la sonda.

En la segunda, el alumno deberá analizar el tráfico recogido por el colector desde la interfaz web o consola que proporciona Pandora FMS mediante gráficos, aplicando filtros, generando informes, etc.

ENTORNO DE TRABAJO

Se va a monitorizar el tráfico que entra y sale del servidor Atlas del laboratorio que es un proxy a través del cual podemos acceder a Internet.



La observación de paquetes, su introducción en flujos y su exportación hacia el colector, se hará a través de una sonda Netflow o "flow probe" que en este caso será la Raspberry Pi 3. Habrá que configurar el dispositivo para que, mediante su interfaz cableada, conectada al switch del laboratorio, escuche los datos de tráfico, convierta este tráfico en flujos Netflow mediante la herramienta fprobe, y exporte esta información por su interfaz wifi a un colector.

La interfaz wifi de la Raspberry estará conectada a otro punto de acceso del laboratorio, router con dirección IP 192.168.110.90, para que pueda enviar los datos al colector.

El colector Netflow será un ordenador del alumno en el cual estará instalado el software Pandora FMS y que estará conectado al mismo punto de acceso que la Raspberry, para que pueda recibir los datos que ésta le envíe.

TRABAJO PREVIO

El alumno deberá instalar la imagen del sistema operativo Raspbian en la Raspberry antes de acudir al laboratorio. Descargar la imagen de la página web oficial www.raspberrypi.org, así nos aseguramos de obtener la última versión la última versión de la imagen. Para grabar la imagen se puede utilizar el programa Win32DiskImager.

** Antes de grabar la imagen asegurarse de que la tarjeta SD está formateada. Un programa para formatear tarjetas SD para Windows es SDFormatter.

Además, es necesario que para esta práctica el alumno lleve al laboratorio un ordenador portátil con sistema operativo Ubuntu 16.04 o con una máquina virtual con la imagen del sistema operativo instalada. Dicho ordenador hará de colector Netflow y en él habrá que instalar el servidor Pandora FMS.

En el anexo de esta práctica se explica cómo instalar tanto el servidor como la consola de Pandora FMS en el sistema operativo Ubuntu 16.04. Es aconsejable que el alumno lo instale antes de acudir a la práctica.

** Es aconsejable que, tras la instalación de Pandora, se configure la dirección IP del ordenador o de la máquina virtual de manera estática y que corresponda con la dirección 192.168.110.9X (X = número de grupo).

DESARROLLO DE LA PRÁCTICA

1. Configuración de la captura de datos del switch

Hay que configurar el switch del laboratorio (con dirección IP 192.168.110.20) para que todo el tráfico de datos que haya en la red LAN, y que pasa a través del servidor Atlas, pueda ser observado por la sonda Netflow.

Se va a configurar desde el terminal de Ubuntu mediante una sesión telnet, con usuario *admin* y contraseña *telematica*:

telnet 192.168.110.20

Hay que configurar el switch de tal manera que el tráfico que pase a través de la interfaz ethernet 1/13, que es donde está conectado el servidor Atlas, sea reenviado a la interfaz donde tenemos conectada la Raspberry Pi (en el ejemplo de la imagen sería la interfaz ethernet 1/7).

Vty-0# config
Vty-0(config)# interface ethernet 1/7
Vty-0(config-if)# port monitor ethernet 1/13 both

La palabra "both" hace que se reflejen tanto los paquetes recibidos como los transmitidos por dicha interfaz.

2. Configuración de la Raspberry Pi como una sonda Netflow

Antes de configurar la sonda, vamos a hacer unos cambios en el Raspberry para una mejor gestión de la misma. Como se va utilizar la interfaz ethernet del dispositivo para escuchar el tráfico de red, utilizaremos la interfaz wifi para exportar los flujos Netflow al colector.

Primero desde nuestro terminal nos conectaremos remotamente a la Raspberry:

ssh pi@dirección_IP_Raspberry

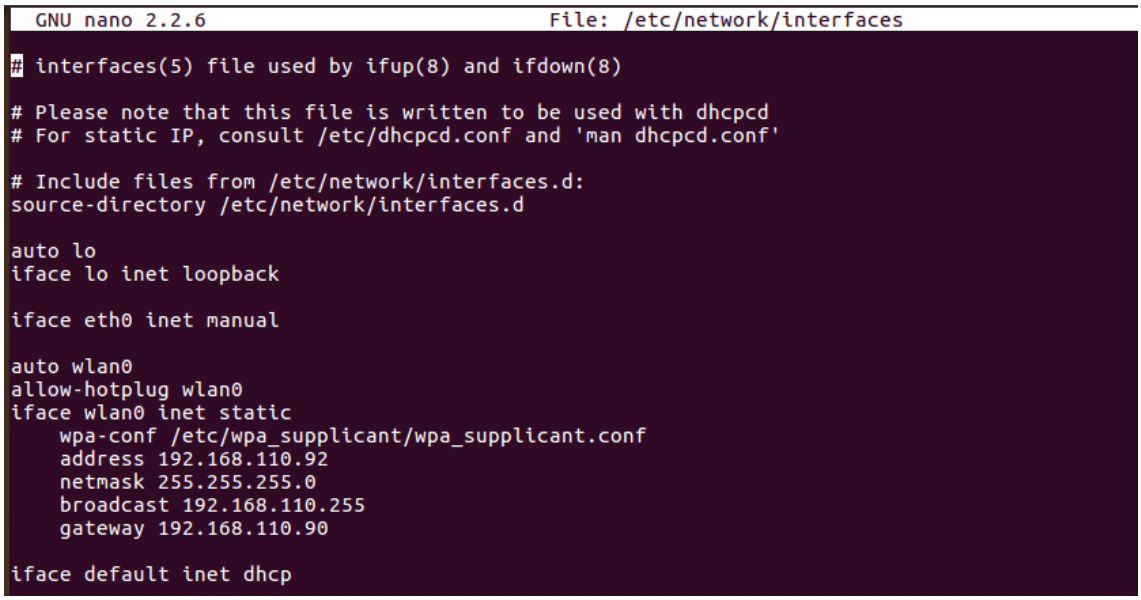
Editaremos los ficheros /etc/wpa_supplicant/wpa_supplicant.conf y /etc/network/interfaces, de la siguiente manera:

```
  GNU nano 2.2.6                File: /etc/wpa_supplicant/wpa_supplicant.conf

country=GB
ctrl_interface=DIR=/var/run/wpa_supplicant GROUP=netdev
update_config=1

network={
        ssid="LABTLMAT"
        psk="telematica"
}
```

Primero conectaremos la Raspberry Pi a otro router del laboratorio (dirección IP 192.168.110.90), para que tanto la sonda netflow como el colector estén en otra subred distinta y se puedan intercambiar la información.



En el fichero /etc/network/interfaces hay que configurar una IP estática para la interfaz wifi. **El alumno deberá preguntar al profesor la dirección IP que debe poner.**

Deshabilitamos la interfaz ethernet con el siguiente comando:

sudo ip addr flush dev eth0

Habilitaremos el ip_forwarding entre ambas interfaces para que los paquetes que se reciben por la interfaz ethernet se retransmitan hacia la dirección IP y puerto del colector Netflow.

sudo /sbin/sysctl -w net/ipv4/ip_forward=1

Ahora si vamos a configurar la sonda. Para recolectar los datos de tráfico utilizaremos la herramienta fprobe. Esta herramienta recopila la información y la exporta en flujos Netflow al dispositivo colector.

sudo apt-get install fprobe

Al instalarlo pedirá que indiques la interfaz desde la que se escuchan los datos, en este caso **eth0**, y la dirección IP y puerto donde va a escuchar los datos el dispositivo colector, en este caso dirección IP **192.168.110.96** puerto **9995** (porque es el puerto por defecto que escucha UDP y los datos se envía mediante dicho protocolo).

3. Configuración del colector Netflow

En el ordenador donde está instalado el software Pandora FMS y con dirección IP 192.168.110.9X (X = número de grupo), hay que instalar la herramienta nfdump. Esta herramienta incluye nfcapd que es la que se encarga de leer los datos netflow de la red y los almacena en ficheros.

Por defecto, nfcapd escucha el tráfico Netflow por el puerto 9995. Este puerto se utiliza para recibir datos a través del protocolo UDP.

1) Para comprobar que el colector está recibiendo los flujos correctamente, el alumno debe realizar una captura de Wireshark en la que se observe el tráfico enviado por la Raspberry Pi hacia el colector. ¿Sobre qué protocolo viajan los datos Netflow? Analizar la captura.
Es conveniente que, una vez capturado el tráfico, se aplique un filtro para que solo se vean las tramas que nos interesan. Un ejemplo de filtro es el siguiente: ip.src == dirección IP de la Raspberry.

Instalamos la herramienta nfdump desde el terminal de Ubuntu:

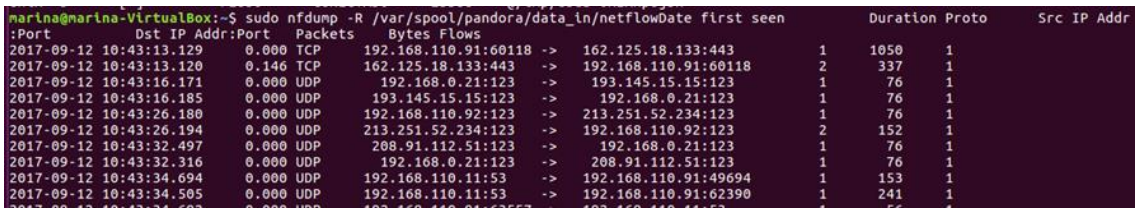
sudo apt-get install nfdump
nfcapd -l /var/spool/pandora/data_in/netflow -D

Así los datos netflow quedarán guardado en la carpeta /var/spool/pandora/data_in/netflow.

Si todo está correctamente configurado, el colector ya empezará a recibir los flujos Netflow de la sonda. Lo comprobamos con el siguiente comando:

nfdump –R /var/spool/pandora/data_in/netflow

Deberemos obtener un resultado similar al que vemos en la siguiente imagen, donde se ven qué tipo de paquetes se están enviando y las direcciones IP origen y destino y la longitud de los paquetes:

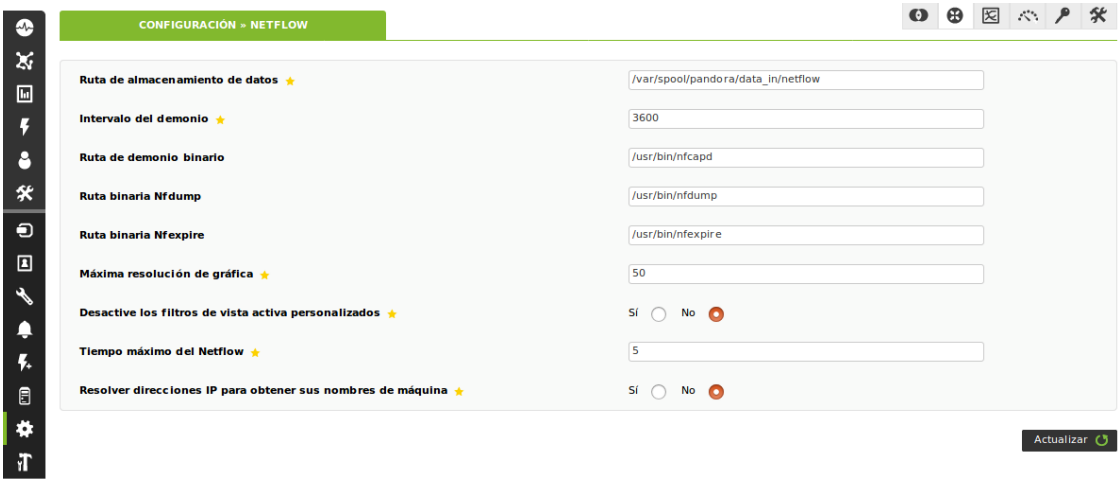


4. Configuración de la consola de Pandora FMS

Para poder analizar los datos Netflow recogidos por la herramienta nfcapd, hay que hacer algunos cambios en la configuración de la consola de Pandora FMS.

Desde la pestaña Ajustes, habilitamos Netflow como en la siguiente imagen.

Y en la configuración correspondiente a Netflow, tendremos que comprobar que el fichero de la opción “Data storage path” es /var/spool/pandora/data_in/netflow.



5. Visualización de resultados: Filtros e informes

Los resultados de monitorización serán mostrados a través de la consola de Pandora FMS. Accederemos a ella desde la url http://dirección_IP_servidor_Pandora/console ; el usuario por defecto es *admin* y la contraseña *pandora*. Es conveniente que esta contraseña se cambie.

En el menú de Vistas, hay una pestaña llamada “Netflow en tiempo real” donde se podrá observar el tráfico recibido por la sonda; tanto en tiempo real como en el pasado.

Los datos se pueden filtrar de múltiples maneras para que la búsqueda sea más personalizada:

Fecha	Se puede elegir tanto la fecha y hora actuales para observar el tráfico.
Intervalo	Hace referencia a que se mostrará el tráfico durante ese intervalo de tiempo elegido.
Tipo	Hay 6 tipos de gráficas/tablas para mostrar la información: gráfico del área, gráfico de tarta y tabla resumen, tabla de datos, tabla de estadísticas, malla circular, tráfico detallado de la máquina.
Valores máximos	Número máximo de elementos que se incluyen en los gráficos.

Cargar filtro	Se pueden aplicar filtros ya creados anteriormente.
Filtro	Se puede filtrar el tráfico haciendo referencia a una o varias direcciones IP o puertos destino u origen específicos e incluso por la dirección IP del router o mediante expresiones pcap si quieres filtrar la información de manera más avanzada.
Agregado por	Este campo hace referencia a la manera en la que se agrupa la información del tráfico mostrada al usuario. Los gráficos se pueden agregar por la dirección IP destino, la dirección IP origen, el puerto de destino, el puerto de origen o los protocolos (TCP, UDP, etc.). Por ejemplo, si elegimos que sea agregado por la dirección IP destino, los flujos se agruparán para mostrar el tráfico para cada dirección IP destino diferente.
Formato de salida	Los resultados se pueden mostrar en bytes, bytes por segundo, kilobytes, kilobytes por segundo, megabytes o megabytes por segundo.

2) Visualizar en un gráfico del área, el tráfico Netflow recolectado con dirección IP origen la del servidor Atlas (192.168.110.11) en una hora. Para un mejor análisis, reducir el número de puntos de la gráfica a 5.

3) Realizar el mismo filtro que en la cuestión anterior, cambiando el tipo de gráfico al de tarta. ¿Qué dirección IP destino es la que ocupa más porción del tráfico? ¿Cuántos kilobytes por segundo se están enviando?

Como se ha dicho anteriormente, es posible agrupar los flujos Netflow por protocolos.

4) Realizar un filtro en el que se agrupe el tráfico que recibe el servidor Atlas por los protocolos. ¿Qué campos se han de cambiar para obtener dicha información?

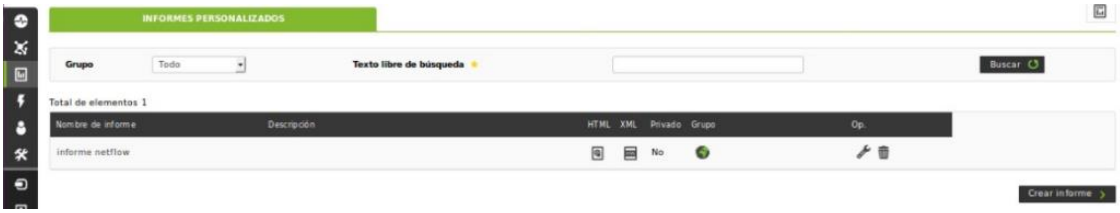
Desde la pestaña de “Visualización en tiempo real” cuando se filtran los datos Netflow para analizarlos al momento también se pueden guardar dichos filtros para un posterior uso de ellos, por ejemplo, a la hora de crear informes.

Para definir y guardar un filtro solo se necesitan los siguientes campos: nombre, grupo, la dirección IP/puerto origen o destino sobre el que se quiera filtrar el tráfico, agregado por y el formato de salida.

5) Realizar un filtro que muestre las direcciones IP que envían información al servidor Atlas. El formato de salida será en bytes.

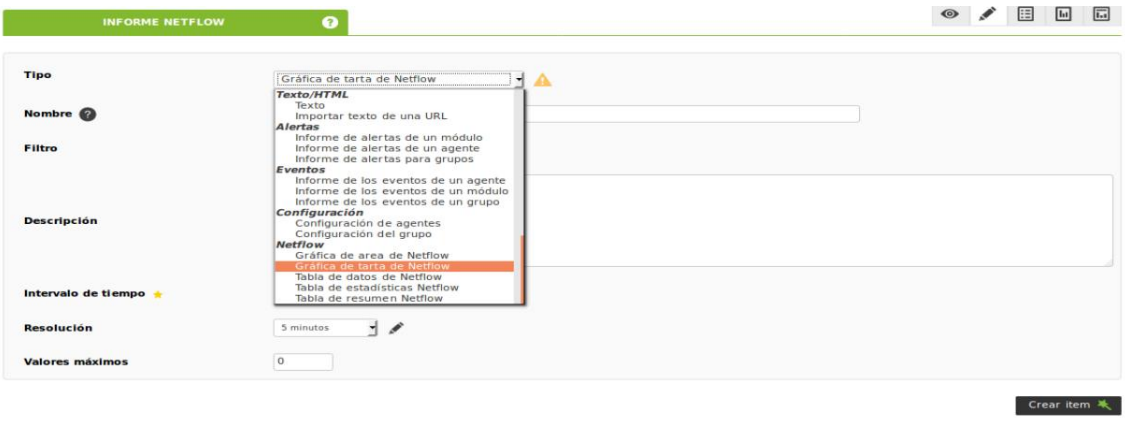
Para guardar el filtro, al lado de la opción “Dibujar”, está la opción “Guardar nuevo filtro”. Al guardarlo es obligatorio ponerle un nombre y le tendréis que añadir al grupo “Todo”.

Pandora FMS permite crear informes a partir de filtros previamente creados. Los informes Netflow están integrados con los informes de Pandora FMS en la pestaña Reporting/Informes Personalizados.



6) Crear un informe con el nombre del Alumno, el grupo “Todo”, privado y una descripción del mismo. Este informe posteriormente contendrá información Netflow, esto es importante a la hora de escribir el nombre y la descripción.

Una vez creado el informe, este se puede editar y añadir elementos que son los que van a incluir la información del tráfico Netflow. Los tipos de elementos corresponden con los tipos de gráficas que se podían elegir para representar los datos.



7) Añadir un elemento al informe, que sea de tipo “Gráfica de tarta Netflow” y que muestre los datos recogidos durante 1 hora, utilizando el filtro creado en la cuestión 5. La resolución se dejará la que viene por defecto y es aconsejable que los valores máximos no sean más de 10. Analizar los resultados. ¿Es posible que un informe tenga más de un elemento Netflow?

ANEXO

Pandora FMS es capaz de monitorizar el tráfico IP haciendo uso del protocolo Netflow. Permite mostrar patrones y datos generales del tráfico que resultan de gran utilidad.

Existen imágenes que instalan Pandora FMS y se pueden descargar de la página web oficial https://pandorafms.org/es/. Aunque en este apartado se va a explicar cómo instalar y configurar Pandora FMS sobre Ubuntu 16.04 LTS.

Abrir la terminal de Ubuntu y actualizar lista de repositorios e instalar actualizaciones:

sudo apt-get update && sudo apt-get upgrade

Modificamos la lista de repositorios que se encuentra en el fichero /etc/apt/sources.list, agregándole el repositorio de Ártica que son necesarios para la instalación de Pandora. Como no hay unos repositorios específicos para Ubuntu, descargaremos los correspondientes a Debian Wheezy.

sudo nano /etc/apt/sources.list

Añadimos: **deb http://firefly.artica.es/debian/wheezy**

Actualizamos la base de datos de repositorios para guardar los cambios.

sudo apt-get update

Hay que descargar e instalar el cliente WMI.

cd ~/Downloads
wget
http://ufpr.dl.sourceforge.net/project/pandora/Tools%20and%20dependencies%20%28All%20versions%29/DEB%20Debian%2C%20Ubuntu/wmi-client_0112-1_amd64.deb
sudo dpkg -i wmi-client_0112-1_amd64.deb

Partiendo de un sistema operativo recién instalado, tendremos que descargar algunas dependencias necesarias como apache, mysql, PHP, … Pandora FMS requiere de PHP en una versión 5 asique si el sistema operativo que se está utilizando es Ubuntu 14.04 se deberá instalar dicha versión; en el caso de Ubuntu 16.04 se deberá descargar la versión 5.6 de PHP.

En algunos casos para poder descargar e instalar la versión PHP 5.6 es necesario realizar lo siguiente:

sudo apt-get install software-properties-common

sudo add-apt-repository -y ppa:ondrej/php
sudo apt-get update
Instalamos las dependencias necesarias para instalar el servidor y la consola de Pandora:

sudo apt-get install snmp snmpd libtime-format-perl libxml-simple-perl libxml-twig-perl libdbi-perl libnetaddr-ip-perl libhtml-parser-perl wmi-client xprobe2 nmap libmail-sendmail-perl traceroute libio-socket-inet6-perl libhtml-tree-perl libsnmp-perl snmp-mibs-downloader libio-socket-multicast-perl libsnmp-perl libjson-perl php5.6 libapache2-mod php5.6 apache2 mysql-server php5.6-gd php5.6-mysql php-pear php5.6-snmp php-db php-gettext graphviz mysql-client php5.6-curl php5.6-xmlrpc php5.6-ldap dbconfig-common php5.6-mbstring php5.6-zip

Entre estas herramientas, se encuentra mysql que es un servidor en el que se va a crear una base de datos para guardar los datos de Pandora FMS. Al instalarlo pide un usuario y contraseña; por defecto, el usuario será root. Esto será relevante para un proceso de instalación que veremos más adelante.
Ubuntu 16.04 LTS utiliza la versión 7.0 de PHP, por lo tanto, es posible que sea necesario desactivar esta versión y activar PHP5.6.

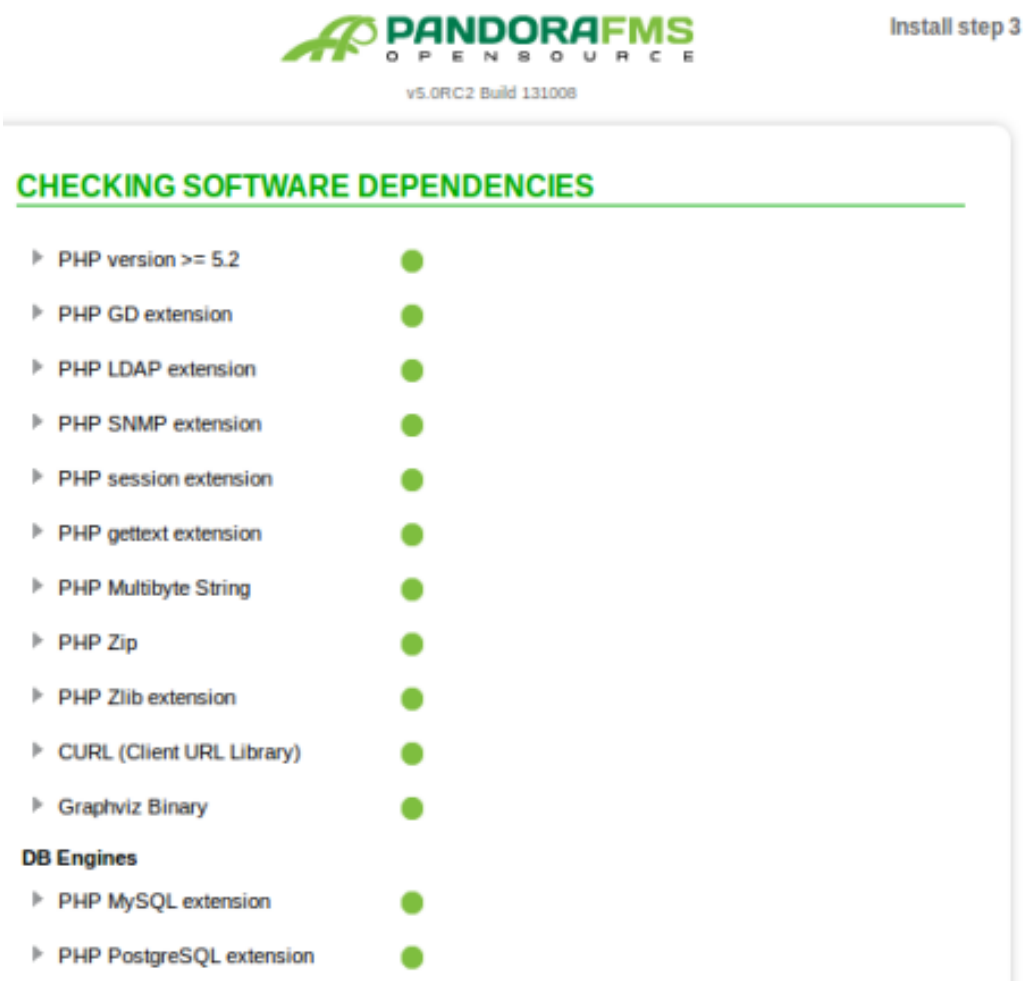
sudo a2dismod php7.0
sudo a2enmod php5.6
sudo service apache2 restart

Ahora instalamos los paquetes de Pandora FMS: servidor, consola y agente.

sudo apt-get install pandorafms-console pandorafms-server pandorafms-agent-unix

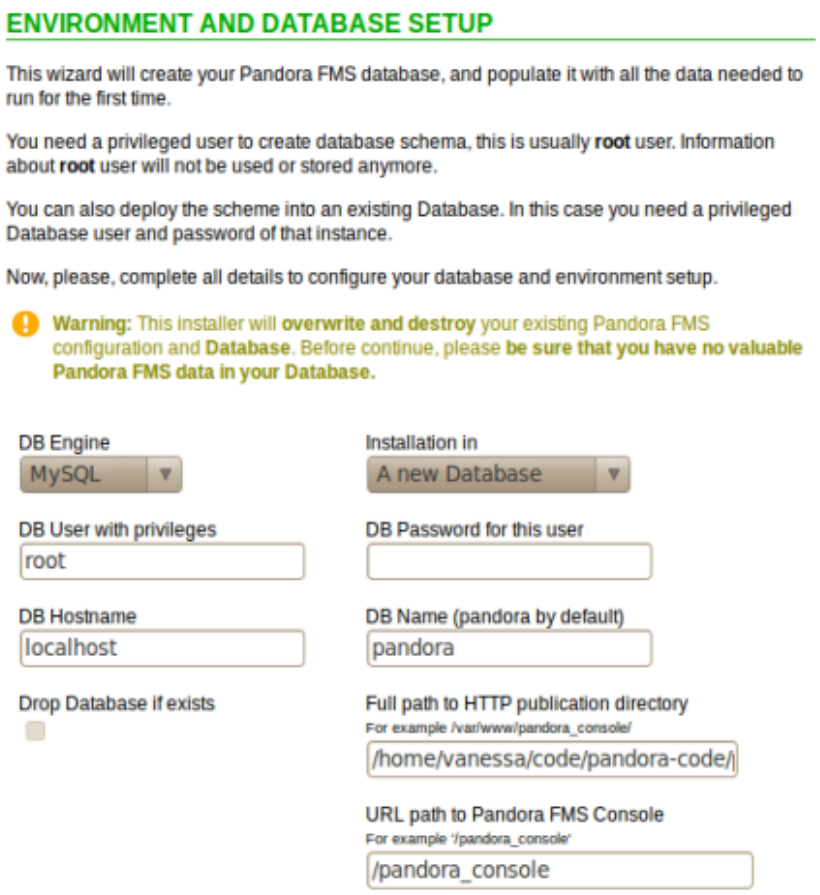
Una vez instalado todo desde la terminal de Ubuntu, tendremos que terminar la instalación de la consola desde la siguiente URL: http://dirección_IP_servidor_Pandora/pandora_console/install.php.

Ahora solo habrá que seguir los pasos indicados para crear la base de datos de Pandora. Se hará una revisión de las dependencias instaladas anteriormente.



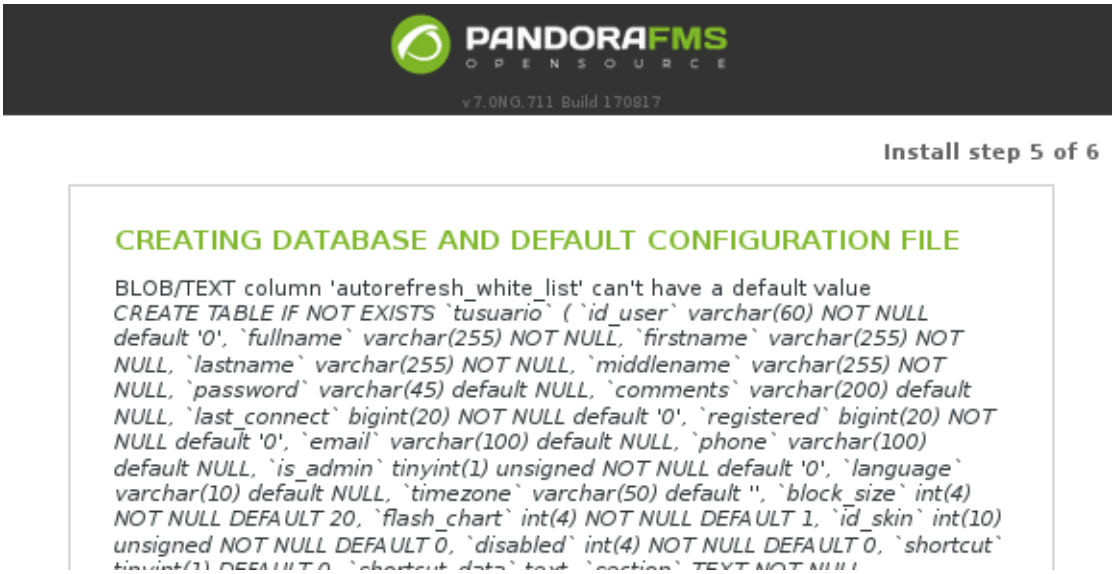
Si alguno de los círculos estuviera en rojo significaría que falta esa dependencia y no se podría continuar. Es posible que con el comando **sudo apt-get -f install** se instalen las dependencias que faltan o sino habría que instalarlas independientemente.

Una vez corregido esto, se pasará a crear la base datos a partir de los datos de acceso al servidor mysql, que se configuraron durante su instalación.



En “DB User with privileges” se debe escribir el usuario del servidor de mysql, en este caso *root*, y en “DB Password for this user”, la contraseña elegida al instalar mysql.

Es posible que, a la hora de crear el esquema de la base de datos, aparezca este error en la pantalla:



En tal caso, el error se soluciona buscando el fichero my.cnf:

sudo find / -name "*.cnf"

Y editar este fichero añadiendo:

[mysqld]
sql-mode="NO_AUTO_CREATE_USER,NO_ENGINE_SUBSTITUTION"

Así se quitaría el error y crearía la base de datos de Pandora.

Es importante que una vez creada, en la pantalla te aparece una contraseña aleatoria para la base de datos. Hay que configurar el fichero **/etc/pandora/pandora_server.conf** añadiendo dicha contraseña donde ponga “dbpass”.