



**UNIVERSIDAD POLITECNICA SALESIANA
SEDE GUAYAQUIL**

**CARRERA
INGENIERIA DE SISTEMAS**

**Tesis de grado previa a la obtención del título de
INGENIERO DE SISTEMAS**

TEMA

**“ANÁLISIS, DISEÑO E IMPLEMENTACIÓN DE UNA HERRAMIENTA DE
MONITOREO Y CONTROL DE DATACENTER BASADO EN
HERRAMIENTAS OPEN SOURCE. APLICADO AL BANCO DE GUAYAQUIL”**

AUTOR

ALEJANDRO ALFONSO ALVAREZ CEVALLOS

DIRECTOR:

ING. RICHARD ROMERO IZURIETA

GUAYAQUIL, ABRIL DEL 2015

**DECLARATORIA DE RESPONSABILIDAD DEL USO DEL TRABAJO DE
GRADO**

Yo Alejandro Alfonso Alvarez Cevallos autorizo a la Universidad Politécnica Salesiana la publicación total o parcial de este trabajo de grado y su reproducción sin fines de lucro.

Además declaro que los conceptos y análisis desarrollados y las conclusiones del presente trabajo son de exclusiva responsabilidad del autor.

(f) _____

Alejandro Alfonso Alvarez Cevallos

CC: 0925692188

DEDICATORIA

Este trabajo de tesis va dedicado sobre todo a Dios. A mis padres la Psic. Carmen Amelia Cevallos Moncada y el MsC. Ing. Alejandro Alfonso Alvarez Arias por su esfuerzo, dedicación y apoyo incondicional que siempre me impulsó a cumplir este logro. A mis hermanos, Katty Alvarez Cevallos, Alejandro Alvarez Cevallos, Jackeline Alvarez Cevallos, a mi sobrina Amelia Arias Alvarez, por ser parte fundamental en mi vida y una motivación continua durante este proceso.

Alejandro Alfonso Alvarez Cevallos

ÍNDICE DE CONTENIDOS

1. CAPITULO I.....	16
1.1 Enunciado del problema.....	16
1.1.1 Factores estructurales.....	16
1.1.2 Factores intermedios	17
1.1.3 Factores inmediatos	17
1.2 Formulación del problema de investigación	18
1.3 Objetivos de la investigación	18
1.3.1 Objetivo general.....	18
1.3.2 Objetivos específicos	18
1.4 Justificación de la investigación	19
1.5 Importancia de la investigación	19
1.6 Necesidad de la investigación	19
1.7 Beneficios de la investigación.....	20
1.8 Beneficiarios	20
2. CAPITULO II.....	21
2.1 Antecedentes de la investigación	21
2.1.1 Datacenter	22

2.1.2	Administración de redes	23
2.1.3	Que es un administrador de redes?	24
2.1.4	Objetivos de la administración de redes	25
2.1.5	Razones por las cuales la administración de redes es importante y difícil	25
2.1.6	Arquitectura de la Administración de Redes	26
2.1.7	Protocolos de Administración de Red TCP/IP	27
2.1.8	SNMP (Protocolo Simple de Administración de Red).	28
2.1.9	Arquitectura de protocolo SNMP	30
2.1.10	Monitoreo de red.....	32
2.1.11	Recursos administrados	33
2.1.12	Hardware.....	33
2.1.13	Software	34
2.2	Fundamentación legal	34
2.2.1	Norma TIER IV	34
3.	CAPITULO III	38
3.1	Requerimientos Funcionales	38
3.1.1	Identificación de actores	38
3.1.2	Identificación de escenarios.....	40
3.1.3	Identificación de casos de uso	43

3.2	Requerimientos No Funcionales	45
3.3	Definición de roles en los módulos.....	47
3.3.1	Roles en NAGIOS:	47
3.3.2	Roles en CACTI.....	48
4.	CAPITULO IV	50
4.1	Diseño de la arquitectura del sistema.....	50
4.1.1	Diseño arquitectónico	50
4.1.2	Módulos del sistema	52
4.2	Diagrama de clases del sistema.....	69
4.3	Modelo Lógico de la Base de Datos	75
5.	CAPITULO V	98
5.1	Capas del sistema y comunicaciones entre capas	98
5.2	Plan de pruebas	99
5.2.1	Pruebas de tiempos de respuestas hacia dispositivos en Matriz	99
5.2.2	Pruebas de tiempos de respuestas hacia dispositivos de agencias	99
5.2.3	Pruebas de tiempos de respuestas hacia dispositivos de datacenter ..	99
5.2.4	Prueba de servicios de comunicación hacia puertos de servicio	99
5.2.5	Pruebas de recepción de datos de interfaces de red	100
5.2.6	Pruebas recepción de datos de performance de equipos.....	100

5.2.7	Pruebas de envío y recepción de alertas mediante correo electrónico	100
5.2.8	Pruebas de envío y recepción de alertas mediante windows pop-up	100
5.2.9	Pruebas de envío y recepción de alertas mediante SMS.....	100
5.2.10	Pruebas de status de disponibilidad de host y servicios monitoreados ...	101
5.3	Resultado de las pruebas y métricas tomadas	101
6.	CAPITULO VI.....	102
6.1	Conclusión	102
6.2	Recomendaciones.....	102
7.	BIBLIOGRAFÍA.....	104
	Archivos de recursos – timeperiods.cfg-,htpasswd.users.....	137
	Archivos de definición de objetos –hosts.cfg-, -services.cfg-, -contacts.cfg-, - commands.cfg.....	137
	Archivos de configuración cgi – cgi.cfg-	137

ÍNDICE DE IMÁGENES

Figura 1: Arquitectura de administración de redes.....	27
Figura 2 Arquitectura de protocolo SNMP	30
Figura 3 Método de recolección de datos mediante SNMP	31
Figura 4 Método de recolección de datos mediante SNMP	31
Figura 5: Funciones de Oficial de Networking	38
Figura 6: Funciones de Oficial de Base de Datos.....	39
Figura 7 Arquitectura de NAGIOS.....	51
Figura 8 Arquitectura de CACTI.....	52
Figura 9: NAGIOS opción de Mapa.....	53
Figura 10: NAGIOS opción de Hosts.....	53
Figura 11: NAGIOS opción de Services	54
Figura 12: NAGIOS opción de Hostgroups	55
Figura 13: NAGIOS opción de Reporte de Disponibilidad.....	56
Figura 14: NAGIOS opción de Gráfica de Disponibilidad	57
Figura 15: NAGIOS opción de Reporte de alertas	57
Figura 16: NAGIOS opción de Reporte de notificaciones	58
Figura 17: NAGIOS opción de Reporte de logs de eventos.....	59
Figura 18: NAGIOS opción de Información de proceso nagios	60
Figura 19: NAGIOS opción de Información de rendimiento de monitoreo.....	61
Figura 20: NAGIOS opción de configuración de Host	62
Figura 21: NAGIOS opción de Revisión de cola de programación	63
Figura 22: CACTI opción de Gráficos	64
Figura 23: CACTI opción de árbol gráfico	64

Figura 24: CACTI opción de Grupo de notificaciones.....	65
Figura 25: CACTI opción de Plantilla de gráficos	65
Figura 26: CACTI opción de Plantilla de host	66
Figura 27: CACTI opción de Plantilla de datos	66
Figura 28: CACTI opción de módulo de configuración.....	67
Figura 29: CACTI opción de Administración de plugins	67
Figura 30: CACTI opción de revisión de logs del poller	68
Figura 30: CACTI opción de revisión de logs de SNMP	68
Figura 32: CACTI opción de Administración de usuarios	69
Figura 33: CACTI Módulo de mantenimiento de software.....	69
Figura 34: CACTI Diagrama de clases	70
Figura 35: NAGIOS Diagrama de clases	71
Figura 36: CACTI Diagrama de clases	72
Figura 37: CACTI Diagrama de clases	73
Figura 38: CACTI Diagrama de clases	74
Figura 39: CACTI Modelo lógico de Base de datos	97
Figura 40: Capas del sistema del sistema NAGIOS+CACTI.....	98

ÍNDICE DE TABLAS

Tabla 1 Tabla de Actores.....	38
Tabla 2 Funciones de oficial de networking.....	39
Tabla 3 Funciones de oficial de base de datos.....	40
Tabla 4 Escenario 1 de uso de NAGIOS	40
Tabla 5 Escenario 2 de uso de NAGIOS	40
Tabla 6 Escenario 3 de uso de NAGIOS	41
Tabla 7 Escenario 4 de uso de NAGIOS	41
Tabla 8 Escenario 5 de uso de NAGIOS	41
Tabla 9 Escenario 1 de uso de CACTI	42
Tabla 10 Escenario 2 de uso de CACTI	42
Tabla 11 Escenario 3 de uso de CACTI	43
Tabla 12 Escenario 4 de uso de CACTI	43
Tabla 13 Caso 1 de uso del software	43
Tabla 14 Caso 2 de uso del software	44
Tabla 15 Caso 3 de uso del software	44
Tabla 16 Requerimiento no funcional 1	45
Tabla 17 Requerimiento no funcional 2	45
Tabla 18 Requerimiento no funcional 3	45
Tabla 19 Requerimiento no funcional 4	45
Tabla 20 Requerimiento no funcional 5	46
Tabla 21 Requerimiento no funcional 6	46
Tabla 22 Requerimiento no funcional 7	46
Tabla 23 Requerimiento no funcional 8	46

Tabla 24 Requerimiento no funcional 9	47
Tabla 25 Estructura de tabla cdef	75
Tabla 26 Estructura de tabla cdef_items.....	75
Tabla 27 Estructura de tabla colors	76
Tabla 28 Estructura de tabla data_input	76
Tabla 29 Estructura de tabla data_input_data.....	76
Tabla 30 Estructura de tabla data_input_fields	77
Tabla 31 Estructura de tabla data_local.....	77
Tabla 32 Estructura de tabla data_template.....	78
Tabla 33 Estructura de tabla data_template_data	78
Tabla 34 Estructura de tabla data_template_data_rra.....	79
Tabla 35 Estructura de tabla data_template_rrd	79
Tabla 36 Estructura de tabla graph_local	80
Tabla 37 Estructura de tabla graph_templates.....	81
Tabla 38 Estructura de tabla graph_templates_graph.....	81
Tabla 39 Estructura de tabla graph_templates_item.....	83
Tabla 40 Estructura de tabla graph_template_input	84
Tabla 41 Estructura de tabla graph_template_input_defs	84
Tabla 42 Estructura de tabla graph_tree	85
Tabla 43 Estructura de tabla graph_tree_items	85
Tabla 44 Estructura de tabla host	86
Tabla 45 Estructura de tabla host_snmp_cache.....	87
Tabla 46 Estructura de tabla host_snmp_query.....	87
Tabla 47 Estructura de tabla host_template.....	87

Tabla 48 Estructura de tabla host_template_graph.....	88
Tabla 49 Estructura de tabla poller.....	88
Tabla 50 Estructura de tabla poller_command.....	88
Tabla 51 Estructura de tabla poller_item.....	89
Tabla 52 Estructura de tabla poller_output.....	90
Tabla 53 Estructura de tabla poller_reindex.....	90
Tabla 54 Estructura de tabla poller_time.....	90
Tabla 55 Estructura de tabla rra.....	91
Tabla 56 Estructura de tabla rra_cf.....	91
Tabla 57 Estructura de tabla settings_graphs.....	92
Tabla 58 Estructura de tabla settings_tree.....	92
Tabla 59 Estructura de tabla snmp_query.....	92
Tabla 60 Estructura de tabla snmp_query_graph.....	93
Tabla 61 Estructura de tabla snmp_query_graph_rrd.....	93
Tabla 62 Estructura de tabla snmp_query_graph_rrd_sv.....	94
Tabla 63 Estructura de tabla snmp_query_graph_rv.....	94
Tabla 64 Estructura de tabla user_auth.....	95
Tabla 65 Estructura de tabla user_auth_perms.....	95
Tabla 66 Estructura de tabla user_auth_realm.....	96

RESUMEN

El presente proyecto de tesis para la obtención de título de Ingeniero en Sistemas titulado: "Análisis, diseño e implementación de una herramienta de monitoreo y control de datacenter basado en herramientas Open Source. Aplicado al banco de Guayaquil" consta de la implementación de la herramienta NAGIOS la cual se encargara de monitorear los elementos de hardware (equipos de comunicación) y software (servicios publicados) dentro de la infraestructura de datacenter facilitando a los administradores de red la detección problemas y notificando de manera oportuna vía correo electrónico, SMS, y otros medios.

Todo evento presentado en la red, también el software nos brindara la facilidad de generar un reporte de disponibilidad en los equipos. La herramienta CACTI es una herramienta de control histórico de consumo de interfaces de red ya sean estas de enlaces internos o externos, la cual facilitará gráficamente detectar comportamientos anómalos en la red y en los consumos de CPU y memoria RAM de los equipos de datacenter. La solución propuesta ha sido implementada bajo GNU/LINUX lo cual nos ha brindado las facilidades en cuanto a costo del proyecto, resultados esperados y en personalización del monitoreo.

ABSTRACT

This thesis project for obtaining title Systems Engineer entitled. "Analysis, design and implementation of a tool for monitoring and control of datacenter based on Open Source tools applied to Banco Guayaquil" is based on the implementation of the NAGIOS tool which would be responsible for monitoring the hardware elements (communications equipment) and software (public services) within the datacenter infrastructure easier for network administrators the trouble detection and timely notice via email, SMS, and others.

All events presented in the network, the software also handed us the ease of generating an uptime report on computers. The CACTI tool is a historical control consumption of network interfaces and whether they are internal or external links, which provide graphically detect anomalous behavior in the network and in the consumption of CPU and RAM of the devices on datacenter. The proposed solution has been implemented under GNU / LINUX which has given us the facilities in terms of project cost, expected results and customization of monitoring.

INTRODUCCION

Este proyecto de tesis está desarrollado en 6 capítulos, el mismo que contiene información esencial respecto a la implementación de un sistema de monitoreo de datacenter basado en open source aplicado en Banco Guayaquil, a continuación se detalla cada capítulo:

Capítulo I

En este capítulo se desarrollará el problema detallándolo de manera breve y se plantearán los objetivos a obtener en la implementación.

Capítulo II

En este capítulo se detallaran los conceptos básicos y la fundamentación legal en que está basado este proyecto de desarrollo e implementación de software.

Capítulo III

En este capítulo se detallaran los requerimientos que se necesitarán para el correcto funcionamiento del sistema de monitoreo de Datacenter en Banco Guayaquil.

Capítulo IV

En este capítulo se describirá la arquitectura del sistema, también se explicaran los diferentes módulos en que lo componen y también se diagramará el código fuente del sistema y su respectiva base de datos.

Capítulo V

En este capítulo se explicara las diferentes pruebas de estrés realizadas al sistema de monitoreo para evaluar la rapidez y precisión al momento de obtener los resultados.

Capítulo VI

En este capítulo se describirán ciertas conclusiones y recomendaciones encontradas para un mejor desempeño de la herramienta de monitoreo.

CAPITULO I

PLANTEAMIENTO DEL PROBLEMA

1.1 Enunciado del problema

1.1.1 Factores estructurales

Las entidades financieras al igual que las entidades con fines comerciales dentro de sus bienes más preciados que poseen están los datos de sus clientes y la información transaccional tanto de la empresa como de sus clientes por tal motivo la inversión en centros de datos han ido incrementando a la par con la tecnología, mejorando sus técnicas de almacenamiento y métodos de acceso a la información a través de los sistemas de comunicación y software especializados; también éstas entidades al ser regidas por organismos de control han tenido que cumplir con estándares de servicio apropiados para poder brindar un mejor servicio y competir a la vanguardia de las TIC, llegando a dar el nombre de datacenter al lugar donde la interacción de los elementos tecnológicos de red y de seguridad llegando a formar este lugar en factor vital para la continuidad del negocio.

Debido a que los datacenter son primordiales para las comunicaciones entre entidades y para ofrecer los diferentes servicios a los clientes se requiere de un correcto control y gestión hacia los diferentes eventos de carácter físico / lógico.

Banco Guayaquil como una entidad financiera caracterizada por la innovación y generación de nuevos métodos para sus clientes en los últimos 2 años ha realizado una renovación tecnológica en cuanto a su infraestructura de datacenter, llegando a ser el

primer banco en Ecuador en tener su datacenter con la certificación TIER4; por tal motivo el área de infraestructura se ve en la necesidad de contar con un software el cual será el encargado del monitoreo de los equipos de comunicación, servicios alojados en el datacenter y enlaces de red hacia las diferentes marcas proveedoras o entidades con relación de negocio.

1.1.2 Factores intermedios

Los software encargados del monitoreo de datacenter en el medio actualmente se manejan en diferentes funciones en donde a su vez se manejan con su respectivo costo a nivel de desarrollo propietario; la diferencia en los software de open source se radica en la parte funcional y en la facilidad de administración e instalación. Dentro de las funcionalidades que Banco Guayaquil busca es la flexibilidad y múltiples métodos de notificación de eventos, para lo cual se ha propuesto la implementación de la herramienta NAGIOS y CACTI que permitirá se aprovecharan sus diferentes funcionalidades a un costo mínimo ya que dichos software cuentan con licencia GPL (Global Public License).

1.1.3 Factores inmediatos

Los beneficios a obtener en datacenter con la herramienta NAGIOS + CACTI son los siguientes:

- Supervisión continua de la plataforma de TI
- Mejorar los SLA y mejorar los tiempos de disponibilidad
- Alertar al team de TI ante alertas preventivas (Warning) o críticas (Critical)

- Reaccionar de manera preventiva y no reactiva ante los eventos que NAGIOS detecte. Lo que implica aumentar la productividad de las TIC
- Generar reportes de los eventos.
- Planificar mantenimientos del hardware o de servicios.
- Planificar el cambio o renovación de la infraestructura de TIC
- Datos históricos de consumo por interfaz de cada dispositivo de red en datacenter.

1.2 Formulación del problema de investigación

¿Cómo se puede monitorear, controlar y notificar los eventos de fallo que ocurren dentro de un centro de cómputo con una herramienta de bajo costo?

¿Qué elementos críticos de red se puede monitorear en el Datacenter?

¿Qué se logrará obtener al desarrollar una herramienta de monitoreo basada en open source?

¿Qué se puede demostrar al obtener los resultados de la implementación del sistema de monitoreo?

1.3 Objetivos de la investigación

1.3.1 Objetivo general

Construir un software de monitoreo y control de equipos de comunicaciones en el datacenter de Banco Guayaquil mediante el uso de herramientas open source.

1.3.2 Objetivos específicos

- Monitorear equipos y servicios críticos y no críticos dentro de una infraestructura de datacenter.

- Incentivar a los administradores de datacenter a utilizar software libre.
- Demostrar que se obtienen buenos resultados a un bajo costo al implementar y personalizar herramientas open source.

1.4 Justificación de la investigación

Debido al crecimiento en infraestructura de datacenter, y a las diferentes aplicaciones de monitoreo en open source nace la idea de elaborar una herramienta que brinde la ayuda necesaria para los administradores de red y datacenter de una manera flexible y personalizable de bajo costo y de resultados óptimos para una correcta notificación de eventos dentro de la infraestructura administrada.

1.5 Importancia de la investigación

Los datacenter cumplen un papel importante dentro de la infraestructura de una empresa ya que concentran todo los recursos tecnológicos necesarios para el procesamiento de datos, brindando garantías en la disponibilidad, confidencialidad e integridad de la información. El correcto monitoreo y control de un datacenter permitirá el cumplimiento de las características antes mencionadas, esto permitirá estar alerta ante cualquier evento para actuar con eficiencia antes de un incidente.

1.6 Necesidad de la investigación

Al tener diversidad de software de costo considerables y de bajo costo, es conveniente generar una alternativa cero costo la cual tenga la flexibilidad necesaria

para poder ser implementada en la infraestructura de datacenter de una entidad bancaria capaz de alertar los diferentes eventos que se presentan dentro de la infraestructura, facilitar y ayuda a los administradores de red a cumplir sus funciones.

1.7 Beneficios de la investigación

Los beneficios tangibles que se obtendrá de esta investigación son los siguientes:

- Brindar alternativas de software a comparación a los software licenciados
- Un correcto control de alertas y manejo de notificaciones óptimo.
- Generar beneficios a los administradores de red con las notificaciones de eventos de hardware y software.
- Establecer parámetros de monitoreo y control de la infraestructura basados en servicios bancarios.

1.8 Beneficiarios

Como beneficiarios directos se tiene a los administradores de redes ya que son los encargados del control preventivo y correctivo del estado de salud de los dispositivos de red en el datacenter.

Se puede decir que colateralmente los beneficiados ante todo el correcto estado de la red y de los servicios sobre la red serán los clientes de Banco Guayaquil ya que ellos son quienes ponen a prueba el performance y desempeño de los servicios ofrecidos.

CAPITULO II

MARCO TEÓRICO

2.1 Antecedentes de la investigación

En la actualidad la sociedad se mueve a una velocidad impresionante. Todos los días aparecen nuevos productos en el mercado que sustituyen a los ya existentes, la moda, lo novedoso y las producciones en general tienen, en su mayoría, un ciclo de vida fugaz.

Los mercados se tornan muy competitivos y para poder insertarse en ellos es necesaria la constante renovación e innovación.

La búsqueda de la competitividad en los servicios bancarios es una tarea de primer orden para la dirección empresarial. El desarrollo de la mentalidad innovadora constituye un aspecto fundamental para las áreas de Infraestructura, así a partir del planteamiento de una estrategia de ciencia e innovación tecnológica se debe lograr un adecuado nivel de gestión de tecnología que posibilite la adquisición e incorporación de nuevos conocimientos científico-tecnológicos a la actividad productiva de los bancos, con el objetivo de mantener e incrementar sus niveles de competitividad y eficiencia con los estándares internacionales de calidad.

Según el artículo de Grupo del banco Mundial (2015) la banca a nivel mundial se ha sentido una fuerte tendencia a optimizar los procesos y mejorar la productividad a través de la tecnología lo cual se convierte en un reto para las áreas de Sistemas e

Infraestructura en cuanto a la adquisición de hardware, software y equipos de TI. Lo cual llega a ser un nuevo reto a controlar y medir para tomar acciones contra eventos que puedan ocurrir dentro de los centros de datos, donde la tecnología adquirida se convierte en un punto vital del negocio.

2.1.1 Datacenter

Un Centro de Procesamiento de Datos (CPD) según Asenjo Group (2015) es un espacio de gran tamaño donde se emplaza el equipamiento electrónico que guarda toda la información de una organización. El término proviene del inglés “Data Center” y en España se conoce comúnmente como Centro de datos.

Dentro de las características que posee un datacenter están:

- **Energía garantizada**

La energía eléctrica es la llave de todas las operaciones que se realizan en los centros de datos. Sin energía eléctrica fiable, este tipo de **infraestructura** no podría funcionar. Pero no es suficiente con estar conectado a la red eléctrica tradicional, sino que es necesario contar con equipos de apoyo capaces de aportar la energía suficiente para el buen funcionamiento del CPD en caso de apagón. Por ello los generadores eléctricos (sistemas de almacenamiento de energía) son parte fundamental para asegurar el servicio en caso de cortes de luz.

- **Conexión a Internet**

Los centros de datos están conectados a Internet a través de conexiones Gigabit Ethernet redundantes, por lo que en caso de caída de una línea, el servicio seguirá funcionando sin problemas.

- **Seguridad**

Debido a la gran cantidad de información valiosa que se almacena en los servidores hospedados en los CPD, la seguridad es primordial para evitar cualquier tipo de robo de información u otra serie de problemas. Servicios de video vigilancia y presencia de personal las 24 horas del día son algunas medidas que todo centro de datos deben implementar para garantizar la seguridad de los datos de sus clientes.

- **Sistemas de control de climatización**

Una temperatura óptima es fundamental para sacar el máximo rendimiento a las máquinas ahí instaladas, por eso los centros de datos utilizan sistemas de aire acondicionado que mantienen la temperatura de las salas en una franja de entre los 15 y 25 grados, evitando el sobrecalentamiento de los servidores.

2.1.2 Administración de redes

Según Sergio Talens-Oliag (2007) la administración de redes es una rama de la ingeniería que se ocupa de la gestión de sistemas formados por computadoras y usuarios; trata de organizar redes de ordenadores, hacer que funcionen y mantenerlos en marcha a pesar de lo que hagan sus usuarios.

2.1.3 Que es un administrador de redes?

Según el sitio Web de Ecured (2015) los administradores de red son básicamente el equivalente de red de los administradores de sistemas: mantienen el Hardware y Software de la red. Esto incluye el despliegue, mantenimiento y monitoreo del engranaje de la red: Switches, Routers, Cortafuegos, etc. Las actividades de administración de una red por lo general incluyen la asignación de direcciones, asignación de protocolos de ruteo y configuración de tablas de Ruteo así como, configuración de Autenticación y autorización de los servicios.

Frecuentemente se incluyen algunas otras actividades como el mantenimiento de las instalaciones de red tales como los controladores y ajustes de las Computadoras e Impresoras. A veces también se incluye el mantenimiento de algunos tipos de servidores como VPN, Sistemas detectores de intrusos, etc.

Las responsabilidades de un administrador de la red se dividen en siete áreas.

- Responder a las necesidades de los usuarios.
- Diseñar la instalación, incluyendo el cableado, el lugar donde se va a instalar las estaciones, los derechos de acceso, las interfaces de los usuarios, y la seguridad.
- Configurar la red al ponerla en marcha y siempre que se haga algún cambio.
- Mantener y administrar la red.
- Diagnosticar problemas y efectuar reparaciones sencillas.

- Evaluar el rendimiento de la red.
- Planificar los cambios a corto y largo plazo.

2.1.4 Objetivos de la administración de redes

Según Ford, M y Kim, Lew (1998) los objetivos de la administración de redes son:

- Mantener operativa la red satisfaciendo las necesidades de los usuarios.
- Mejorar la continuidad en la operación de la red con mecanismos adecuados de control y monitoreo, de resolución de problemas y de suministro de recursos.
- Hacer uso eficiente de la red y utilizar mejor los recursos.
- Asegurar el funcionamiento de la red, protegiéndola contra el acceso no autorizado, impidiendo que personas ajenas puedan acceder a la información que circula en ella.
- Controlar los cambios y actualizaciones en la red de modo que ocasionen las menos interrupciones posibles. En el servicio a los usuarios.

2.1.5 Razones por las cuales la administración de redes es importante y difícil

Según Ford, M y Kim, Lew (1998) las razones por la cual la administración de redes es importante y difícil son:

- Se mezclan diversas señales como voz, datos, imágenes y gráficas.
- Se interconectan varios tipos de redes de acuerdo a su cobertura: LAN, MAN y WAN.
- El empleo de varios sistemas operativos.

- Se utilizan diversas arquitecturas de red.

2.1.6 Arquitectura de la Administración de Redes

Según la Mc. Cintia Quezada Reyes (2012) las arquitectura para la administración de redes utiliza la misma estructura y conjuntos básicos de relaciones. Las estaciones terminales, como los sistemas de cómputo y otros dispositivos de red, utilizan un software que les permite enviar mensajes de alerta cuando se detecta algún problema. Al recibir estos mensajes de alerta las entidades de administración son programadas para reaccionar, ejecutando una o varias acciones que incluyen la notificación al administrador, el cierre del sistema, y un proceso automático para la posible reparación del sistema.

Las entidades de administración también pueden registrar la información de las estaciones terminales para verificar los valores de ciertas variables. Esta verificación puede realizarse automáticamente o ejecutada por algún administrador de red, pero los agentes en los dispositivos que se están administrando responden a todas las verificaciones.

Los agentes son módulos de software que, en primer lugar, compilan información acerca de los dispositivos administrados en los que residen, después almacenan esta información en una base de datos de administración y, por último la ponen a disposición (de manera proactiva o reactiva) de las entidades que forman parte de los sistemas de administración de red vía un protocolo de administración de red, como por ejemplo,

SNMP (Protocolo Simple de Administración de Redes) y CMPIIP (Protocolo de Información de Administración Común).

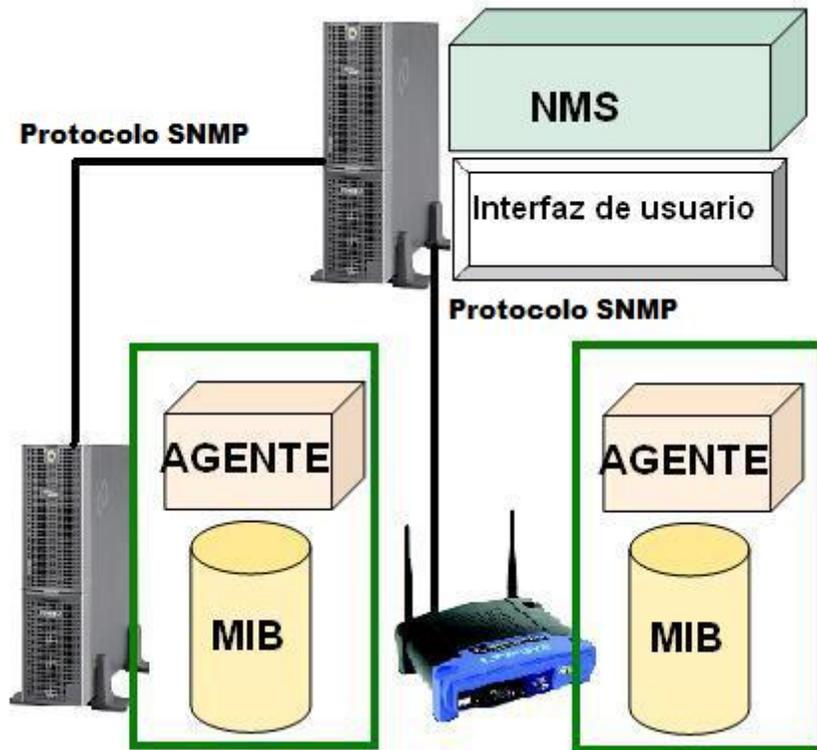


Figura 1: Arquitectura de administración de redes

Fuente: <http://velezconde.wordpress.com/2009/06/20/fundamentos-sobre-la-gestion-monitorizacion-y-control-de-redes/>

2.1.7 Protocolos de Administración de Red TCP/IP

Según el libro del autor Black, U (2000) el sistema de administración de red de TP/IP se basa en el protocolo SNMP (Protocolo Simple de Administración de Redes), que ha llegado a ser un estándar de ISO en la industria de comunicación de datos para la administración de redes de computadora, ya que ha sido instalado poro múltiples fabricantes de puentes, repetidores, ruteadores, servidores y otros componentes de l red.

Para hacer más eficiente la administración de la red, la comunidad TCP/IP divide las actividades en dos partes:

- Monitoreo, o proceso de observar el comportamiento de la red y de sus componentes, para detectar problemas y mejorar su funcionamiento.
- Control. O proceso de cambiar el comportamiento de la red en tiempo real ajustando parámetros, mientras la red está en operación, para mejorar el funcionamiento y repara fallas.

2.1.8 SNMP (Protocolo Simple de Administración de Red).

Según Ford, M y Kim, Lew (1998) SNMP surge para devolver los problemas de administración de redes TCP/IP, debido a que el crecimiento apresurado y desmesurado de este tipo de redes ha hecho que la administración y gestión de las mismas se convierta en una labor intensa. Un caso muy particular es el de Internet, debido a su complejidad y gran tamaño. La arquitectura de este protocolo se diseñó tomando en cuenta el modelo OSI.

El protocolo sencillo de administración de red (SNMP) es el protocolo de administración de redes estándar usado en Internet. Este protocolo, define la comunicación de un administrador con un agente.

Es un protocolo de gestión de red muy utilizado ya que permite obtener información de dispositivos de la red, memoria libre, uso de CPU, detección de errores, establecer alarmas, estado de funcionamiento, etc.

SNMP está formado por cuatro componentes básicos:

- **Base de datos lógica:** SNMP sigue el modelo de la base de datos lógica, en la misma se almacena información referente a la configuración, estado, error y rendimiento.
- **Agentes:** El agente es un software, que permite el acceso a la información. Dicho agente responde a peticiones, realiza actualizaciones e informa los problemas.
- **Administradores:** La estación de administración, contiene un software de administrador, el cual se encarga de enviar y recibir los mensajes SNMP. Además de esto existen otra serie de aplicaciones de administración que se comunican con los sistemas de red mediante el administrador.
- **Base de información de administración:** La base de información de administración, denominada MIB, constituye la descripción lógica de todos los datos de administración de la red. La MIB contiene información de estado y del sistema, estadísticas de rendimiento y parámetros de configuración.

(Ford, M y Kim, Lew, 1998)

2.1.9 Arquitectura de protocolo SNMP

El modelo de la arquitectura del protocolo SNMP es el siguiente:

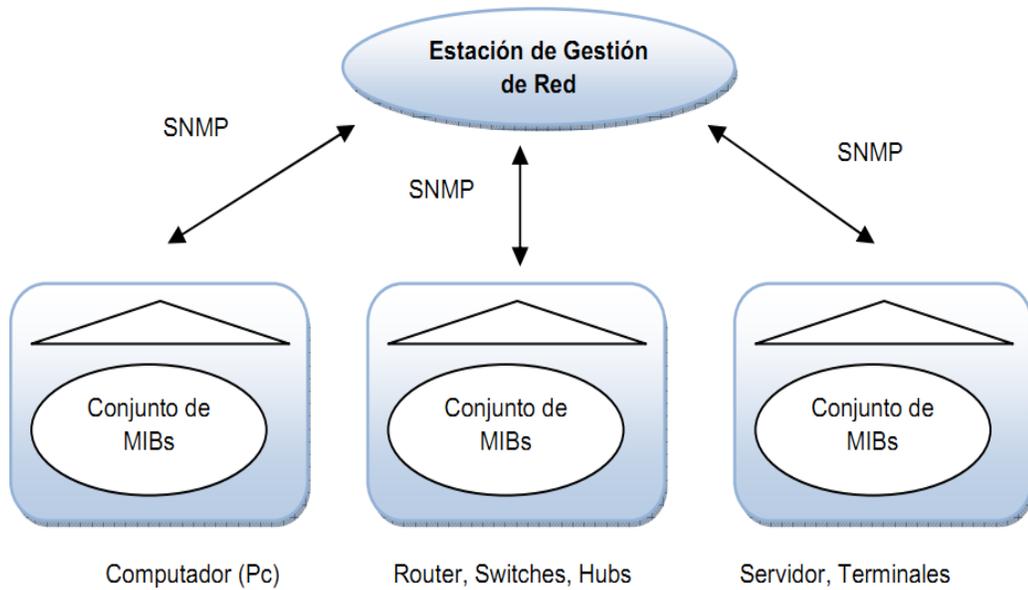


Figura 2 Arquitectura de protocolo SNMP

Fuente: <http://redalyc.uaemex.mx/pdf/784/78430108.pdf>

Según el M.Sc. Gerardo Junco Romero (2011) Los métodos de adquisición de datos y de información bajo el protocolo SNMP son los siguientes:

Mediante un query SNMP hacia el agente SNMP

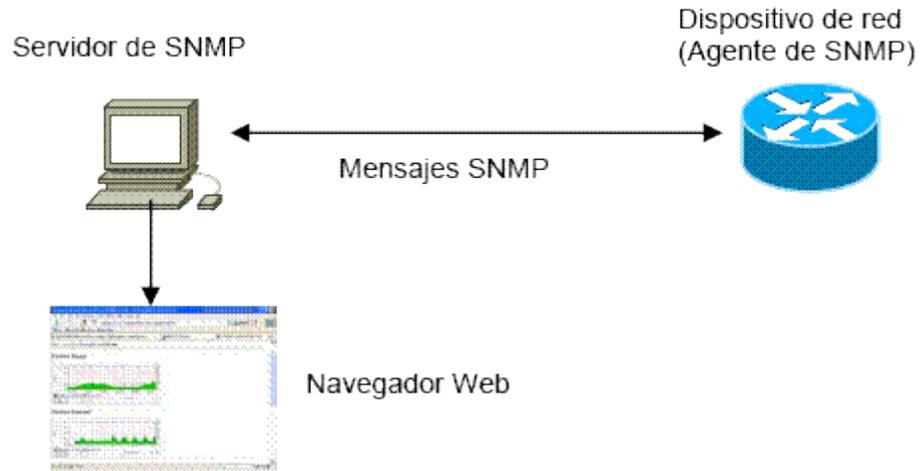


Figura 3 Método de recolección de datos mediante SNMP

Fuente: <http://www.monografias.com/trabajos95/recursos-red-y-su-monitoreo/recursos-red-y-su-monitoreo.shtml>

Mediante traps SNMP los cuales son enviados hacia el servidor SNMP al momento de existir un evento en el agente SNMP.

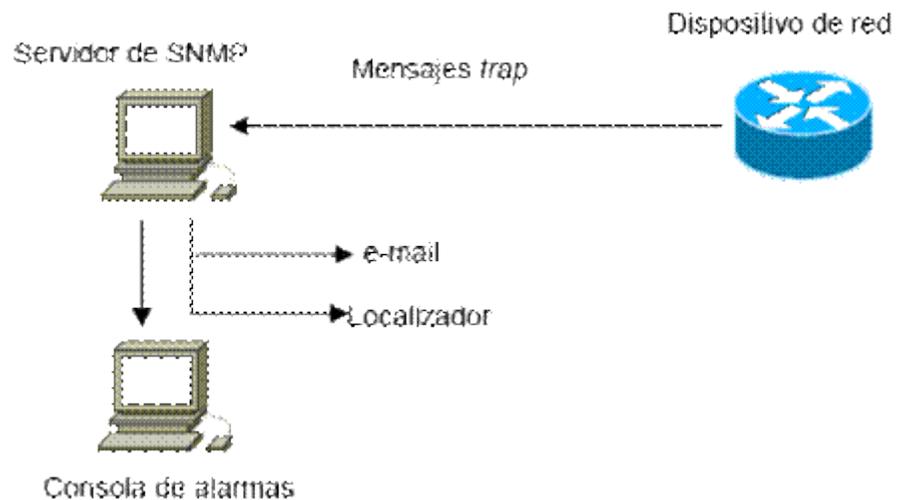


Figura 4 Método de recolección de datos mediante SNMP

Fuente: <http://www.monografias.com/trabajos95/recursos-red-y-su-monitoreo/recursos-red-y-su-monitoreo.shtml>

2.1.10 Monitoreo de red

Según Ford, M y Kim, Lew (1998) el monitoreo de red es el seguimiento, vigilancia y control permanente hacia los diferentes equipos de comunicación (router, switch, firewall, IPS, IDS, etc.) y servicios mediante el uso de un software especializado el cual censa constantemente la red en busca de componentes defectuosos o lentos, para luego notificar a los administradores de red a través de diferentes medios (SMS, correo electrónico, alertas pop-up, etc.).

El monitoreo de una red abarca 4 fases:

- Definición de la información de administración que se monitorea.
- Acceso a la información.
- Diseño de políticas de administración
- Procesamiento de la información

Los tipos de monitoreo son:

- Local.
- Remoto.
- Automático.
- Manual.

Los elementos monitoreados pueden ser:

- En su totalidad
- En segmentos

El monitoreo puede ser realizado en forma

- Continua

- Eventual

2.1.11 Recursos administrados

Según Ford, M y Kim, Lew (1998) la administración y monitoreo de redes de computadoras abarca monitoreo y control de hardware y componentes de software de redes diferente.

2.1.12 Hardware

Según Ford, M y Kim, Lew (1998) estos son algunos de los componentes de hardware:

- Conexiones físicas: incluye equipo relacionado con las capas físicas y de enlace.

Los protocolos usados son FDDI, frame relay, BISDN, ATM, SONET. Además incluye switches y concentradores.

- Componentes de Computadora: incluye dispositivos de almacenamiento, procesadores, impresoras y otros. Ethernet, Token Ring y Token Bus se consideran parte de los componentes de computadoras.
- Componentes de interconexión y conectividad: se refiere a los componentes de hardware tales como repetidores, bridges, ruteadores, gateways, hubs y módems.
- Hardware de telecomunicaciones: estos son módems, mutiplexadores y switches.

2.1.13 Software

Según Ford, M y Kim, Lew (1998) el software típico incluye:

- Software del sistema operativo: Windows, Linux, Unix, DOS, etc.
- Herramientas de software y software de aplicación: el software de aplicación hace a las computadoras más populares y productivas.
- Software del sistema en modelo cliente servidor: Banca electrónica, Bancos del barrio, etc.
- Software de interconexión: software usado en repetidores, bridges, ruteadores, gateways, hubs, módems.
- Software de aplicación en modelo cliente servidor: incluye servidores de base datos, servidor de archivos y servidores de impresión.
- Software de telecomunicaciones y comunicación de datos: software de administración relacionado a la comunicación de datos y protocolos de telecomunicaciones tales como FDDI, frame relay, MPLS, ATM, etc.
- Software de telecomunicaciones: backbone.

2.2 Fundamentación legal

2.2.1 Norma TIER IV

Según Uptime Institute, un Data Center TIER IV debe estar construido a prueba de fallos (Fault Tolerant) y para ello se requiere sistemas múltiples, independientes, y físicamente aislados, con componentes redundantes de capacidad y vías de distribución independiente y activa que sirvan simultáneamente a la carga IT. Además se requiere

refrigeración continua y respuesta autónoma de los sistemas para identificar, aislar y reparar una falla.

Veamos que significan esos requerimientos para cada uno de los sistemas:

- **Ingeniería civil:** desde el punto de vista de ingeniería civil, la única diferencia entre un TIER III y un TIER IV es la separación física entre los componentes y rutas activas. Esto se puede conseguir mediante la “compartimentalización”, es decir, creando cuartos y muros para separar los componentes y/o una distribución de espacios que separe físicamente ambas rutas, por ejemplo en lados opuestos del edificio principal.
- **Sistema eléctrico:** el sistema eléctrico de un TIER IV se diferencia de un TIER III en que ambas rutas deben ser activas, y que los tableros deben ser automáticos. La mayor diferencia de costo estaría en las UPS si no fuera porque la mayoría de los TIER III ya tienen UPS en ambas ramas, entonces realmente la única diferencia sería la respuesta autónoma del sistema eléctrico ante una eventual falla, punto que también gran parte de los TIER III ya poseen, debido a que con un buen diseño, esta automatización se puede limitar a algunos pocos tableros.
- **Sistema mecánico:** aquí la principal diferencia radica en el enfriamiento continuo, es decir el respaldo por UPS de los ventiladores de las manejadoras de aire acondicionado, de las válvulas y de las bombas de agua del sistema de agua helada (en caso de enfriamiento por agua helada, lo más común en grandes data centers), además de requerir de un almacenamiento térmico (Thermal Energy Storage) por el mismo tiempo de autonomía de las baterías de las UPS de la

carga crítica. Sin embargo, en grandes Data Centers TIER III es recomendable y muy común encontrar que ya se ha incluido el enfriamiento continuo, luego en esos casos la diferencia radicaría en la capacidad de respuesta autónoma. Esta pueda ser una de las mayores diferencias en costos, y que represente entre un 7% a un 10% del Capex del Data Center. Un buen diseño TIER IV minimiza la cantidad de válvulas para reducir costos.

- **Sistema de monitoreo y gestión:** aquí radica la principal diferencia en un TIER IV frente a un TIER III. El sistema de gestión debe asegurar la capacidad del sistema de identificar, aislar y reparar cualquier falla. Se requiere un BMS mucho más sofisticado y con un nivel mucho mayor de instrumentalización y control. Así y todo, un BMS muy sofisticado no debe representar más de un 5% del valor del proyecto.
- **Otros sistemas especiales:** Para el sistema de detección y extinción de incendio, el sistema de seguridad física, etc. no hay diferencias entre un TIER III y un TIER IV siempre y cuando los diseños sean independientes del sistema electromecánico.

Es importante señalar, que la certificación TIER (I,II, III y IV) de Facilidad Construida solamente hace referencia a la disponibilidad del sistema electromecánico desde un punto de vista de diseño y construcción. La certificación TIER solo nos garantiza que la instalación se ha diseñado y construido de acuerdo a un conjunto de recomendaciones, pero lo que nos va a asegurar la máxima disponibilidad durante la vida del Data Center es su operación y mantenimiento. Para eso razón Uptime Institute sacó la certificación

TIER de Sustentabilidad Operacional (Bronze, Silver y Gold) y que si valida como se opera y mantiene el Data Center, además de evaluar el edificio y la ubicación del Data Center.

CAPITULO III
ANÁLISIS DEL SISTEMA

3.1 Requerimientos Funcionales

3.1.1 Identificación de actores

Tabla 1 Tabla de Actores

ACTORES	Oficial de Networking	Es la persona encargada de la administración del software
	Oficial de Base de Datos	Es la persona encargada de generar reportes e indicadores en base a los eventos presentados

Elaborado por: Autor

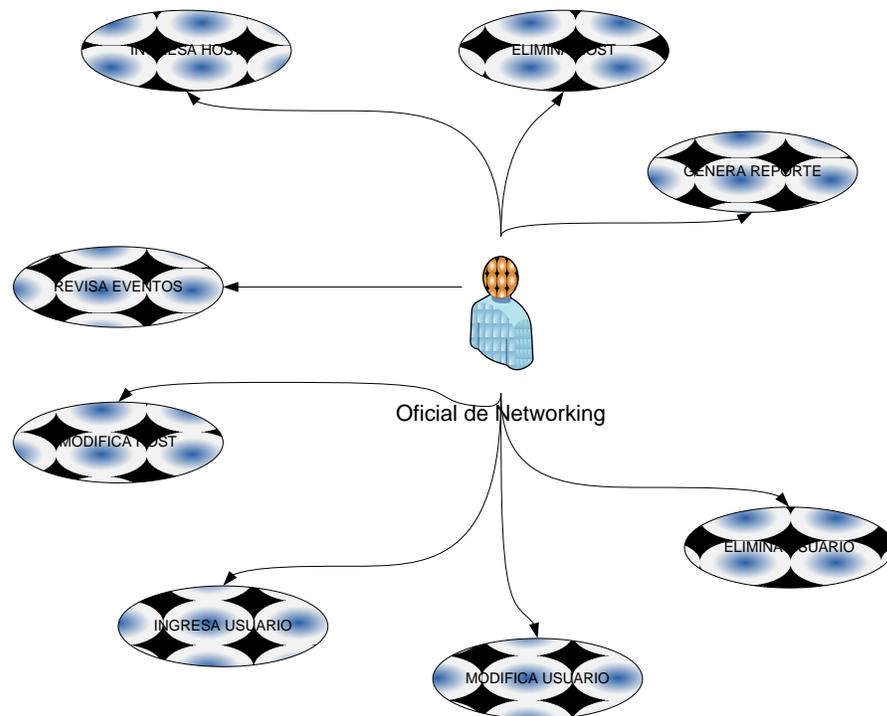


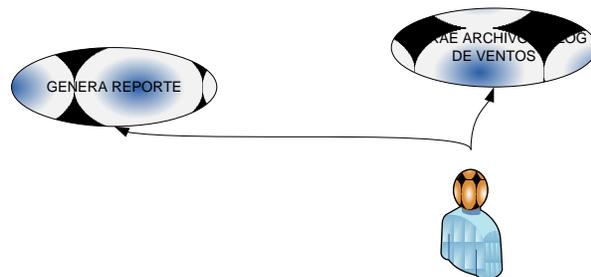
Figura 5: Funciones de Oficial de Networking

Fuente: Autor

Tabla 2 Funciones de oficial de networking

Actor	Caso de Uso	Entradas	Precondiciones	Resultados
Oficial de Networking	Ingresar Host	Crea archivo	NAGIOS no tiene error en su archivo de configuración	Se ha podido ingresar el host
	Modificar Host	Modificar archivo	NAGIOS no tiene error en su archivo de configuración	Se ha podido modificar el host
	Eliminar Host		NAGIOS no tiene error en su archivo de configuración	Se ha eliminado el host
	Ingresar Usuario	Crear usuario	NAGIOS no tiene error en su archivo de configuración	Se ha ingresado el usuario
	Modificar Usuario	Modificar usuario		Se ha ingresado el usuario
	Eliminar Usuario	Selecciona usuario a eliminar		Se ha ingresado el usuario
	Generar Reporte	Fecha de reporte	Formatos de fechas correctos	Se ha generado el reporte
	Revisar eventos	Fecha de eventos	Fecha correcta	Se ha podido revisar eventos del host

Elaborado por: Autor



Oficial de Base de Datos

Figura 6: Funciones de Oficial de Base de Datos

Fuente: Autor

Tabla 3 Funciones de oficial de base de datos

Actor	Caso de Uso	Entradas	Precondiciones	Resultados
Oficial de Base de Datos	Genera Reporte	Fecha de reporte		Se genera exitosamente un reporte de disponibilidad
	Extrae archivos de log	Copia archivo		Se ha copiado el archivo de logs exitosamente

Elaborado por: Autor

3.1.2 Identificación de escenarios

A continuación se detallara los escenarios de uso de la herramienta NAGIOS.

Tabla 4 Escenario 1 de uso de NAGIOS

ID:	1	Relación:	Ingreso de nuevo host
Prioridad:	Alta		
Descripción:	El Oficial de Networking ingresa al sistema y genera el archivo de configuración del host y sus servicios a monitorear		
	<ul style="list-style-type: none"> - El usuario ingresa via CLI al servidor - Ingresa a la ruta donde se declaran los objetos monitoreados - Se crea El archivo con El nombre del host - Se edita El archivo con El nombre del host y con la IP - Se reinicia El servicio 		

Elaborado por: Autor

Tabla 5 Escenario 2 de uso de NAGIOS

ID:	2	Relación:	Modificación de host
Prioridad:	Alta		
Descripción:	El Oficial de Networking ingresa al sistema para realizar		

	la modificación de algún parámetro del host
	<ul style="list-style-type: none"> - El usuario ingresa vía CLI al servidor - Ingresa a la ruta donde está el archivo a modificar - Se edita el archivo con el parámetro a cambiar - Se reinicia el servicio

Elaborado por: Autor

Tabla 6 Escenario 3 de uso de NAGIOS

ID:	3	Relación:	Eliminación de host
Prioridad:	Alta		
Descripción:	El Oficial de Networking ingresa al sistema vía CLI y elimina el archivo de configuración del host a eliminar		
	<ul style="list-style-type: none"> - El usuario ingresa vía CLI al servidor - Ingresa a la ruta donde está el archivo a eliminar - Se elimina el archivo - Se reinicia el servicio 		

Elaborado por: Autor

Tabla 7 Escenario 4 de uso de NAGIOS

ID:	4	Relación:	Revisión de eventos de un host
Prioridad:	Alta		
Descripción:	El Oficial de Networking ingresa al sistema y en las alertas revisa los eventos que ha tenido un host en específico		
	<ul style="list-style-type: none"> - Se ingresa vía GUI (Web) al software - Se selecciona la opción HOST - Se elige el host a monitorear - Se selecciona la opción de ver alertas del host 		

Elaborado por: Autor

Tabla 8 Escenario 5 de uso de NAGIOS

ID:	5	Relación:	Generar reporte histórico de un evento
Prioridad:	Medio		
Descripción:	El Oficial de Networking ingresa al sistema y en las		

	alertas revisa los eventos que ha tenido un host en específico
	<ul style="list-style-type: none"> - Se ingresa vía GUI (Web) al software - Se selecciona la opción “disponibilidad” - Se elige el host o grupo de host a generar reporte de disponibilidad - Se selecciona el tiempo del reporte - Se genera el reporte

Elaborado por: Autor

A continuación se detallara los escenarios de uso de la herramienta CACTI.

Tabla 9 Escenario 1 de uso de CACTI

ID:	1	Relación:	Ingreso de host
Prioridad:	Alta		
Descripción:	El Oficial de Networking ingresa al sistema y agrega el host a monitorear sus interfaces		
	<ul style="list-style-type: none"> - Se ingresa vía Web a la herramienta - Se va al menú “devices” - Se selecciona “add devices” - Se llena información del host - Se seleccionan las interfaces a monitorear del host - Se valida que se haya creado el host 		

Elaborado por: Autor

Tabla 10 Escenario 2 de uso de CACTI

ID:	2	Relación:	Modificación de host
Prioridad:	Alta		
Descripción:	El Oficial de Networking ingresa al sistema y modifica algún parámetro del host seleccionado.		
	<ul style="list-style-type: none"> - Se ingresa vía Web a la herramienta - Se va al menú “devices” - Se busca el host a modificar - Se agrega o elimina algún parámetro del host - Se valida que se haya modificado el host - Se valida que se haya creado el host 		

Elaborado por: Autor

Tabla 11 Escenario 3 de uso de CACTI

ID:	3	Relación:	Eliminación de host
Prioridad:	Alta		
Descripción:	El Oficial de Networking ingresa al sistema y elimina el host seleccionado.		
<ul style="list-style-type: none"> - Se ingresa vía Web a la herramienta - Se va al menú “devices” - Se busca el host - Se selecciona “delete host and graphs” - Se acepta la confirmación de eliminación - Se valida que se haya eliminado el host 			

Elaborado por: Autor

Tabla 12 Escenario 4 de uso de CACTI

ID:	4	Relación:	Revisión de tráfico en interfaz de host
Prioridad:	Alta		
Descripción:	El Oficial de Networking ingresa al sistema y revisa el tráfico en el tiempo de una interfaz o recurso de algún host		
<ul style="list-style-type: none"> - Se ingresa vía Web a la herramienta - Se va al menú “graphs” - Se busca el host - Se configura el tiempo de revisión - Se revisa los datos del host - 			

Elaborado por: Autor

3.1.3 Identificación de casos de uso

Tabla 13 Caso 1 de uso del software

Caso de Uso: 1	Revisión de caída de host o interfaz
Descripción:	Al Oficial de Networking le llega mediante correo electrónico, mediante SMS, o mediante un mensaje pop-up en el equipo una alerta de que un equipo o un interfaz de uno de los equipos monitoreados esta caída, inmediatamente

	el Oficial ingresa vía Web a NAGIOS y revisa en la opción de host y revisa el host que este caído y el tiempo en que este está.
Observaciones:	
Escenarios:	
<ol style="list-style-type: none"> 1. Alerta de caída de host 2. Revisión histórica de eventos 	

Elaborado por: Autor

Tabla 14 Caso 2 de uso del software

Caso de Uso: 2	Revisión de consumo de tráfico en una interfaz o enlace.
Descripción:	El Oficial de Networking deberá acceder vía Web a CACTI e ingresar a la pestaña de gráficas por equipo y selecciona la interfaz del equipo de red que requiere revisar el consumo; dicho consumo podrá ser customizado por un rango de tiempo
Observaciones:	
Escenarios:	
<ol style="list-style-type: none"> 1. Revisión mensual de consumos 2. Análisis de crecimiento 3. Monitoreo preventivo 	

Elaborado por: Autor

Tabla 15 Caso 3 de uso del software

Caso de Uso: 3	Generación de reporte de disponibilidad
Descripción:	El Oficial de Base de Datos ingresa al sistema e ingresa a la opción de disponibilidad en donde se configura el host o grupo de hosts, el tiempo del reporte y se presiona el botón generar para que luego de esperar la recopilación de datos se genera el reporte de disponibilidad que estemos buscando.
Observaciones:	
Escenarios:	
<ol style="list-style-type: none"> 1. Revisión mensual de disponibilidad 	

Elaborado por: Autor

3.2 Requerimientos No Funcionales

Tabla 16 Requerimiento no funcional 1

ID:	1	Relación:	
Descripción:	Interfaz grafica		
La interfaz gráfica es un elemento primordial para el éxito de cualquier aplicación por tal motivo ésta debe ser amigable, cumplir con los estándares de moldeamiento de una interfaz y ser plenamente intuitivo.			

Elaborado por: Autor

Tabla 17 Requerimiento no funcional 2

ID:	2	Relación:	
Descripción:	Protocolos de descubrimiento de host		
El software debe tener la capacidad de soportar los principales protocolos de descubrimiento de host, lo cual ayudará a incluir diferentes tipos de equipos de comunicación sin importar el fabricante.			

Elaborado por: Autor

Tabla 18 Requerimiento no funcional 3

ID:	3	Relación:	
Descripción:	Lenguaje de programación		
El lenguaje de programación del sistema de monitoreo debe ser un lenguaje muy orientado a objetos y de fácil entendimiento y capaz de poder soportar diferentes tecnologías de presentación de información, ya que al ser un producto pre-fabricado, éste podrá ser modificado y mejorado.			

Elaborado por: Autor

Tabla 19 Requerimiento no funcional 4

ID:	4	Relación:	
Descripción:	Precisión en detectar un evento		
La lógica manejada en el sistema deberá ser no muy permisible al momento de alertar algún tipo de evento en la red por tal motivo deberá notificar y cambiar el estado de los elementos afectados a tiempo.			

Elaborado por: Autor

Tabla 20 Requerimiento no funcional 5

ID:	5	Relación:	
Descripción:	Base de datos nativa o distribuida		
El almacenamiento de los datos deberá ser de forma nativa y manejando una lógica de programación y modelamiento de base de datos para la mejor administración de la información tanto para ser almacenada como para ser consultada.			

Elaborado por: Autor

Tabla 21 Requerimiento no funcional 6

ID:	6	Relación:	
Descripción:	Sistema Operativo		
El sistema operativo deberá ser capaz de soportar el sistema y que a su vez brinde los soportes necesarios y las características de administración de recursos al nivel del software para garantizar su estabilidad al momento de implementar la herramienta.			

Elaborado por: Autor

Tabla 22 Requerimiento no funcional 7

ID:	7	Relación:	
Descripción:	Tiempos de respuesta		
Los tiempos de respuesta deben ser menores a 5 segundos para garantizar una mejor interacción con el usuario y que esto a su vez sea un beneficio y no una molestia al momento de procesar la información ingresada.			

Elaborado por: Autor

Tabla 23 Requerimiento no funcional 8

ID:	8	Relación:	
Descripción:	Número de usuarios o sesiones concurrentes		

El software está en la capacidad de ser “multitasking” gracias a que es rico en arquitectura de diseño de software y en hardware, brindando la capacidad de soportar múltiples sesiones de usuarios al momento de administrarlo.

Elaborado por: Autor

Tabla 24 Requerimiento no funcional 9

ID:	9	Relación:	
Descripción:	Políticas de recuperación y backup de configuración		
Dentro de las políticas de recuperación de desastre el software deberá ser capaz de brindar la seguridad de la recuperación de la información o del reemplazo de la plataforma base (upgrade) sin comprometer la información recopilada. A su vez el software deberá tener la opción de auto respaldarse en caso de un evento de fallo de hardware o software.			

Elaborado por: Autor

3.3 Definición de roles en los módulos

3.3.1 Roles en NAGIOS:

ROOT: El rol de “root” es aquel rol de administrador de bajo nivel del software; es decir que será quien se encargue de la instalación, actualización, modificación y eliminación de algún paquete relacionado con la herramienta o con cualquier software que coexista con la misma.

ADMINISTRADOR: Este tipo de usuario será aquel que tenga los máximos privilegios en la aplicación y podrá tener acceso a los diferentes módulos de la aplicación, pudiendo obtener la información procesada a través de la interfaz web de NAGIOS; entre las principales funciones de este rol tiene las siguientes

- Ver/Modificar procesos que se estén ejecutando en NAGIOS

- Reiniciar el servicio de NAGIOS
- Ver información detallada de los host y servicios monitoreados
- Generación de reportes de disponibilidad
- Programar acciones de monitoreo sobre cualquier host o servicio
- Emitir cualquier comando permitido sobre cualquier host o servicio mediante la interfaz gráfica.

Usuario sólo lectura (READ ONLY): Este tipo de usuario podrá obtener la misma información que un administrador, con la diferencia que las opciones de modificación de algún parámetro estarán deshabilitadas.

3.3.2 Roles en CACTI

ROOT: El rol de “root” es aquel rol de administrador de bajo nivel del software; es decir que será el administrador del servidor en donde puede coexistir más de un software, por lo tanto este rol tendrá el control a nivel de instalación, modificación o eliminación de cualquiera de los archivos de configuración de CACTI.

ADMINISTRADOR: En el rol de administrador se podrán realizar todas las acciones permitidas dentro de lo que la interfaz web lo permita, ya que existe la limitante de no poder acceder a la base de datos al ser ésta administrada desde línea de comandos o con algún IDE de interpretación instalado sobre el equipo. Dentro de los privilegios que podrá realizar el usuario Administrador sobre la herramienta tiene:

- Agregar/Modificar/Eliminar usuarios de acceso a la herramienta.
- Agregar/Modificar/Eliminar un dispositivo o un gráfico asociado hacia el mismo.
- Generar graficas de un dispositivo de acuerdo al lapso de tiempo seleccionado.
- Instalar plugins adicionales a la herramienta
- Importar/Exportar templates personalizados de gráficos o de dispositivos disponibles en Internet.
- Utilizar las herramientas de mantenimiento del software.

OBSERVADOR: El rol de observador (viewer) está disponible para usuarios que solo tendrán disponible la información de graficas de consumo de interfaces o de performance de los dispositivos en el lapso de tiempo seleccionado, sin poder realizar alguna modificación en la información mostrada.

CAPITULO IV

DISEÑO DEL SISTEMA

4.1 Diseño de la arquitectura del sistema

4.1.1 Diseño arquitectónico

4.1.1.1 Arquitectura de NAGIOS

NAGIOS posee de una arquitectura simple de administración ya que consta de una interfaz Web la cual es una ventana a la visualización de los diferentes eventos que ocurran en los equipos o servicios monitoreados, dicha información es obtenida mediante archivos de log, de status, de retención de información volátil o plugins los cuales serán empleados a través del motor de NAGIOS el cual es ejecutado en el Kernel como demonio (definición de servicio en lenguaje Linux) donde se maneja la lógica de monitoreo, eventos, notificaciones, etc. Hacia los equipos y servicios; almacenando la información de cada query o consulta en archivos de registro locales o externos.

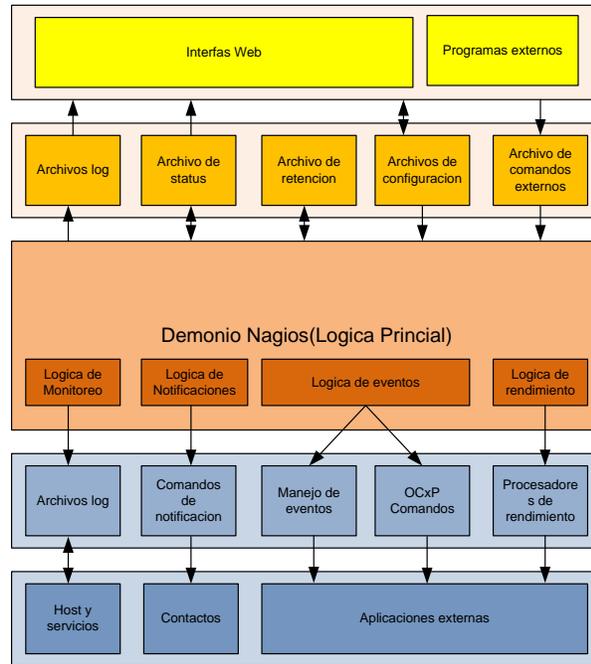


Figura 7 Arquitectura de NAGIOS

Fuente: Autor

4.1.1.2 Arquitectura de CACTI

Una MIB es una base de datos jerárquica de objetos y sus valores, almacenados en un agente SNMP. Cada MIB individual es un subárbol de la estructura total de MIB definida por la ISO. La RFC 1156, llamada MIB-I, especifica ciertas informaciones de primer nivel. La RFC 1158, llamada MIB-II, es más exhaustiva.

Sin embargo como estas especificaciones no permiten describir, con la precisión requerida, todo tipo de agentes, los fabricantes de hardware y programadores de software están desarrollando MIB propietarias. De esta forma una organización puede tener autoridad sobre los objetos y ramas de una MIB. Generalmente, los objetos de la MIB son referenciados por un identificador.

CACTI es un cliente de RRDTool, éste almacena toda la información necesaria para crear gráficos en una base de datos MYSQL.

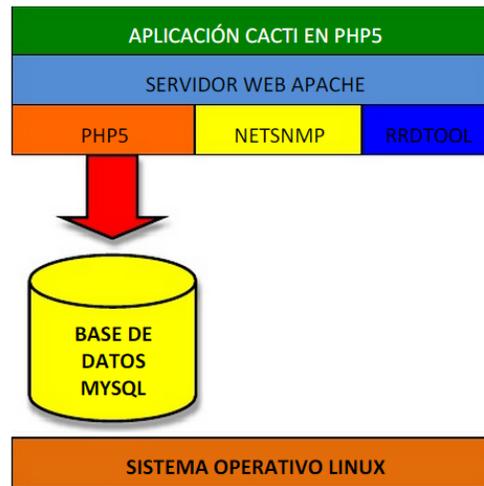


Figura 8 Arquitectura de CACTI

Fuente: <https://es.scribd.com/doc/30455122/Procedimiento-Para-La-Instalacion-de-CACTI>

4.1.2 Módulos del sistema

4.1.2.1 NAGIOS

4.1.2.1.1 MÓDULO DE MONITOREO

Este módulo tiene como función presentar la información actual de los host y servicios monitoreados sobre NAGIOS.

Mapa de host: Se muestra la información en un modo gráfico nativo de NAGIOS en donde los host se ordenan de una manera no ordenada alrededor del servicio de NAGIOS. Ejemplo: Figura 9

The screenshot displays the Nagios web interface. On the left is a navigation menu with categories like General, Current Status, Reports, and System. The main content area shows details for host 'DC-GYE', including its name, alias, address, and current status (UP). Below this, there's a 'Services' section. To the right, a network map is visible, showing a central node connected to various other nodes in a radial pattern. A legend on the right side of the map allows for layer management and scaling.

Figura 9: NAGIOS opción de Mapa

Fuente: Autor

Hosts: En esta opción se muestra un listado de los host monitoreados en donde se toma en cuenta el color del host en donde se representa el estado de salud de los host.

Ejemplo: Figura 10

The screenshot shows the 'Hosts' monitoring page in Nagios. It features summary statistics for Host Status Totals (44 OK, 1219 Warning) and Service Status Totals (364 OK, 5327 Warning). Below these is a table titled 'Host Status Details For All Host Groups' listing individual hosts with their status, last check time, duration, and service information.

Host	Status	Last Check	Duration	Status Information
000753_ag_iblog_pkiza_CHT	UP	05-25-2015 20:00:12	6d 10h 49m 23s	PRNG OK - Packet loss = 0%, RTA = 23.91 ms
000798_ag_iblog_CHT	UP	05-25-2015 20:00:21	31d 11h 38m 33s	PRNG OK - Packet loss = 0%, RTA = 5.62 ms
000799_ag_cenar_CHT	UP	05-25-2015 20:00:12	6d 12h 23m 31s	PRNG OK - Packet loss = 0%, RTA = 43.78 ms
000832_ag_terrenal_terrestre_CHT	UP	05-25-2015 20:00:12	6d 4h 7m 52s	PRNG OK - Packet loss = 0%, RTA = 28.45 ms
000881_ag_cenarupa_CHT	UP	05-25-2015 20:00:11	7d 7h 48m 51s	PRNG OK - Packet loss = 0%, RTA = 11.38 ms
000871_ag_machachi_CHT	UP	05-25-2015 20:00:12	8d 9h 26m 30s	PRNG OK - Packet loss = 0%, RTA = 37.87 ms
000874_ag_aki_saklers_CHT	UP	05-25-2015 20:00:12	12d 11h 50m 20s	PRNG OK - Packet loss = 0%, RTA = 20.92 ms
000923_ag_dombajo_cenar_CHT	UP	05-25-2015 20:00:12	5d 21h 42m 54s	PRNG OK - Packet loss = 0%, RTA = 24.50 ms
000919_ag_pactiza_machala_CHT	UP	05-25-2015 20:00:12	2d 19h 4m 14s	PRNG OK - Packet loss = 0%, RTA = 22.31 ms
000991_ag_mel_aki_CHT	DOWN	05-25-2015 20:09:01	8d 3h 48m 7s	Host Check Timed Out
001016_ag_aborada_CHT	UP	05-25-2015 20:00:12	17d 23h 3m 0s	PRNG OK - Packet loss = 0%, RTA = 18.80 ms
001021_ag_amarillo_CHT	UP	05-25-2015 20:00:11	4d 23h 32m 4s	PRNG OK - Packet loss = 0%, RTA = 10.31 ms
001062_ag_aki_mel_CHT	UP	05-25-2015 20:00:11	21d 15h 32m 3s	PRNG OK - Packet loss = 0%, RTA = 16.82 ms
001142_ag_morayo_CHT	UP	05-25-2015 20:07:31	6d 5h 11m 14s	PRNG OK - Packet loss = 16%, RTA = 121.21 ms
002081_ag_sombrero_CHT	UP	05-25-2015 20:00:12	6d 7h 23m 24s	PRNG OK - Packet loss = 0%, RTA = 31.91 ms
002057_ag_sombrero_CHT	UP	05-25-2015 20:00:12	7d 8h 55m 45s	PRNG OK - Packet loss = 0%, RTA = 28.00 ms
002055_ag_foca_CHT	UP	05-25-2015 20:00:12	5d 4h 32m 35s	PRNG OK - Packet loss = 0%, RTA = 88.29 ms
003096_ag_2010_CHT	UP	05-25-2015 20:00:11	4d 10h 41m 43s	PRNG OK - Packet loss = 0%, RTA = 18.93 ms
003028_ag_cumbuco_CHT	UP	05-25-2015 20:00:11	26d 10h 58m 29s	PRNG OK - Packet loss = 0%, RTA = 10.32 ms
004047_ag_aguero_CHT	UP	05-25-2015 20:00:12	16 9h 41m 34s	PRNG OK - Packet loss = 0%, RTA = 20.29 ms
004008_ag_bosque_CHT	UP	05-25-2015 20:00:12	11d 10h 36m 45s	PRNG OK - Packet loss = 0%, RTA = 24.18 ms
004013_ag_aborada_CHT	UP	05-25-2015 20:07:31	6d 11m 2m 30s	PRNG OK - Packet loss = 0%, RTA = 22.92 ms
004017_ag_cenar_de_convenciones_CHT	UP	05-25-2015 20:00:12	15d 17h 57m 29s	PRNG OK - Packet loss = 0%, RTA = 21.74 ms
004018_ag_centro_de_convenciones_CHT	UP	05-25-2015 20:00:12	2d 20h 42m 25s	PRNG OK - Packet loss = 0%, RTA = 22.86 ms
004025_ag_pactiza_CHT	UP	05-25-2015 20:00:11	8d 9h 26m 30s	PRNG OK - Packet loss = 0%, RTA = 7.31 ms
004025_ag_pactiza_CHT	UP	05-25-2015 20:00:12	5d 5h 18m 45s	PRNG OK - Packet loss = 0%, RTA = 16.42 ms
004026_ag_pactiza_CHT	UP	05-25-2015 20:00:12	2d 10h 42m 23s	PRNG OK - Packet loss = 0%, RTA = 23.22 ms
004035_ag_pactiza_cobos_CHT	UP	05-25-2015 20:07:31	6d 4h 15m 54s	PRNG OK - Packet loss = 0%, RTA = 52.28 ms
004035_ag_darwin_CHT	UP	05-25-2015 20:00:12	18d 17h 57m 49s	PRNG OK - Packet loss = 0%, RTA = 27.50 ms
004039_ag_pactiza_morayo_CHT	UP	05-25-2015 20:07:31	6d 10h 13m 31s	PRNG OK - Packet loss = 16%, RTA = 72.91 ms

Figura 10: NAGIOS opción de Hosts

Fuente: Autor

Services: En esta página se presentan los servicios de los host que se están monitoreando en donde se muestran diferentes datos importantes como lo son el tiempo de respuesta y el tiempo de caída del servicio. Ejemplo: Figura 11

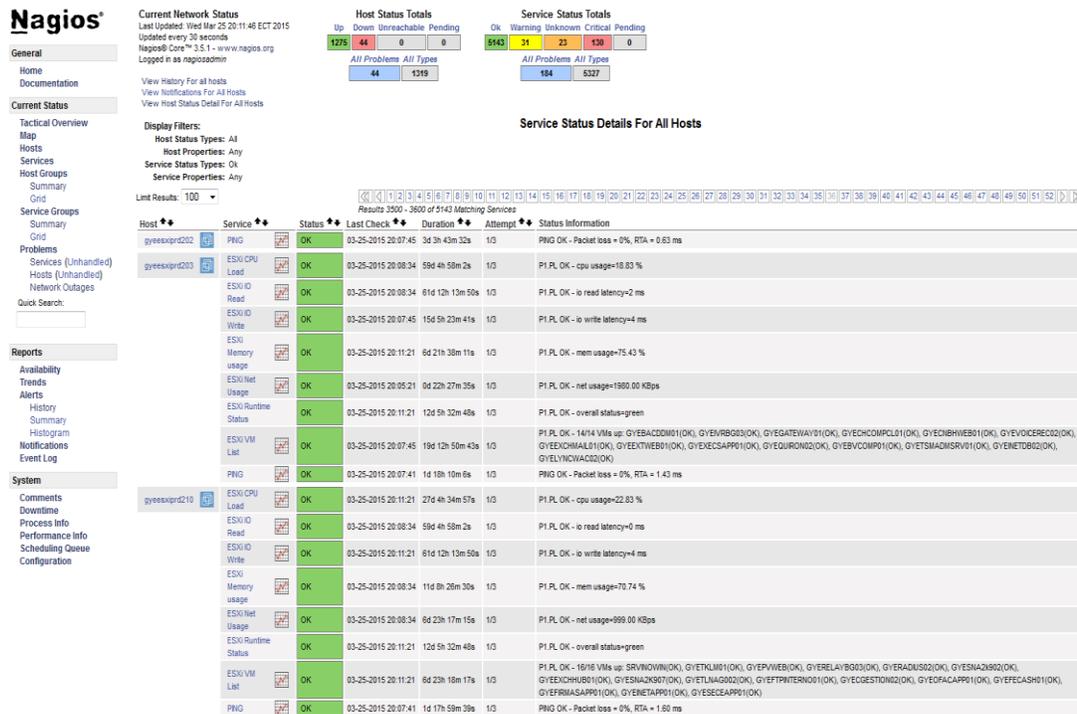


Figura 11: NAGIOS opción de Services

Fuente: Autor

- **Hostgroups:** En esta opción se muestra los host y servicios de una manera organizada y agrupada ya que los host al ser creados se configuran dentro de un grupo de host. Ejemplo: Figura 12



Figura 12: NAGIOS opción de Hostgroups

Fuente: Autor

4.1.2.1.1 MÓDULO DE REPORTE

Este módulo presenta toda la información recopilada de NAGIOS y la presenta en forma de reportes personalizados en base al tiempo, permitiendo al usuario obtener información estadística de los diferentes equipos o servicios que monitoree.

Reporte de Disponibilidad: Esta pantalla es destinada para para la generación de reportes de disponibilidad de los host, grupo de host y servicios que se monitorean.

Ejemplo: Figura 13

Hostgroup 'dc-guayaquil-hosts' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
CONVERTDOR_SP	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
FREWALL_OOB	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
GVEBLAH01	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
GVEBLAH02	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
GVEBLAH03	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
GVEBLAH04	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
GVEBLAH05	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
GVEDS800	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
GVEFWGT300C01	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
GVEFWGT400C01	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
GVEFWGT820B01	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
GVEFWGT800C01	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
GVEFWZYW01	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
GVENW01	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
GVENW03	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
GVENCENTER01	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
GVEQSN01	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
GVEQSN02	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
GERADAPP01	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
GERADAPP02	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
GERADIMGMT01	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
GERADPRO01	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
GERADWALL01	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
GYESACCESS0001	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
GYESW1K01	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
GYESW1K02	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
GYESW4K01_01	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
GYESW4K01_02	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
GYESW4K02_01	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
GYESW4K02_02	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
GYESW4K03_01	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
GYESW4K03_02	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
GYESW4K04_01	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
GYESW4K04_02	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
GYESW4K05_01	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
GYESW4K05_02	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
GYESW5K01	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
GYESW5K02	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
GYESW5K03	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
GYESW5K04	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
GYESW7K01_AGG	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
GYESW7K01_CHPS	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
GYESW7K01_CORE	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%

Figura 13: NAGIOS opción de Reporte de Disponibilidad

Fuente: Autor

Graficas de disponibilidad: En esta pantalla se muestra la disponibilidad por equipo de una manera gráfica donde el reporte es personalizado en base al tiempo seleccionado. Ejemplo: Figura 14

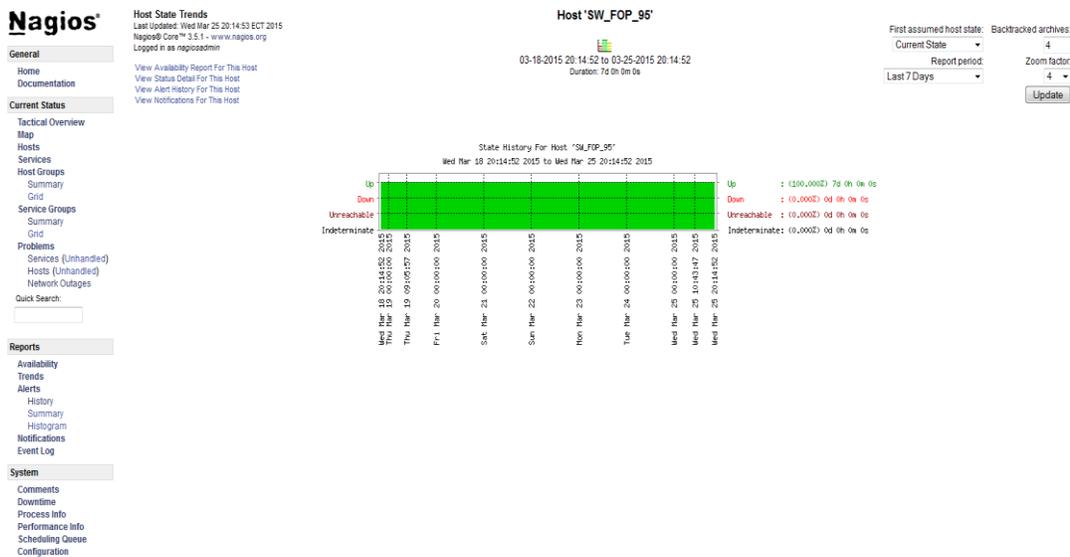


Figura 14: NAGIOS opción de Gráfica de Disponibilidad

Fuente: Autor

Reporte de alertas: En esta pantalla se pueden ver las alertas generadas hora a hora de los diferentes host y servicios, con el detalle de monitoreo. Ejemplo: Figura 15

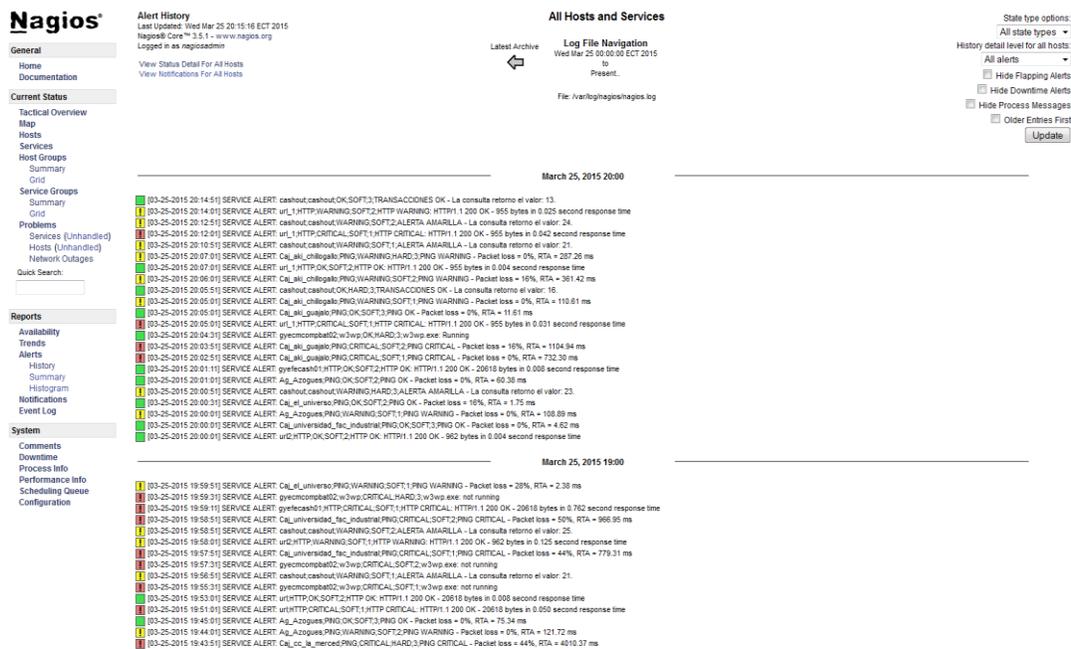


Figura 15: NAGIOS opción de Reporte de alertas

Fuente: Autor

The screenshot shows the Nagios web interface. On the left is a sidebar with navigation menus. The main area is titled 'Current Event Log' and shows a list of events for 'March 25, 2015 20:00'. Each event line includes a timestamp, a status icon (e.g., yellow for warning, red for error), and a detailed log message. The messages describe various system events such as service alerts, host notifications, and warnings.

Figura 17: NAGIOS opción de Reporte de logs de eventos

Fuente: Autor

4.1.2.1.2 MÓDULO DE INFORMACIÓN DEL SISTEMA

Este módulo tiene como objetivo presentar al administrador las facilidades de gestionar los servicios ejecutados en el servidor y además permite ver de una manera detallada el performance del equipo y la cantidad de host y servicios monitoreados y cada que tiempo se monitorean.

Información del proceso: En esta pantalla se muestra el status actual del proceso de NAGIOS en donde se puede ver el tiempo de disponibilidad o uptime, el ID del proceso en el sistema operativo, la opción de reinicio del servicio y adicional a esto manejar de manera general todas las notificaciones y alertas del motor de NAGIOS. Ejemplo:

Figura 18

General

[Home](#)
[Documentation](#)

Current Status

[Tactical Overview](#)
[Map](#)
[Hosts](#)
[Services](#)
[Host Groups](#)
 [Summary](#)
 [Grid](#)
[Service Groups](#)
 [Summary](#)
 [Grid](#)
[Problems](#)
 [Services \(Unhandled\)](#)
 [Hosts \(Unhandled\)](#)
 [Network Outages](#)

Quick Search:

Reports

[Availability](#)
[Trends](#)
[Alerts](#)
 [History](#)
 [Summary](#)
 [Histogram](#)
[Notifications](#)
[Event Log](#)

System

[Comments](#)
[Downtime](#)
[Process Info](#)
[Performance Info](#)
[Scheduling Queue](#)
[Configuration](#)

Process Information

Program Version:	3.5.1
Program Start Time:	03-25-2015 10:45:00
Total Running Time:	0d 9h 31m 45s
Last External Command Check:	03-25-2015 20:16:36
Last Log File Rotation:	N/A
Nagios PID	4542
Notifications Enabled?	YES
Service Checks Being Executed?	YES
Passive Service Checks Being Accepted?	YES
Host Checks Being Executed?	YES
Passive Host Checks Being Accepted?	YES
Event Handlers Enabled?	Yes
Obsessing Over Services?	No
Obsessing Over Hosts?	No
Flap Detection Enabled?	Yes
Performance Data Being Processed?	Yes

Process Commands

- Shutdown the Nagios process
- Restart the Nagios process
- Disable notifications
- Stop executing service checks
- Stop accepting passive service checks
- Stop executing host checks
- Stop accepting passive host checks
- Disable event handlers
- Start obsessing over services
- Start obsessing over hosts
- Disable flap detection
- Disable performance data

Figura 18: NAGIOS opción de Información de proceso nagios

Fuente: Autor

Información de rendimiento de monitoreo: En esta pantalla se tiene la información estadística en porcentajes del total de servicios y host monitoreados en los periodos de tiempo en 1, 5, 15 y 60 minutos. Ejemplo: Figura 19

- General**
- Home
- Documentation
- Current Status**
- Tactical Overview
- Map
- Hosts
- Services
- Host Groups
- Summary
- Grid
- Service Groups
- Summary
- Grid
- Problems
- Services (Unhandled)
- Hosts (Unhandled)
- Network Outages
- Quick Search:
-
- Reports**
- Availability
- Trends
- Alerts
- History
- Summary
- Histogram
- Notifications
- Event Log
- System**
- Comments
- Downtime
- Process Info
- Performance Info
- Scheduling Queue
- Configuration

Program-Wide Performance Information

Time Frame	Services Checked	Metric	Min.	Max.	Average
<= 1 minute:	971 (18.2%)	Check Execution Time:	0.01 sec	30.01 sec	1.508 sec
<= 5 minutes:	2881 (54.1%)	Check Latency:	0.00 sec	10.70 sec	0.295 sec
<= 15 minutes:	5024 (94.3%)	Percent State Change:	0.00%	26.38%	0.04%
<= 1 hour:	5299 (99.5%)				
Since program start:	5301 (99.5%)				

Time Frame	Services Checked	Metric	Min.	Max.	Average
<= 1 minute:	0 (0.0%)	Percent State Change:	0.00%	0.00%	0.00%
<= 5 minutes:	0 (0.0%)				
<= 15 minutes:	0 (0.0%)				
<= 1 hour:	0 (0.0%)				
Since program start:	0 (0.0%)				

Time Frame	Hosts Checked	Metric	Min.	Max.	Average
<= 1 minute:	966 (73.2%)	Check Execution Time:	0.47 sec	30.02 sec	4.305 sec
<= 5 minutes:	1303 (98.8%)	Check Latency:	0.00 sec	42.25 sec	0.529 sec
<= 15 minutes:	1303 (98.8%)	Percent State Change:	0.00%	10.13%	0.10%
<= 1 hour:	1303 (98.8%)				
Since program start:	1304 (98.9%)				

Time Frame	Hosts Checked	Metric	Min.	Max.	Average
<= 1 minute:	0 (0.0%)	Percent State Change:	0.00%	0.00%	0.00%
<= 5 minutes:	0 (0.0%)				
<= 15 minutes:	0 (0.0%)				
<= 1 hour:	0 (0.0%)				
Since program start:	0 (0.0%)				

Type	Last 1 Min	Last 5 Min	Last 15 Min
Active Scheduled Host Checks	949	1460	4249
Active On-Demand Host Checks	9	86	280
Parallel Host Checks	949	1464	4289
Serial Host Checks	0	0	0
Cached Host Checks	9	82	240
Passive Host Checks	0	0	0
Active Scheduled Service Checks	956	2884	11310
Active On-Demand Service Checks	0	0	0
Cached Service Checks	0	0	0
Passive Service Checks	0	0	0
External Commands	0	0	0

Type	In Use	Max Used	Total Available
External Commands	0	7	8192

Figura 19: NAGIOS opción de Información de rendimiento de monitoreo

Fuente: Autor

Información de configuración de host: En esta pantalla se puede obtener la información detallada de cada host monitoreado en NAGIOS, en donde esta información ayudará a tener un mejor control de las direcciones IP, intervalos de monitoreo y tipo de comandos que se ejecutan por cada uno. Ejemplo: Figura 20

- General
- Home
- Documentation
- Current Status
- Tactical Overview
- Map
- Hosts
- Services
- Host Groups
- Summary
- Grid
- Service Groups
- Summary
- Grid
- Problems
- Services (Unhandled)
- Hosts (Unhandled)
- Network Outages
- Quick Search:
-
- Reports
- Availability
- Trends
- Alerts
- History
- Summary
- Histogram
- Notifications
- Event Log
- System
- Comments
- Downtime
- Process Info
- Performance Info
- Scheduling Queue
- Configuration

Hosts

Host Name	Alias/Description	Address	Parent Hosts	Max. Check Attempts	Check Interval	Retry Interval	Host Check Command	Check Period	Obsess Over	Enable Active Checks	Enable Passive Checks	Check Freshness	Freshness Threshold
000753_sq_village_piazza_CNT	000753_sq_village_piazza_CNT	10.124.124.48		2	0h 5m 0s	0h 1m 0s	check-host-alive	24x7	Yes	Yes	Yes	No	Auto-determined value
000796_sq_milagro_CNT	000796_sq_milagro_CNT	10.10.7.238		2	0h 5m 0s	0h 1m 0s	check-host-alive	24x7	Yes	Yes	Yes	No	Auto-determined value
000799_sq_canar_CNT	000799_sq_canar_CNT	10.10.8.26		2	0h 5m 0s	0h 1m 0s	check-host-alive	24x7	Yes	Yes	Yes	No	Auto-determined value
000832_sq_terminal_terrestre_CNT	000832_sq_terminal_terrestre_CNT	10.124.124.27		2	0h 5m 0s	0h 1m 0s	check-host-alive	24x7	Yes	Yes	Yes	No	Auto-determined value
000861_sq_carpungu_CNT	000861_sq_carpungu_CNT	10.10.8.6		2	0h 5m 0s	0h 1m 0s	check-host-alive	24x7	Yes	Yes	Yes	No	Auto-determined value
000871_sq_machachi_CNT	000871_sq_machachi_CNT	10.10.8.70		2	0h 5m 0s	0h 1m 0s	check-host-alive	24x7	Yes	Yes	Yes	No	Auto-determined value
000874_sq_aki_astillero_CNT	000874_sq_aki_astillero_CNT	10.10.8.66		2	0h 5m 0s	0h 1m 0s	check-host-alive	24x7	Yes	Yes	Yes	No	Auto-determined value
000923_sq_domingo_comin_CNT	000923_sq_domingo_comin_CNT	10.10.8.102		2	0h 5m 0s	0h 1m 0s	check-host-alive	24x7	Yes	Yes	Yes	No	Auto-determined value
000970_sq_piazza_machala_CNT	000970_sq_piazza_machala_CNT	10.10.8.98		2	0h 5m 0s	0h 1m 0s	check-host-alive	24x7	Yes	Yes	Yes	No	Auto-determined value
000991_sq_mal_del_re_CNT	000991_sq_mal_del_re_CNT	10.10.40.6		2	0h 5m 0s	0h 1m 0s	check-host-alive	24x7	Yes	Yes	Yes	No	Auto-determined value
001010_sq_alborada_CNT	001010_sq_alborada_CNT	10.124.124.6		2	0h 5m 0s	0h 1m 0s	check-host-alive	24x7	Yes	Yes	Yes	No	Auto-determined value
001021_sq_simon_bolivar_CNT	001021_sq_simon_bolivar_CNT	10.10.6.70		2	0h 5m 0s	0h 1m 0s	check-host-alive	24x7	Yes	Yes	Yes	No	Auto-determined value

Figura 20: NAGIOS opción de configuración de Host

Fuente: Autor

Revisión de cola de programación: Esta opción permite ver la lista de programación de chequeos de servicio o host, es decir permite ver el poller de monitoreo en tiempo real.

Ejemplo: Figura 21

Entries sorted by next check time (ascending)

Host	Service	Last Check	Next Check	Type	Active Checks	Actions
igreqview001		03-25-2015 20:15:31	03-25-2015 20:15:31	Normal	ENABLED	⊗ ⊕
Sw_Datacard		03-25-2015 20:16:21	03-25-2015 20:17:31	Normal	ENABLED	⊗ ⊕
Sw_Core_4510-02		03-25-2015 20:16:21	03-25-2015 20:17:31	Normal	ENABLED	⊗ ⊕
Sw_Core_4510-01		03-25-2015 20:16:21	03-25-2015 20:17:31	Normal	ENABLED	⊗ ⊕
Sw_Glas		03-25-2015 20:16:21	03-25-2015 20:17:31	Normal	ENABLED	⊗ ⊕
Fw_Datacard		03-25-2015 20:16:21	03-25-2015 20:17:31	Normal	ENABLED	⊗ ⊕
uioesxpr513	UIO ESXi Memory usage	03-25-2015 20:07:41	03-25-2015 20:17:41	Normal	ENABLED	⊗ ⊕
uioesxpr513	UIO ESXi IO Write	03-25-2015 20:07:41	03-25-2015 20:17:41	Normal	ENABLED	⊗ ⊕
uioesxpr512	UIO ESXi Net Usage	03-25-2015 20:07:41	03-25-2015 20:17:41	Normal	ENABLED	⊗ ⊕
uioesxpr512	UIO ESXi IO Read	03-25-2015 20:07:41	03-25-2015 20:17:41	Normal	ENABLED	⊗ ⊕
uioesxpr511	UIO ESXi Memory usage	03-25-2015 20:07:41	03-25-2015 20:17:41	Normal	ENABLED	⊗ ⊕
uioesxpr511	UIO ESXi IO Write	03-25-2015 20:07:41	03-25-2015 20:17:41	Normal	ENABLED	⊗ ⊕
uioesxpr504	UIO ESXi IO Write	03-25-2015 20:07:41	03-25-2015 20:17:41	Normal	ENABLED	⊗ ⊕
uioesxpr504	UIO ESXi CPU Load	03-25-2015 20:07:41	03-25-2015 20:17:41	Normal	ENABLED	⊗ ⊕
uioesxpr504	PING	03-25-2015 20:07:41	03-25-2015 20:17:41	Normal	ENABLED	⊗ ⊕
uioesxpr412	UIO ESXi Runtime Status	03-25-2015 20:07:41	03-25-2015 20:17:41	Normal	ENABLED	⊗ ⊕
uioesxpr412	UIO ESXi IO Read	03-25-2015 20:07:41	03-25-2015 20:17:41	Normal	ENABLED	⊗ ⊕
uioesxpr411	UIO ESXi Runtime Status	03-25-2015 20:07:41	03-25-2015 20:17:41	Normal	ENABLED	⊗ ⊕
uioesxpr411	UIO ESXi Net Usage	03-25-2015 20:07:41	03-25-2015 20:17:41	Normal	ENABLED	⊗ ⊕
uioesxpr411	UIO ESXi IO Read	03-25-2015 20:07:41	03-25-2015 20:17:41	Normal	ENABLED	⊗ ⊕
uioesxpr404	UIO ESXi VM List	03-25-2015 20:07:41	03-25-2015 20:17:41	Normal	ENABLED	⊗ ⊕
uioesxpr404	UIO ESXi CPU Load	03-25-2015 20:07:41	03-25-2015 20:17:41	Normal	ENABLED	⊗ ⊕
uioesxpr403	UIO ESXi IO Write	03-25-2015 20:07:41	03-25-2015 20:17:41	Normal	ENABLED	⊗ ⊕
uioesxpr402	UIO ESXi VM List	03-25-2015 20:07:41	03-25-2015 20:17:41	Normal	ENABLED	⊗ ⊕
uioesxpr402	UIO ESXi Runtime Status	03-25-2015 20:07:41	03-25-2015 20:17:41	Normal	ENABLED	⊗ ⊕
uioesxpr402	UIO ESXi Net Usage	03-25-2015 20:07:41	03-25-2015 20:17:41	Normal	ENABLED	⊗ ⊕
uioesxpr402	UIO ESXi Memory usage	03-25-2015 20:07:41	03-25-2015 20:17:41	Normal	ENABLED	⊗ ⊕
uioesxpr402	UIO ESXi IO Read	03-25-2015 20:07:41	03-25-2015 20:17:41	Normal	ENABLED	⊗ ⊕
uioesxpr402	UIO ESXi CPU Load	03-25-2015 20:07:41	03-25-2015 20:17:41	Normal	ENABLED	⊗ ⊕
uioesxpr401	UIO ESXi VM List	03-25-2015 20:07:41	03-25-2015 20:17:41	Normal	ENABLED	⊗ ⊕

Figura 21: NAGIOS opción de Revisión de cola de programación

Fuente: Autor

4.1.2.2 CACTI

4.1.2.2.1 MÓDULO DE ADMINISTRACIÓN

Gráficos: En este sitio se puede ver un listado del total de gráficos que están recolectando información en CACTI y a la vez permitirá la creación de los mismos para poder monitorear otra interfaz u otro parámetro de performance.

Graph Management				Add
Host:	Any	Template:	Any	Go Clear
Search:		Rows per Page:	30	
<< Previous				Next >>
Showing Rows 1 to 30 of 4473 [1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21...]				
Graph Title*	ID	Template Name	Size	
Ag. CC El Recreo - CPU Usage	575	Cisco - CPU Usage	120x500	<input type="checkbox"/>
Ag. CC El Recreo - Memory Usage	574	2 Cisco - Memory Usage	120x500	<input type="checkbox"/>
Ag. CC El Recreo - Ping Latency	576	Unix - Ping Latency	120x500	<input type="checkbox"/>
Ag. CC El Recreo - Ping Latency	3176	Unix - Ping Latency	120x500	<input type="checkbox"/>
Ag. CC El Recreo - TELCONET	577	Interface - Traffic (bits/sec)	120x500	<input type="checkbox"/>
Ag. CC El Recreo - Traffic - Fa0/7	3175	Interface - Traffic (bits/sec)	120x500	<input type="checkbox"/>
Ag. 10 de Agosto - CNT DATOS	505	Interface - Traffic (bits/sec)	120x500	<input type="checkbox"/>
Ag. 10 de Agosto - CNT VOZ	504	Interface - Traffic (bits/sec)	120x500	<input type="checkbox"/>
Ag. 10 de Agosto - CONEXION TELCO	503	Interface - Traffic (bits/sec)	120x500	<input type="checkbox"/>
Ag. 10 de Agosto - CPU Usage	501	Cisco - CPU Usage	120x500	<input type="checkbox"/>
Ag. 10 de Agosto - Memory Usage	500	2 Cisco - Memory Usage	120x500	<input type="checkbox"/>
Ag. 10 de Agosto - Ping Latency	502	Unix - Ping Latency	120x500	<input type="checkbox"/>
Ag. 6 de Diciembre - CNT DATOS	498	Interface - Traffic (bits/sec)	120x500	<input type="checkbox"/>
Ag. 6 de Diciembre - CNT VOZ	499	Interface - Traffic (bits/sec)	120x500	<input type="checkbox"/>
Ag. 6 de Diciembre - conexion a Telconet	497	Interface - Traffic (bits/sec)	120x500	<input type="checkbox"/>
Ag. 6 de Diciembre - CPU Usage	495	Cisco - CPU Usage	120x500	<input type="checkbox"/>
Ag. 6 de Diciembre - Memory Usage	494	2 Cisco - Memory Usage	120x500	<input type="checkbox"/>
Ag. 6 de Diciembre - Ping Latency	496	Unix - Ping Latency	120x500	<input type="checkbox"/>
Ag. 9 de Octubre 200 - CNT DATOS	34	Interface - Traffic (bits/sec)	120x500	<input type="checkbox"/>
Ag. 9 de Octubre 200 - Conexion a CNT_Voz	59	Interface - Traffic (bits/sec)	120x500	<input type="checkbox"/>
Ag. 9 de Octubre 200 - CPU Usage	132	Cisco - CPU Usage	120x500	<input type="checkbox"/>
Ag. 9 de Octubre 200 - Memory Usage	133	2 Cisco - Memory Usage	120x500	<input type="checkbox"/>
Ag. 9 de Octubre 200 - Ping Latency	11	Unix - Ping Latency	120x500	<input type="checkbox"/>
Ag. 9 de Octubre 200 - Servidor_Denwa_Agencias	100	Interface - Traffic (bits/sec)	120x500	<input type="checkbox"/>
Ag. 9 de Octubre 202 - CONEXION TELCONET	33	Interface - Traffic (bits/sec)	120x500	<input type="checkbox"/>
Ag. 9 de Octubre 202 - CPU Usage	134	Cisco - CPU Usage	120x500	<input type="checkbox"/>
Ag. 9 de Octubre 202 - Memory Usage	135	2 Cisco - Memory Usage	120x500	<input type="checkbox"/>
Ag. Aguirre - CNT DATOS	206	Interface - Traffic (bits/sec)	120x500	<input type="checkbox"/>
Ag. Aguirre - CNT VOZ	205	Interface - Traffic (bits/sec)	120x500	<input type="checkbox"/>
Ag. Aguirre - conexion a Telco	207	Interface - Traffic (bits/sec)	120x500	<input type="checkbox"/>
<< Previous				Next >>
Showing Rows 1 to 30 of 4473 [1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21...]				
				Choose an action: Delete <input type="button" value="Go"/>

Figura 22: CACTI opción de Gráficos

Fuente: Autor

Árbol de gráfico: CACTI posee una manera gráfica en forma de árbol jerárquico la organización de la información para una mejor lectura. En esta pantalla se puede generar arboles de información o modificar los que ya estén creados.

Graph Trees		Add
Name:	Banco Guayaquil	<input type="button" value="X"/>

Figura 23: CACTI opción de árbol gráfico

Fuente: Autor

Grupo de notificaciones: En esta pantalla se puede crear grupos de notificaciones los cuales serán utilizados para el envío de alertas y notificaciones cuando el consumo de un recurso llegue a un valor configurado como notificación.



Figura 24: CACTI opción de Grupo de notificaciones

Fuente: Autor

MÓDULO DE IMPORTACIÓN Y EXPORTACIÓN DE PLANTILLAS

Plantilla de gráficos: En esta pantalla se detalla los tipos de plantillas que se utilizaran para monitorear algún evento del equipo o servicio monitoreado.

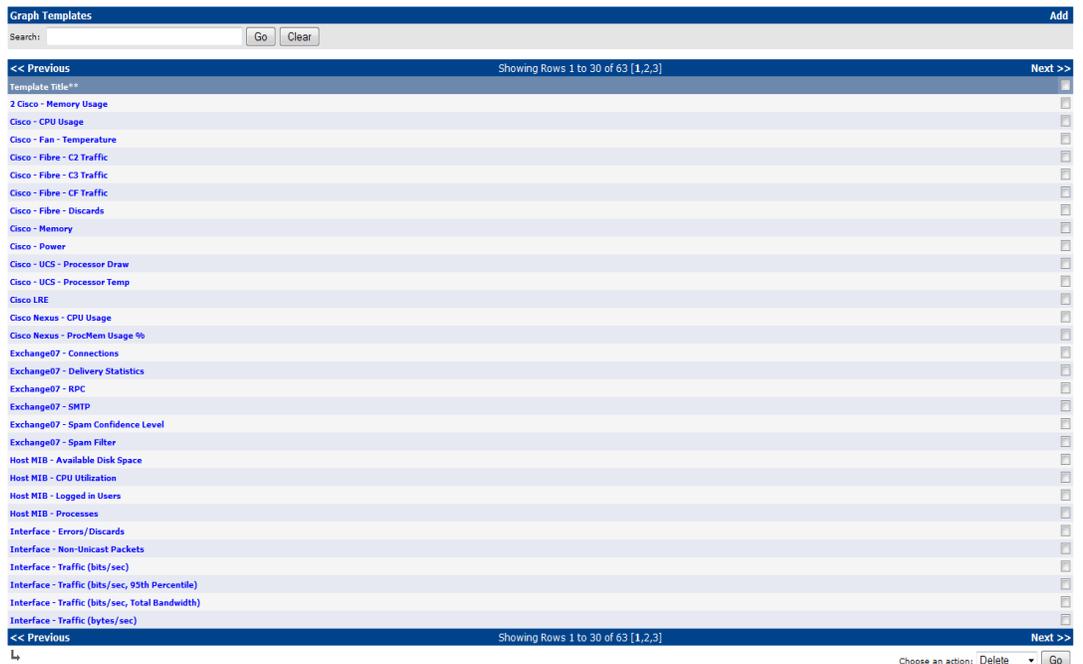


Figura 25: CACTI opción de Plantilla de gráficos

Fuente: Autor

Plantilla de host: En esta pantalla se puede ver las plantillas que hayan sido generadas para clasificar cada gráfico de acuerdo al equipo o servicio que se está monitoreando.

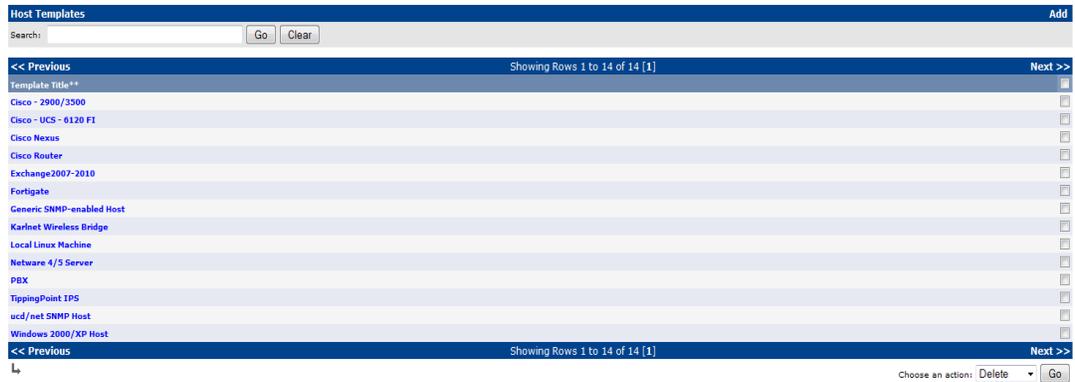


Figura 26: CACTI opción de Plantilla de host

Fuente: Autor

Plantilla de datos: La información mostrada en la siguiente pantalla dará la información detallada de los gráficos utilizados en los diferentes equipos y el tipo de medición que se aplicara para su respectivo cálculo.



Figura 27: CACTI opción de Plantilla de datos

Fuente: Autor

Módulo de Configuración: Esta es la interfaz que presenta el software para poder agregar y modificar la configuración de los diferentes host o servicios monitoreados.

The screenshot shows the 'Cacti Settings (General)' interface. It includes tabs for General, Paths, Poller, Graph Export, Visual, Authentication, Mail / DNS, Misc, and Thresholds. The 'General' tab is active, displaying various configuration sections:

- Event Logging:** Log File Destination (Logfile Only), Web Events (Web SNMP Messages, Web RRD Graph Syntax, Graph Export Messages).
- Poller Logging Level:** Level (LOW - Statistics and Errors).
- Poller Syslog/Eventlog Selection:** Poller Statistics, Poller Warnings, Poller Errors.
- Required Tool Versions:** SNMP Utility Version (NET-SNMP 5.x), RRDTool Utility Version (RRDTool 1.3.x).
- SNMP Defaults:**
 - SNMP Version: Version 3
 - SNMP Community: (empty field)
 - SNMP Username (v3): Bg123456
 - SNMP Password (v3): (masked with dots)
 - SNMP Auth Protocol (v3): MD5 (default)
 - SNMP Privacy Passphrase (v3): (empty field)
 - SNMP Privacy Protocol (v3): DES (default)
 - SNMP Timeout: 500
 - SNMP Port Number: 161
 - SNMP Retries: 3
- Other Defaults:** Reindex Method for Data Queries (Uptime Goes Backwards), Deletion Verification (checked).

Figura 28: CACTI opción de módulo de configuración

Fuente: Autor

Administración de plugins: CACTI posee la ventaja de poder instalar plugins que ayuden a obtener más datos de los equipos monitoreados y a la vez mejorar las funcionalidades de monitoreo, gracias a la colaboración de la comunidad de CACTI que libera versiones gratuitamente para su respectiva prueba y uso. En esta pantalla se puede obtener la información de los plugins que tengamos activados o desactivados en CACTI.

The screenshot shows the 'Plugin Management' interface for Cacti Version 0.8.8b, Plugin Architecture Version: 3.1. It includes a search bar and a table of installed plugins:

Actions	Name	Version	Load Order	Description*	Type	Status	Author
	Settings	0.71		Global Plugin Settings	System	Active	Jimmy Conner
	Realtime	0.5		Realtime Graph Viewer	General	Active	Mathieu Virbel
	Routerconfigs	0.3		Router Configs	General	Active	Jimmy Conner
	Thold	0.5		Thresholds	General	Active	Jimmy Conner

NOTE: Please sort by 'Load Order' to change plugin load ordering.
NOTE: SYSTEM plugins can not be ordered.

Figura 29: CACTI opción de Administración de plugins

Fuente: Autor

Revisión de logs del poller: En esta pantalla se tiene el beneficio de obtener el detalladamente las consultas del poller o disparador de queries SNMP hacia los diferentes dispositivos o servicios que estén siendo monitoreados en CACTI.

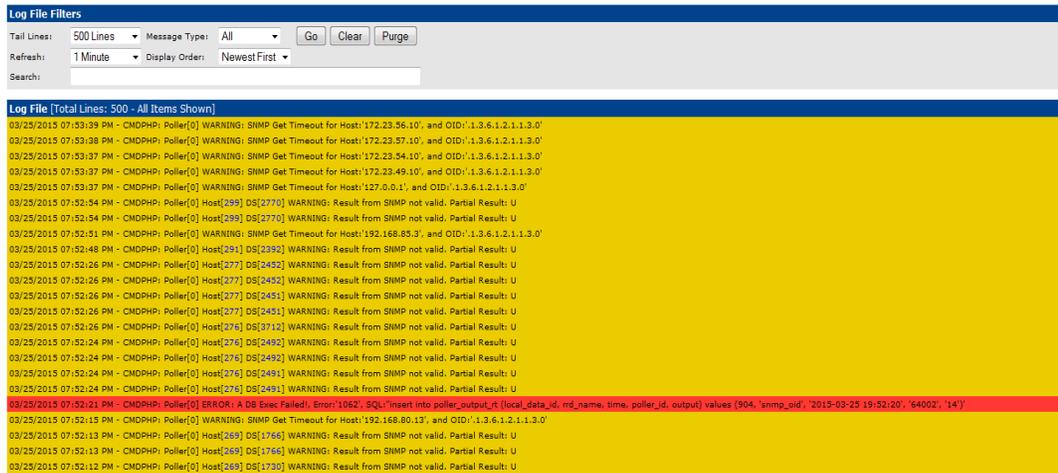


Figura 30: CACTI opción de revisión de logs del poller

Fuente: Autor

Revisión de logs de SNMP: En esta pantalla se tiene la información detallada por OID y host que se esté monitoreando mediante el protocolo SNMP.

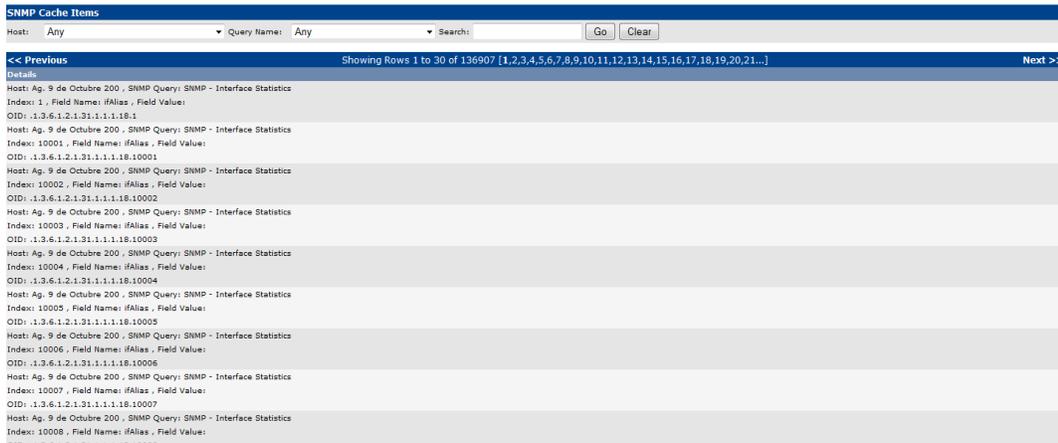


Figura 31: CACTI opción de revisión de logs de SNMP

Fuente: Autor

Administración de usuarios: En esta pantalla se tiene la información de los usuarios que ingresarán a CACTI ya sea como administradores o como usuarios no privilegiados.

User Name*	Full Name	Enabled	Realm	Default Graph Policy	Last Login
admin	Administrator	Yes	Local	ALLOW	Wednesday, March 25, 2015 13:55:59
amiranda	Angelo Miranda	Yes	Local	ALLOW	Friday, June 28, 2013 11:32:50
azambano	Andres Zambrano	Yes	Local	ALLOW	Tuesday, August 13, 2013 09:26:58
ccoppiano	Christian Coppiano	Yes	Local	ALLOW	Thursday, July 04, 2013 17:07:04
dvera	David Vera	Yes	Local	ALLOW	Thursday, October 02, 2014 13:07:41
gmartinez	Gian Carlo Martinez	Yes	Local	ALLOW	Thursday, July 11, 2013 09:14:41
guest	Guest Account	No	Local	ALLOW	N/A
iperez	Isabel Perez	Yes	Local	ALLOW	N/A
jbarragan	Johnny Barragan	Yes	Local	ALLOW	N/A
jmariduena	Jose Mariduena	Yes	Local	ALLOW	Thursday, July 04, 2013 15:50:04
jreca	Juan Luis Reza	Yes	Local	ALLOW	N/A
lvazquez	Luis Vasquez	Yes	Local	ALLOW	Wednesday, July 03, 2013 15:41:27
lnunez	Nell Nunez	Yes	Local	ALLOW	Wednesday, September 25, 2013 10:22:08
rroman	Richard Roman	Yes	Local	ALLOW	Tuesday, August 19, 2014 08:51:47
wreyes	Willie Reyes	Yes	Local	ALLOW	Tuesday, July 02, 2013 11:57:38

Figura 32: CACTI opción de Administración de usuarios

Fuente: Autor

Módulo de mantenimiento de software: En esta pantalla se tiene varias opciones las cuales servirán para dar mantenimiento al software a nivel de servicio, es decir se tiene opciones como refrescar el disparador de queries SNMP, ver logs de usuarios para autoría,

Cacti System Utilities	
Technical Support	Cacti technical support page. Used by developers and technical support persons to assist with issues in Cacti. Includes checks for common configuration issues.
Log Administration	
View Cacti Log File	The Cacti Log File stores statistic, error and other message depending on system settings. This information can be used to identify problems with the poller and application.
View User Log	Allows Administrators to browse the user log. Administrators can filter and export the log as well.
Poller Cache Administration	
View Poller Cache	This is the data that is being passed to the poller each time it runs. This data is then in turn executed/interpreted and the results are fed into the rrd files for graphing or the database for display.
View SNMP Cache	The SNMP cache stores information gathered from SNMP queries. It is used by cacti to determine the OID to use when gathering information from an SNMP-enabled host.
Rebuild Poller Cache	The poller cache will be cleared and re-generated if you select this option. Sometimes host/data source data can get out of sync with the cache in which case it makes sense to clear the cache and start over.

Figura 33: CACTI Módulo de mantenimiento de software

Fuente: Autor

4.2 Diagrama de clases del sistema

Diagrama de clases de NAGIOS:

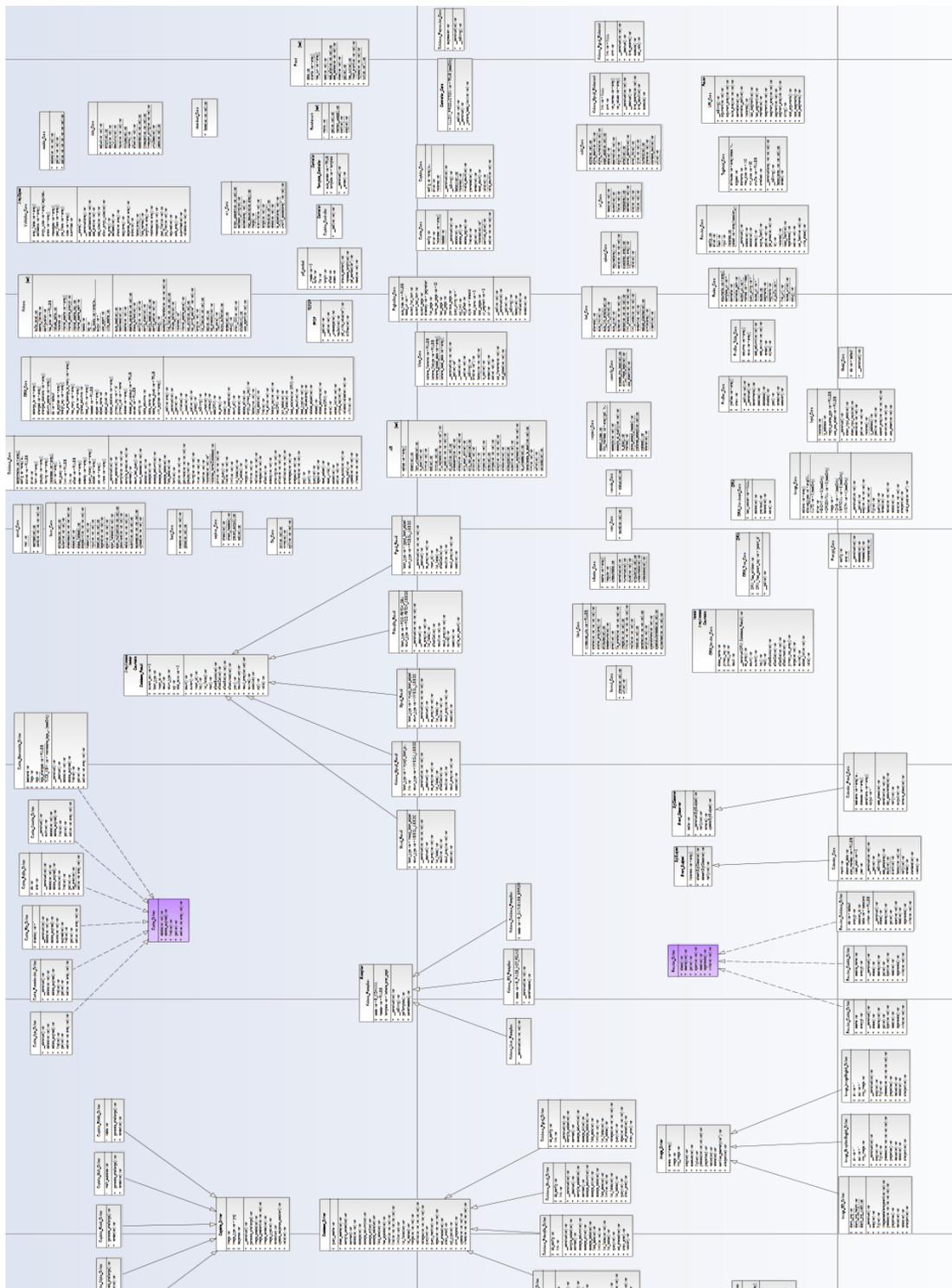


Figura 35: NAGIOS Diagrama de clases

Fuente: Autor

4.3 Modelo Lógico de la Base de Datos

En NAGIOS la información no se almacena en base de datos sino que se almacena en archivos de texto en donde se leen los logs de eventos de una manera compuesta por fecha, tiempo y eventos.

En CACTI la información es almacenada en una base de datos MySQL en donde entre la información presentada se tiene la siguiente:

Tabla **cdef** para registros de gráficos

Tabla 25 Estructura de tabla cdef

Field	Type	Attributes	Null	Default	Extra	Links to	Comments	MIME
id	mediumint(8)	UNSIGNED	No		auto_increment			
hash	varchar(32)		No					
name	varchar(255)		No					

Elaborado por: Autor

Tabla **cdef_items** sirve para tabla intermedia entre los registros de graficos y la información de los gráficos

Tabla 26 Estructura de tabla cdef_items

Field	Type	Attributes	Null	Default	Extra	Links to	Comments	MIME
id	mediumint(8)	UNSIGNED	No		auto_increment			
hash	varchar(32)		No					
cdef_id	mediumint(8)	UNSIGNED	No	0		cdef->id		
sequence	mediumint(8)	UNSIGNED	No	0				
type	tinyint(2)		No	0				
value	varchar(150)		No					

Elaborado por: Autor

Tabla **colors** sirve para personalizar los colores que se manejaran en los gráficos utilizados

Tabla 27 Estructura de tabla colors

Field	Type	Attributes	Null	Default	Extra	Links to	Comments	MIME
id	mediumint(8)	UNSIGNED	No		auto_increment			
hex	varchar(6)		No					

Elaborado por: Autor

Tabla **data_input** para registrar datos ingresados en los gráficos

Tabla 28 Estructura de tabla data_input

Field	Type	Attributes	Null	Default	Extra	Links to	Comments	MIME
id	mediumint(8)	UNSIGNED	No		auto_increment			
hash	varchar(32)		No					
name	varchar(200)		No					
input_string	varchar(255)		Yes	NULL				
type_id	tinyint(2)		No	0				

Elaborado por: Autor

Tabla **data_input_data** sirve para registrar los comentarios de las plantillas de datos

Tabla 29 Estructura de tabla data_input_data

Field	Type	Attributes	Null	Default	Extra	Links to	Comments	MIME
data_input_field_id	mediumint(8)	UNSIGNED	No	0		data_input_fields -> id		
data_template_data_id	mediumint(8)	UNSIGNED	No	0		data_template_data -> id		
t_value	char(2)		Yes	NULL				
value	text		Yes	NULL				

Tabla **data_input_fields** sirve de table intermedia para actualización de información obtenida en los comandos ejecutados

Tabla 30 Estructura de tabla data_input_fields

Field	Type	Attributes	Null	Default	Extra	Links to	Comments	MIME
id	mediumint(8)	UNSIGNED	No		auto_increment			
hash	varchar(32)		No					
data_input_id	mediumint(8)	UNSIGNED	No	0		data_input -> id		
name	varchar(200)		No					
data_name	varchar(50)		No					
input_output	char(3)		No					
update_rra	char(2)		Yes	0				
sequence	smallint(5)		No	0				
type_code	varchar(40)		Yes	NULL				
regexp_match	varchar(200)		Yes	NULL				
allow_nulls	char(2)		Yes	NULL				

Elaborado por: Autor

Tabla **data_local** para registro de dispositivos

Tabla 31 Estructura de tabla data_local

Field	Type	Attributes	Null	Default	Extra	Links to	Comments	MIME
id	mediumint(8)	UNSIGNED	No		auto_increment			
data_template_id	mediumint(8)	UNSIGNED	No	0				
host_id	mediumint(8)	UNSIGNED	No	0				

	8)	D						
snmp_query_id	mediumint(8)		No	0				
snmp_index	varchar(60)		No					

Elaborado por: Autor

Tabla **data_template** para registro de plantillas

Tabla 32 Estructura de tabla data_template

Field	Type	Attributes	Null	Default	Extra	Links to	Comments	MIME
id	mediumint(8)	UNSIGNED	No		auto_increment			
hash	varchar(32)		No					
name	varchar(150)		No					

Elaborado por: Autor

Tabla **data_template_data** para registro de plantillas

Tabla 33 Estructura de tabla data_template_data

Field	Type	Attributes	Null	Default	Extra	Links to	Comments	MIME
id	mediumint(8)	UNSIGNED	No		auto_increment			
local_data_template_data_id	mediumint(8)	UNSIGNED	No	0				
local_data_id	mediumint(8)	UNSIGNED	No	0		data_template_data -> id		
data_template_id	mediumint(8)	UNSIGNED	No	0		data_local -> id		
data_input_id	mediumint(8)	UNSIGNED	No	0		data_template_data -> id		
t_name	char(2)		Yes	NUL		data_input -> id		
name	varchar(250)		No					
name_cache	varchar(255)		No					
data_source_path	varchar(255)		Yes	NUL				

t_active	char(2)		Yes	NUL				
active	char(2)		Yes	NUL				
t_rrd_step	char(2)		Yes	NUL				
rrd_step	mediumint(8)		No	0				
t_rra_id	char(2)		Yes	NUL				

Elaborado por: Autor

Tabla **data_template_data_rra** para asociación de plantillas a registros rra

Tabla 34 Estructura de tabla data_template_data_rra

Field	Type	Attributes	Null	Default	Extra	Links to	Comments	MI ME
data_template_data_id	mediumint(8)	UNSIGNED	No	0	data_template_data -> id			
rra_id	mediumint(8)	UNSIGNED	No	0	rra -> id			

Elaborado por: Autor

Tabla **data_template_rrd** para asociación de plantillas a registros rrd

Tabla 35 Estructura de tabla data_template_rrd

Field	Type	Attributes	Null	Default	Extra	Links to	Comments	MI ME
id	mediumint(8)	UNSIGNED	No		auto_increment			
hash	varchar(32)		No					
local_data_template_rrd_id	mediumint(8)	UNSIGNED	No	0		data_template_rrd -> id		
local_data_id	mediumint(8)	UNSIGNED	No	0		data_local -> id		
data_template_id	mediumint(8)	UNSIGNED	No	0		data_template -> id		

t_rrd_maximum	char(2)		Yes	NUL				
rrd_maximum	bigint(20)		No	0				
t_rrd_minimum	char(2)		Yes	NUL				
rrd_minimum	bigint(20)		No	0				
t_rrd_heartbeat	char(2)		Yes	NUL				
rrd_heartbeat	mediumint(6)		No	0				
t_data_source_type_id	char(2)		Yes	NUL				
data_source_type_id	smallint(5)		No	0				
t_data_source_name	char(2)		Yes	NUL				
data_source_name	varchar(19)		No					
t_data_input_field_id	char(2)		Yes	NUL				
data_input_field_id	mediumint(8)	UNSIGNED	No	0				

Elaborado por: Autor

Tabla **graph_local** para registro de gráficos

Tabla 36 Estructura de tabla graph_local

Field	Type	Attributes	Null	Default	Extra	Links to	Comments	MIME
id	mediumint(8)	UNSIGNED	No		auto_increment			
graph_template_id	mediumint(8)	UNSIGNED	No	0				
host_id	mediumint(8)	UNSIGNED	No	0				
snmp_query_id	mediumint(8)		No	0				
snmp_index	varchar(60)		No					

Elaborado por: Autor

Tabla **graph_templates** para registro de plantillas de gráficos

Tabla 37 Estructura de tabla graph_templates

Field	Type	Attributes	Null	Default	Extra	Links to	Comments	MIME
id	mediumint(8)	UNSIGNED	No		auto_increment			
hash	char(32)		No					
name	char(255)		No					

Elaborado por: Autor

Tabla **graph_templates_graph** para asociar plantillas de gráficos a un gráfico en específico

Tabla 38 Estructura de tabla graph_templates_graph

Field	Type	Attributes	Null	Default	Extra	Links to	Comments	MIME
id	mediumint(8)	UNSIGNED	No		auto_increment			
local_graph_template_graph_id	mediumint(8)	UNSIGNED	No	0		graph_templates_graph -> id		
local_graph_id	mediumint(8)	UNSIGNED	No	0		graph_local -> id		
graph_template_id	mediumint(8)	UNSIGNED	No	0		graph_templates -> id		
t_image_format_id	char(2)		Yes	0				
image_format_id	tinyint(1)		No	0				
t_title	char(2)		Yes	0				
title	varchar(255)		No					
title_cache	varchar(255)		No					
t_height	char(2)		Yes	0				
height	mediumint(8)		No	0				
t_width	char(2)		Yes	0				

width	medium int(8)		N o	0				
t_upper_limit	char(2)		Ye s	0				
upper_limit	bigint(1 2)		N o	0				
t_lower_limit	char(2)		Ye s	0				
lower_limit	bigint(1 2)		N o	0				
t_vertical_label	char(2)		Ye s	0				
vertical_label	varchar(200)		Ye s	NUL L				
t_auto_scale	char(2)		Ye s	0				
auto_scale	char(2)		Ye s	NUL L				
t_auto_scale_opts	char(2)		Ye s	0				
auto_scale_opts	tinyint(1)		N o	0				
t_auto_scale_log	char(2)		Ye s	0				
auto_scale_log	char(2)		Ye s	NUL L				
t_auto_scale_rigid	char(2)		Ye s	0				
auto_scale_rigid	char(2)		Ye s	NUL L				
t_auto_padding	char(2)		Ye s	0				
auto_padding	char(2)		Ye s	NUL L				
t_base_value	char(2)		Ye s	0				
base_value	medium int(8)		N o	0				
t_grouping	char(2)		Ye s	0				
grouping	char(2)		N o					
t_export	char(2)		Ye s	0				
export	char(2)		Ye s	NUL L				
t_unit_value	char(2)		Ye	0				

			s					
unit_value	varchar(20)		Yes	NUL				
t_unit_exponent_value	char(2)		Yes	0				
unit_exponent_value	varchar(5)		No					

Elaborado por: Autor

Tabla **graph_templates_item** para registro de características de gráficos en las gráficas creadas

Tabla 39 Estructura de tabla graph_templates_item

Field	Type	Attributes	Null	Default	Extra	Links to	Comments	MI ME
id	int(12)	UNSIGNED	No		auto_increment			
hash	varchar(32)		No					
local_graph_template_item_id	int(12)	UNSIGNED	No	0		graph_templates_item -> id		
local_graph_id	mediumint(8)	UNSIGNED	No	0		graph_local -> id		
graph_template_id	mediumint(8)	UNSIGNED	No	0		graph_templates -> id		
task_item_id	mediumint(8)	UNSIGNED	No	0		data_template_rrd -> id		
color_id	mediumint(8)	UNSIGNED	No	0		colors -> id		
graph_type_id	tinyint(3)		No	0				
cdef_id	mediumint(8)	UNSIGNED	No	0		cdef -> id		
consolidation_function_id	tinyint(2)		No	0				
text_format	varchar(255)		Yes	NUL				
value	varchar(255)		Yes	NUL				
hard_return	char(2)		Yes	NUL				
gprint_id	mediumint(8)	UNSIGNED	No	0				

sequence	medium int(8)	UNSIG NED	N o	0				
----------	------------------	--------------	--------	---	--	--	--	--

Elaborado por: Autor

Tabla **graph_template_input** para agregar detalles en los gráficos de las plantillas creadas

Tabla 40 Estructura de tabla graph_template_input

Field	Type	Attribu es	Nu ll	Defau lt	Extra	Link s	Commen ts	MIM E
id	mediumint (8)	UNSIGN ED	No		auto_increment			
hash	varchar(32)		No					
graph_template _id	mediumint (8)	UNSIGN ED	No	0	data_template - > id			
name	varchar(25 5)		No					
description	text		Ye s	NULL				
column_name	varchar(50)		No					

Elaborado por: Autor

Tabla **graph_template_input_defs** para asociación de graficas a los dispositivos creados

Tabla 41 Estructura de tabla graph_template_input_defs

Field	Type	Attribu tes	N ull	Defa ult	Extra	Links to	Comm ents	MI ME
graph_template_i nput_id	mediumi nt(8)	UNSIG NED	N o	0	graph_template_in put -> id			
graph_template_i tem_id	int(12)	UNSIG NED	N o	0	graph_templates_it em -> id			

Elaborado por: Autor

Tabla **graph_tree** para configuración de árbol de gráficos

Tabla 42 Estructura de tabla graph_tree

Field	Type	Attributes	Null	Default	Extra	Links to	Comments	MIME
id	smallint(5)	UNSIGNED	No		auto_increment			
sort_type	tinyint(3)	UNSIGNED	No	1				
name	varchar(255)		No					

Elaborado por: Autor

Tabla **graph_tree_items** para asociación de dispositivos a los gráficos en el diagrama tipo árbol

Tabla 43 Estructura de tabla graph_tree_items

Field	Type	Attributes	Null	Default	Extra	Links to	Comments	MIME
id	smallint(5)	UNSIGNED	No		auto_increment			
graph_tree_id	smallint(5)	UNSIGNED	No	0		graph_tree -> id		
local_graph_id	mediumint(8)	UNSIGNED	No	0		graph_local -> id		
rra_id	smallint(8)	UNSIGNED	No	0		rra -> id		
title	varchar(255)		Yes	NULL				
host_id	mediumint(8)	UNSIGNED	No	0		host -> id		
order_key	varchar(100)		No	0				
host_grouping_type								
tinyint(3)		UNSIGNED	No	1				
sort_children_type								
tinyint(3)		UNSIGNED	No	1				

Elaborado por: Autor

Tabla **host** es el registro principal de los dispositivos monitoreados en CACTI

Tabla 44 Estructura de tabla host

Field	Type	Attributes	Null	Default	Extra	Links to	Comments	MI ME
id	mediumint(8)	UNSIGNED	No		auto_increment			
host_template_id	mediumint(8)	UNSIGNED	No	0				
description	varchar(150)		No					
hostname	varchar(250)		Yes	NULL				
snmp_community	varchar(100)		Yes	NULL				
snmp_version	tinyint(1)	UNSIGNED	No	1				
snmp_username	varchar(50)		Yes	NULL				
snmp_password	varchar(50)		Yes	NULL				
snmp_port	mediumint(5)	UNSIGNED	No	161				
snmp_timeout	mediumint(8)	UNSIGNED	No	500				
disabled	char(2)		Yes	NULL				
status	tinyint(2)		No	0				
status_event_count	mediumint(8)	UNSIGNED	No	0				
status_fail_date	datetime		No	0000-00-00 0:00:00				
status_rec_date	datetime		No	0000-00-00 0:00:00				
status_last_error	varchar(50)		Yes					
min_time	decimal(7,5)		Yes	999.999				
max_time	decimal(7,5)		Yes	0.00000				
cur_time	decimal(7,5)		Yes	0.00000				
avg_time	decimal(7,5)		Yes	0.00000				
total_polls	int(12)	UNSIGNED	Yes	0				

failed_polls	int(12)	UNSIGNED	Yes	0				
availability	decimal(7,5)		No	10.000.000				

Elaborado por: Autor

Tabla **host_snmp_cache** para parámetros de dispositivos con configuración SNMP

Tabla 45 Estructura de tabla host_snmp_cache

Field	Type	Attributes	Null	Default	Extra	Links	Comments	MIME
host_id	mediumint(8)	UNSIGNED	No	0		host -> id		
snmp_query_id	mediumint(8)	UNSIGNED	No	0		snmp_query -> id		
field_name	varchar(50)		No					
field_value	varchar(255)		Yes	NULL				
snmp_index	varchar(60)		No					
oid	varchar(255)		No					

Elaborado por: Autor

Tabla **host_snmp_query** para el registro de la información obtenida de los query SNMP

Tabla 46 Estructura de tabla host_snmp_query

Field	Type	Attributes	Null	Default	Extra	Links	Comments	MIME
host_id	mediumint(8)	UNSIGNED	No	0		host -> id		
snmp_query_id	mediumint(8)	UNSIGNED	No	0		snmp_query -> id		
sort_field	varchar(50)		No					
title_format	varchar(50)		No					
reindex_method	tinyint(3)	UNSIGNED	No	0				

Elaborado por: Autor

Tabla **host_template** para el registro de las plantillas de host en CACTI

Tabla 47 Estructura de tabla host_template

Field	Type	Attributes	Null	Default	Extra	Links	Comments	MIME
id	mediumint(8)	UNSIGNED	No		auto_increment			

hash	varchar(32)		No					
name	varchar(100)		No					

Elaborado por: Autor

Tabla **host_template_graph** para asociar la plantilla de host con la plantilla de gráficos

Tabla 48 Estructura de tabla host_template_graph

Field	Type	Attributes	Null	Default	Extra	Links	Comments	MIME
host_template_id	mediumint(8)	UNSIGNED	No	0		host_template -> id		
graph_template_id	mediumint(8)	UNSIGNED	No	0		graph_templates -> id		

Elaborado por: Autor

Tabla **poller** sirve para el registro de cambios y de datos de los dispositivos en CACTI

Tabla 49 Estructura de tabla poller

Field	Type	Attributes	Null	Default	Extra	Links	Comments	MIME
id	smallint(5)	UNSIGNED	No		auto_increment			
hostname	varchar(250)		No					
ip_address	int(11)	UNSIGNED	No	0				
last_update	datetime		No	0000-00-00 0:00:00				

Elaborado por: Autor

Tabla **poller_command** sirve para registrar los comandos a ejecutar en el disparador de consultas

Tabla 50 Estructura de tabla poller_command

Field	Type	Attributes	Null	Default	Extra	Links	Comments	MIME
poller_id	smallint(5)	UNSIGNED	No	0		poller -> id		
time	datetime		No	0000-00-00 0:00:00				

action	tinyint(3)	UNSIGNED	No	0				
command	varchar(200)		No					

Elaborado por: Autor

Tabla **poller_item** sirve para el registro de la información de SNMP configurada en los dispositivos.

Tabla 51 Estructura de tabla poller_item

Field	Type	Attributes	Null	Default	Extra	Links	Comments	MIME
local_data_id	mediumint(8)	UNSIGNED	No	0		data_local -> id		
poller_id	smallint(5)	UNSIGNED	No	0		poller -> id		
host_id	mediumint(8)		No	0		host -> id		
action	tinyint(2)	UNSIGNED	No	1				
hostname	varchar(250)		No					
snmp_community	varchar(100)		No					
snmp_version	tinyint(1)	UNSIGNED	No	0				
snmp_username	varchar(50)		No					
snmp_password	varchar(50)		No					
snmp_port	mediumint(5)	UNSIGNED	No	161				
snmp_timeout	mediumint(8)	UNSIGNED	No	0				
rrd_name	varchar(19)		No					
rrd_path	varchar(255)		No					
rrd_num	tinyint(2)	UNSIGNED	No	0				
arg1	varchar(255)		Yes	NULL				
arg2	varchar(255)		Yes	NULL				
arg3	varchar(255)		Yes	NULL				

)							
--	---	--	--	--	--	--	--	--

Elaborado por: Autor

Tabla **poller_output** sirve para registrar la información obtenida de las consultas realizadas

Tabla 52 Estructura de tabla poller_output

Field	Type	Attributes	Null	Default	Extra	Links	Comments	MIME
local_data_id	mediumint(8)	UNSIGNED	No	0		data_local -> id		
rrd_name	varchar(19)		No					
time	datetime		No	0000-00-00 0:00:00				
output	text		No					

Elaborado por: Autor

Tabla **poller_reindex** sirve para registrar los disparadores de consultas.

Tabla 53 Estructura de tabla poller_reindex

Field	Type	Attributes	Null	Default	Extra	Links	Comments	MIME
host_id	mediumint(8)	UNSIGNED	No	0		host -> id		
data_query_id	mediumint(8)	UNSIGNED	No	0		snmp_query -> id		
action	tinyint(3)	UNSIGNED	No	0				
op	char(1)		No					
assert_value	varchar(100)		No					
arg1	varchar(100)		No					

Elaborado por: Autor

Tabla **poller_time** sirve para configurar el tiempo de envío de consultas

Tabla 54 Estructura de tabla poller_time

Field	Type	Attributes	Null	Default	Extra	Links	Comments	MIME
id	mediumint(8)	UNSIGNED	No		auto_increment			
poller -> id_id	smallint(5)	UNSIGNED	No	0		poller -> id		
start_time	datetime		No	0000-00-00 0:00:00				
end_time	datetime		No	0000-00-00 0:00:00				

Elaborado por: Autor

Tabla **rra** sirve para identificar los gráficos en el registro de información RRD

Tabla 55 Estructura de tabla rra

Field	Type	Attributes	Null	Default	Extra	Links	Comments	MIME
id	mediumint(8)	UNSIGNED	No		auto_increment			
hash	varchar(32)		No					
name	varchar(100)		No					
x_files_factor	double		No	0.1				
steps	mediumint(8)		Yes	1				
rows	int(12)		No	600				
timespan	int(12)	UNSIGNED	No	0				

Elaborado por: Autor

Tabla **rra_cf** sirve para asociar los gráficos RRD con una función

Tabla 56 Estructura de tabla rra_cf

Field	Type	Attributes	Null	Default	Extra	Links	Comments	MIME
rra_id	mediumint(8)	UNSIGNED	No	0		rra -> id		
consolidation_function_id	smallint(5)	UNSIGNED	No	0				

Elaborado por: Autor

Tabla **settings_graphs** sirve para registro de gráficos generados con CACTI

Tabla 57 Estructura de tabla settings_graphs

Field	Type	Attributes	Null	Default	Extra	Links	Comments	MIME
user_id	smallint(8)	UNSIGNED	No	0		user_auth -> id		
name	varchar(50)		No					
value	varchar(255)		No					

Elaborado por: Autor

Tabla **settings_tree** sirve para asociar gráficos generados con los miembros del árbol gráfico

Tabla 58 Estructura de tabla settings_tree

Field	Type	Attributes	Null	Default	Extra	Links	Comments	MIME
user_id	mediumint(8)	UNSIGNED	No	0		user_auth -> id		
graph_tree_item_id	mediumint(8)	UNSIGNED	No	0				
status	tinyint(1)		No	0		graph_tree_items -> id		

Elaborado por: Autor

Tabla **snmp_query** sirve para agrupar los gráfico con los query de consulta SNMP

Tabla 59 Estructura de tabla snmp_query

Field	Type	Attributes	Null	Default	Extra	Links	Comments	MIME
id	mediumint(8)	UNSIGNED	No		auto_increment			
hash	varchar(32)		No					
xml_path	varchar(255)		No					
name	varchar(100)		No					
description	varchar(255)		Yes	NULL				
graph_template_id	mediumint(8)	UNSIGNED	No	0		graph_templates -> id		

data_input -> id_id	mediumint(8)	UNSIGNED	No	0		data_input -> id		
------------------------	--------------	----------	----	---	--	------------------	--	--

Elaborado por: Autor

Tabla **snmp_query_graph** sirve para identificar por el ID del grafico a que query SNMP está asociado

Tabla 60 Estructura de tabla snmp_query_graph

Field	Type	Attributes	Null	Default	Extra	Links	Comments	MI ME
id	mediumint(8)	UNSIGNED	No		auto_increment			
hash	varchar(32)		No					
snmp_query_id	mediumint(8)	UNSIGNED	No	0		snmp_query -> id		
name	varchar(100)		No					
graph_template_id	mediumint(8)	UNSIGNED	No	0		graph_templates -> id		

Elaborado por: Autor

Tabla **snmp_query_graph_rrd** sirve para asociar los datos rrd con los gráficos que se encuentran creados en CACTI

Tabla 61 Estructura de tabla snmp_query_graph_rrd

Field	Type	Attributes	Null	Default	Extra	Links	Comments	MI ME
snmp_query_graph_id								
mediumint(8)		UNSIGNED	No	0		snmp_query -> id_graph -> id		
data_template -> id_id	mediumint(8)	UNSIGNED	No	0		data_template -> id		
data_template_rrd_id	mediumint(8)	UNSIGNED	No	0		data_template -> id_rrd		
snmp_field_name	varchar(50)		No	0				

Elaborado por: Autor

Tabla **snmp_query_graph_rrd_sv** sirve para autoría de las plantillas de datos de los gráficos que están trabajando en CACTI

Tabla 62 Estructura de tabla snmp_query_graph_rrd_sv

Field	Type	Attributes	Null	Default	Extra	Links	Comments	MI ME
id	medium int(8)		UNSIGNED	No	auto_increment			
hash	varchar(32)			No				
snmp_query_graph_id	medium int(8)		UNSIGNED	No	0	snmp_query -> id_graph -> id		
data_template_id	medium int(8)		UNSIGNED	No	0			
sequence	medium int(8)		UNSIGNED	No	0	data_template -> id		
field_name	varchar(100)			No				
text	varchar(255)			No				

Elaborado por: Autor

Tabla **snmp_query_graph_sv** sirve para auditoria de los query SNMP ejecutados y la secuencia de las consultas.

Tabla 63 Estructura de tabla snmp_query_graph_rv

Field	Type	Attributes	Null	Default	Extra	Links	Comments	MI ME
id	medium int(8)		UNSIGNED	No	auto_increment			
hash	varchar(32)			No				
snmp_query_graph_id	medium int(8)		UNSIGNED	No	0	snmp_query -> id_graph -> id		
sequence	medium int(8)		UNSIGNED	No	0			
field_name	varchar(100)			No				
text	varchar(255)			No				

Elaborado por: Autor

Tabla **user_auth** sirve para registro de auditoría de los usuarios

Tabla 64 Estructura de tabla user_auth

Field	Type	Attributes	Null	Default	Extra	Links	Comments	MIME
id	mediumint(8)	UNSIGNED	No		auto_increment			
username	varchar(50)		No	0				
password	varchar(50)		No	0				
realm	mediumint(8)		No	0				
full_name	varchar(100)		Yes	0				
must_change_password	char(2)		Yes	NULL				
show_tree	char(2)		Yes	on				
show_list	char(2)		Yes	on				
show_preview	char(2)		No	on				
graph_settings	char(2)		Yes	NULL				
login_opts	tinyint(1)		No	1				
policy_graphs	tinyint(1)	UNSIGNED	No	1				
policy_trees	tinyint(1)	UNSIGNED	No	1				
policy_hosts	tinyint(1)	UNSIGNED	No	1				
policy_graph_templates	tinyint(1)	UNSIGNED	No	1				

Elaborado por: Autor

Tabla **user_auth_perms** tabla de registro de log de usuario

Tabla 65 Estructura de tabla user_auth_perms

Field	Type	Attributes	Null	Default	Extra	Links	Comments	MIME
user_id	mediumint(8)	UNSIGNED	No	0		user_auth -> id		
item_id	mediumint(8)	UNSIGNED	No	0				
type	tinyint(2)	UNSIGNED	No	0				

Elaborado por: Autor

Tabla **user_auth_realm** sirve para registro independiente de usuarios.

Tabla 66 Estructura de tabla user_auth_realm

Field	Type	Attributes	Null	Default	Extra	Links	Comments	MIME
realm_id	mediumint(8)	UNSIGNED	No	0				
user_id	mediumint(8)	UNSIGNED	No	0		user_auth -> id		

Elaborado por: Autor

El diagrama de entidad / relación entre las tablas es el siguiente:

CAPITULO V

IMPLEMENTACIÓN Y PRUEBAS

5.1 Capas del sistema y comunicaciones entre capas

NAGIOS está estructurado en base al diseño de 3 capas como lo son:

- Presentación
- Lógica de negocio
- Datos

Dichas capas se intercomunican entre sí, e interactúan con el usuario mediante la capa de presentación la cual es vía web. Las alertas y eventos procesados dentro de la capa de lógica de negocio son enviados hacia los miembros del grupo de propagación de mensajes que se haya configurado; los mensajes pueden ser del tipo SMS, correo electrónico, mensaje pop-up winsent, etc.

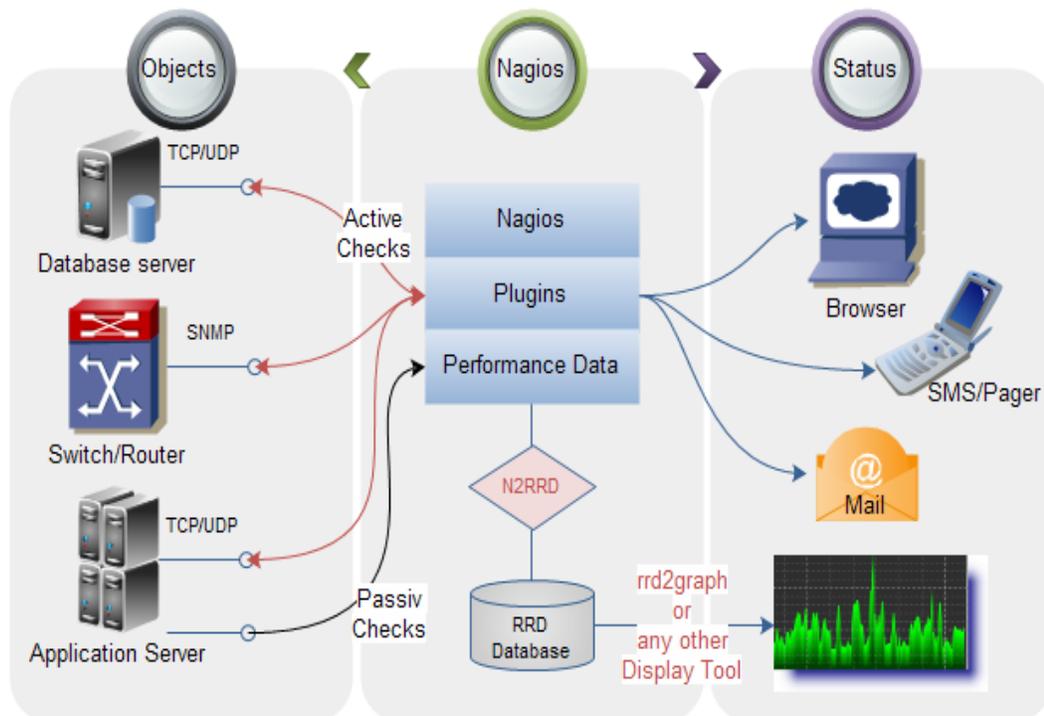


Figura 40: Capas del sistema del sistema NAGIOS+CACTI

Fuente: <http://upload.wikimedia.org/wikipedia/commons/1/1a/Monitoring.png>

5.2 Plan de pruebas

Dentro del plan de pruebas se realizaron las actividades:

5.2.1 Pruebas de tiempos de respuestas hacia dispositivos en Matriz

En esta actividad se realizó un levantamiento de información del tiempo de latencia para los equipos de comunicaciones en matriz y se estableció parámetros de monitoreo para cada uno de estos equipos probando las notificaciones al momento de que el tiempo de respuesta sea mayor al umbral establecido

5.2.2 Pruebas de tiempos de respuestas hacia dispositivos de agencias

En esta actividad se realizó un levantamiento de información del tiempo de latencia para los equipos de comunicaciones en agencias y se estableció parámetros de monitoreo para cada uno de estos equipos probando las notificaciones al momento de que el tiempo de respuesta sea mayor al umbral establecido

5.2.3 Pruebas de tiempos de respuestas hacia dispositivos de datacenter

En esta actividad se realizó un levantamiento de información del tiempo de latencia para los equipos de comunicaciones en datacenter y se estableció parámetros de monitoreo para cada uno de estos equipos probando las notificaciones al momento de que el tiempo de respuesta sea mayor al umbral establecido

5.2.4 Prueba de servicios de comunicación hacia puertos de servicio

En esta actividad se realizó un levantamiento de información de los puertos de servicios que están trabajando en la red y se configuraron parámetros de monitoreo para

cada uno de los puertos de servicio y se probaron notificaciones al caer uno de los puertos.

5.2.5 Pruebas de recepción de datos de interfaces de red

Se configura en CACTI mediante SNMP la lectura de los puertos de red de los equipos de comunicación y se valida que el tráfico generado esté correcto y la lectura sea tomada en los intervalos correctos.

5.2.6 Pruebas recepción de datos de performance de equipos

Se configura en CACTI mediante SNMP la lectura de CPU, memoria, sesiones y conexiones entrantes de un equipo de y se valida que los valores capturados estén correcto y la lectura sea tomada en los intervalos correctos.

5.2.7 Pruebas de envío y recepción de alertas mediante correo electrónico

Se genera la caída de uno de los servicios monitoreados y se valida el tiempo de envío y recepción de la notificación de alerta mediante correo electrónico a cada uno de los miembros del grupo de contacto.

5.2.8 Pruebas de envío y recepción de alertas mediante windows pop-up

Se genera la caída de uno de los servicios monitoreados y se valida el tiempo de envío y recepción de la notificación de alerta mediante un pop-up de Windows a cada uno de los miembros del grupo de contacto

5.2.9 Pruebas de envío y recepción de alertas mediante SMS

Se genera la caída de uno de los servicios monitoreados y se valida el tiempo de envío y recepción de la notificación de alerta mediante SMS de Windows a cada uno de los miembros del grupo de contacto

5.2.10 Pruebas de status de disponibilidad de host y servicios monitoreados

Se genera la caída de uno de los servicios monitoreados y se valida el tiempo en que el status del servicio monitoreado cambia en la pantalla de visualización de CACTI.

5.3 Resultado de las pruebas y métricas tomadas

Prueba	Métrica
Pruebas de tiempos de respuestas hacia dispositivos en Matriz	< 100 mseg.
Pruebas de tiempos de respuestas hacia dispositivos de agencias	< 100 mseg.
Pruebas de tiempos de respuestas hacia dispositivos de datacenter	< 100 mseg.
Pruebas de servicios de comunicación hacia puertos de servicio	5 min
Pruebas de recepción de datos de interfaces de red	5 seg
Pruebas recepción de datos de performance de equipos	100%
Pruebas de envío y recepción de alertas mediante correo electrónico	5 min
Pruebas de envío y recepción de alertas mediante windows pop-up	5 min
Pruebas de envío y recepción de alertas mediante SMS	5 min
Pruebas de status de disponibilidad de host y servicios monitoreados	5 min

Luego de las pruebas realizadas en los tiempos de respuesta de equipos y de servicios se concluye que una infraestructura de datacenter no puede ser homogénea en cuanto a los parámetros de monitoreo ya que se manejan diferentes umbrales de tolerancia entre los servicios y equipos de comunicaciones. Además se aprendió a agrupar de manera ordenada los distintos dispositivos de red al momento de monitorear.

CAPITULO VI

CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusión

Como conclusión se puede decir que se ha construido un software de open source capaz de monitorear los diferentes dispositivos, enlaces y servicios que Banco Guayaquil tiene en el datacenter, además concluimos que dicha implementación fue un gran reto para los administradores de red ya que desde el levantamiento de información hasta la implementación de la herramienta se tuvo que investigar mucho sobre alternativas de monitoreo y levantamiento de información sobre los parámetros SLA que se puede tener sobre los equipos en cuanto a tiempos de respuesta y en porcentaje de rendimiento en cuanto a CPU, memoria y consumo de red.

Luego de tener estos parámetros establecidos concluimos que un proyecto de esta magnitud es necesario tener un criterio de formación muy técnico y a su vez es necesario tener clasificados los equipos críticos y no críticos dentro de una infraestructura ya que las notificaciones tendrán un nivel de criticidad a través del medio en que se emplee para envío de notificaciones.

6.2 Recomendaciones

Como recomendaciones se tiene las siguientes:

- Se debe mejorar la parte de cobertura de equipos y servicios de red monitoreados en NAGIOS + CACTI.
- Se deberá agregar mejoras en las notificaciones de eventos y en los parámetros de monitoreo de los diferentes servicios y equipos que se tiene en constante monitoreo.

- Se debe entregar una mejora en cuanto a la visualización de alertas en tiempo real con alguna herramienta grafica para la visualización de los eventos.

BIBLIOGRAFÍA

Recursos de Internet:

ABC, D. (2007 - 2015). *Definicion ABC*. Obtenido de Definicion ABC:

<http://www.definicionabc.com/tecnologia/http.php>

Viera, A. E. (2012). *Concepto PHP*. Obtenido de Concepto PHP:

<http://phpconceptoalonso.blogspot.com/>

Canello, P. (05 de Noviembre de 2009). *Tutorial de lenguaje Perl*. Obtenido de Tutorial

de lenguaje Perl.: <http://www.pablin.com.ar/computer/cursos/varios/perl1.htm>

García, Á. L. (2011). *Fundamentos de Phyton*. Obtenido de Fundamentos de Phyton.

About en español. (2009). *About en español*. Obtenido de

<http://aprenderinternet.about.com/od/Glosario/fl/iquestQueacute-es-SMS.htm>

Microsoft. (2015). *Microsoft (s.f.) MSDN, Microsoft Developer Network*. Obtenido de

<http://msdn.microsoft.com/es-es/library/cc780057%28v=ws.10%29.aspx>

Microsoft. (2015). *Microsoft. (s.f.). Soporte técnico de Microsoft*. Obtenido de

<http://support.microsoft.com/kb/87022/es>

Microsoft. (2015). *Microsoft. (s.f.). Soporte tecnico de Microsoft*. Obtenido de

<http://support.microsoft.com/kb/170292>

Kioskea. (2015). *Kioskea - Comunidad informática*. Obtenido de

<http://es.kioskea.net/faq/1559-diferencias-entre-los-protocolos-tcp-y-udp>

Ecured. (04 de Febrero de 2015). *RRDTool - EcuRed*. Obtenido de

<http://www.ecured.cu/index.php/RRDtool>

Chile, N. (2015). *Nagios Chile Community Site*. Obtenido de <http://www.nagios-cl.org/nagios-nrpe-supervisando-maquinas-linux>

Libros:

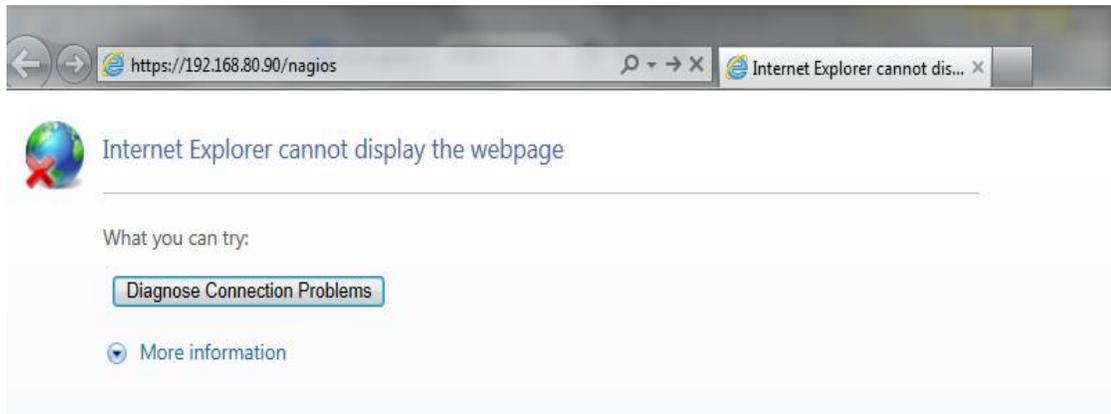
Rabago, J. (2000). *Introducción a las redes locales*. Madrid, España: Anaya.

Ford, M y Kim, Lew. (1998). *Tecnologías de Interconectividad de Redes*. México:
Prentice Hall.

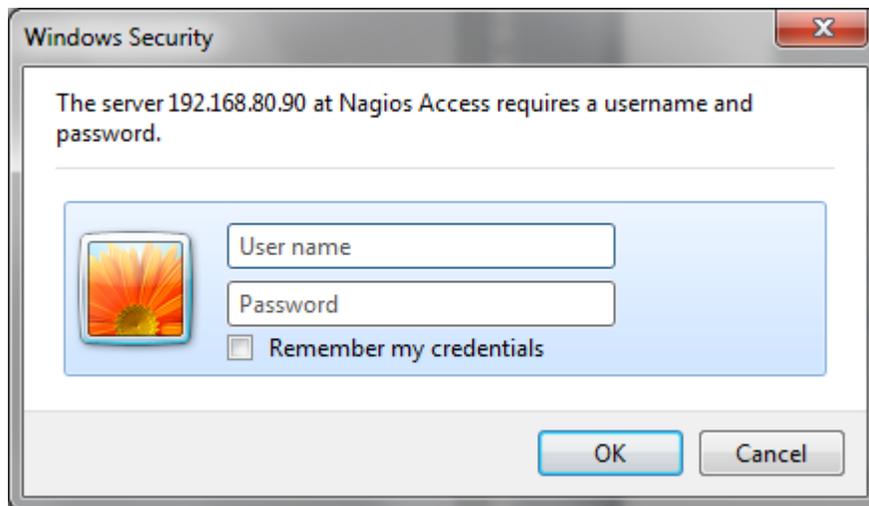
Black, U. (2000). *Redes de Computadoras, Protocolos, normas e interface*. México,
D.F.: Alaomega ra-ma.

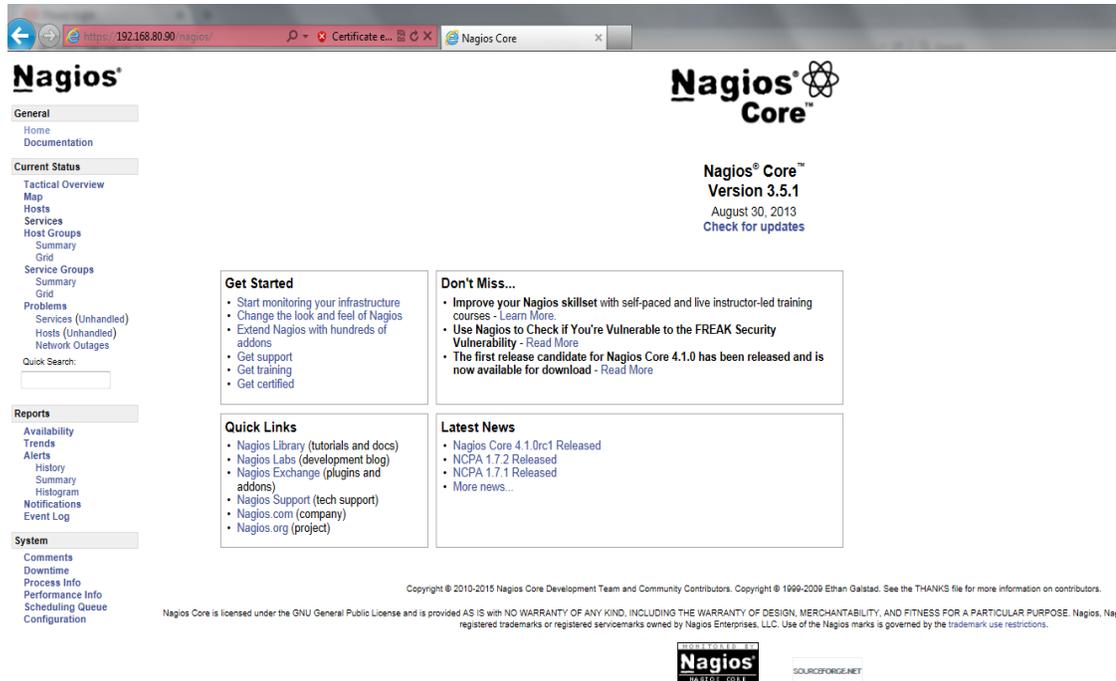
MANUAL DE USUARIO

Para ingresar a NAGIOS abrimos el navegador (Internet Explorer, Mozilla Firefox o Google Chrome) y ponemos la IP del servidor seguida de la siguiente línea “/nagios” donde está instalado el software.



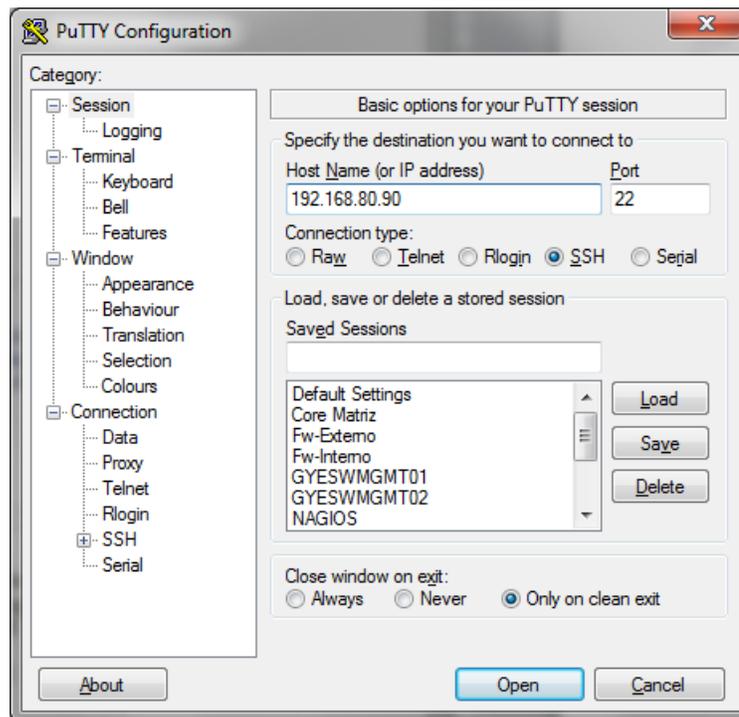
Usuario y password por default es nagiosadmin/admin





Crear una definición de host

Se ingresa mediante putty SSH al servidor de nagios y creamos un host con el siguiente comando:



```
root@gyenagios01:~  
login as: root  
root@192.168.80.90's password:  
Last login: Thu Apr 16 11:35:06 2015 from nnunez.bggrupo.bank  
[root@gyenagios01 ~]#
```

`touch /usr/local/nagios/etc/objects/remotehost.cfg`

Luego de crear el archivo de configuración procedemos a modificarlo con el siguiente comando:

`Vim /usr/local/nagios/etc/objects/remotehost.cfg`

```
define host{  
  
use          generic-host      ; herencia de plantillas  
host_name    host_name        ; nombre del equipo  
alias        host_name        ; alias que se mostrará  
address      192.168.1.3      ; dirección del equipo  
  
check_period 24x7              ; se comprueba el equipo 24/7  
check_interval 5              ; se comprueba cada 5 minutos  
retry_interval 1              ; reintenta cada minuto  
max_check_attempts 10        ; 10 reintentos  
check_command check-host-alive ; comando chequeo (ping)  
  
}
```

Crear una definición de servicio: HTTP

Se ingresa mediante putty SSH al servidor de NAGIOS y modificamos un host con el siguiente comando:

```
vim /usr/local/nagios/etc/objects/remotehost.cfg
```

Luego se agrega lo siguiente bajo la configuración del host en el archivo. Con esto podremos monitorear el servicio de HTTP de un servidor.

```
define service{
    use                generic-service
    host_name          host_name          ; host para el que se mostrará el servicio
    service_description HTTP              ; nombre del servicio
    check_command      check_http         ; comando para comprobar el servicio
}

```

Añadir al archivo nagios.cfg la siguiente línea con el siguiente comando:

```
vim /usr/local/nagios/etc/nagios.conf
```

```
cfg_file=/usr/local/nagios/etc/objects/remotehost.cfg
```

Crear definiciones de comando: http

Modificar el archivo commands.cfg con el siguiente comando:

```
vim /usr/local/nagios/etc/objects/commands.cfg
```

```
define command{
    command_name      check_http
    command_line      $USER1$/check_http -I $HOSTADDRESS$ $ARG1$
}

```

En este ejemplo se hace la definición de comando check_http el cual monitoreará los servicios sobre HTTP de un host

Verificación de alertas en interfaz WEB

Se ingresa a la opción de Host->Host Status Critical / Service Status Critical y se verifican los servicios y host caídos o con problemas.

Service Status Details For All Host Groups

Host	Service	Status	Last Check	Duration	Attempt	Status Information
80402_ig_mal_ok_sur_CNT	PING	CRITICAL	04-17-2015 22:30:24	905 20h 39m 49s	3/3	FPING CRITICAL - 10.124.124.17 (loss=100%)
Aq_Mat_Del_Sur	CNT DATOS	CRITICAL	04-17-2015 22:35:36	216 17h 42m 30s	3/3	SNMP CRITICAL - "down(2)"
	CNT VOZ	CRITICAL	04-17-2015 22:35:36	216 17h 42m 40s	3/3	SNMP CRITICAL - "down(2)"
Cal_senopuerto_LIO	PING	CRITICAL	04-17-2015 22:34:34	64 12h 23m 44s	3/3	PING CRITICAL - Packet loss = 100%
Cal_empresa_electroa_cuentas	PING	CRITICAL	04-17-2015 22:34:34	231f 13h 20m 31s	3/3	PING CRITICAL - Packet loss = 100%
Cal_farmacia_camita	PING	CRITICAL	04-17-2015 22:34:34	2056 9h 27m 30s	3/3	PING CRITICAL - "down(2)"
Cal_mni_comisarato_pascuales	PING	CRITICAL	04-17-2015 22:33:34	04 0h 24m 32s	1/3	PING CRITICAL - Packet loss = 100%
Cal_mobil_beneficencia	PING	CRITICAL	04-17-2015 22:33:02	04 0h 41m 4s	1/3	PING CRITICAL - Packet loss = 100%
Cal_pharmacy_sc_oplimpio	PING	CRITICAL	04-17-2015 22:34:34	816 10h 40m 23s	3/3	PING CRITICAL - Packet loss = 100%
Cal_sa_escatoriana	PING	CRITICAL	04-17-2015 22:34:34	136f 11h 7m 30s	3/3	PING CRITICAL - Packet loss = 100%
DIPNEO	sonda_DIPNEO	CRITICAL	04-17-2015 22:30:09	846 8h 0m 45s	3/3	CHECK_NRPE: Socket timeout after 30 seconds.
DNS_banocuyayquil	PING	CRITICAL	04-17-2015 22:30:24	365 20h 53m 53s	1/1	PING CRITICAL - Packet loss = 100%
DNS_multibg	PING	CRITICAL	04-17-2015 22:30:24	2566 5h 12m 37s	1/1	PING CRITICAL - Packet loss = 100%
GYESW503	Eh101142	CRITICAL	03-18-2015 08:21:14	656 8h 37m 49s	3/3	SNMP CRITICAL - "down(2)"
GYESW504	Eh101142	CRITICAL	03-18-2015 08:16:24	656 8h 37m 48s	3/3	SNMP CRITICAL - "down(2)"
GYESW608_SUP2	rs215	CRITICAL	04-17-2015 22:33:48	34 13h 4m 20s	3/3	SNMP CRITICAL - "down(2)"
	rs234	CRITICAL	04-17-2015 22:37:14	64 11h 7m 37s	3/3	SNMP CRITICAL - "down(2)"
	rs238	CRITICAL	04-17-2015 22:33:48	656 22h 51m 22s	3/3	SNMP CRITICAL - "down(2)"
GYESWQM201	GI1010	CRITICAL	04-17-2015 22:33:48	1296 5h 15m 56s	3/3	SNMP CRITICAL - "down(2)"
	GI1009	CRITICAL	04-17-2015 22:37:15	1296 5h 15m 57s	3/3	SNMP CRITICAL - "down(2)"
Otp-claro	Otp-claro	CRITICAL	04-17-2015 22:38:03	2046 7h 49m 29s	3/3	(Return code of 125 is out of bounds - plugin may not be executable)
Otp-ont	Otp-ont	CRITICAL	04-17-2015 22:38:03	2046 7h 55m 28s	3/3	(Return code of 125 is out of bounds - plugin may not be executable)
Otp-movistar	Otp-movistar	CRITICAL	04-17-2015 22:38:03	2046 7h 54m 14s	3/3	(Return code of 125 is out of bounds - plugin may not be executable)
SW_GYE2905_C7	PING	CRITICAL	10-26-2014 19:09:47	1716 3h 29m 19s	3/3	FPING CRITICAL - 192.168.70.207 (loss=100%)
SW_GYE3905_41	Fa0/45	CRITICAL	04-17-2015 22:30:22	526 9h 47m 58s	1/1	SNMP CRITICAL - "down(2)"
	PING	CRITICAL	02-23-2015 09:04:22	546 21h 14m 51s	3/3	FPING CRITICAL - 192.168.70.241 (loss=100%)
SW_GYE4000_L3	GI32	CRITICAL	04-17-2015 22:30:22	546 14h 54m 33s	1/1	SNMP CRITICAL - "down(2)"
	GI34	CRITICAL	04-17-2015 22:30:22	546 14h 54m 33s	1/1	SNMP CRITICAL - "down(2)"
	GI910	CRITICAL	04-17-2015 22:30:22	826 18h 48m 44s	1/1	SNMP CRITICAL - "down(2)"
UOFW300C	PING	CRITICAL	04-17-2015 22:35:29	34 6h 43m 37s	1/3	FPING CRITICAL - 192.168.85.56 (loss=100%)

CREACION DE REPORTE DE DISPONIBILIDAD

Se ingresa vía web a NAGIOS y se ingresa a la siguiente opción “Availability”, nos presentara una pantalla donde seleccionaremos el tipo de servicio, host o grupo de host que vayamos a generar el reporte



Nagios®

Availability Report
Last Updated: Fri Apr 17 22:41:58 ECT 2015
Nagios® Core™ 3.5.1 - www.nagios.org
Logged in as nagiosadmin

General
Home
Documentation

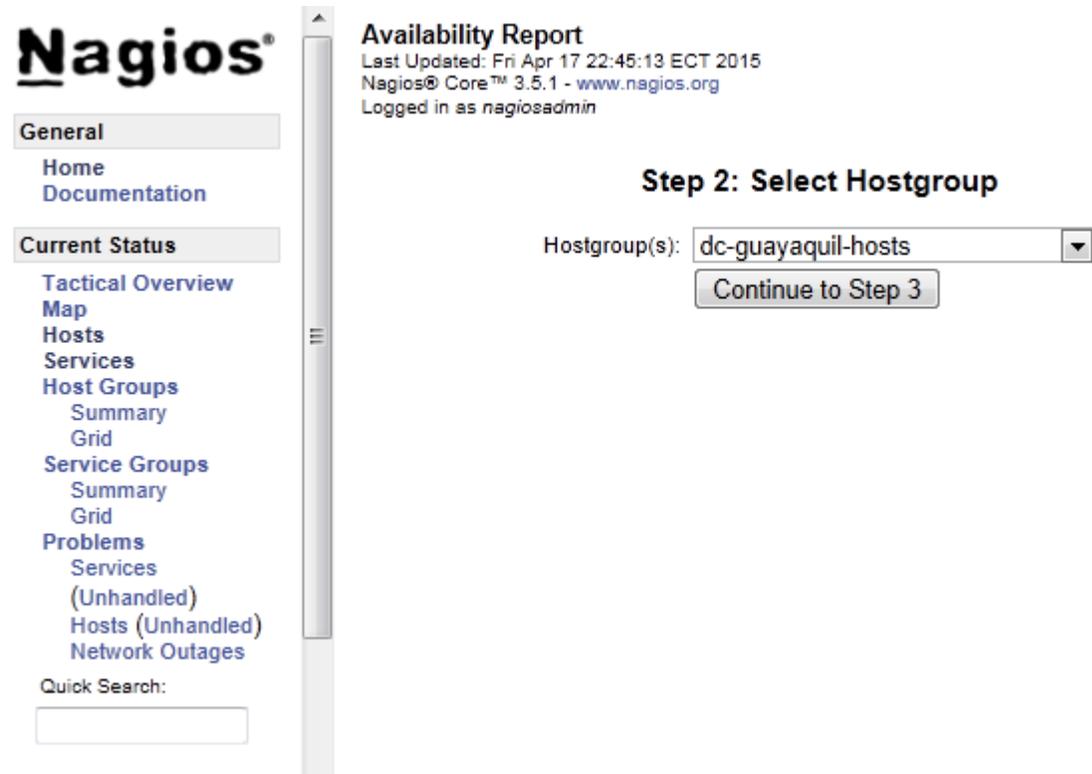
Current Status
Tactical Overview
Map
Hosts
Services
Host Groups
Summary
Grid
Service Groups
Summary
Grid
Problems
Services
(Unhandled)
Hosts (Unhandled)
Network Outages

Quick Search:

Step 1: Select Report Type

Type: ▼

Seleccionamos el grupo de Host o host



Nagios®

Availability Report
Last Updated: Fri Apr 17 22:45:13 ECT 2015
Nagios® Core™ 3.5.1 - www.nagios.org
Logged in as nagiosadmin

General
Home
Documentation

Current Status
Tactical Overview
Map
Hosts
Services
Host Groups
Summary
Grid
Service Groups
Summary
Grid
Problems
Services
(Unhandled)
Hosts (Unhandled)
Network Outages

Quick Search:

Step 2: Select Hostgroup

Hostgroup(s): ▼

Seleccionamos el periodo de tiempo a generar el reporte

General

[Home](#)
[Documentation](#)

Current Status

[Tactical Overview](#)
[Map](#)
[Hosts](#)
[Services](#)
[Host Groups](#)
 [Summary](#)
 [Grid](#)
[Service Groups](#)
 [Summary](#)
 [Grid](#)
[Problems](#)
 [Services](#)
 [\(Unhandled\)](#)
 [Hosts \(Unhandled\)](#)
 [Network Outages](#)

Quick Search:

Reports

[Availability](#)
[Trends](#)
[Alerts](#)

Hostgroup Availability Report

Last Updated: Fri Apr 17 22:48:01 ECT 2015
Nagios® Core™ 3.5.1 - www.nagios.org
Logged in as *nagiosadmin*

Step 3: Select Report Options

Report Period:

If Custom Report Period...

Start Date (Inclusive):

End Date (Inclusive):

Report time Period:

Assume Initial States:

Assume State Retention:

Assume States During Program Downtime:

Include Soft States:

First Assumed Host State:

First Assumed Service State:

Backtracked Archives (To Scan For Initial States):

- General
- Home
- Documentation
- Current Status
- Tactical Overview
- Map
- Hosts
- Services
- Host Groups
- Grid
- Service Groups
- Summary
- Problems
- Grid
- Services (Unhandled)
- Hosts (Unhandled)
- Network Outages
- Quick Search
- Reports
- Availability
- Trends
- Alerts
- History
- Summary
- Histogram
- Notifications
- Event Log
- System
- Comments
- Downtime
- Process Info
- Performance Info
- Scheduling Queue
- Configuration

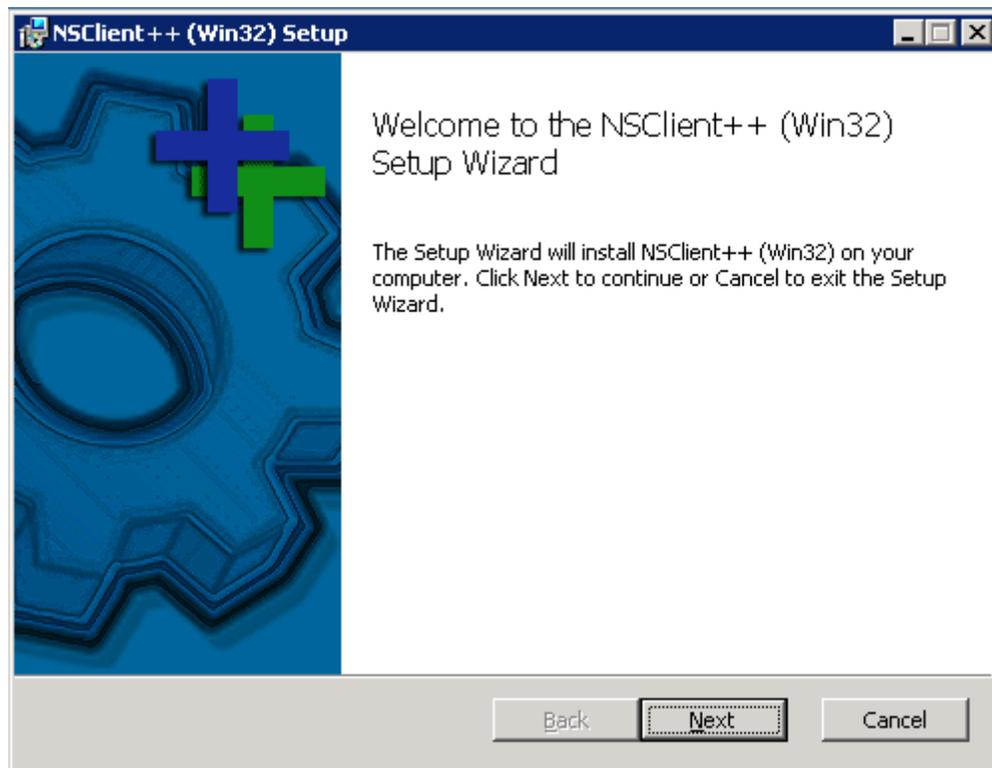
Hostgroup 'dc-guayaquil-hosts' Host State Breakdowns:

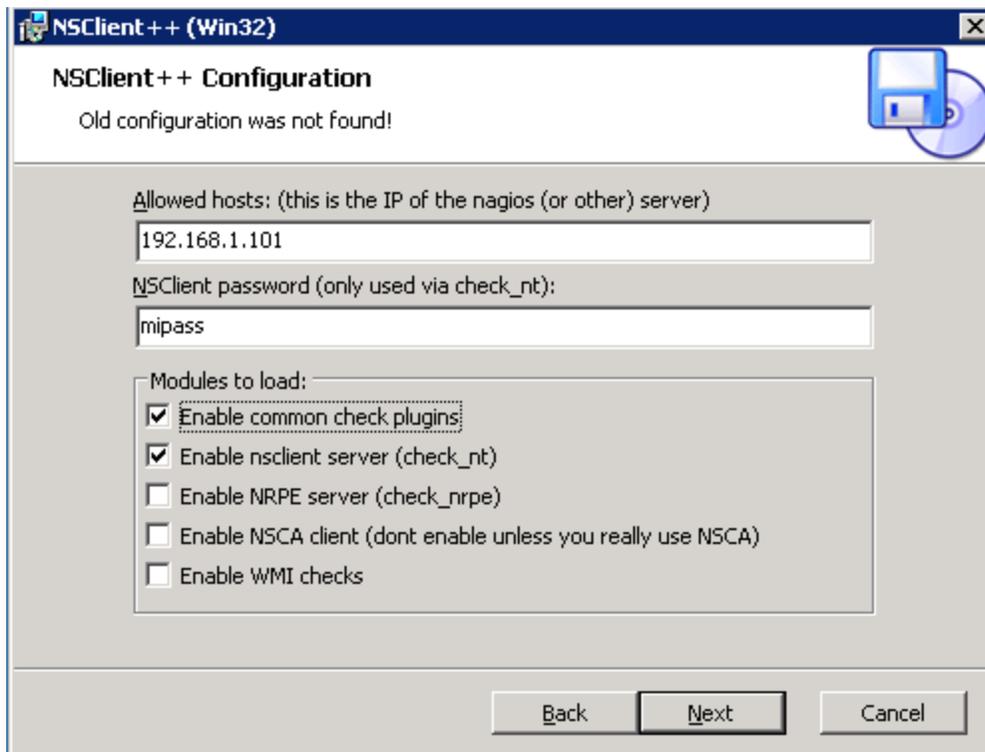
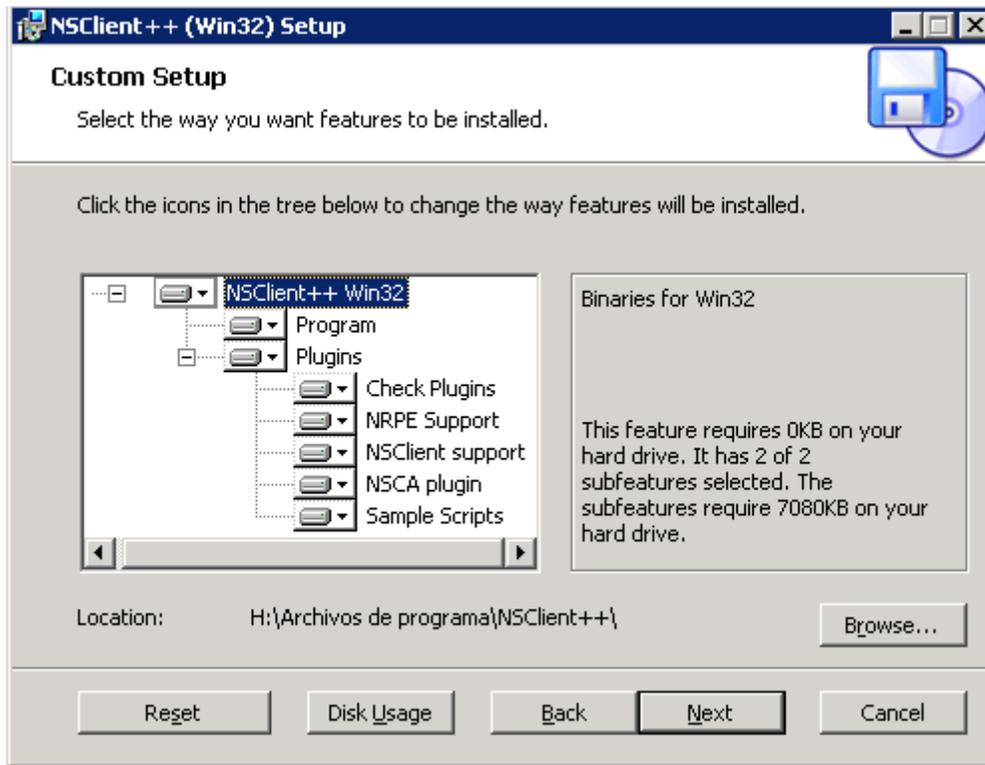
Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
GDNVERTIDOR_BIP	100.00%	(0.00%)	(0.00%)	(0.00%)
FIREWALL_C08	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESLAH01	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESLAH02	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESLAH03	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESLAH04	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESLAH05	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESBEE00	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESWFO7350001	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESWFO7400001	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESWFO7628001	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESWFO7800001	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESWFO7900001	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESWFO1	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESWFO3	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESWENTER01	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESWBNE01	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESWBNE2	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP01	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP02	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP03	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP04	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP05	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP06	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP07	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP08	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP09	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP10	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP11	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP12	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP13	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP14	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP15	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP16	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP17	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP18	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP19	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP20	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP21	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP22	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP23	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP24	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP25	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP26	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP27	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP28	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP29	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP30	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP31	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP32	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP33	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP34	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP35	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP36	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP37	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP38	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP39	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP40	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP41	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP42	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP43	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP44	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP45	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP46	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP47	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP48	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP49	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP50	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP51	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP52	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP53	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP54	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP55	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP56	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP57	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP58	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP59	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP60	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP61	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP62	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP63	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP64	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP65	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP66	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP67	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP68	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP69	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP70	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP71	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP72	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP73	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP74	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP75	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP76	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP77	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP78	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP79	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP80	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP81	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP82	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP83	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP84	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP85	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP86	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP87	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP88	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP89	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP90	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP91	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP92	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP93	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP94	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP95	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP96	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP97	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP98	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP99	100.00%	(0.00%)	(0.00%)	(0.00%)
GYESRAPP100	100.00%	(0.00%)	(0.00%)	(0.00%)
Average	100.00%	(0.00%)	(0.00%)	(0.00%)

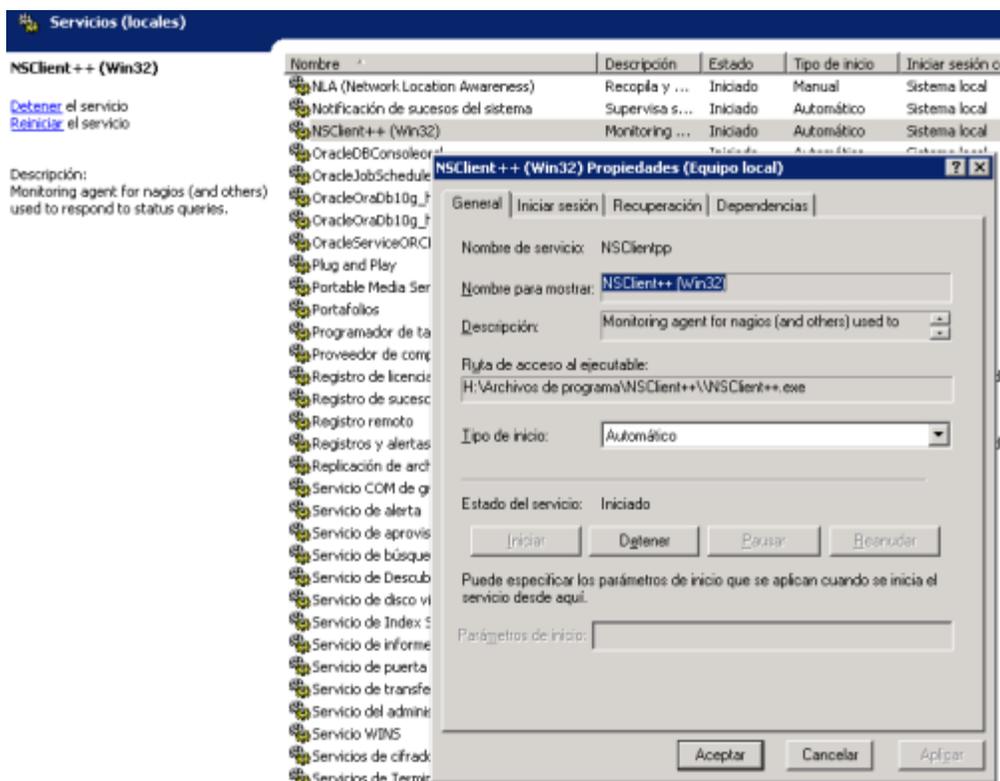
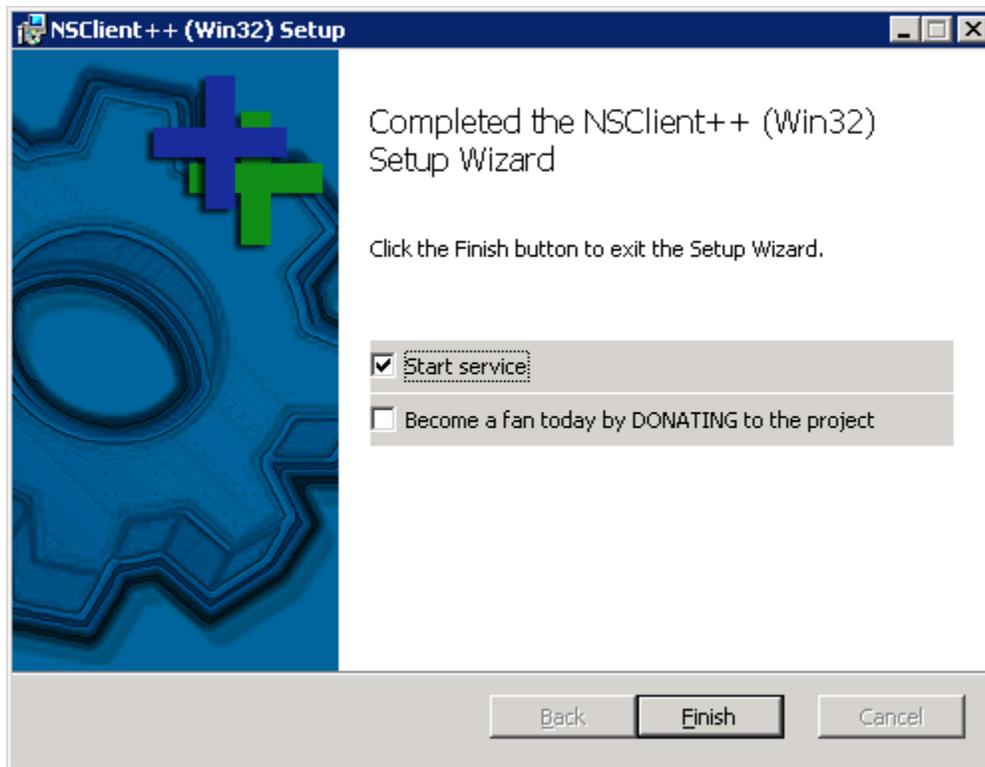
Monitorear un cliente Windows

Instalar el cliente Windows NSClient++

Descargar la última versión del instalador .msi e instalar en el equipo Windows







La configuración la tenemos en `C:\Archivos de programa\NSClient++\NCS.ini`, lo mejor es configurarlo todo a mano. En mi caso se me queda configurado así:

```
[modules]
NSClientListener.dll
FileLogger.dll
CheckSystem.dll
CheckDisk.dll
CheckEventLog.dll
CheckHelpers.dll

[Settings]
use_file=1
allowed_hosts=192.168.1.101
password=mipass
```

Una vez instalado y configurado el cliente windows, nos toca configurar nuestro server Nagios. Pero antes de esto lo mejor es probar directamente desde Linux, que el agente Windows nos responde y está funcionando como toca.

Lo primero asegurarnos que el puerto está abierto en el firewall windows:

```
# nmap IPWINSERVER -p 12489
```

Y luego podemos probar directamente algun comando `check_nt`, por ejemplo ver el espacio en disco C:

```
# /usr/lib/nagios/plugins/check_nt -H IPWINSERVER -p 12489 -v USEDDISKSPACE -d SHOWALL -l
c -s PASSWORD
c:\ - total: 97,65 Gb - used: 8,45 Gb (9%) - free 89,21 Gb (91%) | 'c:\ Used
Space'=8,45Gb;0,00;0,00;0,00;97,65
```

Donde indicamos con: `-H ip_del_host, -p puerto_del_host, -s password_del_agente`, de nuestro server windows.

No está de más revisar el log del agente NSClient++, que está en `H:\Archivos de programa\NSClient++\nsclient.log`

Configuración en Nagios

En esta configuración supongo que Nagios ya lo tenemos configurado y funcionando, lo que voy a añadir es la configuración para el nuevo host windows y sus servicios. Por simplicidad no añado ningún hostgroup.

- Definir el host */etc/nagios3/conf.d/hosts.cfg*

```
define host {
    use generic-host;
    host_name winserver;
    address 192.168.1.102;
}
```

- Definir los nuevos servicios */etc/nagios3/conf.d/services_nagios2.cfg*

```
# SERVICIOS WINDOWS NSClient++
define service{
    use          generic-service
    host_name    winserver
    service_description    NSClient++ Version
    check_command    check_nt!CLIENTVERSION
}
define service{
    use          generic-service
    host_name    winserver
    service_description    Uptime
    check_command    check_nt!UPTIME
}
define service{
    use          generic-service
    host_name    winserver
    service_description    CPU Load
    check_command    check_nt!CPULOAD!-l 5,80,90
}
define service{
    use          generic-service
    host_name    winserver
    service_description    H:\ Drive Space
    check_command    check_nt!USEDISKSPACE!-l h -w 80 -c 90
}
define service{
    use          generic-service
    host_name    poseidon
    service_description    I:\ Drive Space
    check_command    check_nt!USEDISKSPACE!-l i -w 80 -c 90
}
```

```

define service{
    use generic-service
    host_name winserver
    service_description Memory Usage
    check_command check_nt!MEMUSE!-w 80 -c 90
}
# monitoriza que el servicio oracle esta iniciado
define service{
    use generic-service
    host_name winserver
    service_description Oracle 10g Listener
    check_command check_nt!SERVICESTATE!-d SHOWALL -l
OracleOraDb10g_home1TNSListener
}

```

- Configurar el comando check_nt

Editamos `/etc/nagios-plugins/config/nt.cfg` para añadir configurar que el comando coja correctamente: password, puerto y argumentos.

```

# 'check_nt' command definition
define command {
    command_name check_nt
    command_line $USER1$/check_nt -H $HOSTADDRESS$ -p 12489 -s mipass -v $ARG1$ $ARG2
}

```

Por ultimo revisar la configuración y si es correcta reiniciar NAGIOS.

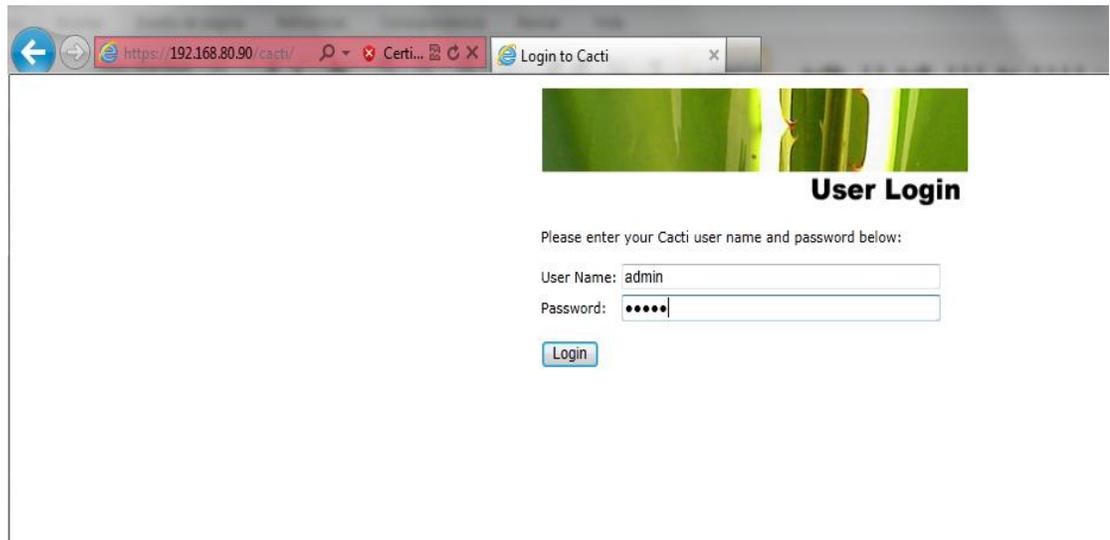
`nagios3 -v /etc/nagios3/nagios.cfg`

Por último una captura de pantalla de NAGIOS, con los servicios que he configurado para el host windows.

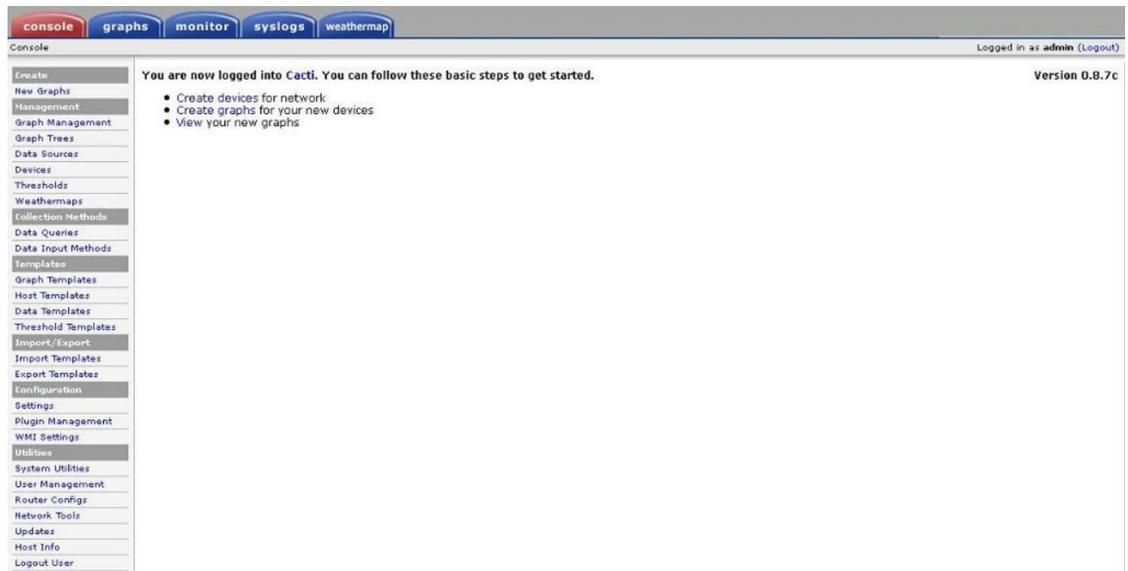
Service ↑	Status ↑	Last Check ↑	Duration ↑	Attempt ↑	Status Information
CPU Load	OK	2009-07-30 14:26:52	0d 0h 26m 21s	1/4	CPU Load 51% (5 min average)
H: Drive Space	OK	2009-07-30 14:24:13	0d 0h 29m 0s	1/4	h: - total: 97,65 Gb - used: 8,45 Gb (9%) - free 89,21 Gb (91%)
I: Drive Space	OK	2009-07-30 14:23:16	0d 0h 4m 57s	1/4	i: - total: 135,16 Gb - used: 15,56 Gb (12%) - free 119,60 Gb (88%)
Memory Usage	OK	2009-07-30 14:25:05	0d 0h 3m 8s	1/4	Memory usage: total:5876,56 Mb - used: 2069,01Mb (35%) - free: 3807,55 Mb
NSClient++ Version	OK	2009-07-30 14:24:45	0d 0h 28m 28s	1/4	NSClient++ 0.3.6.818 2009-06-14
Oracle 10g Listener	OK	2009-07-30 14:26:54	0d 0h 1m 19s	1/4	OracleOraDb10g_home1TNSListener: Started
PING	OK	2009-07-30 14:26:49	15d 21h 6m 24s	1/4	PING OK - Packet loss = 0%, RTA = 0.24 ms
Uptime	OK	2009-07-30 14:23:56	0d 0h 29m 17s	1/4	System Uptime - 17 day(s) 4 hour(s) 26 minute(s)
dns	OK	2009-07-30 14:26:28	1d 2h 31m 45s	1/4	DNS OK: 0,026 seconds response time: www.google.com returns 209.85.227.103,209.85.227.104,209.85.227.147,209.85.227.99

MANUAL DE USUARIO DE CACTI

Para ingresar a NAGIOS abrimos el navegador (Internet Explorer, Mozilla Firefox o Google Chrome) y ponemos la IP del servidor seguida de la siguiente línea “/cacti” donde está instalado el software.



Al introducir el usuario y contraseña facilitados, accedemos a la pantalla principal de Cacti, desde la cual podemos ver todos los contenidos de la aplicación de gestión de dispositivos de red



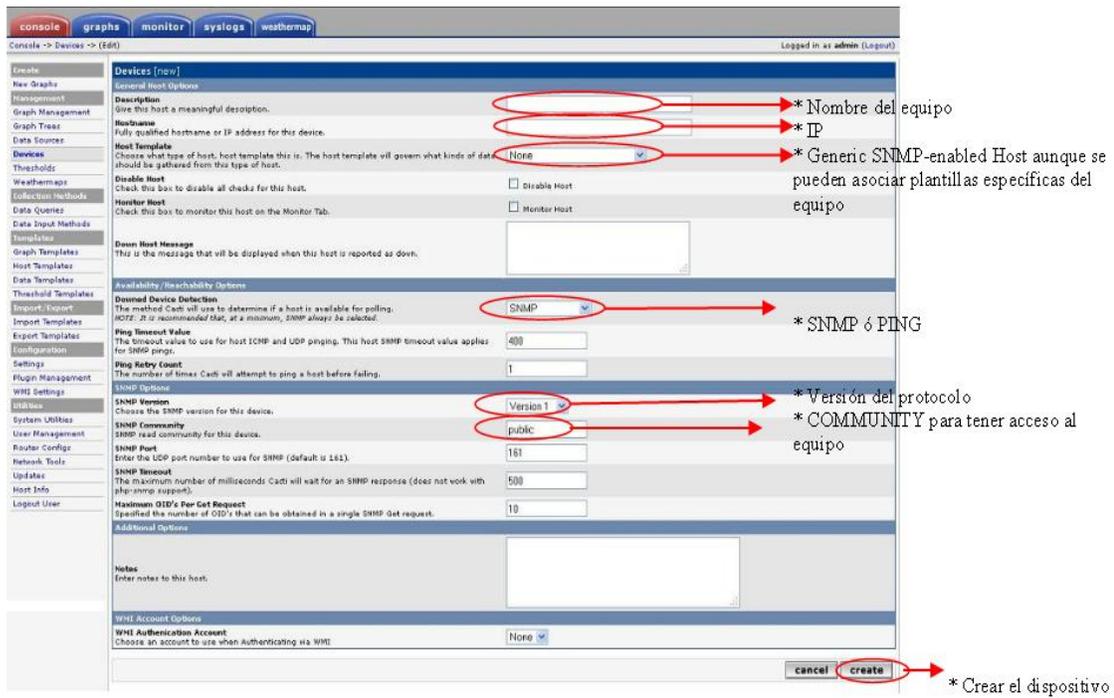
VISUALIZACION DE EQUIPOS

Para ver los elementos pertenecientes a nuestra red vamos a la pestaña Console ->

Management->Devices y nos aparecerá una pantalla como esta:

NUEVOS DISPOSITIVOS

Si en un futuro se agrega algún equipo nuevo a la red habrá que pinchar en “Add” y nos aparecerá una pantalla como esta, donde están marcados los parámetros más importantes:



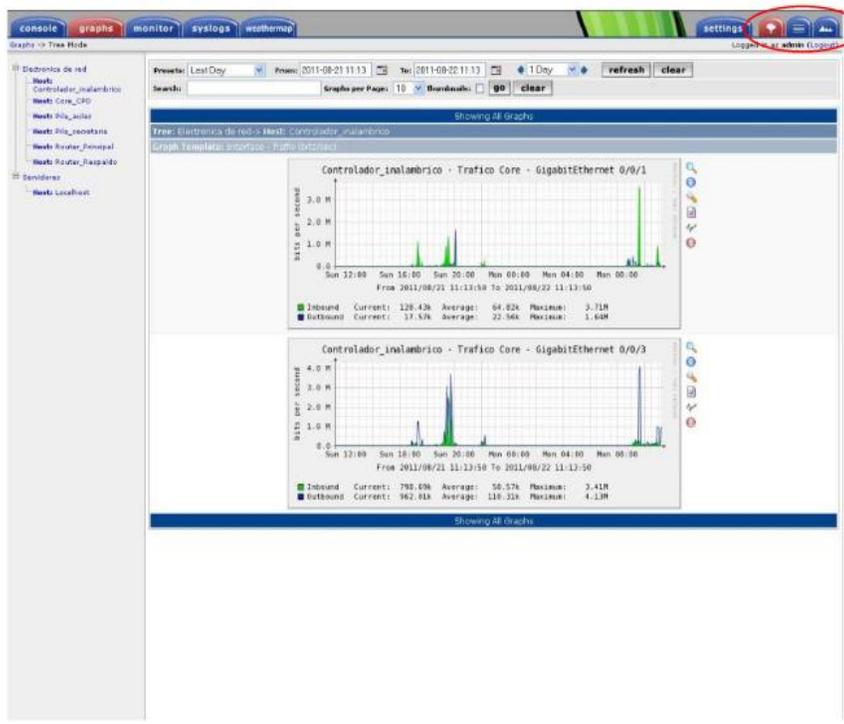
VISUALIZACIÓN:

Como comentamos en la Introducción, CACTI nos permite visualizar gráficas asociadas a cada equipo. Consideramos que las más importantes para monitorizar la red son las siguientes:

- Tráfico de Red
- Uso de la CPU
- Uso de la memoria
- Temperatura

Para visualizar las gráficas asociadas a los equipos que componen lared nos vamos a la pestaña “graphs” y nos encontramos con un árbol desplegable con una rama por cada equipo (o host).

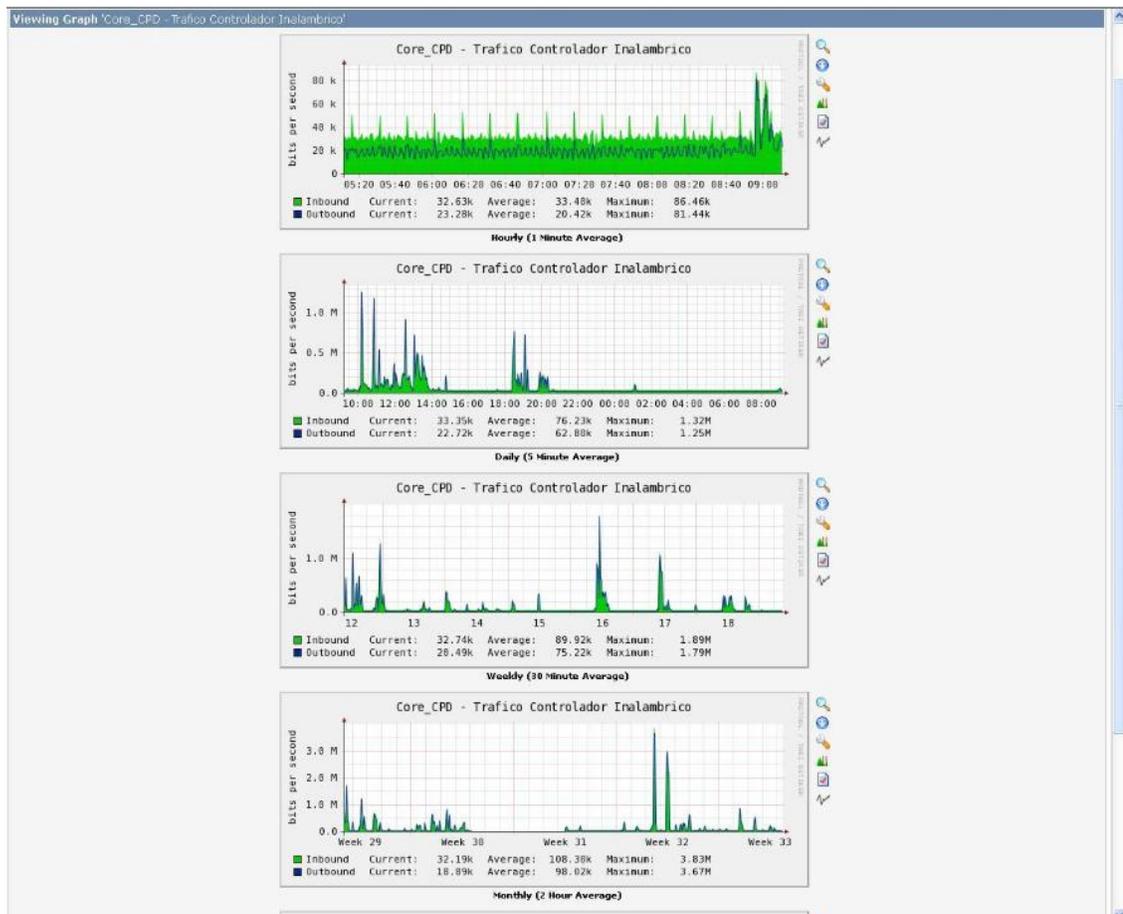
Dando click encima visualizamos las gráficas correspondientes.



Elección de la vista:
* árbol
* lista
* vista previa de todas las gráficas

A través del menú lateral izquierdo podemos navegar por el árbol de dispositivos, y podremos consultar todas las gráficas definidas para ellos.

Si damos click alguna de las gráficas obtendremos la representación de los valores en la última hora, el último día, semana, mes y año. En el caso del tráfico de red, obtendríamos algo como esto:



NUEVAS GRÁFICAS

Para crear nuevos gráficos asociados a nuestros equipos se procede de la siguiente manera: damos click en la pestaña Console ->Create ->New Graphs y elegimos en el desplegable de “Host” qué equipo queremos elegir:

The screenshot shows the Mikrotik WinBox interface. At the top, there are navigation tabs: console, graphs, monitor, syslogs, and weathermap. The user is logged in as 'admin'. The main window is titled 'Create New Graphs' and shows the configuration for a host named 'Pila_secretaria (10.10.80.202)'. The host is identified as a 'Generic SNMP-enabled Host'. A dropdown menu for 'Graph Types' is open, showing options like 'Pila_secretaria (10.10.80.202)', 'Controlador_inalambico (10.20.97.6)', 'Core_CFD (10.10.80.200)', 'Firewall (10.10.10.1)', 'Localhost (127.0.0.1)', and 'Pila_oulos (10.10.80.201)'. Below this, there is a 'Data Query' section for 'SNMP - Interface Statistics'. The table below shows the following data:

Index	Status	Description	Name (IF-MIB)	Alias (IF-MIB)	Type	Speed	Hardware Address	IP Address
1	Up	Vlan1	Vl1		propVirtual(S3)	100000000	00:B8:5E:BF:77:00:C0	10.10.80.202
99	Up	Vlan99	Vl99		propVirtual(S3)	100000000	00:B8:5E:BF:77:00:C1	10.20.99.202
5137	Up	StackPort1	StackPort1		propVirtual(S3)	0		
5138	Up	StackSub-St1-1	StackSub-St1-1		propVirtual(S3)	0		
5139	Down	StackSub-St1-2	StackSub-St1-2		propVirtual(S3)	0		
5140	Up	StackPort2	StackPort2		propVirtual(S3)	0		
5141	Up	StackSub-St2-1	StackSub-St2-1		propVirtual(S3)	0		
5142	Up	StackSub-St2-2	StackSub-St2-2		propVirtual(S3)	0		
5143	Up	StackPort3	StackPort3		propVirtual(S3)	0		
5144	Down	StackSub-St3-1	StackSub-St3-1		propVirtual(S3)	0		
5145	Up	StackSub-St3-2	StackSub-St3-2		propVirtual(S3)	0		
5146	Up	StackPort4	StackPort4		propVirtual(S3)	0		
5147	Up	StackSub-St4-1	StackSub-St4-1		propVirtual(S3)	0		
5148	Up	StackSub-St4-2	StackSub-St4-2		propVirtual(S3)	0		
10101	Up	GigabitEthernet1/0/1	G1/0/1	AP planta	ethernetCsmacd(6)	100000000	00:44:E4:D9:48:81	
10102	Up	GigabitEthernet1/0/2	G1/0/2	AP planta	ethernetCsmacd(6)	100000000	00:44:E4:D9:48:82	
10103	Up	GigabitEthernet1/0/3	G1/0/3	AP planta	ethernetCsmacd(6)	100000000	00:44:E4:D9:48:83	
10104	Up	GigabitEthernet1/0/4	G1/0/4	AP planta	ethernetCsmacd(6)	100000000	00:44:E4:D9:48:84	
10105	Down	GigabitEthernet1/0/5	G1/0/5	AP planta	ethernetCsmacd(6)	10000000	00:44:E4:D9:48:85	
10106	Down	GigabitEthernet1/0/6	G1/0/6	AP planta	ethernetCsmacd(6)	10000000	00:44:E4:D9:48:86	
10107	Down	GigabitEthernet1/0/7	G1/0/7	AP planta	ethernetCsmacd(6)	10000000	00:44:E4:D9:48:87	
10108	Down	GigabitEthernet1/0/8	G1/0/8	AP planta	ethernetCsmacd(6)	10000000	00:44:E4:D9:48:88	
10109	Up	GigabitEthernet1/0/9	G1/0/9	Usuario20	ethernetCsmacd(6)	10000000	00:44:E4:D9:48:89	
10110	Down	GigabitEthernet1/0/10	G1/0/10	Usuario20	ethernetCsmacd(6)	10000000	00:44:E4:D9:48:8A	
10111	Down	GigabitEthernet1/0/11	G1/0/11	Usuario20	ethernetCsmacd(6)	10000000	00:44:E4:D9:48:8B	
10112	Down	GigabitEthernet1/0/12	G1/0/12	Usuario20	ethernetCsmacd(6)	10000000	00:44:E4:D9:48:8C	

Saldrá una lista con las gráficas disponibles para ese dispositivo. Hay que tener en cuenta que dependiendo de la marca y modelo del dispositivo, se podrán monitorizar unos elementos u otros. Marcamos la casilla de la derecha de las gráficas que queremos añadir. El proceso finaliza dando click en Create:

Weathermaps
 Collection Methods
 Data Queries
 Data Input Methods
 Templates
 Graph Templates
 Host Templates
 Data Templates
 Threshold Templates
 Import / Export
 Import Templates
 Export Templates
 Configuration
 Settings
 Plugin Management
 WMI Settings
 Utilities
 System Utilities
 User Management
 Router Configs
 Network Tools
 Updates
 Host Info
 Logout User

Creator 1 Cisco - CPU Usage
 Creator 2 Cisco - Memory Usage
 Creator: (Select a graph type to create)

Data Query [SNMP - Interface Statistics]
 << Previous Showing Rows 1 to 30 of 224 [1,2,3,4,5,6,7,8] Next >>

Index	Status	Description	Name (IF-MIB)	Alias (IF-MIB)	Type	Speed	Hardware Address	IP Address
1	Up	Vlan1	Vlan1		propVirtual(53)	1000000000	00:08:0E:8F:77:00:00	10.10.30.202
99	Up	Vlan99	Vlan99		propVirtual(53)	1000000000	00:08:0E:8F:77:00:C1	10.20.99.202
5137	Up	StackPort1	StackPort1		propVirtual(53)	0		
5138	Up	StackSub-011-1	StackSub-011-1		propVirtual(53)	0		
5139	Down	StackSub-011-2	StackSub-011-2		propVirtual(53)	0		
5140	Up	StackPort2	StackPort2		propVirtual(53)	0		
5141	Up	StackSub-012-1	StackSub-012-1		propVirtual(53)	0		
5142	Up	StackSub-012-2	StackSub-012-2		propVirtual(53)	0		
5143	Up	StackPort3	StackPort3		propVirtual(53)	0		
5144	Down	StackSub-013-1	StackSub-013-1		propVirtual(53)	0		
5145	Up	StackSub-013-2	StackSub-013-2		propVirtual(53)	0		
5146	Up	StackPort4	StackPort4		propVirtual(53)	0		
5147	Up	StackSub-014-1	StackSub-014-1		propVirtual(53)	0		
5148	Up	StackSub-014-2	StackSub-014-2		propVirtual(53)	0		
10101	Up	GigabitEthernet1/0/1	Gi1/0/1	AP planta	ethernetCrmacd(6)	1000000000	00:44:E4:D9:48:148:01	
10102	Up	GigabitEthernet1/0/2	Gi1/0/2	AP planta	ethernetCrmacd(6)	1000000000	00:44:E4:D9:48:148:02	
10103	Up	GigabitEthernet1/0/3	Gi1/0/3	AP planta	ethernetCrmacd(6)	1000000000	00:44:E4:D9:48:148:03	
10104	Up	GigabitEthernet1/0/4	Gi1/0/4	AP planta	ethernetCrmacd(6)	1000000000	00:44:E4:D9:48:148:04	
10105	Down	GigabitEthernet1/0/5	Gi1/0/5	AP planta	ethernetCrmacd(6)	10000000	00:44:E4:D9:48:148:05	<input checked="" type="checkbox"/>
10106	Down	GigabitEthernet1/0/6	Gi1/0/6	AP planta	ethernetCrmacd(6)	10000000	00:44:E4:D9:48:148:06	<input checked="" type="checkbox"/>
10107	Down	GigabitEthernet1/0/7	Gi1/0/7	AP planta	ethernetCrmacd(6)	10000000	00:44:E4:D9:48:148:07	<input type="checkbox"/>
10108	Down	GigabitEthernet1/0/8	Gi1/0/8	AP planta	ethernetCrmacd(6)	10000000	00:44:E4:D9:48:148:08	<input type="checkbox"/>
10109	Up	GigabitEthernet1/0/9	Gi1/0/9	Usuario20	ethernetCrmacd(6)	1000000000	00:44:E4:D9:48:148:09	<input checked="" type="checkbox"/>
10110	Down	GigabitEthernet1/0/10	Gi1/0/10	Usuario20	ethernetCrmacd(6)	10000000	00:44:E4:D9:48:148:0A	<input type="checkbox"/>
10111	Down	GigabitEthernet1/0/11	Gi1/0/11	Usuario20	ethernetCrmacd(6)	10000000	00:44:E4:D9:48:148:0B	<input type="checkbox"/>
10112	Down	GigabitEthernet1/0/12	Gi1/0/12	Usuario20	ethernetCrmacd(6)	10000000	00:44:E4:D9:48:148:0C	<input type="checkbox"/>
10113	Up	GigabitEthernet1/0/13	Gi1/0/13	Usuario20	ethernetCrmacd(6)	1000000000	00:44:E4:D9:48:148:0D	<input checked="" type="checkbox"/>
10114	Up	GigabitEthernet1/0/14	Gi1/0/14	Usuario20	ethernetCrmacd(6)	1000000000	00:44:E4:D9:48:148:0E	<input type="checkbox"/>
10115	Down	GigabitEthernet1/0/15	Gi1/0/15	Usuario20	ethernetCrmacd(6)	10000000	00:44:E4:D9:48:148:0F	<input type="checkbox"/>
10116	Down	GigabitEthernet1/0/16	Gi1/0/16	Usuario20	ethernetCrmacd(6)	10000000	00:44:E4:D9:48:148:10	<input type="checkbox"/>

<< Previous Showing Rows 1 to 30 of 224 [1,2,3,4,5,6,7,8] Next >>

Select a graph type: In/Out Bits

cancel create

Si necesitamos modificar algún valor de la gráfica como puede ser el título, nos vamos a “Console ->Management ->Graph Management” y aparecerá incluida en la lista.

console graphs monitor syslogs weathermap

Console -> Graph Management Logged in as admin (Logout)

Graph Management Add

Host: Any Template: Any

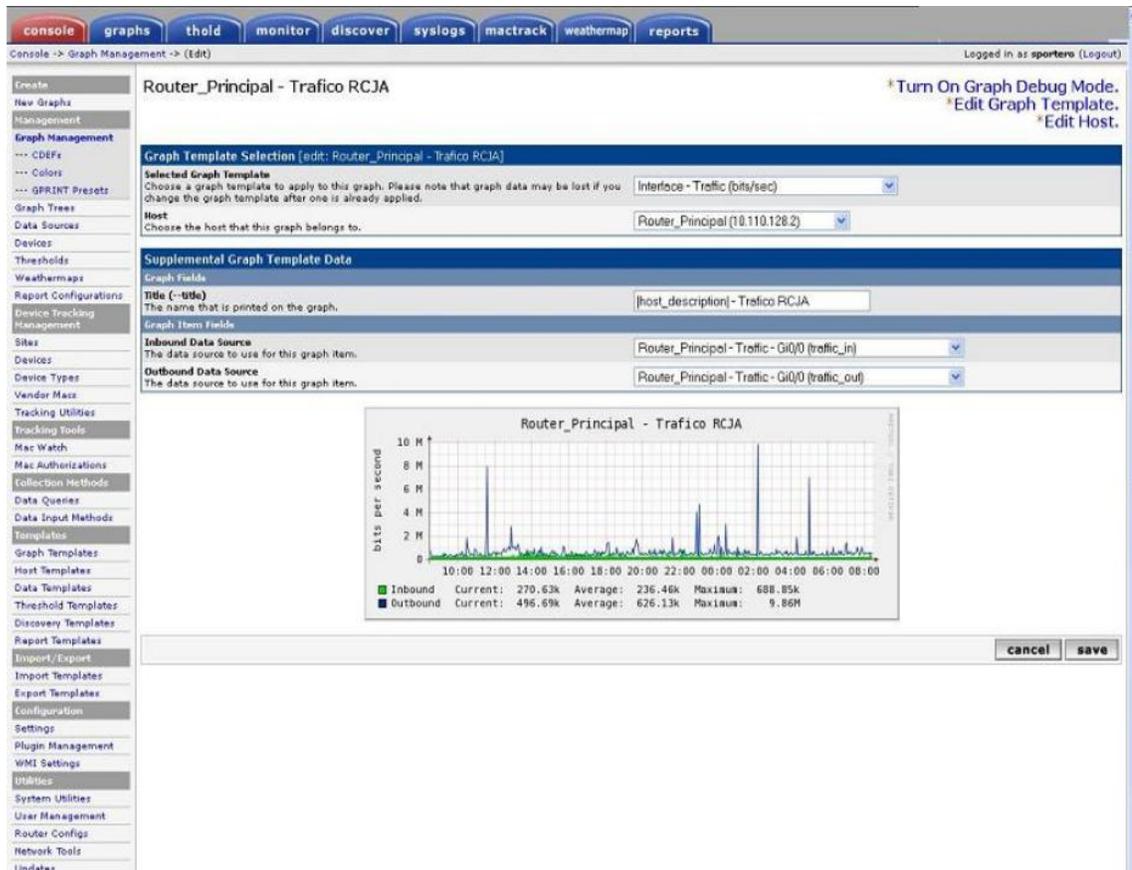
Search: Rows per Page: 30

Graph Title**	ID	Template Name	Size	
Controlador_inalambrico - Trafico Core - GigabitEthernet 9/9/1	202	Interface - Traffic (bits/sec)	120x500	<input type="checkbox"/>
Controlador_inalambrico - Trafico Core - GigabitEthernet 9/9/3	201	Interface - Traffic (bits/sec)	120x500	<input type="checkbox"/>
Core_CPD - AP1-arm1	162	Interface - Traffic (bits/sec)	120x500	<input type="checkbox"/>
Core_CPD - AP18-arm1	170	Interface - Traffic (bits/sec)	120x500	<input type="checkbox"/>
Core_CPD - AP11-arm1	171	Interface - Traffic (bits/sec)	120x500	<input type="checkbox"/>
Core_CPD - AP12-arm1	172	Interface - Traffic (bits/sec)	120x500	<input type="checkbox"/>
Core_CPD - AP13-arm1	173	Interface - Traffic (bits/sec)	120x500	<input type="checkbox"/>
Core_CPD - AP14-arm1	174	Interface - Traffic (bits/sec)	120x500	<input type="checkbox"/>
Core_CPD - AP2-arm1	163	Interface - Traffic (bits/sec)	120x500	<input type="checkbox"/>
Core_CPD - AP3-arm1	164	Interface - Traffic (bits/sec)	120x500	<input type="checkbox"/>
Core_CPD - AP4-arm1	165	Interface - Traffic (bits/sec)	120x500	<input type="checkbox"/>
Core_CPD - AP5-arm1	166	Interface - Traffic (bits/sec)	120x500	<input type="checkbox"/>
Core_CPD - AP6-arm1	167	Interface - Traffic (bits/sec)	120x500	<input type="checkbox"/>
Core_CPD - AP7-arm1	168	Interface - Traffic (bits/sec)	120x500	<input type="checkbox"/>
Core_CPD - AP8-arm1	161	Interface - Traffic (bits/sec)	120x500	<input type="checkbox"/>
Core_CPD - AP9-arm1	169	Interface - Traffic (bits/sec)	120x500	<input type="checkbox"/>
Core_CPD - uno	200	Interface - Traffic (bits/sec)	120x500	<input type="checkbox"/>
Core_CPD - Temperatura	22	3 Cisco - Temperature	120x500	<input type="checkbox"/>
Core_CPD - Traffic - G18/36	178	Interface - Traffic (bits/sec)	120x500	<input type="checkbox"/>
Core_CPD - Traffic - G9/28	213	Interface - Traffic (bits/sec)	120x500	<input type="checkbox"/>
Core_CPD - Traffic - G9/35	177	Interface - Traffic (bits/sec)	120x500	<input type="checkbox"/>
Core_CPD - Trafico Aulas Principal	136	Interface - Traffic (bits/sec)	120x500	<input type="checkbox"/>
Core_CPD - Trafico Aulas Respaldo	139	Interface - Traffic (bits/sec)	120x500	<input type="checkbox"/>
Core_CPD - Trafico Controlador Inalambrico	126	Interface - Traffic (bits/sec)	120x500	<input type="checkbox"/>
Core_CPD - Trafico Po17	143	Interface - Traffic (bits/sec)	120x500	<input type="checkbox"/>
Core_CPD - Trafico Po18	144	Interface - Traffic (bits/sec)	120x500	<input type="checkbox"/>
Core_CPD - Trafico Secretaria Principal	138	Interface - Traffic (bits/sec)	120x500	<input type="checkbox"/>
Core_CPD - Trafico Secretaria Respaldo	142	Interface - Traffic (bits/sec)	120x500	<input type="checkbox"/>
Core_CPD - Uso de la Memoria	21	2 Cisco - Memory Usage	120x500	<input type="checkbox"/>
Local - Poller Statistics	16	Local - Poller Statistics	120x740	<input type="checkbox"/>

<< Previous Showing Rows 1 to 30 of 68 [1,2,3] Next >>

Choose an action:

Podemos tener una lista con todas las gráficas juntas (“Any”) o por equipo haciendo uso del desplegable “Host”. Dando click en la gráfica de interés la podemos visualizar y modificar:



Estas gráficas se incluyen automáticamente en la rama correspondiente del árbol de gráficas al cual podemos acceder haciendo uso del menú lateral izquierdo como se explica a continuación.

VISUALIZACIÓN DEL ARBOL Y MODIFICACIÓN DE RAMAS

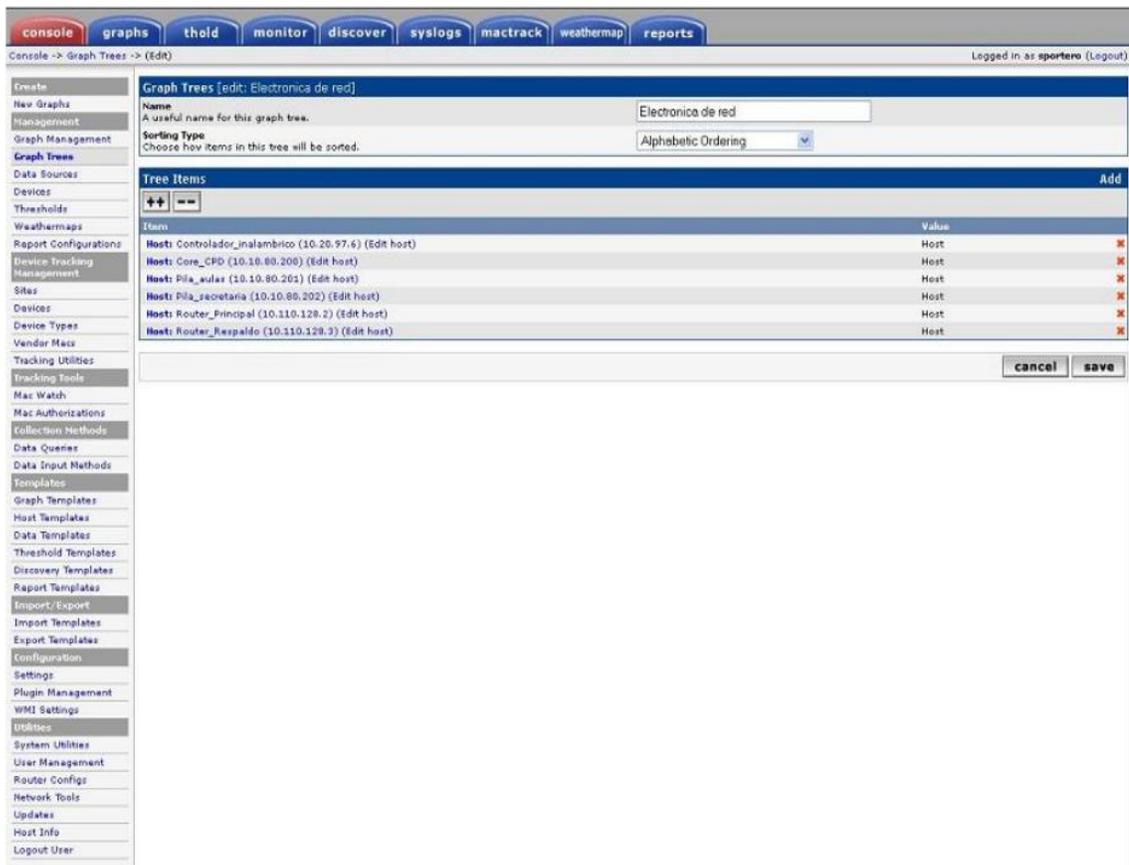
En Cacti, la manera de organizar las gráficas es a través de árboles. Cada árbol a su vez puede tener ramas, que pueden ser o bien “hosts” o bien una “gráfica”. Si elegimos un host, todas sus gráficas asociadas colgarán de esa rama. Sin embargo, al elegir una gráfica sólo se mostrará ella misma. Si tenemos un host con muchas gráficas, es preferible crear siempre ramas de “hosts”.

Podemos crear tantos árboles como ramas sean necesarias para conseguir tener la organización que nos convenga.

Si hemos creado una nueva máquina y le hemos asociado gráficas, lo podremos incluir en cualquiera de los árboles como una nueva rama. Para ello, nos vamos a

“Console ->Management ->Graph Trees” y podremos visualizar los árboles existentes. En la configuración inicial de la sede de trabajo, se han creado dos ramas: una de servidores, que contiene gráficas del propio servidor web, y otra de electrónica de red, con gráficas de los dispositivos.

Si damos click en “Electrónica de red”, aparece una lista con las actuales ramas.



The screenshot shows the 'Graph Trees' configuration page. The main panel is titled 'Graph Trees [edit: Electronica de red]'. It contains the following fields:

- Name:** Electronica de red
- Sorting Type:** Alfabetic Ordering

Below these fields is a table titled 'Tree Items' with an 'Add' button. The table has two columns: 'Items' and 'Value'. The items listed are:

Items	Value
Host: Controlador_inalambrico (10.20.97.6) (Edit host)	Host
Host: Core_CFD (10.10.80.208) (Edit host)	Host
Host: Pila_sulaz (10.10.80.201) (Edit host)	Host
Host: Pila_secretaria (10.10.80.202) (Edit host)	Host
Host: Router_Principal (10.110.128.2) (Edit host)	Host
Host: Router_Respaldo (10.110.128.3) (Edit host)	Host

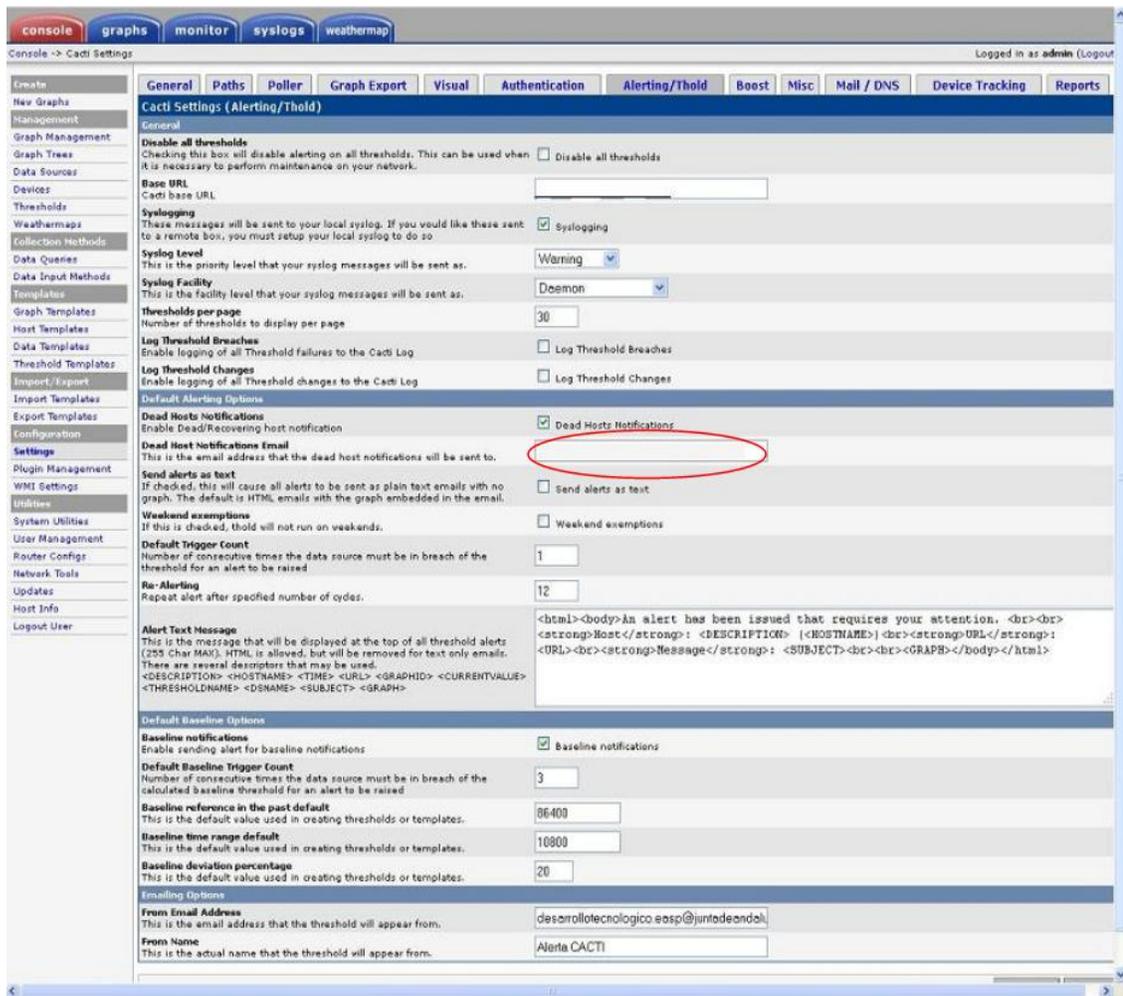
At the bottom of the table are 'cancel' and 'save' buttons.

Si queremos agregar una más, por ejemplo si hemos creado un dispositivo nuevo, damos click en Add y rellenamos el formulario. En “Tree Item Type” elegimos “Host” y debajo el host (ó máquina) en cuestión. Finalizamos el proceso dando click en Create.

Podremos comprobar que se ha incluido en el árbol correspondiente dando click en la pestaña superior “graphs” y navegando por las ramas.

ALERTAS

Como comentamos en la introducción, Cacti nos da la opción de enviar alertas a nuestra cuenta de correo en caso de que ocurra alguna irregularidad en nuestros equipos. Nos vamos a la pestaña Console ->Configuration ->Settings y damos click en la pestaña Alerting/Thold.



Aquí podemos configurar las opciones de alerta tales como el mensaje que queremos que nos llegue, desde qué cuenta, con qué asunto, etc. La configuración del servidor de correo por ejemplo se hace desde la pestaña “Mail/DNS” a la derecha de la pestaña presente. Si además hemos marcado la opción “Dead Hosts Notifications” en la pestaña anterior, recibiremos en la cuenta configurada un correo electrónico cada vez que se pierda la conectividad con un dispositivo.

The screenshot shows the Cacti Settings interface for Mail / DNS configuration. The interface is divided into several sections:

- General**: Includes 'Test Email' (with a 'Send a Test Email' button), 'Mail Services' (set to SMTP), 'From Email Address', 'From Name', and 'Word Wrap' (set to 120).
- Sendmail Options**: Includes 'Sendmail Path' (set to /usr/sbin/sendmail).
- SMTP Options**: Includes 'SMTP Hostname', 'SMTP Port' (set to 25), 'SMTP Username', and 'SMTP Password'.
- DNS Options**: Includes 'Primary DNS IP Address', 'Secondary DNS IP Address', and 'DNS Timeout' (set to 500).

At the bottom right, there are 'cancel' and 'save' buttons.

CAMBIAR/AGREGAR USUARIOS Y PASSWORD

Si queremos cambiar el nombre o la contraseña del usuario que está creado por defecto hay que ir a la pestaña de Console ->Utilities ->User Management donde nos aparecerán los usuarios definidos.

console graphs monitor syslogs weathermap

Console -> User Management Logged in as admin (Logout)

Create
New Graphs
Management
Graph Management
Graph Trees
Data Sources
Devices
Thresholds
Weathermaps
Collection Methods
Data Queries
Data Input Methods
Templates
Graph Templates
Host Templates
Data Templates
Threshold Templates
Import/Export
Import Templates
Export Templates
Configuration
Settings
Plugin Management
WMI Settings
Utilities
System Utilities
User Management
Router Configs
Network Tools
Updates
Host Info
Logout User

User Management Add

Search:

<< Previous Showing Rows 1 to 2 of 2 (1) Next >>

User Name**	Full Name	Enabled	Realm	Default Graph Policy	Last Login
admin	Administrator	Yes	Local	ALLOW	Monday, August 22, 2011 09:06:37
guest	Guest Account	Yes	Local	ALLOW	Thursday, July 14, 2011 11:44:19

<< Previous Showing Rows 1 to 2 of 2 (1) Next >>

Choose an action:

console graphs monitor syslogs weathermap

Console -> User Management -> (Edit) Logged in as admin (Logout)

Create
New Graphs
Management
Graph Management
Graph Trees
Data Sources
Devices
Thresholds
Weathermaps
Collection Methods
Data Queries
Data Input Methods
Templates
Graph Templates
Host Templates
Data Templates
Threshold Templates
Import/Export
Import Templates
Export Templates
Configuration
Settings
Plugin Management
WMI Settings
Utilities
System Utilities
User Management
Router Configs
Network Tools
Updates
Host Info
Logout User

User Management (edit: admin)

User Name
The login name for this user.

Full Name
A more descriptive name for this user that can include spaces or special characters.

Password
Enter the password for this user twice. Remember that passwords are case sensitive!

Enabled
Determines if user is able to login. Enabled

Account Options
Set any user account-specific options here.

User Must Change Password at Next Login
 Allow this User to Keep Custom Graph Settings

Graph Options
Set any graph-specific options here.

User Has Rights to Tree View
 User Has Rights to List View
 User Has Rights to Preview View

Login Options
What to do when this user logs in.

Show the page that user pointed their browser to.
 Show the default console screen.
 Show the default graph screen.

Authentication Realm
Only used if you have LDAP or Web Basic Authentication enabled. Changing this to a non-enabled realm will effectively disable the user.

Email Address

Realm Permissions **Graph Permissions** **Graph Settings**

Realm Permissions
Realm permissions control which sections of Cacti this user will have access to.

<input checked="" type="checkbox"/> User Administration	<input checked="" type="checkbox"/> Configure Threshold Templates
<input checked="" type="checkbox"/> Data Input	<input checked="" type="checkbox"/> Configure Thresholds
<input checked="" type="checkbox"/> Update Data Sources	<input type="checkbox"/> View Thresholds
<input checked="" type="checkbox"/> Update Graph Trees	<input checked="" type="checkbox"/> View Monitoring
<input checked="" type="checkbox"/> Update Graphs	<input type="checkbox"/> View Host Auto-Discovery
<input checked="" type="checkbox"/> View Graphs	<input checked="" type="checkbox"/> View Syslog
<input checked="" type="checkbox"/> Console Access	<input checked="" type="checkbox"/> Configure Syslog Alerts / Reports
<input checked="" type="checkbox"/> Update Round Robin Archives	<input type="checkbox"/> View MacTrack Data
<input checked="" type="checkbox"/> Update Graph Templates	<input type="checkbox"/> Administrate MacTrack
<input checked="" type="checkbox"/> Update Data Templates	<input type="checkbox"/> Manage Mac Authorizations
<input checked="" type="checkbox"/> Update Host Templates	<input checked="" type="checkbox"/> Check for updates
<input type="checkbox"/> Data Queries	<input checked="" type="checkbox"/> View Host Info
<input type="checkbox"/> Update CDEFs	<input checked="" type="checkbox"/> Plugin -> Weathermap: Configure/Manage
<input type="checkbox"/> Global Settings	<input type="checkbox"/> Plugin -> Weathermap: View
<input type="checkbox"/> Export Data	<input type="checkbox"/> Plugin -> Reports: Power User Configuration
<input type="checkbox"/> Import Data	<input type="checkbox"/> Plugin -> Reports: Owner Configuration
<input type="checkbox"/> Plugin Management	<input type="checkbox"/> Plugin -> Reports: View
<input checked="" type="checkbox"/> Plugin -> Router Configs	<input checked="" type="checkbox"/> Plugin -> Realtime

* Contraseña

* Ppermisos

ANEXO

INSTALACION Y CONFIGURACIÓN DE NAGIOS

Instalación de paquetes antes de instalar NAGIOS

Antes de cualquier configuración se requiere de la instalación de los siguientes paquetes:

- Servidor web (Apache2)
- PHP
- GCC
- Librerías GD

```
# apt-get install apache2  
  
# apt-get install libapache2-mod-php5  
  
# apt-get install build-essential  
  
# apt-get install libgd2-noxpm-dev
```

Creación de cuenta de usuario NAGIOS

```
# /usr/sbin/useradd -m -s /bin/bash nagios  
  
# passwd nagios
```

Creación de un grupo nagcmd al que pertenece

```
# /usr/sbin/groupadd nagcmd  
  
# /usr/sbin/usermod -a -G nagcmd nagios  
  
# /usr/sbin/usermod -a -G nagcmd www-data
```

Descargar NAGIOS

```
# mkdir ~/Downloads  
  
# cd ~/Downloads  
  
# wget http://prdownloads.sourceforge.net/sourceforge/nagios/nagios-3.2.3.tar.gz  
  
# wget http://prdownloads.sourceforge.net/sourceforge/nagiosplug/nagios-plugins-1.4.11.tar.gz
```

Extraer NAGIOS

```
# tar xzf nagios-3.2.3.tar.gz  
  
# cd nagios-3.2.3
```

Ejecutar el script de configuración NAGIOS con el nombre del grupo creado y compilar:

```
# ./configure --with-command-group=nagcmd  
  
# make all
```

Instalar

```
# make install

# make install-init

# make install-config

# make install-commandmode
```

Los archivos de configuración se encuentran en:

```
'/usr/local/nagios/etc'
/usr/local/nagios/etc# ls
cgi.cfg  conf.d/  htpasswd.users  nagios.cfg
objects/  resource.cfg
```

Edición de 'objects/contacts.cfg' para configurar el email en el que se recibirán los avisos de NAGIOS

```
define contact{
    contact_name    nagiosadmin
    use              generic-contact
    alias           cesans
    email           me@cesans.net
}
```

ARCHIVOS DE CONFIGURACIÓN EN NAGIOS

Archivos de configuración principal – nagios.cfg

nagios.cfg Este es el principal archivo de configuración de NAGIOS ya que dentro de éste se encuentran las directivas y variables que afectan directamente al comportamiento del demonio NAGIOS en el sistema ya que es leído también por los archivos CGI's.

Archivos de recursos – timeperiods.cfg-,htpasswd.users

Estos ficheros van a servir para configuraciones de usuarios, claves y controlar los accesos permitidos hacia la interfaz Web, también sirven para gestionar accesos programados hacia la aplicación Web.

Archivos de definición de objetos –hosts.cfg-, -services.cfg-, -contacts.cfg-, - commands.cfg

Los archivos de definición de objetos son utilizados para definir los host, contactos, grupos de contacto, grupos de notificaciones, tipos de notificaciones, comandos para monitorear, etc. En estos archivos se definirá el Qué y el Cómo NAGIOS va a monitorear.

Archivos de configuración cgi – cgi.cfg-

cgi.cfg Archivo de configuración para los CGIs que usa el interface web de NAGIOS. Aquí se tienen configuraciones interesantes como donde localizar el archivo

principal de configuración de NAGIOS, nagios.cfg y la parametrización de accesos a las opciones que brinda la interface de acuerdo al usuario que accede.

Edición de 'objects/contacts.cfg' para configurar el email en el que se recibirán los avisos de NAGIOS

Instalación del archivo de configuración en el directorio conf.d de Apache

```
# make install-webconf
```

Crear una cuenta nagiosadmin para entrar a la interfaz web.

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

Reiniciar el servidor Apache para que los cambios tomen efecto:

```
# /etc/init.d/apache2 reload
```

Instalación de PLUGINS de NAGIOS

```
# cd ~/Downloads  
  
# tar xzf nagios-plugins-1.4.11.tar.gz  
  
# cd nagios-plugins-1-4-11  
  
# ./configure --with-nagios-user=nagios --with-nagios-group=nagios  
  
# make  
  
# make install
```

Configuración de arranque al inicio

```
# ln -s /etc/init.d/nagios /etc/rcS.d/S99nagios
```

Comprobación de archivos de configuración

```
# /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg

Total Warnings: 0
Total Errors: 0

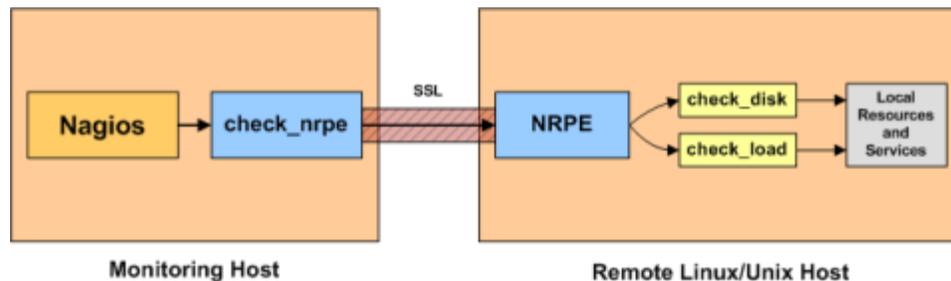
Things look okay - No serious problems were detected during the pre-flight check
```

Si todo ha ido bien, iniciar NAGIOS:

```
# /etc/init.d/nagios start
```

INSTALACION DE NRPE (NAGIOS REMOTE PLUGIN EXECUTOR)

NRPE se ejecuta en el host y hace uso de otros plugins que miden parámetros del sistema



INSTALAR NPPE EN EL HOST

Descargar las librerías necesarias

```
# apt-get install openssl libssl-dev
```

Crear el usuario nagios

```
# useradd nagios
# passwd nagios
```

Descargar los plugins de nagios

```
# wget http://prdownloads.sourceforge.net/sourceforge/nagiosplug/nagios-plugins-1.4.11.tar.gz
# tar xzf nagios-plugins-1.4.11.tar.gz
# cd nagios-plugins-1.4.11
```

Instalar los plugins de nagios y hacer que el usuario nagios sea propietario de los archivos correspondientes

```
# ./configure
# make
# make install

# chown nagios.nagios /usr/local/nagios
# chown -R nagios.nagios /usr/local/nagios/libexec
```

Instalar el demonio xinetd (similar a inetd)

```
# apt-get install xinetd
```

Descargar e instalar NRPE

```
# wget http://downloads.sourceforge.net/project/nagios/nrpe-2.x/nrpe-2.14/nrpe-2.14.tar.gz
# tar xzf nrpe-2.14.tar.gz
# cd nrpe-2.14
```

```
# ./configure
# make all
# make install-plugin
# make install-daemon
# make install-daemon-config
```

Editar el archivo /etc/xinetd.d/nrpe

```
only_from ip_servidor
```

Añadir al archivo /etc/services

```
nrpe 5666/tcp #nrpe
```

Y por último iniciar xinetd

```
# service xinetd restart
```

INSTALAR CHECK_NRPE EN EL MONITOR

```
# wget http://downloads.sourceforge.net/project/nagios/nrpe-2.x/nrpe-2.14/nrpe-2.14.tar.gz
# tar xzf nrpe-2.14.tar.gz
# cd nrpe-2.14.tar.gz
```

Añadir al archivo /etc/services

```
# ./configure
# make all
# make install-plugin
```

Y ya es posible probar que funciona

```
# /usr/local/nagios/libexec/check_nrpe -H ip_host_monitorizado  
NRPE v2.13
```

DEFINIR SERVICIOS CON NRPE

Para usar NRPE añadimos un comando en `/usr/local/nagios/etc/objects/commands.cfg`

```
define command{  
    command_name      check_nrpe  
    command_line      $USER1$/check_nrpe -H $HOSTADDRESS$ -c $ARG1$  
}
```

Ahora es posible utilizar NRPE para monitorizar servicios en equipos remotos

MONITORIZAR HOSTS LINUX: NRPE

Para monitorizar el número de usuarios

```
define service{  
  
    use                generic-service  
    host_name          remotehost  
    service_description CPU Load  
    check_command      check_nrpe!check_users  
  
}
```

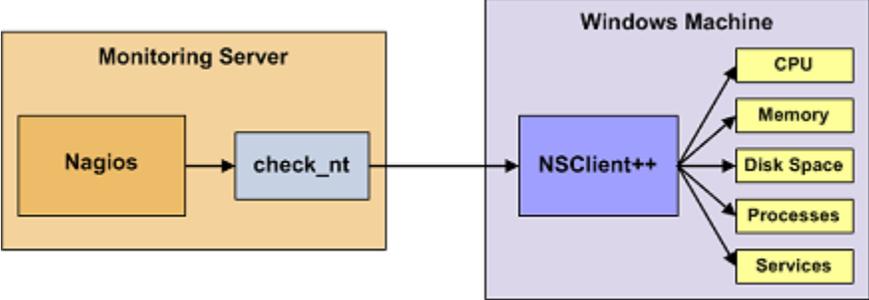
Y en el equipo remote host es posible configurar `check_load` editando `/usr/local/etc/nrpe.cfg`

```
command[check_users]=/usr/local/nagios/libexec/check_users -w 10 -c 20
```

De este modo entrará en estado warning si hay 10 usuarios y critic cuando haya 20.

MONITORIZAR HOSTS WINDOWS

En el caso de Windows se utiliza check_nt y NSClient++



INSTALACION DE CACTI

Serán necesario los siguientes servicios en cual CACTI necesitará para su funcionamiento:

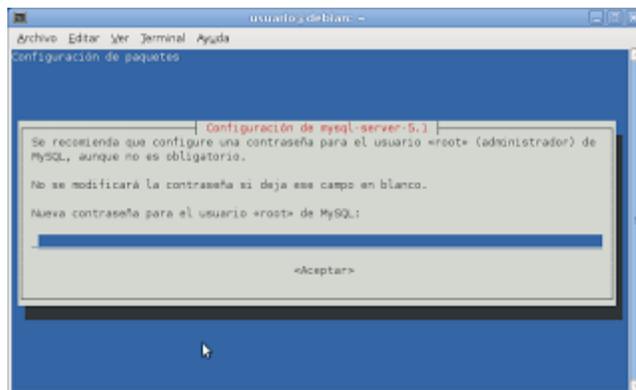
- Apache
- MySQL
- PHP

Para ello, escribimos el siguiente comando en nuestro terminal:

`aptitude install apache2 mysql-server php5 php5-gd php5-mysql`



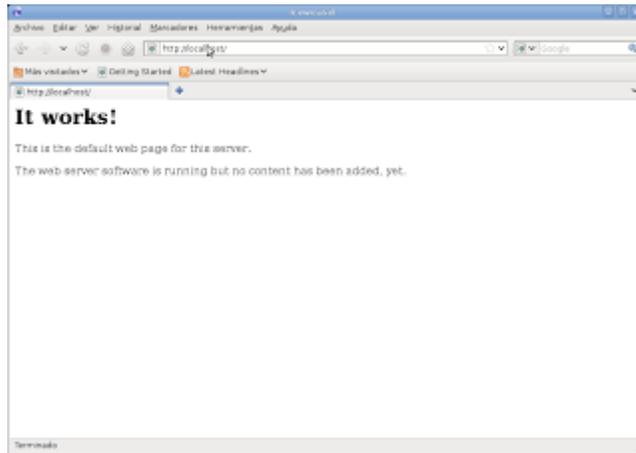
NOTA: Durante la instalación de los paquetes, en el paso de MySQL, indicará que introduzcamos una contraseña para el administrador, la introducimos y seguimos.



Se puede comprobar que está todo correctamente funcionando de la siguiente manera:

Apache

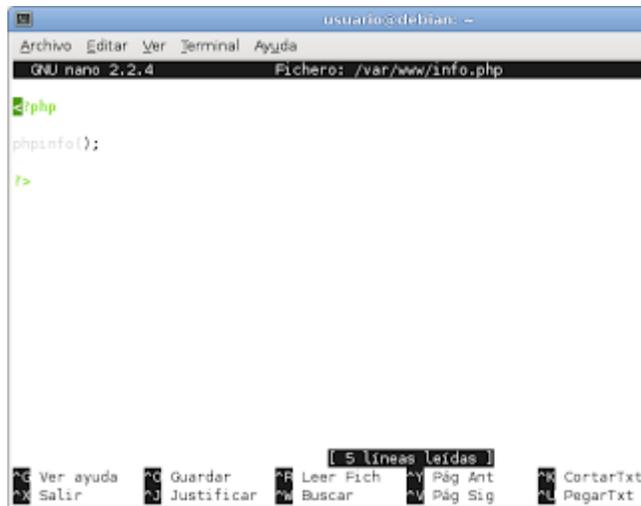
Escribiremos "localhost" en nuestro navegador y veremos el siguiente mensaje:



MySQL y PHP

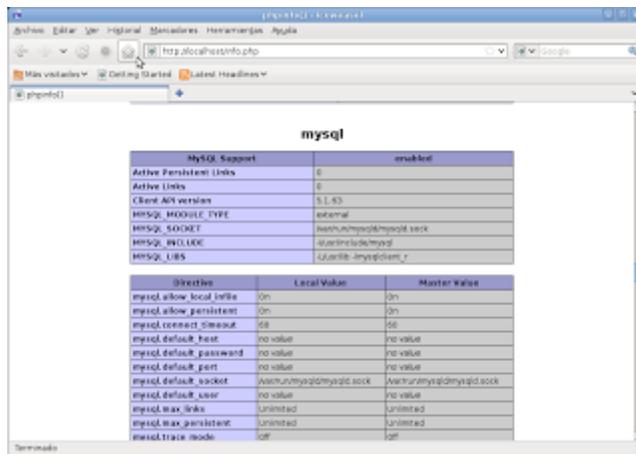
Para comprobar que MySQL y PHP trabajan correctamente entre sí y con el servidor web Apache, creamos el siguiente archivo y su contenido en "/var/www/info.php":





```
usuario@debian: ~  
Archivo Editar Ver Terminal Ayuda  
GNU nano 2.2.4 Fichero: /var/www/info.php  
  
#!php  
phpinfo();  
  
!>  
  
[ 5 líneas leídas ]  
Ver ayuda Guardar Leer Fich Páq Ant CortarTxt  
Salir Justificar Buscar Páq Sig PegarTxt
```

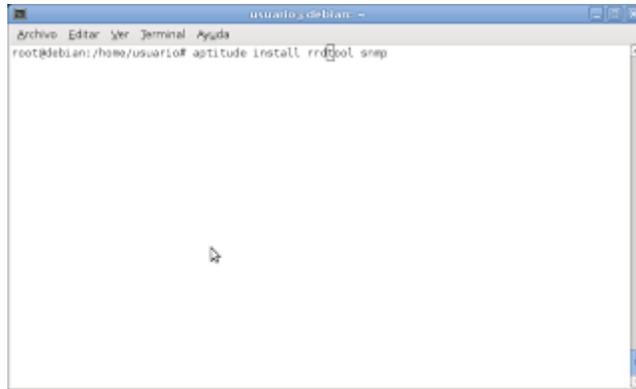
Escribimos en nuestro navegador "localhost/info.php" y buscamos entre los módulos instalados, el módulo de MySQL:



Ya terminada con la instalación de los paquetes, antes de la instalación de CACTI, quedaría instalar varios paquetes necesarios, uno de ellos son RRDTOOL y el protocolo SNMP:

Para su instalación, escribimos en nuestra Shell:

```
aptitude install rrdtool snmp
```



```
usuario@debian: ~  
Archivo Editor Ver Terminal Ayuda  
root@debian:/home/usuario# aptitude install rrdtool snmp
```

Esta instalación de librerías, son necesaria para CACTI para que pueda dibujar las gráficas con los datos obtenidos.



```
usuario@debian: ~  
Archivo Editor Ver Terminal Ayuda  
root@debian:/home/usuario# aptitude install libgng12-dev libg2-aps-dev libjpeg2-dev
```

Instalación de CACTI

Ya tendremos todo listo para empezar con la instalación de CACTI!

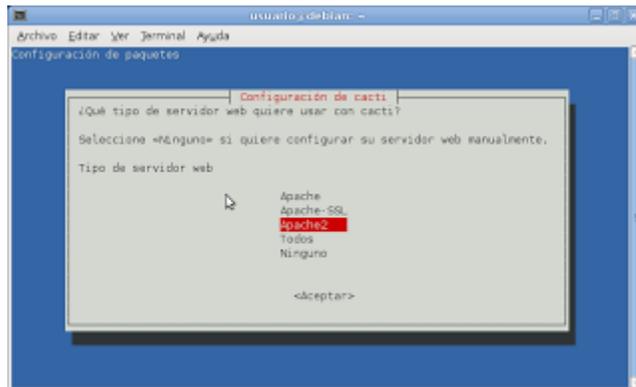
Para comenzar su instalación, escribimos el siguiente comando:

```
aptitude install cacti
```

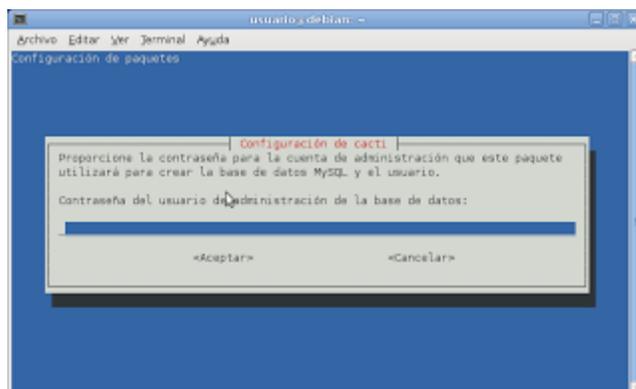


Durante el proceso de instalación, seleccionamos:

1) Servidor Web: Apache 2

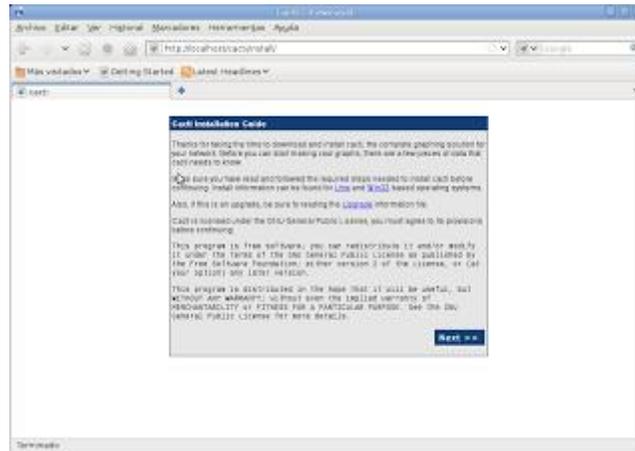


2) MySQL: Indicaremos que deseamos configurar nuestra BD para CACTI e indicaremos la contraseña de administrador y una para él la BD de CACTI.



Para ver que todo está correctamente en funcionamiento, escribimos en nuestro navegador para acceder:

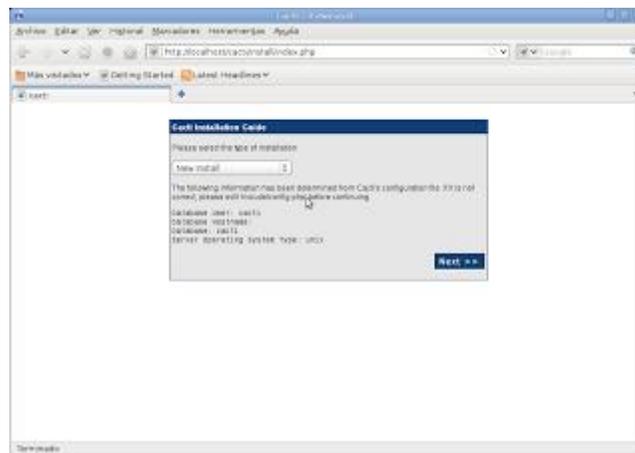
"localhost/cacti"



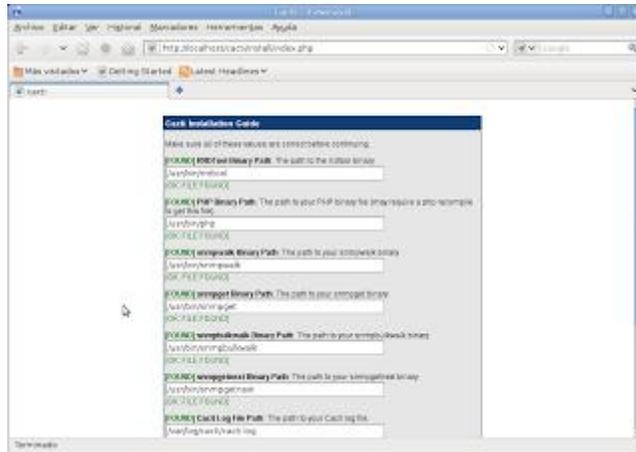
Nos indicará el proceso de instalación de CACTI en nuestro PC.

Proceso de Instalación

En la primera ventana indica si la instalación es "Nueva" o es una "Actualización", en nuestro caso será una instalación limpia de 0.



En la siguiente ventana, vemos si cumplimos los requisitos instalados para que CACTI funcione correctamente, si está todo verde podremos seguir!



NOTA: Abajo podremos indicar la versión de RRDTOOL y SNMP que queremos que use CACTI.

Por último, CACTI indicará que introduzcamos el usuario y contraseña por defecto, es:

Usuario: admin

Pass: admin

Una vez introducido, indicará que introduzcamos una nueva clave por seguridad.

Y listo! Ya tendremos instalado nuestro sistema de monitorización CACTI!

