



Universidad del Azuay

Facultad de Administración

Escuela de Ingeniería de Sistemas

Monitoreo de Red Implementando Nagios

Trabajo de graduación previo a la obtención del título de  
Ingeniero de Sistemas

Autores:

Ma. Antonia Astudillo Pesántez

José Luis Pesántez Manzano

Director:

Ing. Pablo Esquivel León

Cuenca, Ecuador

2006

Las ideas expuestas en el siguiente  
documento, son de exclusiva  
responsabilidad de los autores.

Antonia Astudillo

José Pesántez

## **DEDICATORIA**

Este trabajo lo dedicamos a nuestros padres que nos han apoyado incondicionalmente en cada uno de nuestros proyectos de vida y junto con nosotros se han esforzado para verlos realizados.

## INDICE DE CONTENIDOS

<b>Dedicatoria</b>	<b>ii</b>
<b>Índice de contenidos</b>	<b>iii</b>
<b>Resumen</b>	<b>v</b>
<b>Abstract</b>	<b>vi</b>
<b>Introducción</b>	<b>1</b>
<b>Capítulo I: Consideraciones Básicas</b>	<b>2</b>
<b>1.1 Aspectos generales sobre Nagios</b>	<b>2</b>
<b>Capítulo II: Instalación</b>	<b>4</b>
<b>2.1 Requerimientos de Nagios</b>	<b>4</b>
<b>2.2 Instalación de Nagios</b>	<b>4</b>
<b>Capítulo III: Configuración</b>	<b>6</b>
<b>3.1 Descripción de archivos de configuración</b>	<b>6</b>
<b>3.2 Configuración de archivos</b>	<b>7</b>
<b>3.3 Información de los archivos</b>	<b>17</b>
<b>3.4 Verificación de la configuración de Nagios</b>	<b>27</b>
<b>3.5 Determinación del estado y alcance de los host de red</b>	<b>30</b>
<b>3.6 Notificaciones</b>	<b>32</b>
<b>3.7 Períodos de tiempo</b>	<b>33</b>
<b>3.8 Trucos para la definición de objetos con plantillas base</b>	<b>35</b>
<b>3.9 Mejorando Nagios</b>	<b>37</b>
<b>Capítulo IV: Reportes</b>	<b>39</b>
<b>4.1 Guía de uso</b>	<b>39</b>
<b>4.2 Reportes gráficos</b>	<b>50</b>

<b>Conclusiones</b>	<b>70</b>
<b>Recomendaciones</b>	<b>71</b>
<b>Bibliografía</b>	<b>72</b>

## RESUMEN

Nagios es una herramienta que monitorea tanto los equipos como los servicios de una red. Esto lo hace casi en tiempo real. Su función principal es informar sobre el estado de estos, cuando un servicio o host está abajo o crítico envía una notificación de alerta a la(s) personas encargadas.

Para el monitoreo de una red se deben especificar los equipos y servicios a monitorear, así como el tiempo en el que se debe realizar la notificación de su estado. Estas especificaciones se realizan en los archivos que vienen incluidos en Nagios.

A continuación mencionamos los más importantes:

- Nagios.cfg *(principal archivo de configuración)*
- Cgi.cfg *(configuración de cgi's para ambiente web)*
- Hosts.cfg *(definición de los equipos a monitorear)*
- Hostgroups.cfg *(definición de un grupo de hosts a los que pertenecerán los equipos definidos en host.cfg)*
- Contacts.cfg *(contacto al que se le notifica cualquier problema con un equipo)*
- Contactgroups.cfg *(definición de un grupo de contactos al que pertenecerá cada contacto definido en contacts.cfg)*
- Services.cfg *(se definen los servicios que se monitorearan en cada equipo)*

Algunos de los servicios que nos presta Nagios son:

- Monitoreo de servicios de red (SMTP, POP3, HTTP, PING)
- Monitoreo de los recursos de un host (número de procesos, uso del disco, número de usuarios)
- Notificaciones a contactos cuando un servicio o un host tenga problemas (e-mail, pager o definido por el usuario)
- Interfaz web opcional con gráficas que describen cada uno de los estados en los que está o ha estado un servicio o equipo. Además un historial de notificación y problemas.

## ABSTRACT

Nagios is a tool that controls the hosts and network services. It does that almost in the real. It's main function is to inform about how they are working when a service or host are down it send the alert to people who are in charge.

For a network control we should specify the host and services to control, as well as the time in which should be carried out in the notification of their state.

This specifications can be done on a file that comes in Nagios. The following are the most important.

- Nagios.cfg                    (*main file configuration*)
- Cgi.cfg                        (*CGI's configuration for web interphace*)
- Hosts.cfg                     (*hosts definitions*)
- Hostgroups.cfg               (*hostgroups definition that Hill belong to host on host.cfg*)
- Contacts.cfg                 (*contact where any problem with the host will be known* )
- Contactgroups.cfg           (*group of contacts definition that will belong to each defined in contacts.cfg*)
- Services.cfg                 (*the services control are defined in each equipment*)

Some of the services of Nagios:

- Network services control (SMTP, POP3, HTTP, PING)
- Host resources control (number of process, free disk, number of users)
- Informs a contact when a service or host has problem.
- Web interphace optional with graphics that describe each one of the stages of a service or equipment. Also a history of notification and problems.

## INTRODUCCION

En la actualidad existe una creciente necesidad de comunicación y transmisión de datos, cuya infraestructura básica puede ser tanto una red de área local LAN o una red de área extensa WAN según las necesidades del medio en que se implementen. En cualquiera de estos tipos de redes nos podemos encontrar con variedad de equipos para su funcionamiento, los cuales van desde las PC's hasta dispositivos más específicos de una red como lo es un switch. . Estos tipos de redes pueden ser medianas (50 PC's) o grandes (200 PC's en adelante) y el inadecuado monitoreo de las mismas nos puede llevar a perder un tiempo valioso. ¿Cuántas veces nos hemos encontrado horas y horas tratando de localizar donde falla la red y no damos con ella?

De esta necesidad nace nuestro interés por investigar e implementar Nagios, una herramienta de monitoreo de redes poco conocida. Esta trabaja en casi tiempo real, y nos brinda reportes en intervalos de tiempo que nosotros podemos definir según nuestras necesidades, así podemos detectar cualquier problema que se presente ahorrándonos tiempo y por lo tanto dinero.



# CAPITULO I

## 1. Consideraciones básicas

### 1.1 Aspectos generales sobre Nagios

Nagios es una aplicación desarrollada por Ethan Galstad bajo la GNU General Public License. Esto trae los permisos legales para la copia, distribución o modificación de Nagios bajo ciertas condiciones.

Nagios es una herramienta para realizar el monitoreo de máquinas y servicios dentro de una red. La función de esta es informar sobre los problemas que pueden presentarse en la red y en los servicios que esta brinda.

Esta aplicación nos permite monitorizar todo tipo de equipos que uno especifica, estos pueden ser servidores, dispositivos de red y otros, en tiempos especificados de la misma manera.

Los tiempos, los equipos, los servicios que van a ser monitoreados se los configura dentro de los archivos que forman parte de esta aplicación, los mismos que en los siguientes capítulos se detallarán a fondo.

Para acceder a Nagios se necesita de un navegador de Internet, en este se mostrarán varias pantallas que nos indicaran y nos ayudarán a comprobar el estado de los sistemas, detalles de los servidores, etc., todo esto por medio de gráficos, informes y listados.

Algunos de los servicios que nos presta Nagios son:

- Monitoreo de servicios de red (SMTP, POP3, HTTP, PING)
- Monitoreo de los recursos de un host (número de procesos, uso del disco, número de usuarios)
- Notificaciones a contactos cuando un servicio o un host tenga problemas (e-mail, pager o definido por el usuario)
- Interfaz web opcional con gráficas que describen cada uno de los estados en los que está o ha estado un servicio o equipo. Además un historial de notificación y problemas.

Nagios ya cuenta con su nueva versión 2.0, que está aún en desarrollo por lo cual no es muy estable pero incluye algunas mejoras.

Cabe recalcar que Nagios ha ido mejorando de la misma manera que Linux, gracias a la colaboración de varias personas que han aportado con nuevas ideas y modificaciones para mejorarlo.

## CAPITULO II

### 2. Instalación

#### 2.1 Requerimientos de Nagios

- Cualquier máquina que tenga Linux o alguna variante de Unix
- Un compilador de C.

De no desear se puede omitir el uso de los CGI's incluidos en Nagios. Sin embargo si se decide usarlos se requerirá instalar el siguiente software.

- Un web Server (de preferencia Apache)
- Thomas Boutell's gd library versión 1.6.3 o superior, que se requiere para los CGI's del status map y trends.

En este caso nosotros estamos utilizando la distribución llamada Debian, que es muy estable y segura, y al igual que Nagios es GNU (General Public License.).

#### 2.2 Instalación de Nagios

Una vez instalado el Sistema Operativo Debian, procedemos a instalar los paquetes y sus dependencias de los cuales nagios depende para su correcto funcionamiento y configuración.

```
linux# apt-get install nagios-text nagios-plugins apache apache-common
```

En lo posterior se nos preguntará por:

- Tipo de servidor web: Apache
- Nagios web administration password: el login por defecto es *nagiosadmin* y nosotros escogeremos el password.
- Enable Nagios external command interface on web?: yes

Apache debe estar instalado correctamente en la máquina en la que corre Nagios y debe ser capaz de ejecutar CGI's, (estos sirven principalmente para la autenticación).

Cuando se crea o edita algún archivo de configuración debemos tener en cuenta lo siguiente:

- Las líneas que comienzan con “#” son comentarios y no serán procesadas.
- Los nombres de variables deben comenzar al inicio de la línea, los espacios en blanco son permitidos antes del nombre.
- Los nombres de las variables son sensibles a las mayúsculas.

Los principales ficheros los encontraremos bajo /etc/nagios y los que vamos a configurar son:

- Nagios.cfg (*principal archivo de configuración*)
- Cgi.cfg
- Hosts.cfg
- Hostgroups.cfg
- Contacts.cfg
- Contactgroups.cfg
- Miscommands.cfg
- Services.cfg

El resto de los ficheros no serán modificados.

## CAPITULO III

### 3. Configuración

#### 3.1 Descripción de archivos de configuración

A continuación indicaremos la función de cada uno de los archivos de Nagios.

##### **Nagios.cfg**

En este archivo se define la ubicación física de todos los archivos configurables que Nagios utiliza. Contiene varias directivas que pueden modificar la operación de Nagios. Este archivo de configuración es leído tanto por los procesos de Nagios como por los CGI's. Este es el primer archivo de configuración que se debe editar.

##### **Cgi.cfg**

Este archivo define las autorizaciones de acceso a Nagios.

##### **Hosts.cfg**

Este archivo incluye todas las máquinas a ser monitoreadas de acuerdo a su dirección IP y se le puede asignar un nombre para reconocerla fácilmente denominado Alias.

##### **Hostgroups.cfg**

Se define grupos de hosts, en cada uno de estos grupos se puede asociar según su función, ubicación, etc.

Cada hostgroup debe tener por lo menos un contactgroup.

##### **Contacts.cfg**

Se definen las personas a las cuales se les notificará en caso de cualquier problema que se haya presentado en la red o en algún equipo.

##### **Contactgroups.cfg**

Cada una de las personas que serán notificadas de los problemas debe pertenecer a un grupo, estos grupos se pueden clasificar de acuerdo a su función, ubicación, etc.

## Services.cfg

Es el fichero de configuración más importante ya que este va a contener todos los servicios que vamos a monitorizar, los cuales pueden ser PING, HTTP, FTP, entre otros.

## 3.2 Configuración de archivos

### nagios.cfg

log\_file=/var/log/nagios/nagios.log (especifica donde nagios podría crear el archivo principal del log)

cfg\_file=/etc/nagios/checkcommands.cfg

cfg\_file=/etc/nagios/misccommands.cfg

cfg\_file=/etc/nagios/contactgroups.cfg

cfg\_file=/etc/nagios/contacts.cfg

cfg\_file=/etc/nagios/dependencies.cfg

cfg\_file=/etc/nagios/escalations.cfg

cfg\_file=/etc/nagios/hostsgroups.cfg

cfg\_file=/etc/nagios/hosts.cfg

cfg\_file=/etc/nagios/services

(especificar el archivo de configuración de objetos que Nagios podría usar para monitorear)

cfg\_file=/etc/nagios/timeperiods.cfg

Siendo los anteriores los principales. A continuación presentamos el resto de variables que generalmente no se modifican.

cfg\_dir=/etc/nagios-plugins/config/

resource\_file=/etc/nagios/resource.cfg

(para especificar un archivo de recurso opcional que puede contener definiciones de macro de usuario para guarda nombre de usuario, passwd, etc)

status\_file=/var/log/nagios/status.log (aquí se guardan los estados actuales de todos los servicios monitoreados)

nagios\_user=nagios (el nombre de usuario de Nagios)

nagios\_group=Nagios (el nombre de grupo que nagios va a usar)

check\_external\_commands=1 (aquí se determina si Nagios va o no a chequear el archivo de comandos para los comandos internos que puede ejecutar)

command\_check\_interval=-1 (período de tiempo para ejecutar el chequeo externo de comandos, **si se pone la s** luego del número significa **segundos**, **sin s** son **minutos**)

command\_file=/var/run/nagios/nagios.cmd (este es el archivo que Nagios revisa para verificar los comandos externos a procesar)

comment\_file=/var/log/nagios/comment.log (este archivo Nagios lo utilizará para guardar los comentarios de servicios y hosts)

downtime\_file=/var/log/nagios/downtime.log (este archivo Nagios lo utilizará para guardar el organizador de los servicios y hosts que estén caídos)

lock\_file=/var/log/nagios/nagios.lock (aquí se especifica la localización del archivo de seguridad que Nagios podría crear cuando está corriendo como un demonio)

temp\_file=/var/cache/nagios/nagios.tmp (archivo temporal creado cuando se esta actualizando comment data, status data, etc)

log\_rotation\_method=d (método de rotación que nagios podría usar para su archivo de log. Los valores son: **n=ninguno; h=c/hora; d=c/día; w=c/semana; m=c/mes**)

log\_archive\_path=/var/log/nagios/archives (se indica el directorio donde Nagios puede guardar los archivos log que han rotado)

use\_syslog=1 (esta variable determina si los mensajes son anotados en el syslog del local host)

log\_notifications=1 (esta variable determina si o no los mensajes son anotados (logueados))

log\_service\_retries=1 (esta variable determina si los reintentos de chequeo de servicios son o no anotados. Estos reintentos ocurren cuando un resultado de chequeo de servicios es un estado no ok, con esto se configura para que se reintente el chequeo de servicio más de una vez antes de responder a un error)

log\_host\_retries=1 (esta variable determina si el reintento de chequeo de host es anotado)

log\_event\_handlers=1 (esta variable determina si el manejador de eventos de servicios y hosts ha sido anotado o logueado)

log\_initial\_states=0 (esta variable determina si Nagios va a forzar o no a todos los estados de servicios y hosts iniciales a ser anotados incluso si es que ellos resultan en un estado OK)



log_external_commands=1	(esta variable determina si Nagios va o no a anotar los comandos externos que son recibidos desde el archivo de comandos externos)
log_passive_service_checks=1	(esta variable determina si Nagios va o no a anotar el chequeo de los servicios pasivos que recibe desde el archivo de comandos externos)
inter_check_delay_method=s	(esta opción permite que el control de chequeo de servicios sea iniciado en la cola de eventos. Las opciones son: <b>n=no usa retardo; d=retraso 1s; s=retraso calculado inteligente</b> )
service_interleave_factor=s	(esta variable determina como el chequeo de servicio está entrelazado. Sus opciones son: <b>x= &gt;=1; s= entrelazado inteligente</b> )
max_concurrent_checks=0	(esta opción permite especificar el número máximo de chequeo de servicios que pueden correr en paralelo en un intervalo de tiempo)
service_reaper_frequency=10	(esta opción permite el control de la frecuencia en segundos del servicio recolector de eventos)
sleep_time=1	(este es el número de segundo que nagios va a dormir antes de chequear el siguiente servicio en la cola del organizador debe ejecutarse)
service_check_timeout=60	(es el máximo número de segundos que Nagios va a permitir que corra el chequeo de servicios, si el chequeo excede de este

	límite va a ser matado y retorna un estado crítico)
host_check_timeout=30	(es el máximo número de segundos que Nagios va a permitir que corra el chequeo de hosts, si el chequeo excede de este límite va a ser matado y retorna un estado crítico y se asume el estado del host abajo)
event_handler_timeout=30	(máximo número de segundos que Nagios va a permitir que el manejador de eventos corra, si un evento excede este tiempo el evento será matado y un warning será anotado)
notification_timeout=30	(máximo número de segundos que Nagios permitirá que los comandos de notificación corran, si excede este tiempo será matado y un warning será anotado)
ocsp_timeout=5	(máximo número de segundos que Nagios permitirá que un comando de servicio de procesador obsesivo compulsivo corra si excede este tiempo será matado y un warning será anotado)
perfdata_timeout=5	(máximo número de segundos que Nagios permitirá que corra un comando de datos de procesador de rendimiento de host o el comando de rendimiento de datos de rendimiento del procesador corra, si excede este tiempo será matado y un warning será anotado)
retain_state_information=1	(esta opción determina se Nagios va o no a retener el estado de información de los hosts y servicios entre programas reiniciados)

state\_retention\_file=/var/cache/nagios/status.sav  
(este archive Nagios utilizará para guardar la información del estado de los servicios y hosts antes de ser apagados)

retention\_update\_interval=60  
(aquí se configura cuan seguido Nagios va a guardar automáticamente los datos de retención durante su operación normal)

use\_retained\_program\_state=0  
(aquí se determina si Nagios va o no a poner las variables de estado de programas basado en los valores guardados en el archivo de retención)

interval\_length=60  
(este es el número de segundos por unidad de intervalo usado para cronometrar la cola del organizador, renotificaciones, etc)

use\_agressive\_host\_checking=0  
(al deshabilitar esta opción Nagios tomará algunas decisiones inteligentes y chequeara los hosts)

execute\_service\_checks=1  
(aquí se determina si Nagios va o no ejecutar el servicio de chequeo cuando inicia o se reinicia)

accept\_passive\_service\_checks=1  
(aquí se determina si Nagios va o no a aceptar el chequeo pasivo de servicios cuando inicia o se reinicia)

enable\_notifications=1  
(aquí se determina si Nagios va a enviar o no notificaciones cuando es iniciado o reiniciado)

enable\_event\_handlers=1  
(aquí se determina si Nagios va o no a correr el

	manejador de eventos cuando inicia o se reinicia)
process_performance_data=0	(este valor determina si Nagios procesará el chequeo de hosts y servicios mediante rendimiento de datos)
obsess_over_services=0	(esta opción es usada para la ejecución del monitoreo distribuido)
check_for_orphaned_services=0	(esta opción permite que se tenga o no disponible el chequeo para los servicios huérfanos)
check_service_freshness=1	esta opción determina si Nagios periódicamente chequeará o no las novedades en el chequeo de los servicios)
freshness_check_interval=60	esta determina cuán seguido Nagios periódicamente chequeará las novedades de los resultados del chequeo de servicios)
aggregate_status_updates=1	esta opción determina si Nagios va o no a utilizar el ultimo estado de monitoreo de los hosts, servicios, etc.
status_update_interval=15	cuan seguido en segundos Nagios va a actualizar el estado de los datos en el archivo de estados)
enable_flap_detection=0	(esta opción determina si Nagios va a intentar detectar hosts y servicios que pueden estar inestables. Esto ocurre cuando un host o servicio cambia entre estados muy frecuentemente. Cuando esto ocurre nagios suspende las notificaciones hasta que el servicio o host se vuelva más estable)

low_service_flap_threshold=5.0	(esta opción es usada para poner el límite inferior para la detección de servicios inestables)
high_service_flap_thresold=20.0	(esta opción es usada para poner el límite superior para la detección de servicios inestables)
low_host_flap_thresold=5.0	(esta opción es usada para poner el límite inferior para la detección de hosts inestables)
high_host_flap_thresold=20.0	(esta opción es usada para poner el límite inferior para la detección de hosts inestables)
date_format=us	(esta opción permite especificar que tipo de formato se podría usar en la interface web: Opciones: <b>us, euro, iso8601, strict-iso8601</b> )
illegal_object_name_chars=~!\$%^&* ' "<>?,()=	(esta opción permite especificar que caracteres no pueden se usados en nombres de hosts, descripción de servicios o nombres de otros tipos de objetos)
illegal_macro_output_chars=~\$& ' "<>	(esta opción permite especificar los caracteres ilegales que podrían ser sacados de los macros antes de ser usados en notificaciones, manejadores de eventos y otros comandos)
admin_email=nagios	(esta es la dirección mail para el administrador de la máquina local)
admin_pager=pagenagios	(este es el número de beeper para el

administrador de la máquina local)

## **cgi.cfg**

authorized\_for\_system\_information=nagiosadmin

(es la lista de nombres de usuarios autenticados quienes pueden ver los procesos e información del sistema en los cgi's)

authorized\_for\_configuration\_information=nagiosadmin

(lista de nombres de usuarios autenticados quienes pueden ver la información de configuración en el cgi)

authorized\_for\_system\_commands=nagiosadmin

(lista de nombres de usuarios autenticados quienes pueden emitir comandos de procesos y sistemas vía cgi)

authorized\_for\_all\_services=nagiosadmin

(lista de nombres de usuarios autenticados quienes pueden ver el estado y la información de configuración de todos los servicios)

authorized\_for\_all\_hosts=nagiosadmin

(lista de nombres de usuarios autenticados quienes pueden ver el estado y la información de configuración de todos los hosts)

authorized\_for\_all\_service\_commands=nagiosadmin

(lista de nombres de usuarios autenticados quienes pueden emitir comandos para todos los servicios vía cgi)

authorized\_for\_all\_host\_commands=nagiosadmin

(lista de nombres de usuarios autenticados quienes pueden emitir comandos para todos los hosts vía cgi)

Siendo estos los principales. A continuación presentamos los que no se necesitan modificar.

main\_config\_file=/etc/nagios/nagios.cfg

(especifica la localización del archivo principal de configuración)

physical\_html\_path=/usr/share/nagios/htdocs

(este es el path físico donde los archivos html para Nagios son mantenidos en su servidor)

url\_html\_path=/Nagios

(cuando accesa a Nagios vía navegador web se pone la dirección <http://localhost/nagios/>, el valor de esta variable debería ser /nagios)

show\_context\_help=0

nagios\_check\_command=/usr/lib/nagios/plugins/check\_nagios/var/log/nagios/status.log 5 'nagios'

(este es un comando opcional que los cgi's pueden usar para chequear el estado de los procesos de Nagios)

use\_authentication=1

(esta opción controla si Nagios va a usar la funcionalidad de autenticación y autorización cuando determina qué comandos e información tienen acceso los usuarios)

default\_statusmap\_layout=5

(esta opción permite especificar el método de

diseño usado por el statusmap cgi)

default\_statuswrl\_layout=4

(esta opción permite especificar el método de diseño usado por el statuswrl cgi)

ping\_syntax=/bin/ping -n -U -c 5 \$HOSTADDRESS\$

(esta opción determina que sintaxis debería ser usada cuando intentas hacer ping a un host desde la interface wap)

refresh\_rate=90

(esta opción permite especificar el número de segundos entre el refresco de páginas de status, statusmap y extinfo cgi's)

### 3.3 Información de los archivos

Una vez autenticado el usuario se mostrará la siguiente información.

CGI Data	Authenticated Contacts*	Other Authenticated Users*
Host Status Information	Si	No
Host Configuration Information	Si	No
Host History	Si	No
Host Notifications	Si	No
Host Commands	Si	No
Service Status Information	Si	No
Service Configuration Information	Si	No
Service History	Si	No
Service Notifications	Si	No
Service Commands	Si	No
All Configuration Information	No	No
System/Process Information	No	No
System/Process Commands	No	No

Contactos Autenticados, son los que tienen permisos para cada servicio de todos los contactos:

- Autorización para ver la información de estado de servicio.



- Autorización para ver la información de configuración de servicio.
- Autorización para ver el historial y las notificaciones del servicio
- Autorización para emitir comandos de servicio

Contactos Autenticados son los que tienen permisos para cada host de todos los contactos.

- Autorización para ver la información de estado de host.
- Autorización para ver la información de configuración de host.
- Autorización para ver el historial y las notificaciones del host
- Autorización para emitir comandos de host
- Autorización para ver la información de estado de todos los servicios del host
- Autorización para ver la información de configuración de todos los servicios del host
- Autorización para ver el historial y la información de notificación de todos los servicios del host
- Autorización para emitir comandos de todos los servicios del host

Es importante también ver que ninguno está autorizado para:

- Ver el archivo de log
- Ver la información de procesos de Nagios a través de CGIs
- Emitir comandos a través de CGIs
- Ver grupos de host, contactos, grupo de contactos, períodos de tiempo y comando a través de CGIs.

## **hosts.cfg**

### **(plantilla)**

```
define host{
name generic-host           Nombre del template del
                             host
notifications_enabled 1     Notificaciones activadas
event_handler_enabled 0     Host manejador de eventos
                             disponible
flap_detection_enabled 0    Detección de errores
                             inestables activada
process_perf_data 1        Datos de rendimiento de
                             procesos
```

retain_status_information 1	Información de retención de estados frente a reinicio de programas
retain_nonstatus_information 1	Información de retención sin estado frente a reinicio de programas
register 0	No registre esta definición
notification_interval 60	Minutos de espera, antes de notificar que el host ha caído
}	

## hosts.cfg

define host{ use generic-host	Nombre de la plantilla que se va a usar
host_name servidor	Nombre con el que se reconocerá al equipo
alias Equipo Debian con Nagios	Descripción pequeña del equipo
address 192.168.1.10	Dirección IP del equipo
check_command check-host-alive	Nombre del comando a utilizar
max_check_attempts 1	Número de revisiones antes de notificar error
notification_interval 1	Intervalo de tiempo de revisión en segundos
notification_period 24x7	Período en el que va a realizar la revisión
notification_options d,u,r	Opciones de notificación
}	

define host{ use generic-host	Nombre de la plantilla que se va a usar
host_name equipol	Nombre con el que se reconocerá al equipo
alias Equipol con Windows XP	Descripción pequeña del equipo
address 192.168.1.100	Dirección IP del equipo
check_command check-host-alive	Nombre del comando a utilizar
max_check_attempts 1	Número de revisiones antes de notificar error
notification_interval 1	Intervalo de tiempo de

notification_period 24x7	revisión en segundos Período en el que va a realizar la revisión
notification_options d,u,r	Opciones de notificación
}	
define host{	
use generic-host	Nombre de la plantilla que se va a usar
host_name equipo2	Nombre con el que se reconocerá al equipo
alias Equipo2 con Windows XP	Descripción pequeña del equipo
address 192.168.1.200	Dirección IP del equipo
check_command check-host-alive	Nombre del comando a utilizar
max_check_attempts 1	Número de revisiones antes de notificar error
notification_interval 1	Intervalo de tiempo de revisión en segundos
notification_period 24x7	Período en el que va a realizar la revisión
notification_options d,u,r	Opciones de notificación
}	

### **hostgroups.cfg**

```
define hostgroup{
hostgroup_name      Redes
alias               Red Windows
contact_groups      administrador
members             equipo1, equipo2, servidor
}
```

### **contacts.cfg**

```
define contact{
contact_name        nagios
alias               Nagios Admin
service_notification_period 24x7
host_notification_period 24x7
}
```

```

service_notification_options w,u,c,r
host_notification_options   d,u,r
service_notification_commands notify-by-email
host_notification_commands  host-notify-by-email
email                       admin-nagios@servidor.net
}

```

### **contactgroups.fcg**

```

define contactgroup{
contactgroup_name      administrador
alias                  Administrador Windows
members                nagios
}

```

### **services.cfg**

#### **(plantilla)**

```

define service{
name                  generic-service
active_checks_enabled 1
passive_checks_enabled 0
parallelize_check    1
obsses_over_service  1
check_freshness      0
notifications_enabled 0
event_handler_enabled 0
flap_detection_enabled 0
process_perf_data    1
retain_status_information 1
retain_nonstatus_information 1
register              0
}

```

```

define service{
use                  generic-service
host_name           equipol
service_description PING
is_volatile         0
}

```

```

check_period                24x7
max_check_attempts          4
normal_check_interval       5
retry_check_interval        1
contact_groups              administrador
notification_interval       10
notification_period         24x7
notification_options        c,r
check_command               check_ping!10.0,20%!50.0,60%
}

```

```

define service{
use                          generic-service
host_name                    equipol
service_description          Total Processes
is_volatile                  0
check_period                 24x7
max_check_attempts          3
normal_check_interval       5
retry_check_interval        2
contact_groups              administrador
notification_interval       10
notification_period         24x7
notification_options        w,u,c,r
check_command               check_procs!150!200!RSZDT
}

```

```

define service{
use                          generic-service
host_name                    equipol
service_description          Current Users
is_volatile                  0
check_period                 24x7
max_check_attempts          3
normal_check_interval       5
retry_check_interval        2
contact_groups              administrador
notification_interval       10
notification_period         24x7
notification_options        w,u,c,r
check_command               check_users!75!150
}

```

```
}
```

```
define service{  
  use                generic-service  
  host_name          equipo1  
  service_description HTTP  
  is_volatile        0  
  check_period       24x7  
  max_check_attempts 3  
  normal_check_interval 2  
  retry_check_interval 1  
  contact_groups     administrador  
  notification_interval 60  
  notification_period 24x7  
  notification_options c,r  
  check_command      check_http  
}
```

```
define service{  
  use                generic-service  
  host_name          equipo2  
  service_description PING  
  is_volatile        0  
  check_period       24x7  
  max_check_attempts 4  
  normal_check_interval 5  
  retry_check_interval 1  
  contact_groups     administrador  
  notification_interval 10  
  notification_period 24x7  
  notification_options c,r  
  check_command      check_ping!10.0,20%!50.0,60%  
}
```

```
define service{  
  use                generic-service  
  host_name          equipo2  
  service_description Total Processes  
  is_volatile        0  
  check_period       24x7  
  max_check_attempts 3
```

```

normal_check_interval    5
retry_check_interval     2
contact_groups           administrador
notification_interval    10
notification_period      24x7
notification_options     w,u,c,r
check_command            check_procs!150!200!RSZDT
}

```

```

define service{
use                generic-service
host_name          equipo2
service_description Current Users
is_volatile        0
check_period       24x7
max_check_attempts 3
normal_check_interval 5
retry_check_interval 2
contact_groups     administrador
notification_interval 10
notification_period 24x7
notification_options w,u,c,r
check_command      check_users!75!150
}

```

```

define service{
use                generic-service
host_name          equipo2
service_description HTTP
is_volatile        0
check_period       24x7
max_check_attempts 3
normal_check_interval 2
retry_check_interval 1
contact_groups     administrador
notification_interval 60
notification_period 24x7
notification_options c,r
check_command      check_http
}

```

```

define service{
use                generic-service
host_name          servidor
service_description PING
is_volatile        0
check_period       24x7
max_check_attempts 4
normal_check_interval 5
retry_check_interval 1
contact_groups     administrador
notification_interval 10
notification_period 24x7
notification_options c,r
check_command      check_ping!10.0,20%!50.0,60%
}

```

```

define service{
use                generic-service
host_name          servidor
service_description FTP
is_volatile        0
check_period       24x7
max_check_attempts 3
normal_check_interval 2
retry_check_interval 1
contact_groups     administrador
notification_interval 120
notification_period 24x7
notification_options w,u,c,r
check_command      check_ftp
}

```

```

define service{
use                generic-service
host_name          servidor
service_description Total Processes
is_volatile        0
check_period       24x7
max_check_attempts 3
normal_check_interval 5
retry_check_interval 2
}

```



```

contact_groups      administrador
notification_interval 10
notification_period 24x7
notification_options w,u,c,r
check_command       check_procs!150!200!RSZDT
}

```

```

define service{
use          generic-service
host_name    servidor
service_description Current Users
is_volatile  0
check_period 24x7
max_check_attempts 3
normal_check_interval 5
retry_check_interval 2
contact_groups administrador
notification_interval 10
notification_period 24x7
notification_options w,u,c,r
check_command check_users!75!150
}

```

```

define service{
use          generic-service
host_name    servidor
service_description /dev/hda2 Free Space
is_volatile  0
check_period 24x7
max_check_attempts 3
normal_check_interval 5
retry_check_interval 1
contact_groups administrador
notification_interval 10
notification_period 24x7
notification_options w,u,c,r
check_command check_disk!10%2!0%!/dev/hda2
}

```

### 3.4 Verificación de la configuración de Nagios

Una vez ingresada toda la información necesaria en los archivos de configuración, es hora de hacer un chequeo completo. Nagios corre automáticamente el “flight check” antes de iniciar el monitoreo, pero también tiene la opción de correrlo manualmente antes de intentar iniciar Nagios, para lo cual ejecutaremos la siguiente sentencia:

```
linux# nagios -v /etc/nagios.cfg
```

esta leerá todos los archivos de configuración y verificará que sean datos válidos.

Durante el “flight check ” Nagios verifica que todos los datos estén relacionados para la monitorización. Esta es la lista básica de los archivos que Nagios chequeará:

- Verifica que todos los contactos sean miembros de un grupo de contactos.
- Verifica que todos los contactos especificados en cada grupo de contactos sean válidos.
- Verifica que todos los hosts sean miembros de un hostgroup.
- Verifica que todos los hosts especificados en cada hostgroup sean válidos.
- Verifica que todos los hosts tengan un servicio asociado a él.
- Verifica que todos los comandos usados en el chequeo de servicio y host sean válidos.
- Verifica que todos los comandos usados en el manejador de eventos de servicio y host sean válidos.
- Verifica que todos los comandos usados en el servicio de contacto y notificación de host sean válidos.
- Verifica que todas las notificaciones de períodos de tiempo especificados para servicios, hosts y contactos sean válidos.
- Verifica que todos los chequeos de período de tiempo especificados para los servicios sean válidos.

Si es que encontró algún problema crítico Nagios le notificará con un warning o un error y va a dar la ubicación exacta del problema. Los mensajes de error generalmente muestran la línea del archivo de configuración que ocasionó el problema.

Si todo está correcto deberemos tener 0 errores y 0 warnings, en caso de tener algún warning no hay problema porque si funcionará.

Nagios 1.3

Copyright (c) 1999-2004 Ethan Galstad ([nagios@nagios.org](mailto:nagios@nagios.org))

Last Modified: 10-24-2004

License: GPL

Reading configuration data...

Runing pre-fligth check on condiguration data...

Checking services...

Checked 12 services.

Checking hosts...

Checked 3 hosts.

Checking host groups...

Checked 1 host groups.

Checking contacts...

Checked 1 contacts.

Checking contact groups...

Checked 1 contact groups.

Checking service scalations...

Checked 0 service scalations.

Checking host group scalations...

Checked 0 host group scalations.

Checking service dependencies...

Checked 0 service dependencies.

Checking host scalations...

Checked 0 host scalations.

Checking host dependencies...

Checked 0 host dependencies.

Checking commands...

Checked 104 commands.

Checking time periods...

Checked 4 time periods.

Checking for circular paths between hosts...

Checking for circular service execution dependencies...

Checking global event handlers...

Checking obsessive compulsive service processor command...

Checking misc settings...

Total Warnings: 0

Total Errors: 0

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

Ahora tenemos que arrancar el demonio, para lo cual ejecutamos la siguiente sentencia como root:

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

En algunas ocasiones es necesario reiniciar o detener el proceso, se va a indicar a continuación como realizarlo mediante comandos.

Para detener el proceso se ejecutará:

```
linux# /etc/init.d/nagios stop
```

Caso contrario para reiniciarlo se ejecutará

```
linux# /etc/init.d/nagios restart
```

Para recargar la configuración sin reiniciar ni detener podemos ejecutar la siguiente sentencia:

```
linux# /etc/init.d/nagios reload
```

Para tener acceso a Nagios mediante el navegador el servidor Apache debe estar funcionando correctamente y debemos crear el siguiente enlace simbólico

```
ln -s /usr/share/nagios/htdocs/ /var/www/nagios/
```

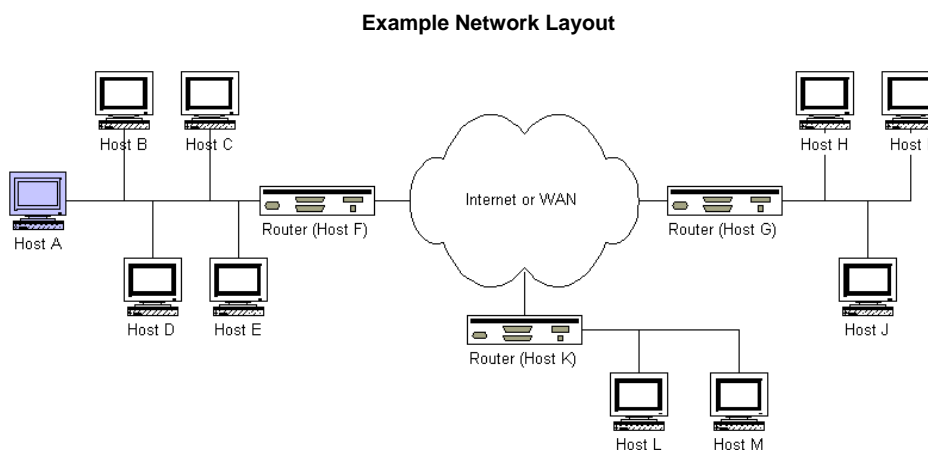
Luego abrimos nuestro navegador e introducimos la siguiente URL:  
<http://127.0.0.1/nagios/>

Si es que estamos accediendo desde otro computador deberemos introducir la IP de la máquina en que está corriendo Nagios y nos va a pedir el nombre de usuario y la contraseña que pusimos en la configuración.

### 3.5 Determinación del estado y alcance de los host de red

El principal propósito de Nagios es monitorear los servicios que están corriendo en los hosts y dispositivos de una red. Si un host o dispositivo de la red está abajo se asume que los servicios que en el corren también están abajo. Nagios reconoce este hecho e intenta chequear todo el conjunto cuando hay problemas con un servicio, sin embargo si el resultado de chequeo del servicio es un estado no OK Nagios intentará chequear y ver si el host en el que está corriendo el servicio está arriba. Generalmente se hace ping al host y se verifica si este envía una respuesta, si el comando de chequeo retorna un estado de no OK Nagios asume que hay un problema con el host. En esta situación Nagios silenciosamente pone todas las alarmas potenciales para los servicios que corren en el host y notifica al contacto indicado que el host esta abajo o inalcanzable. Si el comando de chequeo de host emite un estado OK Nagios asumirá que el host está arriba y no enviará alertas de comportamiento extraño.

#### Local host

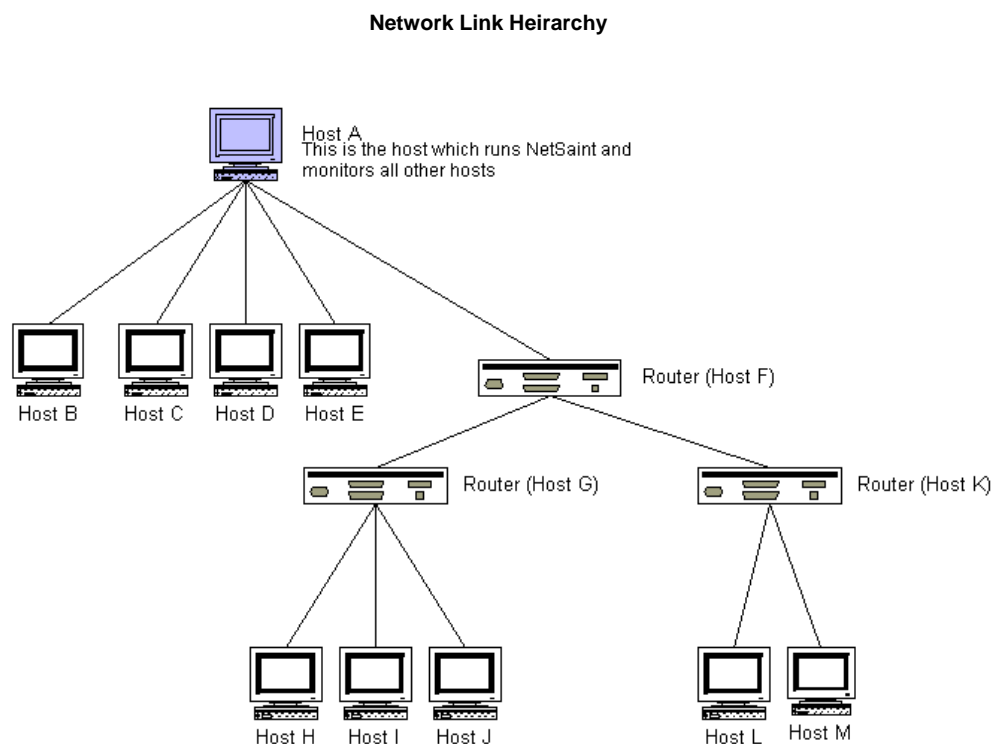


Los local host, son hosts que residen en el mismo segmento de red en el que está corriendo Nagios, como son los hosts B, C, D, E y F. La opción de parent\_hosts en la definición de un host local podría estar en blanco, al ser un local un host este no tiene dependencias o parientes.

Si Nagios necesita chequear y ver si un local host está arriba este simplemente corre el comando de chequeo de host para dicho host, si el comando devuelve un estado OK Nagios asume que el host está arriba, si el comando devuelve otro nivel de estado asume que el host está abajo.

### Hosts remotos

Son hosts que residen en un segmento diferente de red que el host que corre Nagios, estos son G, H, I, J, K, L y M, con relación a A. Para los hosts que están muy lejos podemos construir un árbol de dependencia de host que se muestra a continuación, donde el pariente del host H es el host G, el pariente del host G es el host F y el host F no tiene parientes, tomando en cuenta el segmento del host A.



El chequeo de los hosts remotos es más complicado que el chequeo de los hosts locales. Si Nagios no puede monitorear el servicio de un host remoto este necesita determinar si el host remoto está abajo o inalcanzable, la opción de parent\_host le permite a Nagios hacer esto.

Si el comando de chequeo para un host remoto retorna un estado no OK, Nagios tomará el árbol de dependencia hasta alcanzar el tope, al hacer esto Nagios puede determinar si un problema de servicio es el resultado de un host abajo o de un enlace de red caído..

### 3.6 Notificaciones

Se envían notificaciones de host y servicio cuando ocurren las siguientes instancias:

- Cuando ocurre un estado de cambio firme.
- Cuando un host o servicio permanece en un estado no OK y el tiempo especificado en la opción `notification_interval` en la definición de host o servicio ha pasado desde la última notificación que fue enviada.

Cada definición de servicio tiene un `contactgroup` opción que define que grupo de contacto recibe la notificación de un servicio en particular. Cada `contactgroup` puede contener uno o más contactos individuales. Cuando Nagios envía una notificación de servicios, este notificará a cada miembro de algún grupo de contacto especificado en la opción `contactgroup` en la definición de servicio.

Cada host puede pertenecer a uno o más `hostgroups`. Cuando Nagios envía una notificación de host, este notificará a los contactos que son miembros de todos los `contactgroups` que podrían ser notificados, contactos que son miembros de todos los `contactgroups` que podrían ser notificados por alguno o todos los `hostgroups` de que el host es miembro.

Existen varias vías para configurar a Nagios para que envíe notificaciones, se puede decidir cual se va a usar. Se tiene que instalar el software necesario y configurar los comandos de notificación en sus archivos de configuración antes de usarlos. A continuación presentamos unos de los posibles métodos:

- Email
- Pager
- SMS
- Ventana de Mensaje
- Yahoo, MSN
- Alertas de audio, etc...

## **Tipos de estado**

El estado actual de los servicios y hosts es determinado por dos componentes:

- El estado de servicio o host (OK, Warning, Up, Down, etc)
- Y El tipo de estado (Soft y Hard states)

El tipo de estados es una parte crucial del monitoreo lógico de Nagios, estos son usados para determinar cuando el manejador de eventos es ejecutado y cuando las notificaciones son enviadas.

Los estados soft ocurren cuando el resultado de un chequeo de host o servicio está en no OK y no ha sido chequeado el número de veces especificado en la opción `max_check_attempts` en la definición de host o servicio, a esto lo llamamos soft error state. Cuando un servicio o host se recupera de un soft error state esto es considerado un soft recovery.

Los estados hard ocurren cuando un chequeo de servicio resulta en un estado no OK y este ha sido (re)chequeado el número de veces especificado en la opción `max_check_attempts` en la definición del servicio. Esto es un hard error state. Cuando un servicio se recupera de un hard error state este es considerado un hard recovery.

Cuando un resultado de chequeo de servicio es un estado no OK y esto corresponde al host si está down o unreachable.

Los estados hard de un host ocurren cuando un chequeo de host resulta en un estado no OK y este ha sido (re)chequeado el número de veces especificado en la opción `max_check_attempts` en la definición del host. Esto es un hard error state. Cuando un host se recupera de un hard error state este es considerado un hard recovery.

### **3.7 Periodos de tiempo**

Los periodos de tiempo permiten tener un gran control sobre los chequeos de servicio cuando están corriendo, cuando las notificaciones de host y servicios pueden ser enviadas y cuando los contactos pueden recibir notificaciones.



El argumento `check_period` de cada servicio permite especificar periodos de tiempo en que Nagios va a chequear el servicio. Cuando Nagios intenta reorganizar un chequeo de servicio esto puede hacer que el siguiente chequeo caiga en un rango de tiempo valido definido en el `time_period`, si esto no pasa Nagios ajustara el siguiente chequeo de servicio al siguiente tiempo valido especificado en el `time_period`, esto significa que el servicio no puede ser revisado en horas, días o semanas.

### **Organización de downtime**

Nagios permite organizar periodos para planificar downtime (tiempo fuera) para hosts y servicios de manera que usted puede monitorearlos. Este es usado en eventos que se conocen como apagar un servidor para actualizarlo, etc.

Cuando un host o servicio está en período de downtime programado las notificaciones para ese host son suprimidas.

La organización de downtime para hosts y servicios es guardado en el archivo que usted especifica en el `downtime_file`, en su archivo de configuración principal.

La organización de downtime de hosts y servicios es automáticamente preservada por el reinicio de programa. Cuando Nagios inicia este revisa el `downtime_file` y borra cualquier entrada antigua o inválida.

Se puede organizar un downtime para un host o servicio a través de CGI's haciendo click en "Schedule downtime for this host/service" , luego Nagios adiciona un comentario para aquel host/servicio indicando que ha sido organizado para downtime durante el período de tiempo indicado. Cuando aquel período pasa Nagios automáticamente borra el comentario que fue adicionado.

Existen dos tipos de organización de downtime:

- Fixed, donde el downtime inicia y termina en el período de tiempo especificado al momento de configurarlo.
- Flexible, donde el downtime es planificado y se conoce que un host o servicio va a estar abajo por  $X$  minutos u horas, pero no sabe exactamente en que tiempo se iniciara, cuando se organiza un downtime flexible Nagios va a iniciar el organizador de downtime algunas veces entre el inicio y el fin del tiempo especificado.

Cuando un host o servicio está en un período de downtime Nagios no va a permitir que las notificaciones sean enviadas para un host o servicio. La supresión de notificaciones es acompañada por un filtro adicional `notification_logic`, ya no se verá un icono en los CGI's indicando que las notificaciones de servicio o host no están disponibles. Cuando el horario de downtime ha pasado Nagios va a permitir que las notificaciones sean enviadas normalmente.

### 3.8 Trucos para la definición de objetos con plantillas base

Varios tipos de objetos permiten especificar múltiples nombres de hosts y nombres de hostgroup en las definiciones, permitiendo copiar la definición del objeto para múltiples hosts o servicios. Algunos de los tipos de objetos soportados son Servicios, Hostgroups, etc.

#### Servicios

**Múltiples hosts.-** si se desea crear servicios idénticos y asignarlos a múltiples hosts, usted puede especificarlo a la directiva `host_name`:

```
define service {
    host_name          equipo1, equipo2...
    service_description  SERVICIO1
    otras directivas de servicio
}
```

Esta definición va a crear un servicio llamado "SERVICIO1" en el host `equipo1`, `equipo2`, todas las instancias de "SERVICIO1" podrían ser idénticas.

**Todos los hosts en un múltiple hostgroup.-** si se desea crear servicios idénticos que estén asignados en todos los hosts en uno o más hostgroups, se puede crear una simple definición de servicio, el `hostgroup_name` permite especificar el nombre de uno o más hostgroups para los cuales el servicio fue creado:

```
define service {
    hostgroup_name      grupo1, grupo2...
    service_description  SERVICIO1
}
```

```
    otras directivas de servicio
}
```

Esta definición puede crear un servicio llamado “SERVICIO1” en todos los hosts que son miembros de los hostgroups grupo1, grupo2. Todas las instancias de “SERVICIO1” podrían ser idénticas.

**Todos los hosts.-** si se desea crear servicios idénticos que sean asignados a todos los hosts que están definidos en su archivo de configuración, se puede usar un comodín en la directiva host\_name:

```
define service {
    host_name                *
    service_description      SERVICIO1
    otras directivas de servicio
}
```

Esta definición puede crear un servicio llamado “SERVICIO1” en todos los hosts que están definidos en su archivo de configuración. Todas las instancias del “SERVICIO1” podrían ser idénticas.

## Hostgroups

**Todos los hosts.-** si se desea crear un hostgroup que tenga todos los hosts definidos en su archivo de configuración como miembros usted puede usar un comodín en la directiva members.

```
define hostgroup {
    hostgroup_name           grupo1
    members                  *
    otras directivas de hostgroup
}
```

La definición puede crear un hostgroup llamado grupo1 que va a tener todos los hosts definidos en su archivo de configuración como miembros.

*Seguridad de Nagios*

Nagios no necesita correr como root. Al momento de iniciar Nagios mediante un script usted puede forzarlo a omitir privilegios cuando inicie y correr como otro usuario usando las directivas `nagios_user` y `nagios_group`.

Por defecto los external commands están deshabilitados, esto es para prevenir una configuración de administrador que deje la interfase abierta para que sea usada por otros. Si se habilitan los external commands hay que asegurarse de configurar los permisos apropiadamente, solamente es necesario el usuario nagios el cual va a tener permiso de escritura en el archivo de comandos.

Se sugiere pedir autenticación para acceder a los CGI's. Se puede dar permisos a determinados usuarios para derechos adicionales. Si se tiene deshabilitada la característica de autenticación de CGI's, la directiva `use_authentication` en el archivo de configuración de los CGI's, el command `cgi` va a negar la escritura de cualquier comando en el `external_command_file`.

Cuando se definen comandos hay que asegurarse de especificar el path completo para algunos scripts o binarios que se estén ejecutando.

### **3.9 Mejorando nagios**

Nagios puede restringir el número máximo de chequeo de servicios que se están ejecutando a la vez, especificando esto en la opción `max_concurrent_checks`. Esto es bueno debido a que se permite algún control sobre que tanta carga se impone al host monitoreado, pero esto también puede reducir la velocidad de las cosas.

Si se ve una latencia alta, con valores mayores a 10 y 15 segundos, para la mayoría de sus chequeos de servicios, usted está probablemente está dejando a Nagios ansioso de chequeos. Bajo las condiciones ideales todos los chequeos de servicios pueden tener una latencia de cero, significando que estos fueron ejecutados en un tiempo exacto que fue planificado para ejecutarse. Sin embargo esto es normal para algunos chequeos que tienen valores de latencia pequeños. Se recomienda tomar el número mínimo del máximo de chequeos concurrentes reportados cuando esta corriendo Nagios con el comando `-S`.

Si se chequea el estado de host usando el `check_ping`, se encontrará que el chequeo de host será ejecutado más rápido especificando el `max_attempmts` en 1 en la definición de host y teniendo el `check_ping` enviando 10 paquetes ICMP al host, esto

debería ser mucho más rápido que configurar el `max_attempts` a 10 y solamente enviar un paquete ICMP cada vez. Esto se debe al hecho de que Nagios puede a menudo determinar el estado del host después de ejecutar el plugin.

Se recomienda no utilizar la opción `use_aggressive_host_checking` ya que esta opción apaga los chequeos de host que se van a ejecutar más rápido.

## CAPITULO IV

### 4. Reportes

#### 4.1 Guía de Uso

Luego de configurar correctamente Nagios, indicándole los equipos y servicios que se monitorearán, tener perfectamente instalado apache en la máquina en la que nagios correrá, así como bien configurado el archivo cgi.cfg que es el que nos ayuda en el ambiente web y las seguridades.

A continuación se procede a abrir Nagios en el navegador de nuestra elección. Para esto ponemos en la barra de direcciones la dirección IP de la máquina en la que está instalado Nagios, de la siguiente manera: <http://192.168.1.10/nagios/>

Se presenta un cuadro de diálogo en el cual se debe ingresar el nombre de usuario y contraseña (figura a):

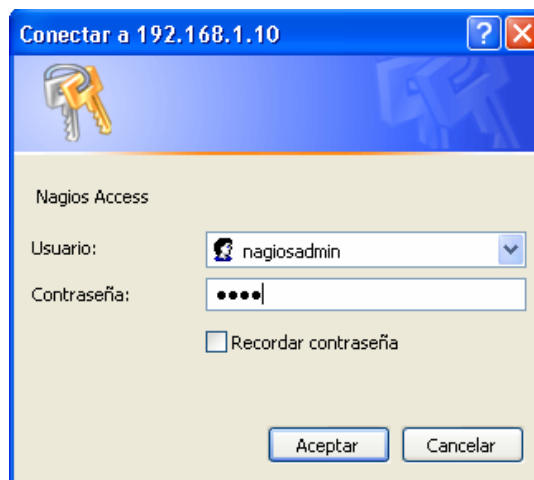


Figura a.

Este nombre de usuario y contraseña son asignados el momento de la instalación de Nagios. Un vez aceptados estos datos se presenta la página principal de Nagios (figura b), en donde se indica su versión y algunos links para obtener ayuda. En la parte izquierda de la pantalla se muestra un índice en el cual encontramos distintas secciones como: Datos Generales sobre Nagios, Monitoreo, Reportes y Detalles sobre la Configuración de Nagios. Cada uno de estos nos brindan tanto información sobre Nagios como reportes sobre la red que se está monitoreando.



Figura b.

A continuación se procederá a indicar cada uno de estos índices:

### General

Aquí encontramos dos enlaces, el primero que nos da la página principal de Nagios (figura b). Y el segundo enlace nos da acceso a la página de documentación de Nagios. (figura c).

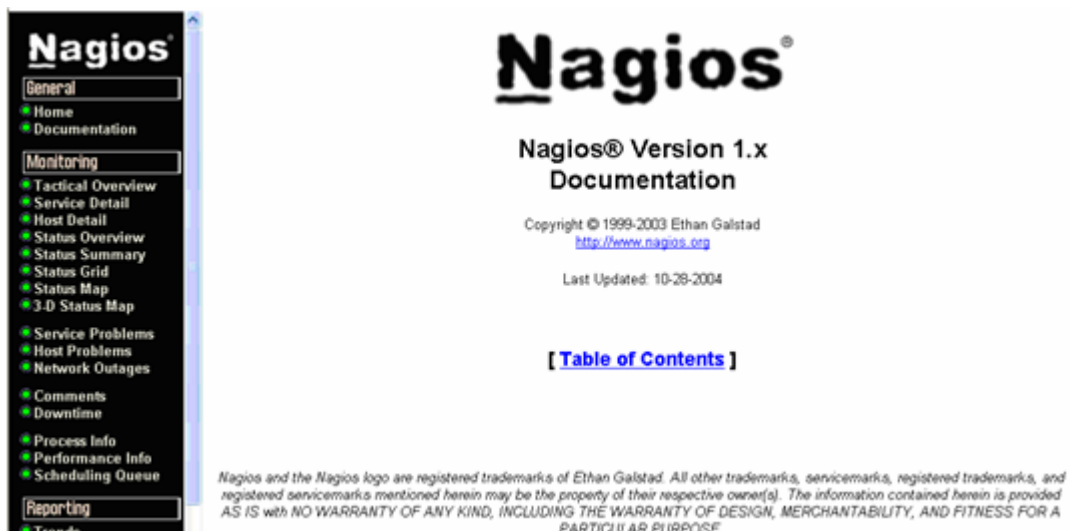


Figura c.

## Monitoring

Nos da reportes sobre el estado de cada uno de los hosts y servicios monitoreados. Los estados se indican con cuatro tipos de colores, estos se explican a continuación:

- Recovery (ok):** Cuando un host está up y/o un servicio esta ok.
- Warning:** Cuando se han detectado problemas en un host o servio, esto antes de volverse crítico.
- Unknown:** Cuando un host es inalcanzable
- Critical:** Cuando un host o servicio han presentado problemas y no se han recuperado de esto.

Cada una de las opciones en esta sección muestran grillas con los colores especificados anteriormente según el estado del host o servicio.

Por ejemplo la siguiente imagen nos muestra una grilla de estado de todos los grupos de hosts (figura d), así como el estado de cada uno de los servicios:

**Status Grid For All Host Groups**

[Red Windows \(Redes\)](#)

Host	Services
anto	Current Users HTTP PING Total Processes
pepe	devhda2 Free Space Current Users FTP HTTP PING Total Processes
prueba	Current Users HTTP PING Total Processes

Figura d.

En esta imagen se indica que los hosts 'anto' y 'pepe' están ok así como todos sus servicios, a diferencia de prueba que se encuentra down.

Si hacemos click en cualquiera de los hosts obtendremos información más detallada de su estado, en este caso haremos click en el host prueba (figura e):



### Host State Information

Host Status:	<b>DOWN</b>
Status Information:	CRITICAL - Host Unreachable (192.168.1.200)
Last Status Check:	01-28-2006 00:00:35
Status Data Age:	0d 0h 0m 22s
Last State Change:	01-27-2006 20:41:08
Current State Duration:	0d 3h 19m 49s
Last Host Notification:	01-27-2006 23:59:05
Current Notification Number:	638
Is This Host Flapping?	N/A
Percent State Change:	N/A
In Scheduled Downtime?	<b>NO</b>
Last Update:	01-28-2006 00:00:45

Host Checks:	<b>ENABLED</b>
Host Notifications:	<b>ENABLED</b>
Event Handler:	<b>DISABLED</b>
Flap Detection:	<b>DISABLED</b>

Figura e.

Aquí encontramos el estado del host down (host status), la información de este estado que es **crítico** (*status information*) indicándose además la dirección IP del mismo. Nos indica además la última vez que se realizó el chequeo (*last status check*), la última vez que se detecto un cambio de estado en el host (*last state change*), que tiempo ha estado el host en ese estado (*current state duration*), la última notificación que se envió (*last host notification*), el número de notificaciones enviadas hasta el momento que en este caso en 638 (*current notification number*). Además nos indica que no ha sido planeado ningún tiempo en el que el host deba estar caído (*in scheduled downtime*), y la última actualización de este reporte (*last update*).

A continuación se va a indicar la función de cada link con su respectivo gráfico.

### Tac CGI

Este CGI es diseñado para servir como un ojo de águila para toda la actividad monitoreada de la red. Esto permite que rápidamente vea cualquier corte de servicio de host o estado de servicio. (figura 1.1)

### **Status CGI**

Este es el CGI más importante incluido en Nagios. Estos permiten ver los estados actuales de todos los hosts y servicios que están siendo monitoreados. El status CGI puede producir dos tipos de salida, un estado general para todos los hostgroups y una lista detallada para todos los servicios. (figura 2.1 – 2.5)

### **Status Map CGI**

Este CGI crea un mapa de todos los hosts que usted tiene definidos en su red, el CGI usa la librería Thomas Boutell's para crear una imagen PNG de su diseño de red, el mismo que se puede visualizar de diferentes formas según la opción que se escoja en Layout Method. (figuras 3.1 – 3.3)

### **Network Outages CGI (outages.cgi)**

Este CGI produce una lista de problemas de los hosts de la red que son causados por los cortes en la red. Esto puede ser usado particularmente si se tiene una red grande y desea identificar rápidamente la fuente del problema.

### **Extended Information CGI (extinfo.cgi)**

Este CGI permite ver información de procesos de Nagios, estadísticas de hosts y servicios, comentarios de hosts y servicios, etc. Esto también sirve como un punto de inicio para enviar comandos a Nagios vía command cgi. Sin embargo este CGI tiene varios argumentos que es mejor dejarlos con su configuración original. Usted puede acceder a este CGI haciendo clic en network health y process information. (figura 4.1 – figura 4.3)

Dentro de esta sección de *monitoring* se puede reprogramar el siguiente chequeo para cualquiera de los servicios de un host que Nagios monitoree. Para hacer esto nos situamos en la pantalla de *status grid* y hacemos click en el servicio al cual deseamos adelantar o retrasar el tiempo de monitoreo (figura f):

## Status Grid For All Host Groups

[Red Windows \(Redes\)](#)

Host	Services
anto	Current Users HTTP PING Total Processes
pepe	/dev/hda2 Free Space Current Users FTP HTTP PING Total Processes
grueba	Current Users HTTP PING Total Processes

Figura f.

A continuación se presentará una pantalla en la cual escogeremos del recuadro derecho la opción *Re-schedule the next check of this service* (figura g):

Service State Information	Service Commands
<p>Current Status: <b>OK</b></p> <p>Status Information: PING OK - Packet loss = 0%, RTA = 0.53 ms</p> <p>Current Attempt: 1/4</p> <p>State Type: HARD</p> <p>Last Check Type: ACTIVE</p> <p>Last Check Time: 01-30-2006 20:00:07</p> <p>Status Data Age: 0d 0h 2m 10s</p> <p>Next Scheduled Active Check: 01-30-2006 20:05:07</p> <p>Latency: &lt; 1 second</p> <p>Check Duration: 4 seconds</p> <p>Last State Change: 01-30-2006 19:50:14</p> <p>Current State Duration: 0d 0h 12m 3s</p> <p>Last Service Notification: N/A</p> <p>Current Notification Number: 0</p> <p>Is This Service Flapping? N/A</p> <p>Percent State Change: N/A</p> <p>In Scheduled Downtime? <b>NO</b></p> <p>Last Update: 01-30-2006 20:02:09</p>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> <a href="#">Disable checks of this service</a></li> <li><input checked="" type="checkbox"/> <a href="#">Re-schedule the next check of this service</a></li> <li><input checked="" type="checkbox"/> <a href="#">Start accepting passive checks for this service</a></li> <li><input checked="" type="checkbox"/> <a href="#">Enable notifications for this service</a></li> <li><input checked="" type="checkbox"/> <a href="#">Schedule downtime for this service</a></li> <li><input checked="" type="checkbox"/> <a href="#">Enable event handler for this service</a></li> <li><input checked="" type="checkbox"/> <a href="#">Enable flap detection for this service</a></li> </ul>
<p>Service Checks: <b>ENABLED</b></p> <p>Passive Checks: <b>DISABLED</b></p> <p>Service Notifications: <b>DISABLED</b></p> <p>Event Handler: <b>DISABLED</b></p> <p>Flap Detection: <b>DISABLED</b></p>	

Figura g.

Y así obtenemos un recuadro en el cual consta el nombre del host, el nombre del servicio y la fecha y hora a la que se realizará el siguiente chequeo, aquí es donde realizaremos el cambio y luego presionamos *commit*, y así podemos esperar el siguiente chequeo que será antes o después de lo inicialmente indicado (figura h):

You are requesting to re-schedule the next check of a service

Command Options		Command Description
Host Name:	<input type="text" value="anto"/>	This command is used to re-schedule the next check of a particular service. Nagios will re-queue the service to be checked at the time you specify. If you select the <i>force check</i> option, Nagios will force a check of the service regardless of both what time the scheduled check occurs and whether or not checks are enabled for the service.
Service:	<input type="text" value="PING"/>	
Check Time:	<input type="text" value="01/30/2006 20:06:54"/>	
Force Check:	<input checked="" type="checkbox"/>	
<input type="button" value="Commit"/> <input type="button" value="Reset"/>		

Please enter all required information before committing the command.  
Required fields are marked in red.  
Failure to supply all required values will result in an error.


Figura h.

Otra opción que nos ofrece Nagios es la posibilidad de planificar un tiempo de downtime que generalmente es utilizado para actualizaciones de servidores. De esta manera Nagios no envía reportes de que dicho host está caído durante el tiempo que se haya indicado que va a durar el *Downtime*.

Par esto escogemos la opción *Downtime* de esta sección de *monitoring* y obtendremos una pantalla en la que se indica el itinerario de downtime tanto para hosts como para servicios (figura i):


[ [Host Downtime](#) | [Service Downtime](#) ]

### Scheduled Host Downtime

 [Schedule host downtime](#)

Host Name	Entry Time	Author	Comment	Start Time	End Time	Fixed?	Duration	Actions
There are no hosts with scheduled downtime								

### Scheduled Service Downtime

 [Schedule service downtime](#)

Host Name	Service	Entry Time	Author	Comment	Start Time	End Time	Fixed?	Duration	Actions
There are no services with scheduled downtime									

Figura i.

Y se procede a escoger la opción deseada ya sea para host *Schedule host downtime* o servicio *Schedule service downtime*. Se muestra una pantalla en la cual ingresamos los datos del host o servicio y el tiempo que se demorará el downtime del mismo (figura j):

**You are requesting to schedule downtime for a particular host**

Command Options	Command Description
<p>Host Name: <input type="text"/></p> <p>Author (Your Name): <input type="text" value="nagiosadmin"/></p> <p>Comment: <input type="text"/></p> <p>Start Time: <input type="text" value="01/30/2006 20:40:15"/></p> <p>End Time: <input type="text" value="01/30/2006 22:40:15"/></p> <p>Fixed: <input checked="" type="checkbox"/></p> <p>Duration: <input type="text" value="2"/> Hours <input type="text" value="0"/> Minutes</p> <p><input type="button" value="Commit"/> <input type="button" value="Reset"/></p>	<p>This command is used to schedule downtime for a particular host. During the specified downtime, Nagios will not send notifications out about the host. When the scheduled downtime expires, Nagios will send out notifications for this host as it normally would. Scheduled downtimes are preserved across program shutdowns and restarts. Both the start and end times should be specified in the following format: <b>mm/dd/yyyy hh:mm:ss</b>. If you select the <i>fixed</i> option, the downtime will be in effect between the start and end times you specify. If you do not select the <i>fixed</i> option, Nagios will treat this as "flexible" downtime. Flexible downtime starts when the host goes down or becomes unreachable (sometime between the start and end times you specified) and lasts as long as the duration of time you enter. The duration fields do not apply for fixed downtime.</p>

**Figura j.**

Hay que recalcar que este procedimiento solo puede realizarse desde el servidor Nagios ya que este no permitirá que se realice esto desde un terminal.

### ***Reporting***

En este encontramos enlaces que nos como resultado de su ejecución gráficos que nos indican las tendencias, reportes, alertas, histogramas y notificaciones sobre cada unos de los hosts y sus servicios.

Al hacer click en *trends*, nos encontramos con el primer paso para conseguir una gráfico de tendencias (figura k), ya sea de un host o servicio según se escoja

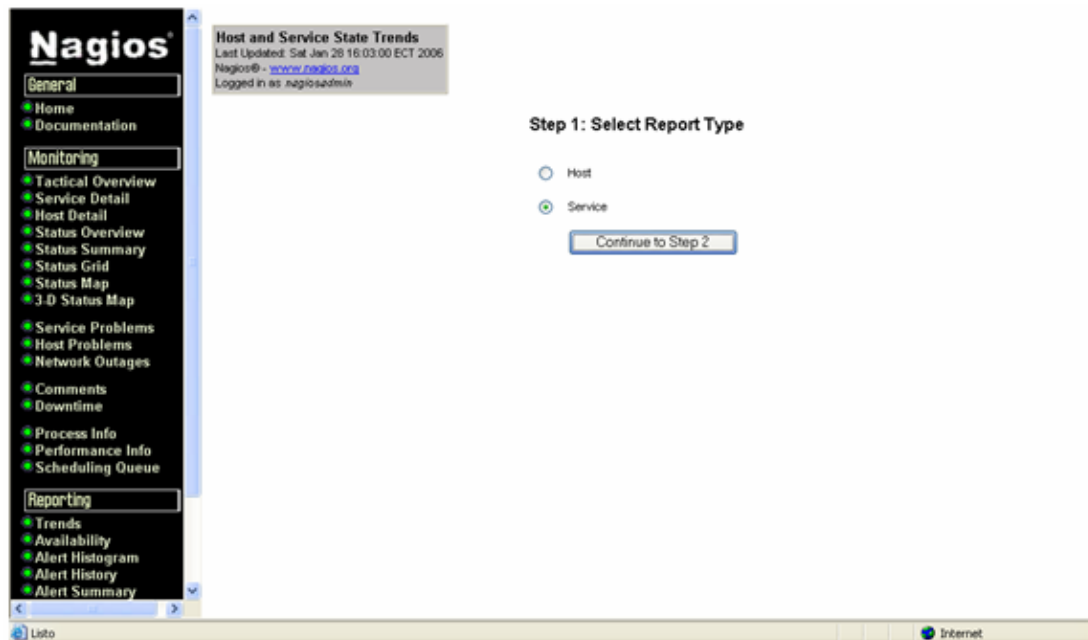


Figura k.

En este caso escogeremos un trend para un servicio, y se presenta el segundo paso (figura l), en donde procedemos a escoger un servicio. Cada servicio está identificado con el nombre del host al que pertenece:

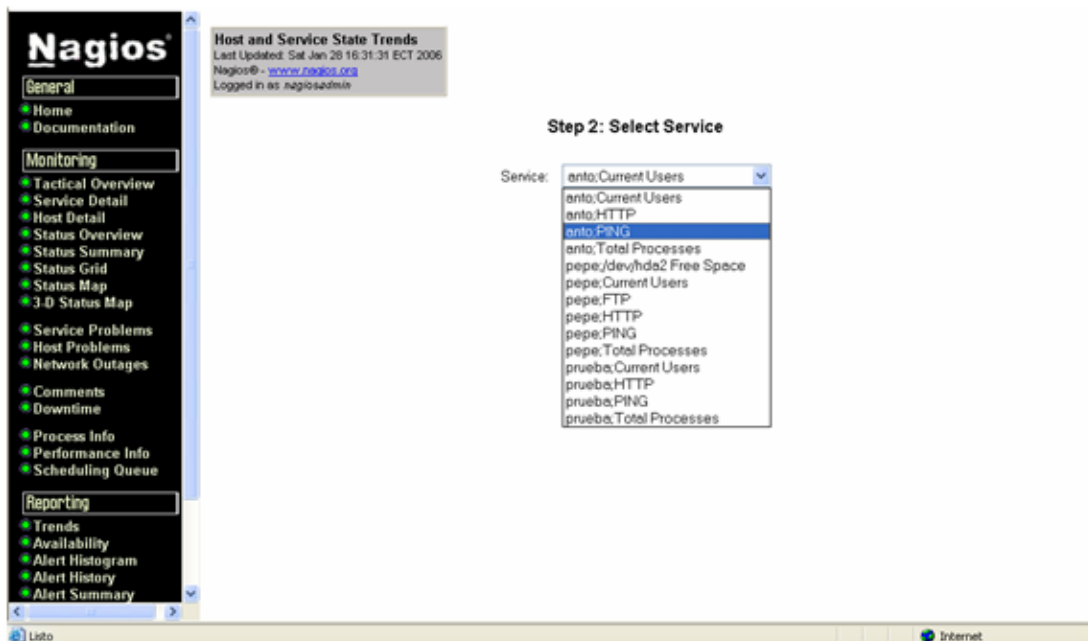


Figura l.

Luego de escoger el servicio, se sigue al tercer paso (figura m), en donde se escoge el período de monitoreo que deseamos que se grafique, además de escoger si deseamos que se asuma un estado inicial. El tiempo puede ser de 'last 24 hours', 'today', 'yesterday', 'this week', 'this month', etc.

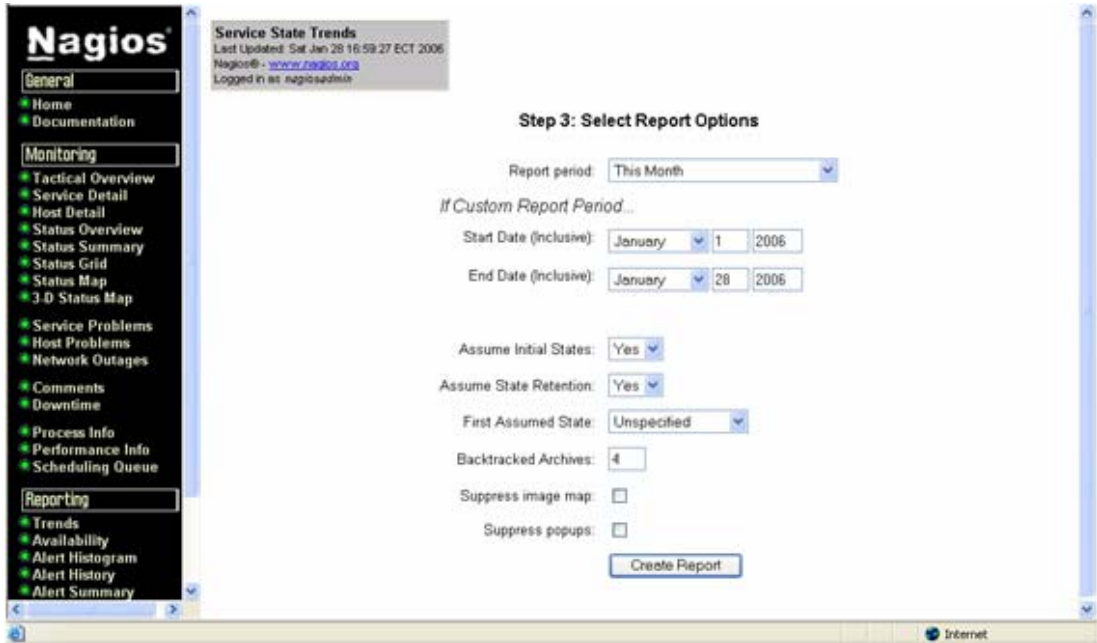


Figura m.

Finalmente obtenemos el gráfico del servicio ping del host 'anto' durante este mes de monitoreo (figura n):

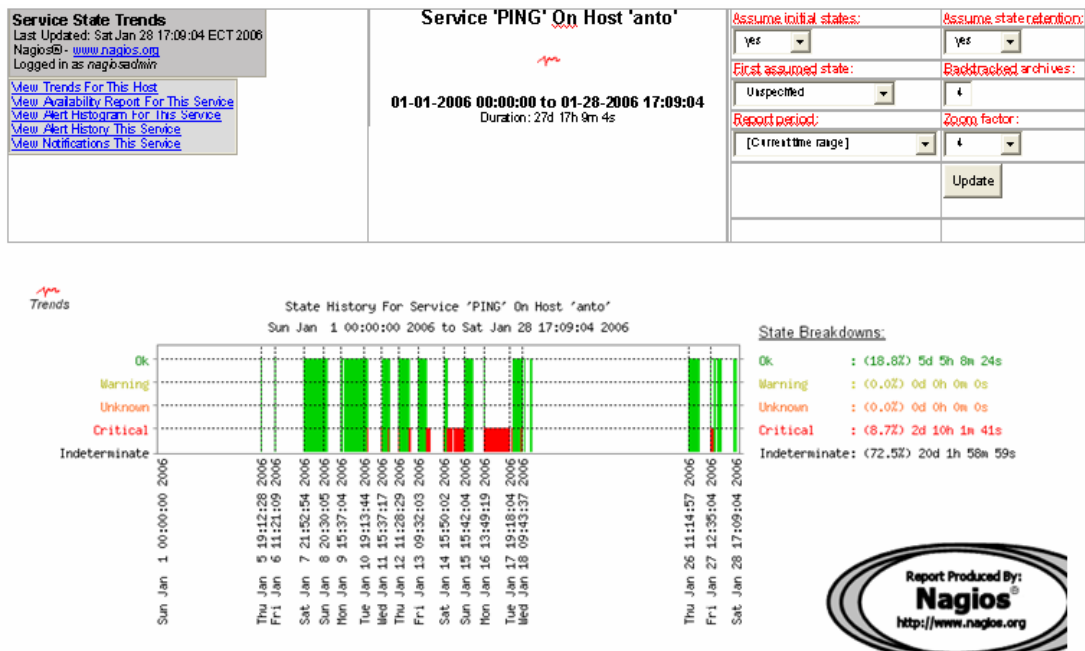


Figura n.

En este gráfico podemos observar con verde los días en los que el ping al host 'anto' ha estado ok. Con rojo cuando ha sido crítico. En esta pantalla también encontramos las opciones del paso 3, así podremos obtener varios reportes sin necesidad de repetir los pasos anteriores. Para obtener un gráfico con distinto rango, escogemos los parámetros presentados en esta pantalla y presionamos *update* (figura o):

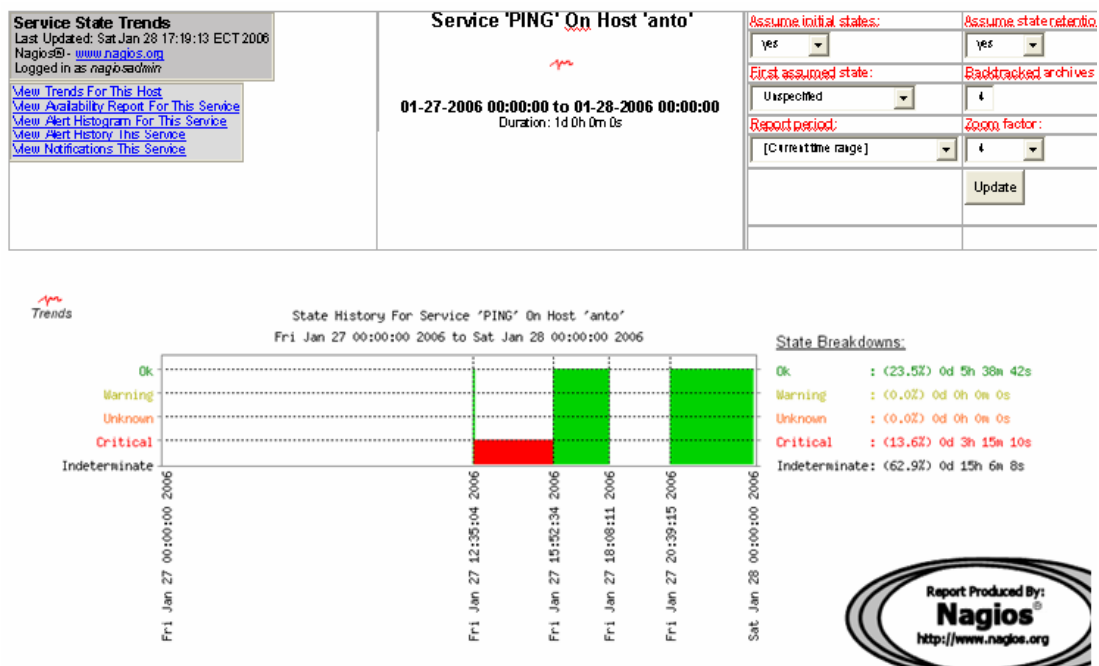


Figura o.

De esta misma manera seguimos los pasos para obtener histogramas, reportes y notificaciones.

A continuación indicaremos cada uno de los links de esta sección de *reporting*, con sus respectivos gráficos.

### Trends CGI (trends.cgi)

Este CGI es usado para crear un gráfico de estado de host o servicio sobre un período de tiempo arbitrario. Para el uso de este cgi es necesario habilitar el log rotation y mantener archivados los logs en path especificado por la directiva `log_archive_path`. (figura 5.1 – 5.7)



### **Availability Reporting CGI (avail.cgi)**

Este CGI es utilizado para reportar la disponibilidad de host y servicio sobre un período de tiempo especificado. Para el uso de este cgi es necesario habilitar el log rotation y mantener archivados los logs en path especificado por la directiva log\_archive\_path. (figura 6.1 – 6.3)

### **Alert Histogram CGI (histogram.cgi)**

Este CGI es utilizado para reportar la disponibilidad de host y servicio sobre un período de tiempo especificado. Para el uso de este cgi es necesario habilitar el log rotation y mantener archivados los logs en path especificado por la directiva log\_archive\_path. (figura 7.1 – 7.4)

### **Alert History CGI (history.cgi)**

Este CGI es usado para ver el historial de problemas con un host particular o todos los hosts, la salida es básicamente un subconjunto de información que es mostrado en el log file cgi. Se tiene la posibilidad de filtrar la salida para mirar solo tipos específicos de problemas que se desee. Si esta habilitado el log rotation usted puede ver la información en el archivo guardado usando links de navegación. (figura 8.1)

### **Alert Summary CGI (summary.cgi)**

Este CGI provee algunos reportes genéricos acerca de los datos de alerta de host y servicio, incluyendo alertas totales, top de alertas, etc. (figura 9.1 – 9.2)

### **Notifications CGI (notifications.cgi)**

Este CGI es usado para ver las notificaciones de host y servicio que han sido enviadas a varios contactos. La salida es un subconjunto de información que es mostrada por el log file cgi. Se tiene la posibilidad de filtrar la salida para mirar solo tipos específicos de notificaciones que se desee. Si esta habilitado el log rotation usted puede ver la información en el archivo guardado usando links de navegación. (figura 10.1)

## Event Log CGI (showlog.cgi)

Este CGI va a mostrar el log file, si usted tiene habilitado log rotation usted puede ver las notificaciones en el archivo log file guardado usando los links de navegación. (figura 11.1)

## Configuration

En este índice podemos ver la configuración de cada uno de los archivos de Nagios como lo son hosts, hostgroups, contacts, contactgroups, services, etc.

Para mirar la configuración de uno de estos archivos lo escogemos del menú desplegable indicado a continuación (figura p):

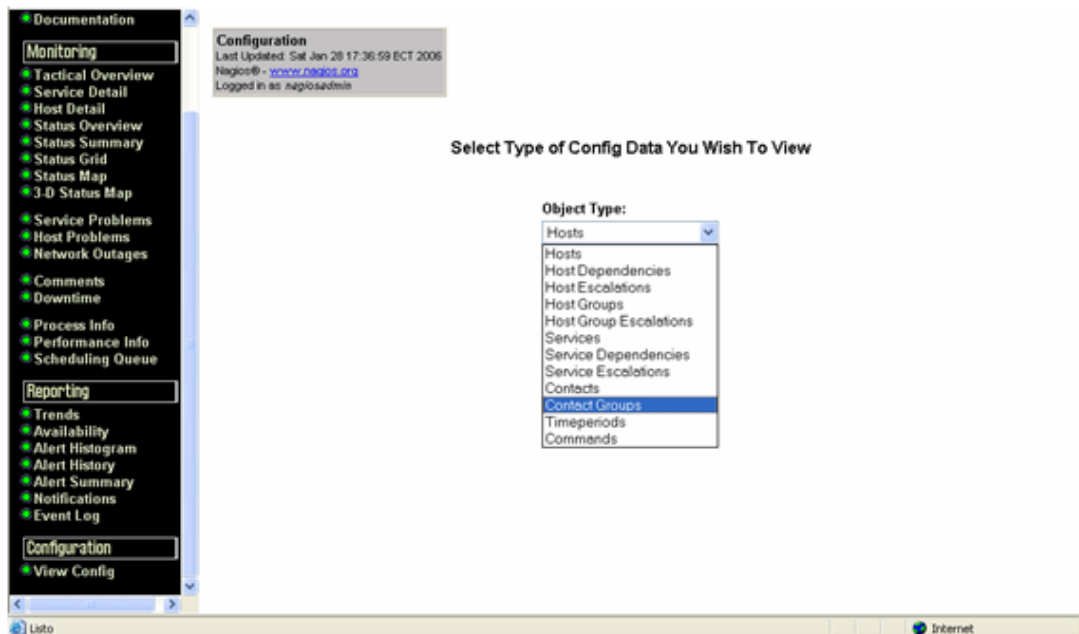


Figura p.

En este caso veremos como está configurado el archivo de contacts.cgi (figura q):

**Configuration**  
 Last Updated: Sat Jan 28 17:42:42 ECT 2006  
 Nagios® - [www.nagios.org](http://www.nagios.org)  
 Logged in as: nagiosadmin

**Object Type:**

**Contacts**

Contact Name	Alias	Email Address	Pager Address/Number	Service Notification Options	Host Notification Options	Service Notification Period	Host Notification Period	Service Notification Commands	Host Notification Commands
jp	Jose Luis	<a href="mailto:jl@nagios.com">jl@nagios.com</a>		Critical, Recovery	Down, Recovery	<a href="#">24x7</a>	<a href="#">24x7</a>	<a href="#">notify-by-email</a>	<a href="#">host-notify-by-email</a>

Figura q.

En esta tabla encontramos el nombre del contacto, el alias, la dirección de email, número de beeper, estados de un servicio en el contacto será notificado, estados de un host en el que el contacto será notificado, en qué período se realizarán las notificaciones (24x7, workhours), y por medio de que sistema se va a notificar el momento de tener un problema con un host o servicio.

### **Configuration CGI (config.cgi)**

Este CGI permite ver los objetos que usted tiene definidos en su archivo de configuración de objetos. (figura 12.1)

## 4.2 Reportes gráficos

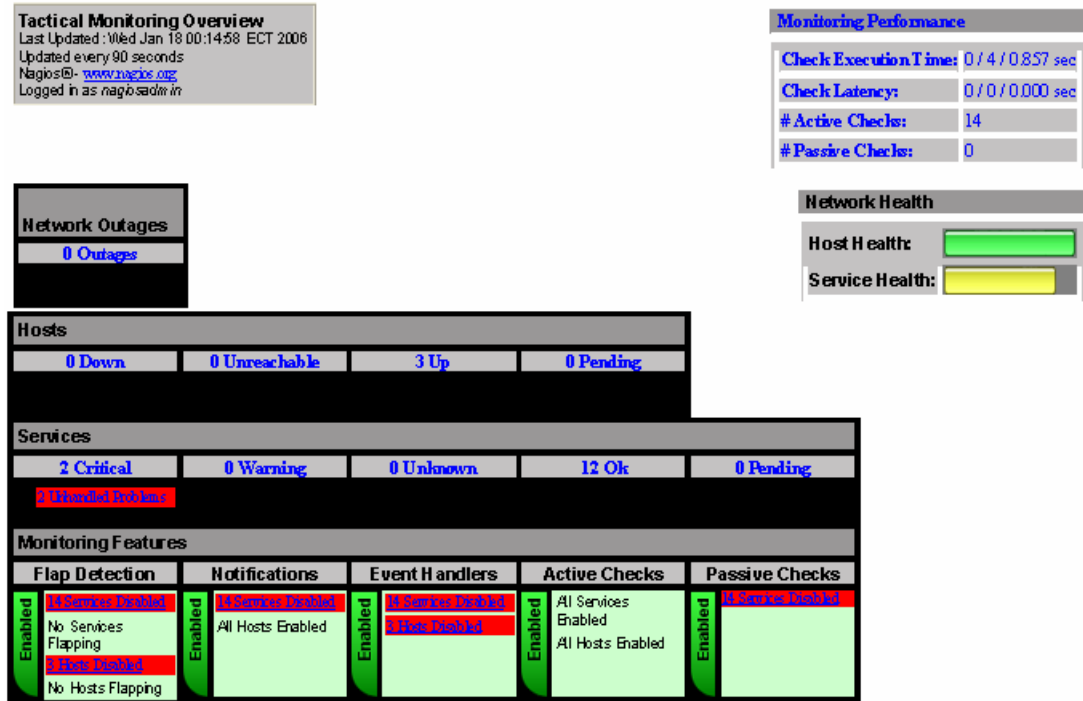


Figura 1.1 Tactical overview

### Service Status Details For All Hosts

Host	Service	Status	Last Check	Duration	Attempt	Status Information
anto	Current Users	OK	01-17-2006 23:40:24	20d 1h 32m 49s	1/3	USERS OK - 2 users currently logged in
	HTTP	CRITICAL	01-17-2006 23:43:18	10d 1h 47m 52s	3/3	Connection refused
	PING	OK	01-17-2006 23:42:11	0d 0h 26m 27s	1/4	PING OK - Packet loss = 0%, RTA= 0.31 ms
	Total Processes	OK	01-17-2006 23:43:04	22d 1h 14m 59s	1/3	PROCS OK:86 processes
pepe	Netwda2 Free Space	OK	01-17-2006 23:39:36	12d 4h 10m 12s	1/3	DISK OK - free space: /1724 MB (46%)
	Current Users	OK	01-17-2006 23:40:42	20d 1h 39m 37s	1/3	USERS OK - 2 users currently logged in
	FTP	OK	01-17-2006 23:43:35	7d 2h 8m 39s	1/3	FTP OK - 0.005 second response time on port 21 [220 (vsFTPd 2.0.3)]
	HTTP	OK	01-17-2006 23:42:29	0d 0h 1m 27s	1/3	HTTP OK HTTP/1.1 200 OK - 1290 bytes in 0.053 seconds
	PING	OK	01-17-2006 23:43:22	22d 1h 33m 29s	1/4	PING OK - Packet loss = 0%, RTA= 0.09 ms
	Total Processes	OK	01-17-2006 23:38:20	20d 1h 47m 24s	1/3	PROCS OK:87 processes
prueba	Current Users	OK	01-17-2006 23:41:00	0d 23h 36m 57s	1/3	USERS OK - 2 users currently logged in
	HTTP	CRITICAL	01-17-2006 23:41:53	10d 1h 9m 17s	3/3	Connection refused
	PING	OK	01-17-2006 23:42:46	0d 0h 26m 37s	1/4	PING OK - Packet loss = 0%, RTA= 0.44 ms
	Total Processes	OK	01-17-2006 23:43:40	0d 23h 34m 9s	1/3	PROCS OK:86 processes

14 Matching Service Entries Displayed

Figura 2.1 Service detail

### Host Status Details For All Host Groups

Host	Status	Last Check	Duration	Status Information
anto	UP	01-17-2006 23:43:27	0d 1h 2m 40s	PING OK - Packet loss = 0%, RTA= 0.32 ms
pepe	UP	01-17-2006 23:40:42	22d 1h 34m 48s	(Host assumed to be up)
prueba	UP	01-17-2006 23:43:57	0d 0h 28m 16s	PING OK - Packet loss = 0%, RTA= 0.38 ms

3 Matching Host Entries Displayed

Figura 2.2 Host detail

### Service Overview For All Host Groups

Red Windows (Redes)

Host	Status	Services	Actions
<a href="#">anto</a>	DOWN	2 OK 3 CRITICAL	
<a href="#">pepe</a>	UP	5 OK	
<a href="#">prueba</a>	UP	1 OK 1 CRITICAL	

Figura 2.3 Status overview

### Service Overview For All Host Groups

Red Windows (Redes)

Host	Status	Services	Actions
<a href="#">anto</a>	UP	3 OK 2 CRITICAL	
<a href="#">pepe</a>	UP	5 OK	
<a href="#">prueba</a>	UP	3 OK 1 CRITICAL	

Figura 2.4 Status overview

### Status Summary For All Host Groups

Host Group	Host Status Totals	Service Status Totals
<a href="#">Red Windows (Redes)</a>	3 UP	12 OK 2 CRITICAL

Figura 2.5 Status summary

### Status Grid For All Host Groups

[Red Windows \(Redes\)](#)




Host	Services
<a href="#">anto</a> 	<a href="#">Dument Users</a> <a href="#">HTTP</a> <a href="#">PING</a> <a href="#">Total Processes</a>
<a href="#">pepe</a> 	<a href="#">Nvidia2 Free Space</a> <a href="#">Dument Users</a> <a href="#">FTP</a> <a href="#">HTTP</a> <a href="#">PING</a> <a href="#">Total Processes</a>
<a href="#">pruebas</a> 	<a href="#">Dument Users</a> <a href="#">HTTP</a> <a href="#">PING</a> <a href="#">Total Processes</a>

Figura 2.6 Status grid

**Network Map For All Hosts**  
 Last Updated: Tue Jan 17 23:51:13 ECT 2006  
 Updated every 90 seconds  
 Nagios@- www.nagios.org  
 Logged in as nagiosadmin

[View Status Detail For All Hosts](#)  
[View Status Overview For All Hosts](#)

Layout Method: Circular (Marked Up)      Scaling factor: 0.0

Drawing Layers: Red Windows

Layer mode:  
 Include  
 Exclude

Supress popups:

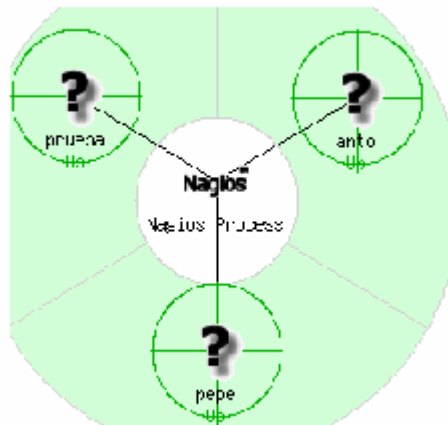


Figura 3.1 Status map

**Network Map For All Hosts**  
 Last Updated: Tue Jan 17 23:53:15 ECT 2006  
 Updated every 90 seconds  
 Nagios@- www.nagios.org  
 Logged in as nagiosadmin

[View Status Detail For All Hosts](#)  
[View Status Overview For All Hosts](#)

Layout Method: Collapsed tree      Scaling factor: 0.0

Drawing Layers: Red Windows

Layer mode:  
 Include  
 Exclude

Supress popups:

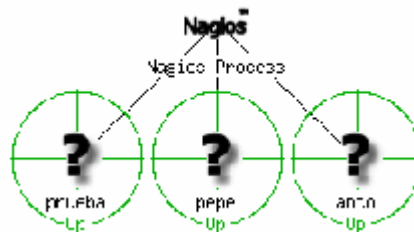


Figura 3.2 Status map



**Network Map For All Hosts**  
 Last Updated: Tue Jan 17 23:54:03 ECT 2006  
 Updated every 90 seconds  
 Nagios@ - [www.nagios.org](http://www.nagios.org)  
 Logged in as *nagiosadmin*

[View Status Detail For All Hosts](#)  
[View Status Overview For All Hosts](#)

Layout Method: Circular (Balloon)      Scaling factor: 0.0

Drawing Layers: Red Windows

Layer mode:  
 Include  
 Exclude

Supress popups:

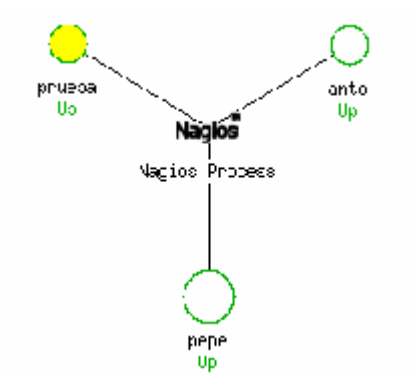


Figura 3.3 Status map

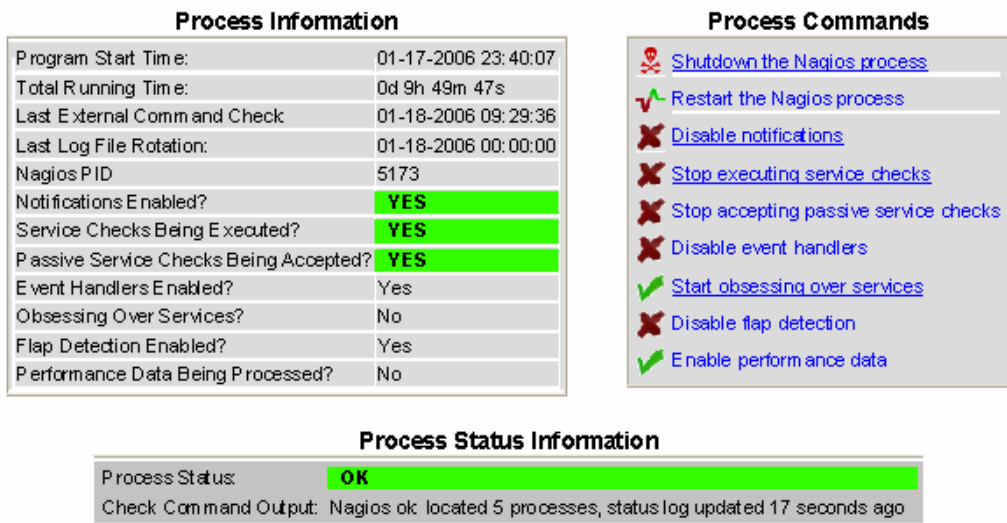


Figura 4.1 Extended Information

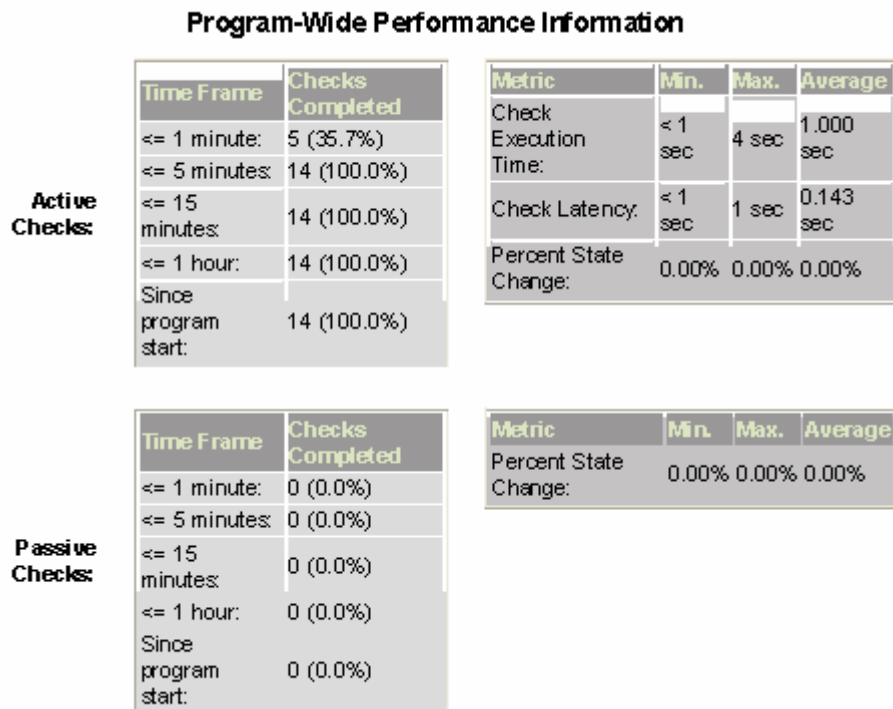


Figura 4.2 Extended Information

### Host Comments

 [Add a new host comment](#)

Host Name	Entry Time	Author	Comment	Comment ID	Persistent	Actions
<a href="#">anto</a>	01-18-2006 09:33:22	nagios.admin	C lon	1	Yes	

### Service Comments

 [Add a new service comment](#)

Host Name	Service	Entry Time	Author	Comment	Comment ID	Persistent	Actions
There are no service comments							

Figura 4.3 Extended Information

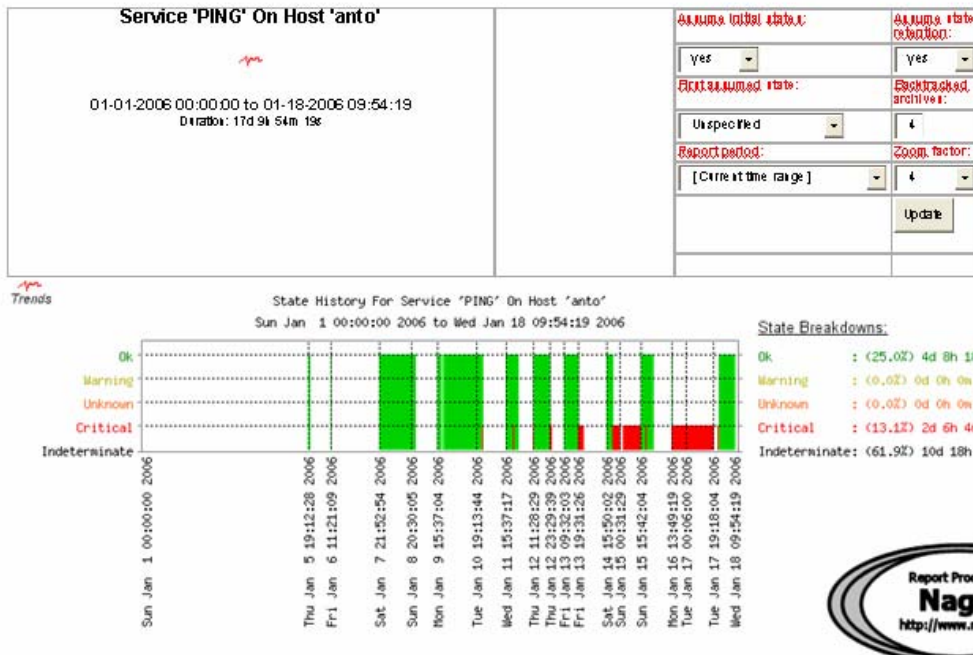


Figura 5.1 Trends

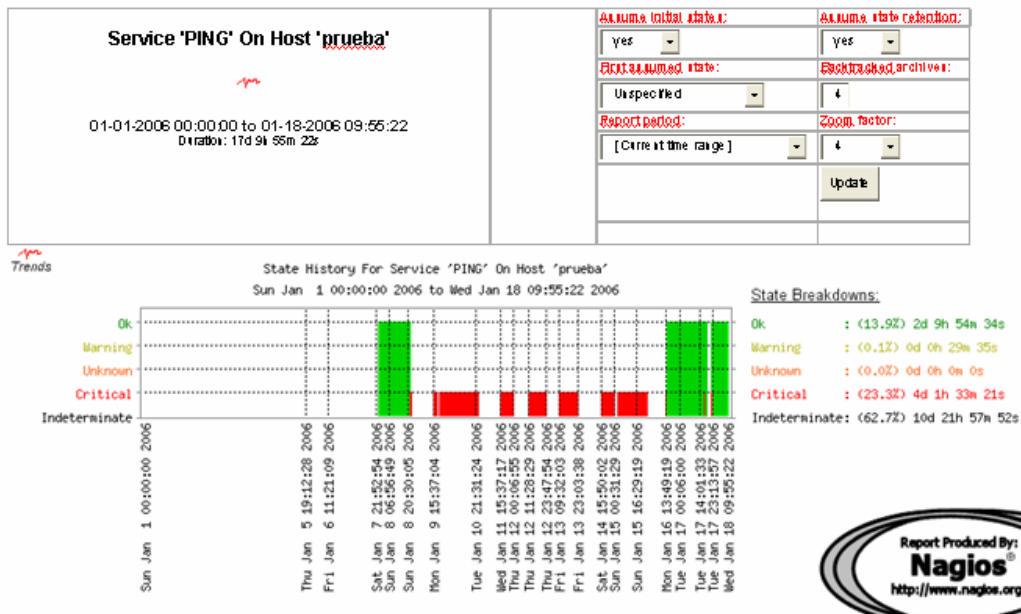


Figura 5.2 Trends

<p><b>Service 'HTTP' On Host 'pepe'</b></p> <p>01-11-2006 09:56:39 to 01-18-2006 09:56:39 Duration: 7d0h 0m 0s</p>	<p>Assume initial state:</p> <p>yes</p>	<p>Assume state retention:</p> <p>yes</p>
	<p>Assumed state:</p> <p>Current state</p>	<p>Backtracked archives:</p> <p>↓</p>
	<p>Report period:</p> <p>[Current range]</p>	<p>Zoom factor:</p> <p>↓</p>
	<p>Update</p>	
	<p> </p>	
	<p> </p>	

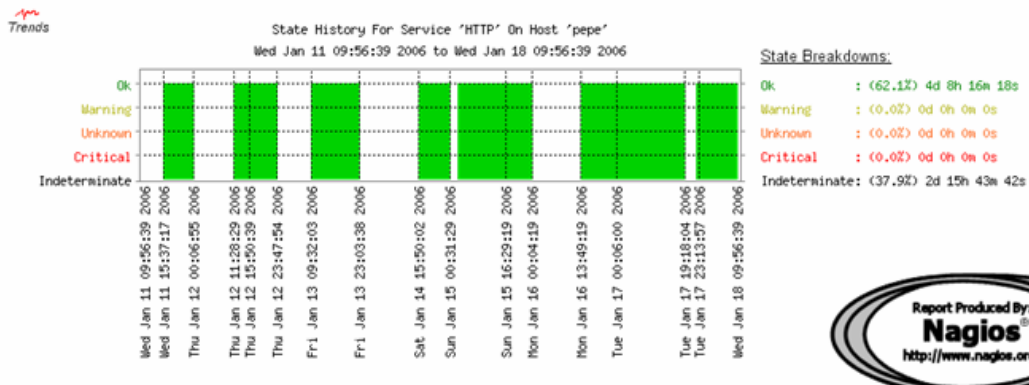


Figura 5.3 Trends

<p><b>Service '/dev/hda2 Free Space' On Host 'pepe'</b></p> <p>01-11-2006 09:57:31 to 01-18-2006 09:57:31 Duration: 7d0h 0m 0s</p>	<p>Assume initial state:</p> <p>yes</p>	<p>Assume state retention:</p> <p>yes</p>
	<p>Assumed state:</p> <p>Current state</p>	<p>Backtracked archives:</p> <p>↓</p>
	<p>Report period:</p> <p>[Current range]</p>	<p>Zoom factor:</p> <p>↓</p>
	<p>Update</p>	
	<p> </p>	
	<p> </p>	

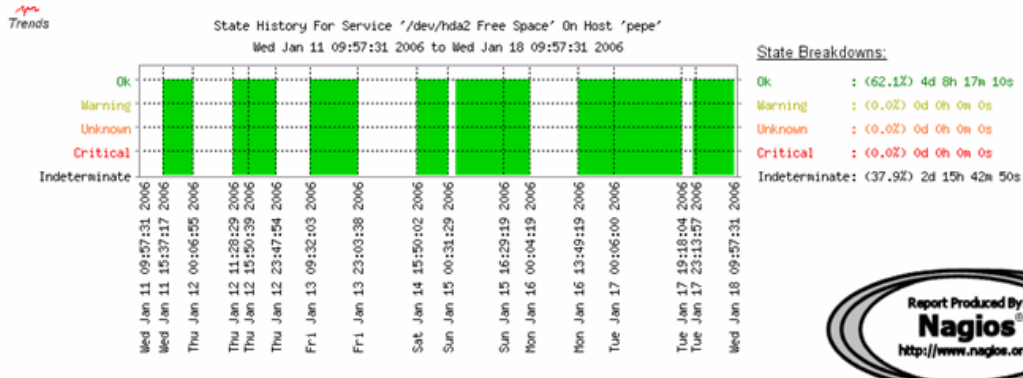


Figura 5.4 Trends

<b>Host 'anto'</b>  01-11-2006 09:58:43 to 01-18-2006 09:58:43 Duration: 7d0h 0m 0s	<b>Assume initial state:</b> <input type="button" value="yes"/>	<b>Assume state retention:</b> <input type="button" value="yes"/>
	<b>Exclude assumed state:</b> <input type="button" value="Unspecified"/>	<b>Exclude tracked archives:</b> <input type="button" value="1"/>
	<b>Report period:</b> <input type="button" value="[ Current range ]"/>	<b>Zoom factor:</b> <input type="button" value="1"/>
	<input type="button" value="Update"/>	

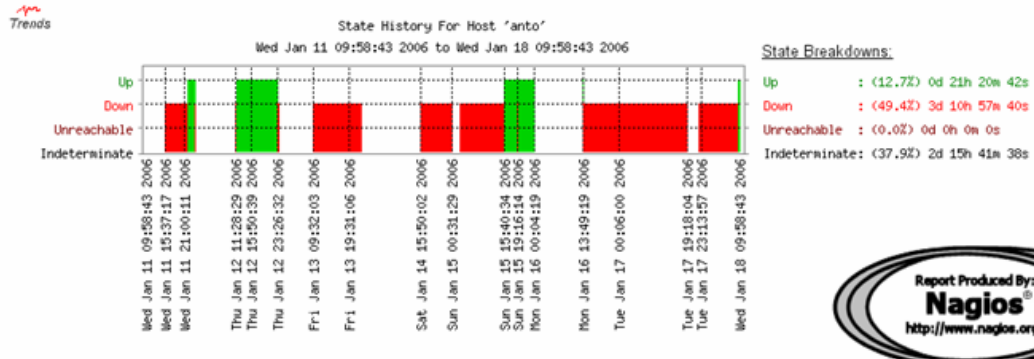


Figure 5.5 Trends

<b>Host 'pepe'</b>  01-11-2006 09:59:42 to 01-18-2006 09:59:42 Duration: 7d0h 0m 0s	<b>Assume initial state:</b> <input type="button" value="yes"/>	<b>Assume state retention:</b> <input type="button" value="yes"/>
	<b>Exclude assumed state:</b> <input type="button" value="Current State"/>	<b>Exclude tracked archives:</b> <input type="button" value="1"/>
	<b>Report period:</b> <input type="button" value="[ Current range ]"/>	<b>Zoom factor:</b> <input type="button" value="1"/>
	<input type="button" value="Update"/>	

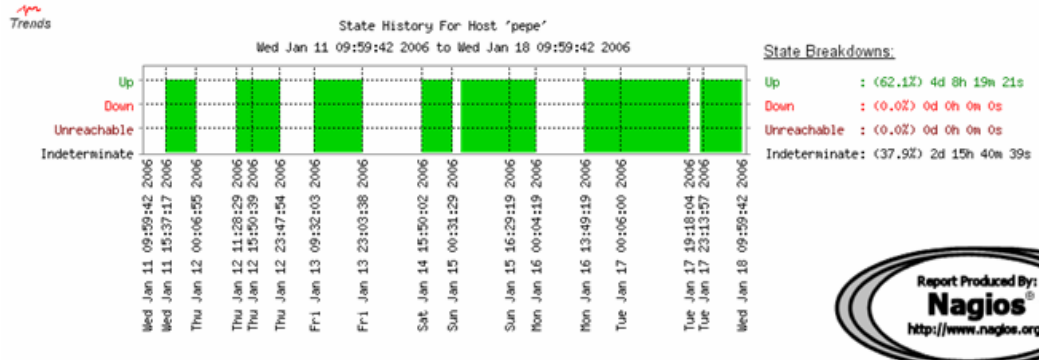


Figure 5.6 Trends

<b>Host 'prueba'</b>    01-01-2006 00:00:00 to 01-18-2006 10:00:49 Duration: 17d 10h 49s	<b>Assume initial state:</b> <input type="button" value="yes"/>	<b>Assume state retention:</b> <input type="button" value="yes"/>
	<b>Expected state:</b> <input type="button" value="Unspecified"/>	<b>Expected archive:</b> <input type="button" value="4"/>
	<b>Report period:</b> <input type="button" value="[Current range]"/>	<b>Zoom factor:</b> <input type="button" value="4"/>
	<input type="button" value="Update"/>	

Trends

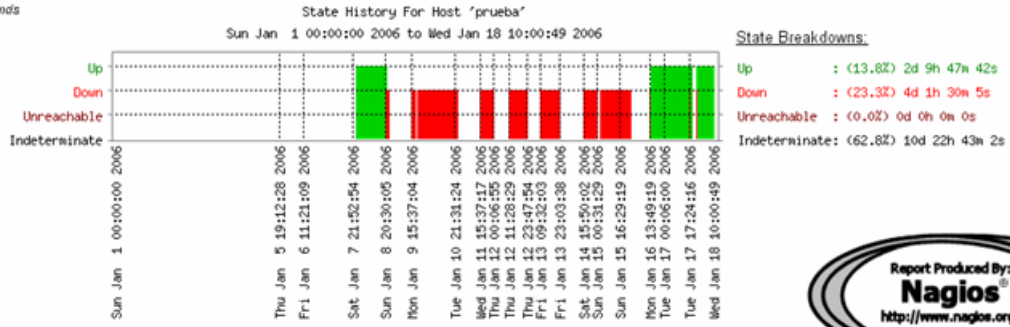


Figura 5.7 Trends

**Service State Breakdowns:**

Host	Service	% Time OK	% Time Warning	% Time Unknown	% Time Critical	% Time Undetermined
anto	Current Users	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	100.000%
	HTTP	0.000% (0.000%)	0.233% (0.611%)	0.000% (0.000%)	37.854% (99.389%)	61.914%
	PING	24.984% (65.597%)	0.000% (0.000%)	0.000% (0.000%)	13.103% (34.403%)	61.914%
	Total Processes	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	100.000%
pepe	/dev/hda2 Free Space	98.001% (99.955%)	0.000% (0.000%)	0.000% (0.000%)	0.017% (0.045%)	61.982%
	Current Users	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	100.000%
	FTP	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	37.894% (100.000%)	62.106%
	HTTP	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	100.000%
prueba	PING	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	100.000%
	Total Processes	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	100.000%
	Current Users	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	100.000%
	HTTP	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	37.647% (100.000%)	62.353%
prueba	PING	13.881% (37.180%)	0.118% (0.316%)	0.000% (0.000%)	23.336% (62.504%)	62.664%
	Total Processes	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	100.000%

Figura 6.1 Availability Reporting

**Host State Breakdowns:**

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
anto	12.751% (20.523%)	49.382% (79.477%)	0.000% (0.000%)	37.867%
pepe	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	100.000%
prueba	22.617% (36.400%)	39.517% (63.600%)	0.000% (0.000%)	37.867%

Figura 6.2 Availability Reporting

Figura 6.3

**Hostgroup 'Redes' Host State Breakdowns:**

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
anto	12.758% (20.532%)	49.382% (79.468%)	0.000% (0.000%)	37.860%
pepe	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	100.000%
prueba	22.623% (36.407%)	39.517% (63.593%)	0.000% (0.000%)	37.860%

Figura 6.3 Availability Reporting



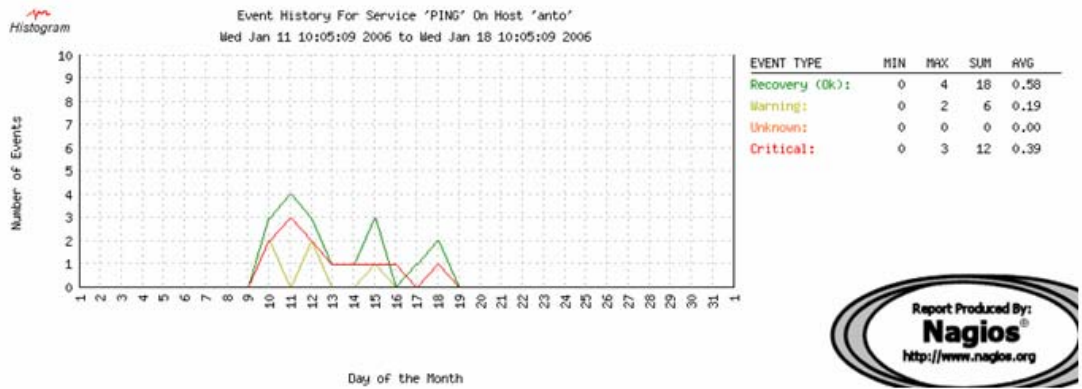


Figura 7.1 Alert histogram

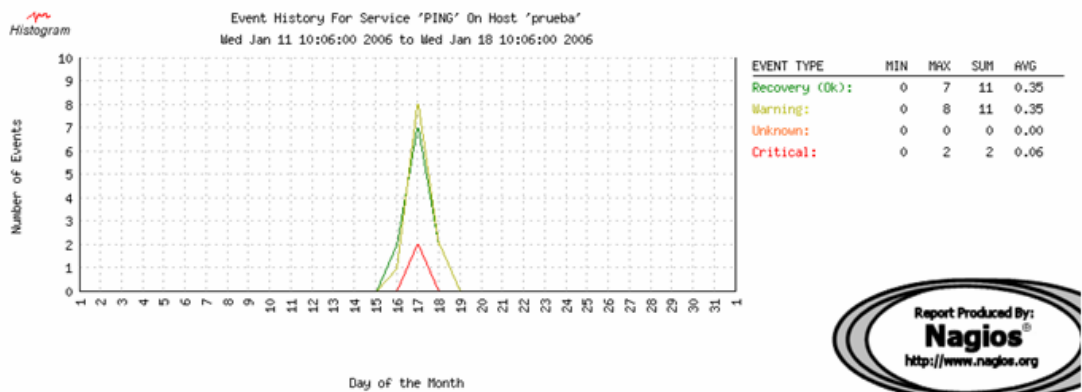


Figura 7.2 Alert histogram

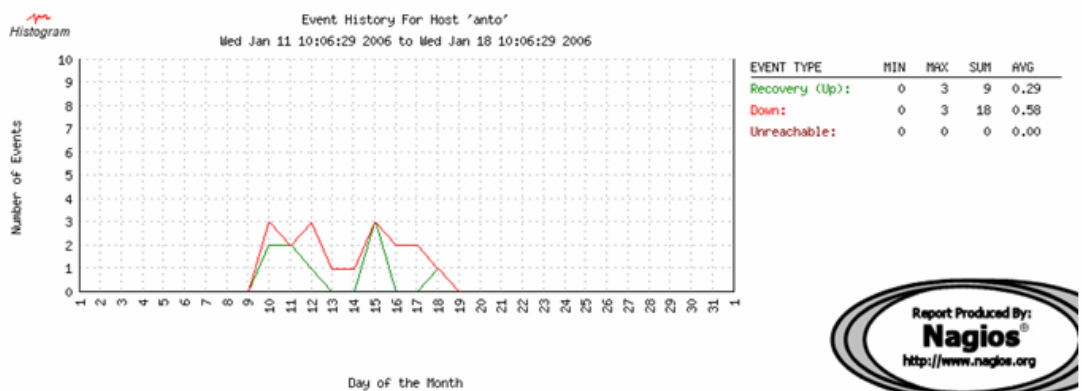


Figura 7.3 Alert histogram

All Hosts and Services		
<a href="#">Latest</a> <a href="#">Archive</a>	Log File Navigation Wed Jan 18 00:00:00 ECT 2006 to Present	
File: /var/log/majordomo.log		
<div style="float: right;"> <b>State type options:</b>            All table types <input type="text"/>            History detail level for all hosts:            All alerts <input type="text"/>  <input type="checkbox"/> Hide Flapping Alerts  <input type="checkbox"/> Hide Downtime Alerts  <input type="checkbox"/> Hide Process Messages  <input type="checkbox"/> Older Entries First  <input type="button" value="Update"/> </div>		

January 18, 2006 09:00

- ! [01-18-2006 09:08:17] SERVICE ALERT: auto;PING;CRITICAL;HARD;1;CRITICAL - Host Unreachable (192.168.1.100)
- ! [01-18-2006 09:03:37] HOST ALERT: auto;DOWN;HARD;1;CRITICAL - PING timed out after 10

January 18, 2006 01:00

- ! [01-18-2006 01:18:57] SERVICE ALERT: prieba;PING;WARNING;SOFT;1;PING WARNING - Packet loss = 0% , RTA = 13.10 ms
- ! [01-18-2006 01:18:17] SERVICE ALERT: auto;PING;OK;SOFT;2;PING OK - Packet loss = 0% , RTA = 0.31 ms
- ! [01-18-2006 01:17:17] SERVICE ALERT: auto;PING;WARNING;SOFT;1;PING WARNING - Packet loss = 0% , RTA = 12.65 ms
- ! [01-18-2006 01:03:57] SERVICE ALERT: prieba;PING;OK;SOFT;2;PING OK - Packet loss = 0% , RTA = 8.01 ms
- ! [01-18-2006 01:02:57] SERVICE ALERT: prieba;PING;WARNING;SOFT;1;PING WARNING - Packet loss = 0% , RTA = 38.81 ms
- ! [01-18-2006 01:19:57] SERVICE ALERT: prieba;PING;OK;SOFT;2;PING OK - Packet loss = 0% , RTA = 8.38 ms

Figura 8.1 Alert history

Displaying most recent 25 of 56 total matching alerts

Time	Alert Type	Host	Service	State	State Type	Information
01-18-2006 09:50:37	Host Alert	<a href="#">prueba</a>	N/A	UP	HARD	PING OK - Packet loss = 0%, RTA = 0.40 ms
01-18-2006 09:48:37	Host Alert	<a href="#">prueba</a>	N/A	DOWN	HARD	CRITICAL - Plugin timed out after 10 seconds
01-18-2006 09:43:37	Service Alert	<a href="#">anto</a>	PING	OK	HARD	PING OK - Packet loss = 0%, RTA = 0.30 ms
01-18-2006 09:43:17	Host Alert	<a href="#">anto</a>	N/A	UP	HARD	PING OK - Packet loss = 0%, RTA = 0.26 ms
01-18-2006 09:08:17	Service Alert	<a href="#">anto</a>	PING	CRITICAL	HARD	CRITICAL - Host Unreachable (192.168.1.100)
01-18-2006 09:03:37	Host Alert	<a href="#">anto</a>	N/A	DOWN	HARD	CRITICAL - Plugin timed out after 10 seconds
01-17-2006 23:17:29	Service Alert	<a href="#">anto</a>	PING	OK	HARD	PING OK - Packet loss = 0%, RTA = 0.32 ms
01-17-2006 23:17:19	Service Alert	<a href="#">prueba</a>	PING	OK	HARD	PING OK - Packet loss = 0%, RTA = 0.39 ms
01-17-2006 23:16:59	Host Alert	<a href="#">prueba</a>	N/A	UP	HARD	PING OK - Packet loss = 0%, RTA = 0.35 ms
01-17-2006 23:16:02	Host Alert	<a href="#">prueba</a>	N/A	DOWN	HARD	CRITICAL - Host Unreachable (192.168.1.200)
01-17-2006 22:43:02	Service Alert	<a href="#">prueba</a>	PING	CRITICAL	HARD	CRITICAL - Host Unreachable (192.168.1.200)
01-17-2006 22:42:35	Host Alert	<a href="#">anto</a>	N/A	DOWN	HARD	CRITICAL - Host Unreachable (192.168.1.100)
01-17-2006 22:42:05	Host Alert	<a href="#">prueba</a>	N/A	DOWN	HARD	CRITICAL - Host Unreachable (192.168.1.200)
01-17-2006 18:41:43	Service Alert	<a href="#">prueba</a>	PING	OK	HARD	PING OK - Packet loss = 0%, RTA = 0.80 ms
01-17-2006 18:37:46	Host Alert	<a href="#">prueba</a>	N/A	UP	HARD	PING OK - Packet loss = 0%, RTA = 0.54 ms
01-17-2006 17:26:33	Service Alert	<a href="#">prueba</a>	PING	CRITICAL	HARD	CRITICAL - Host Unreachable (192.168.1.200)
01-17-2006 17:24:16	Host Alert	<a href="#">prueba</a>	N/A	DOWN	HARD	CRITICAL - Host Unreachable (192.168.1.200)
01-17-2006 14:06:33	Service Alert	<a href="#">prueba</a>	PING	OK	HARD	PING OK - Packet loss = 0%, RTA = 0.35 ms
01-17-2006 14:01:33	Service Alert	<a href="#">prueba</a>	PING	WARNING	HARD	PING WARNING - Packet loss = 0%, RTA = 14.18 ms
01-17-2006 00:08:26	Host Alert	<a href="#">anto</a>	N/A	DOWN	HARD	CRITICAL - Host Unreachable (192.168.1.100)
01-16-2006 14:55:08	Host Alert	<a href="#">anto</a>	N/A	DOWN	HARD	CRITICAL - Host Unreachable (192.168.1.100)
01-16-2006 14:49:17	Service Alert	<a href="#">prueba</a>	PING	OK	HARD	PING OK - Packet loss = 0%, RTA = 0.67 ms
01-16-2006 14:48:57	Host Alert	<a href="#">prueba</a>	N/A	UP	HARD	PING OK - Packet loss = 0%, RTA = 0.35 ms
01-16-2006 13:53:29	Service Alert	<a href="#">anto</a>	PING	CRITICAL	HARD	CRITICAL - Host Unreachable (192.168.1.100)
01-16-2006 13:52:02	Host Alert	<a href="#">anto</a>	N/A	DOWN	HARD	CRITICAL - Host Unreachable (192.168.1.100)

Figura 9.1 Alert summary

Displaying most recent 25 of 30 total matching alerts

Time	Alert Time	Host	Service	State	State Type	Information
01-18-2006 09:50:37	Host Alert	<a href="#">prueba</a>	N/A	UP	HARD	PING OK - Packet loss = 0%, RTA = 0.40 ms
01-18-2006 09:48:37	Host Alert	<a href="#">prueba</a>	N/A	DOWN	HARD	CRITICAL - Plugin timed out after 10 seconds
01-18-2006 09:43:17	Host Alert	<a href="#">anto</a>	N/A	UP	HARD	PING OK - Packet loss = 0%, RTA = 0.26 ms
01-18-2006 09:03:37	Host Alert	<a href="#">anto</a>	N/A	DOWN	HARD	CRITICAL - Plugin timed out after 10 seconds
01-17-2006 23:16:59	Host Alert	<a href="#">prueba</a>	N/A	UP	HARD	PING OK - Packet loss = 0%, RTA = 0.35 ms
01-17-2006 23:16:02	Host Alert	<a href="#">prueba</a>	N/A	DOWN	HARD	CRITICAL - Host Unreachable (192.168.1.200)
01-17-2006 22:42:35	Host Alert	<a href="#">anto</a>	N/A	DOWN	HARD	CRITICAL - Host Unreachable (192.168.1.100)
01-17-2006 22:42:05	Host Alert	<a href="#">prueba</a>	N/A	DOWN	HARD	CRITICAL - Host Unreachable (192.168.1.200)
01-17-2006 18:37:46	Host Alert	<a href="#">prueba</a>	N/A	UP	HARD	PING OK - Packet loss = 0%, RTA = 0.54 ms
01-17-2006 17:24:16	Host Alert	<a href="#">prueba</a>	N/A	DOWN	HARD	CRITICAL - Host Unreachable (192.168.1.200)
01-17-2006 00:08:26	Host Alert	<a href="#">anto</a>	N/A	DOWN	HARD	CRITICAL - Host Unreachable (192.168.1.100)
01-16-2006 14:55:08	Host Alert	<a href="#">anto</a>	N/A	DOWN	HARD	CRITICAL - Host Unreachable (192.168.1.100)
01-16-2006 14:48:57	Host Alert	<a href="#">prueba</a>	N/A	UP	HARD	PING OK - Packet loss = 0%, RTA = 0.35 ms
01-16-2006 13:52:02	Host Alert	<a href="#">anto</a>	N/A	DOWN	HARD	CRITICAL - Host Unreachable (192.168.1.100)
01-15-2006 19:38:31	Host Alert	<a href="#">anto</a>	N/A	UP	HARD	PING OK - Packet loss = 0%, RTA = 392.35 ms
01-15-2006 19:22:13	Host Alert	<a href="#">anto</a>	N/A	DOWN	HARD	CRITICAL - Host Unreachable (192.168.1.100)
01-15-2006 19:17:12	Host Alert	<a href="#">anto</a>	N/A	UP	HARD	PING OK - Packet loss = 0%, RTA = 0.30 ms
01-15-2006 19:16:14	Host Alert	<a href="#">anto</a>	N/A	DOWN	HARD	CRITICAL - Host Unreachable (192.168.1.100)
01-15-2006 15:40:34	Host Alert	<a href="#">anto</a>	N/A	UP	HARD	PING OK - Packet loss = 0%, RTA = 0.60 ms
01-15-2006 03:08:57	Host Alert	<a href="#">anto</a>	N/A	DOWN	HARD	CRITICAL - Host Unreachable (192.168.1.100)
01-14-2006 19:17:02	Host Alert	<a href="#">anto</a>	N/A	DOWN	HARD	CRITICAL - Host Unreachable (192.168.1.100)
01-13-2006 19:31:06	Host Alert	<a href="#">anto</a>	N/A	DOWN	HARD	CRITICAL - Host Unreachable (192.168.1.100)
01-12-2006 23:26:32	Host Alert	<a href="#">anto</a>	N/A	DOWN	HARD	CRITICAL - Host Unreachable (192.168.1.100)
01-12-2006 11:49:19	Host Alert	<a href="#">anto</a>	N/A	UP	HARD	PING OK - Packet loss = 0%, RTA = 0.43 ms
01-12-2006 11:31:12	Host Alert	<a href="#">anto</a>	N/A	DOWN	HARD	CRITICAL - Host Unreachable (192.168.1.100)

Figura 9.2 Alert summary


All Contacts						
		<a href="#">Latest Archive</a> 			Log File Navigation Wed Jan 18 00:00:00 ECT 2006 to Present	
File: /var/log/nagios/nagios.log						
Notification detail level for all contacts: All notifications <input type="checkbox"/> Older Emails Elct: <input type="button" value="Update"/>						
Host	Service	Type	Time	Contact	Notification Command	Information
<a href="#">prieba</a>	N/A	HOST UP	01-18-2006 09:50:37	<a href="#">ip</a>	<a href="#">ios@ottw-by-e.mail</a>	PING OK - Packet loss = 0%, RTA = 0.40 ms
<a href="#">prieba</a>	N/A	HOST DOWN	01-18-2006 09:50:17	<a href="#">ip</a>	<a href="#">ios@ottw-by-e.mail</a>	CRITICAL - <a href="#">ping</a> timed out after 10 seconds
<a href="#">prieba</a>	N/A	HOST DOWN	01-18-2006 09:48:37	<a href="#">ip</a>	<a href="#">ios@ottw-by-e.mail</a>	CRITICAL - <a href="#">ping</a> timed out after 10 seconds
<a href="#">aito</a>	N/A	HOST UP	01-18-2006 09:43:17	<a href="#">ip</a>	<a href="#">ios@ottw-by-e.mail</a>	PING OK - Packet loss = 0%, RTA = 0.26 ms
<a href="#">aito</a>	N/A	HOST DOWN	01-18-2006 09:41:47	<a href="#">ip</a>	<a href="#">ios@ottw-by-e.mail</a>	CRITICAL - Host Unreachable (192.168.1.100)
<a href="#">aito</a>	N/A	HOST DOWN	01-18-2006 09:39:47	<a href="#">ip</a>	<a href="#">ios@ottw-by-e.mail</a>	CRITICAL - Host Unreachable (192.168.1.100)
<a href="#">aito</a>	N/A	HOST DOWN	01-18-2006 09:37:47	<a href="#">ip</a>	<a href="#">ios@ottw-by-e.mail</a>	CRITICAL - Host Unreachable (192.168.1.100)
<a href="#">aito</a>	N/A	HOST DOWN	01-18-2006 09:35:47	<a href="#">ip</a>	<a href="#">ios@ottw-by-e.mail</a>	CRITICAL - Host Unreachable (192.168.1.100)
<a href="#">aito</a>	N/A	HOST DOWN	01-18-2006 09:33:20	<a href="#">ip</a>	<a href="#">ios@ottw-by-e.mail</a>	CRITICAL - Host Unreachable (192.168.1.100)
<a href="#">aito</a>	N/A	HOST DOWN	01-18-2006 09:31:47	<a href="#">ip</a>	<a href="#">ios@ottw-by-e.mail</a>	CRITICAL - Host Unreachable (192.168.1.100)

Figure 10.1 Notifications

<b>Current Event Log</b> Last Update: Wed Jan 18 09:36:08 ECT 2006 Nagios® - <a href="http://www.nagios.org">www.nagios.org</a> Logged in as: nagios@redhat	<b>Labels Archive</b> 	<b>Log File Navigation</b> Wed Jan 18 00:00:00 ECT 2006 to Present,	<b>Older Entries First</b> <input type="button" value="Update"/>
File: /var/log/nagios/magic.log			

January 18, 2006 09:00

01-18-2006 09:35:47 HOST NOTIFICATION: ipa1b.DOWN:localhost:bre-mail:CRITICAL - Host Unreachable (192.168.1.100)

01-18-2006 09:33:47 EXTERNAL COMMAND: ADD\_HOST\_COMMENT: ipa1b; nagiosadmin: C:lo

01-18-2006 09:33:20 HOST NOTIFICATION: ipa1b.DOWN:localhost:bre-mail:CRITICAL - Host Unreachable (192.168.1.100)

01-18-2006 09:31:47 HOST NOTIFICATION: ipa1b.DOWN:localhost:bre-mail:CRITICAL - Host Unreachable (192.168.1.100)

01-18-2006 09:29:47 HOST NOTIFICATION: ipa1b.DOWN:localhost:bre-mail:CRITICAL - Host Unreachable (192.168.1.100)

01-18-2006 09:27:47 HOST NOTIFICATION: ipa1b.DOWN:localhost:bre-mail:CRITICAL - Host Unreachable (192.168.1.100)

01-18-2006 09:25:47 HOST NOTIFICATION: ipa1b.DOWN:localhost:bre-mail:CRITICAL - Host Unreachable (192.168.1.100)

01-18-2006 09:23:20 HOST NOTIFICATION: ipa1b.DOWN:localhost:bre-mail:CRITICAL - Host Unreachable (192.168.1.100)

01-18-2006 09:21:47 HOST NOTIFICATION: ipa1b.DOWN:localhost:bre-mail:CRITICAL - Host Unreachable (192.168.1.100)

01-18-2006 09:19:47 HOST NOTIFICATION: ipa1b.DOWN:localhost:bre-mail:CRITICAL - Host Unreachable (192.168.1.100)

01-18-2006 09:17:47 HOST NOTIFICATION: ipa1b.DOWN:localhost:bre-mail:CRITICAL - Host Unreachable (192.168.1.100)

01-18-2006 09:15:47 HOST NOTIFICATION: ipa1b.DOWN:localhost:bre-mail:CRITICAL - Host Unreachable (192.168.1.100)

01-18-2006 09:13:17 HOST NOTIFICATION: ipa1b.DOWN:localhost:bre-mail:CRITICAL - Host Unreachable (192.168.1.100)

01-18-2006 09:11:27 HOST NOTIFICATION: ipa1b.DOWN:localhost:bre-mail:CRITICAL - Host Unreachable (192.168.1.100)

01-18-2006 09:09:27 HOST NOTIFICATION: ipa1b.DOWN:localhost:bre-mail:CRITICAL - Host Unreachable (192.168.1.100)

01-18-2006 09:08:17 SERVICE ALERT: ipa1b;PING:CRITICAL;HARD;1;CRITICAL - Host Unreachable (192.168.1.100)

01-18-2006 09:07:27 HOST NOTIFICATION: ipa1b.DOWN:localhost:bre-mail:CRITICAL - Host Unreachable (192.168.1.100)

01-18-2006 09:05:30 HOST NOTIFICATION: ipa1b.DOWN:localhost:bre-mail:CRITICAL - Host Unreachable (192.168.1.100)

01-18-2006 09:03:37 HOST NOTIFICATION: ipa1b.DOWN:localhost:bre-mail:CRITICAL - Ping timed out after 10 seconds

01-18-2006 09:03:37 HOST ALERT: ipa1b;DOWN;HARD;1;CRITICAL - Ping timed out after 10 seconds

January 18, 2006 08:00

01-18-2006 08:40:07 A rib-s-aue: of retention data completed successfully.

January 18, 2006 07:00

01-18-2006 07:40:07 A rib-s-aue: of retention data completed successfully.

January 18, 2006 06:00

01-18-2006 06:40:07 A rib-s-aue: of retention data completed successfully.

January 18, 2006 05:00

01-18-2006 05:40:07 A rib-s-aue: of retention data completed successfully.

January 18, 2006 04:00

01-18-2006 04:40:07 A rib-s-aue: of retention data completed successfully.

January 18, 2006 03:00

01-18-2006 03:40:07 A rib-s-aue: of retention data completed successfully.

January 18, 2006 02:00

01-18-2006 02:40:07 A rib-s-aue: of retention data completed successfully.

Figura 11.1 Event log

Host Name	Alias/Descript	Address	Parent Hosts	Notification Interval	Notification Options	Notification Period	Max. Check Attempts	Host Check Command	Enable Checks
Anto	clon	192.168.1.100		0h 1m 0s	Down, Unreachable, Recovery	24x7	1	check-host-alive	No
Pepe	servidor nagios	192.168.1.10		0h 1m 0s	Down, Unreachable, Recovery	24x7	1	check-host-alive	No
prueba	clon	192.168.1.200		0h 1m 0s	Down, Unreachable, Recovery	24x7	1	check-host-alive	No

Event Handler	Enable Event Handler	Stalking Options	Enable Flap Detection	Low Flap Threshold	High Flap Threshold	Process Performance Data	Enable Failure Prediction	Failure Prediction Options	Retention Options
	No	None	No	Program-wide value	Program-wide value	Yes	Yes		Status Information, Non-Status Information
	No	None	No	Program-wide value	Program-wide value	Yes	Yes		Status Information, Non-Status Information
	No	None	No	Program-wide value	Program-wide value	Yes	Yes		Status Information, Non-Status Information

Figura 12.1 Configuration

## CONCLUSIONES

Hemos comprobado que Nagios es una herramienta de monitoreo muy eficiente, y la mejor parte de esto es que no tiene costo, siendo una gran ventaja para la institución, empresa o persona que lo requiera ya que puede ser implementado en una red pequeña o en la red de una empresa a nivel nacional. Al momento de configurar Nagios podemos decidir los equipos a monitorear los cuales pueden ir desde un router hasta una impresora

Otra de las ventajas que Nagios nos brinda y tal vez la más importante es la de obtener gráficos y listas en los cuales podemos detectar problemas, operatividad y disponibilidad tanto de equipos como de servicios. . Además permite enviar notificaciones de problemas a una persona o grupo de personas según el equipo o servicio en problemas.

La instalación y configuración de Nagios luego de analizar la documentación sugerida no es muy complicada pero requiere de mucha dedicación y paciencia hasta encontrar el mecanismo de monitoreo que utiliza.

Esta herramienta ayuda a los administradores de red ha mantener una estrategia proactiva ante los posibles problemas que pueden darse en la red que maneja, evitando así el chequeo personalizado de un equipo de la red sin que este o sus servicios sean los causantes de un problema, por lo tanto nos alertaría de situaciones que tomarían mucho tiempo para localizarlas.



## RECOMENDACIONES

Nagios es una buena herramienta de monitoreo por lo cual recomendamos su uso en cualquier red, pero hay que tener paciencia y dedicación para ello. Esta aplicación es muy extensa en cuanto a su funcionalidad, pero esta debe ser explotada a medida que se conoce más a fondo la misma, ya que solo con la práctica, estudio y observación diaria de Nagios se podrá desarrollar al máximo sus capacidades.

Podemos acotar que nosotros inicialmente pensamos trabajar con CentOS que es un clon de Red Hat Linux pero que no lleva los logos de este. Instalamos y compilamos Nagios sin problema alguno, al momento de abrirlo en el navegador no funcionaron los cgi's de la autenticación de usuario, lo que por ese momento no representó mayor problema, pero al esperar los reportes de que el host que se monitoreaba estaba up (ok), cosa que debía pasar en 90 segundos, nunca sucedió, a pesar de que se hacía correctamente ping una máquina a otra. Se intentó instalar tanto CentOS como Nagios nuevamente pero no funcionó. Decidimos cambiar de distribución a Debian y funcionó a la primera. Pero no todo fue fácil ya que deseábamos trabajar con una portátil hp Pavilion dv1135la, en la cual CentOS se instaló correctamente al igual que Nagios, pero éste presentó el problema anteriormente descrito, y al tratar de instalar Debian no se tuvo éxito debido a una incompatibilidad de hardware.

Cabe recalcar que Debian cuenta con 14 cd's de instalación en los cuales incluye todos sus paquetes, por lo cual para instalar alguna aplicación adicional simplemente se recurre a sus cd's, a diferencia de CentOS cuyos paquetes adicionales se los encuentra en Internet.

Nagios cuenta ya con una nueva versión la 2.0b, pero de esta solo hay una versión demo no estable ya que aún se encuentra en desarrollo y perfeccionamiento.

## BIBLIOGRAFÍA

**Bulma**, Instalando y Configurando Nagios 1.2 [en línea]. Agosto 2004 [citado diciembre 10, 2005]. Disponible en <http://bulma.net/body.phtml?nIdNoticia=2075>

**Bulma**, Instalando y Configurando Nagios 1.2 [en línea]. Enero 2005 [citado diciembre 10, 2005]. Disponible en <http://bulma.net/body.phtml?nIdNoticia=2144>

**Galstad**, Ethan. Nagios Home [en línea]. Diciembre de 2005 [citada diciembre 10, 2005]. Disponible en Internet: <http://www.nagios.org>

**Galstad**, Ethan. Nagios Documentation [en línea]. Diciembre de 2005 [citada diciembre 10, 2005]. Link Documentation. Disponible en Internet: <http://www.nagios.org/docs/>

**Galstad**, Ethan. Nagios Versión 1x Documentation. [en línea]. Noviembre 2004 [citada diciembre 10, 2005]. Disponible en Internet: [http://nagios.sourceforge.net/docs/1\\_0/](http://nagios.sourceforge.net/docs/1_0/)

**González de la Herrán**, Eduardo. Herramienta Libre para la Monitorización de Sistemas [en línea]. Febrero 2005. [citado diciembre 14, 2005]. Disponible en Internet: [http://www.e-ghost.deusto.es/docs/2005/cursos/charlaNagios\\_20050224.pdf](http://www.e-ghost.deusto.es/docs/2005/cursos/charlaNagios_20050224.pdf)

**Sourceforge.org**. Nagios [en línea]. Agosto 2002. [citado diciembre 17, 2005]. Disponible en Internet: [http://nagios.sourceforge.net/download/contrib/documentation/english/Nagios\\_1\\_0\\_Docs.pdf](http://nagios.sourceforge.net/download/contrib/documentation/english/Nagios_1_0_Docs.pdf)

**Totkat.org**. Installing Nagios [en línea]. s.d [citado diciembre 15, 2005]. Disponible en Internet: <http://totkat.org/pages/nagios-conf.html>

**s.a.** Nagios [en línea] s.d [citado diciembre 8, 2005]. Disponible en Internet: <http://jornadespl.upc.es/vell-02/jplupc2003/NAGIOS/html/nagios.html>