

Nagios:

Herramienta libre para la

monitorización de Sistemas

Eduardo González de la Herrán
NHT-Norwick (<http://www.nht-norwick.com>)

egonzalez@nht-norwick.com

Febrero 2005

Resumen de contenidos

- Presentación de Nagios como solución al problema de la monitorización de Sistemas y Red.
- Posibilidades de la plataforma para una Pyme.
- Instalación y Configuración inicial de Nagios.
- Ficheros de configuración.
- Consola web de monitorización.
- Escalabilidad, personalización, plugins y addons.
- Demostración, ejemplos y conclusiones.

Presentación de Nagios (I)

- Utilidad y Necesidad de un buen sistema de monitorización de servicios, hosts y red.
 - Permite desarrollar una estrategia proactiva ante determinados problemas frente al típico enfoque reactivo.
 - Libera a los administradores de realizar chequeos periódicos a determinados servicios críticos.
 - Alerta situaciones sobre las que tardaríamos mucho en darnos cuenta en otras circunstancias. Llenado de filesystems, perdidas de servicio, etc.

Presentación de Nagios (II)

- Herramientas de monitorización:
 - Aplicaciones sencillas de escritorio como netoscope, mars, etc:
 - Orientadas sólo al chequeo de puertos.
 - Muy fáciles de utilizar pero poco adaptables a nuestras necesidades.
 - Software privativo con licencias baratas y software libre.
 - Sniffers, analizadores de red: tcpdump, ettercap, ethereal, iptraff, etc.
 - Muy útiles en la resolución y análisis de problemas, pero no aconsejados para el uso habitual en la monitorización.

Presentación de Nagios (III)

- Herramientas de monitorización:
 - Macro-sistemas de monitorización complejos como HP Openview, Tivoli, etc.
 - Aplicaciones muy potentes que consumen muchos recursos.
 - Licencias desorbitadas e inaccesibles o no reentables para muchas empresas.
 - Funcionalidades no necesarias en numerosos entornos.
 - Poco flexibles.

Presentación de Nagios (IV)

- Herramientas de monitorización:
 - Sistemas de monitorización completos basados en Software Libre (Nagios):
 - Cubren necesidades básicas de forma sencilla.
 - Completamente adaptables y modificables para necesidades específicas.
 - Fácil integración con scripts y aplicaciones externas.
 - Licencia libre.

Presentación de Nagios (V)

- ¿Qué es Nagios?
 - Nagios es una aplicación para la monitorización de Red y Sistemas escrita por Ethan Galstad.
 - Nagios vigila constantemente hosts, servicios y cualquier cosa que definamos alertándonos cuando aparecen los problemas y cuando se solucionan.
 - Nagios está escrito en C y es Software Libre (Licencia GPL versión 2).
 - Nagios es muy flexible y adaptable a cualquier situación o necesidad.

Presentación de Nagios (VI)

- Características principales de Nagios versión 1.2:
 - Monitorización de servicios de red: SMTP, POP3, HTTP, SSH, DNS, etc.
 - Monitorización de recursos: Carga de procesador, espacio libre en filesystems, uso de la memoria, etc.
 - Capacidad de desarrollar plugins de forma sencilla que permite a los usuarios programar sus propios chequeos. Flexibilidad!!
 - Capacidad de definir una topología o jerarquía de red que permita distinguir entre servicios caídos o inaccesibles.

Presentación de Nagios (VII)

- Características principales de Nagios versión 1.2:
 - Envío de notificaciones mediante múltiples métodos cuando los problemas aparecen y cuando se resuelven (vía email, SMS, im, alertas sonoras, ...). Flexibilidad!!
 - Capacidad de definir eventos para que se ejecuten en caso de problemas, lo que permite utilizar una estrategia proactiva en la resolución de problemas.
 - Consola web para la visualización del estado actual de todos los servicios, generación de estadísticas, historial de alarmas, etc.
 - Soporte de bases de datos para el almacenamiento de datos externos (por defecto se utilizan ficheros de texto).

Posibilidades de la plataforma para una PYME

- Como servicio para la propia empresa:
 - La monitorización de la red ayuda a prevenir problemas y a obtener tiempos de respuesta menores ante incidencias.
- Como negocio:
 - Un nivel de conocimiento alto de Nagios va a permitir ofrecer servicios de consultoría, desarrollos a medida e implantación a clientes.
 - Servicio de monitorización a terceros sobre una plataforma existente.

Instalación y Configuración de Nagios (I)

- Consejos generales.
 - Paciencia: La instalación y configuración completa no es un proceso fácil. Requiere un tiempo de aprendizaje.
 - Leer la documentación oficial: Nagios tiene una documentación muy extensa y detallada. Intentar configurar Nagios tras leer la documentación es suficientemente difícil como para no intentarlo sin haberla leído.
 - Utilizar los ficheros de configuración de ejemplo: Estos ficheros ayudan a conocer la sintaxis. Editándolos aprenderemos más rápido (pero no limitarse a los ficheros de ejemplo).

Instalación y Configuración de Nagios (II)

- Instalación: Requisitos previos.
 - Requerimientos Software:
 - El requerimiento principal es una máquina ejecutando el sistema operativo GNU/Linux y un compilador de C.
 - Apache.
 - Librerías gráficas GD, JPEG y PNG.
 - (opcionales) SNMP, MySQL o PostgreSQL.

Instalación y Configuración de Nagios (III)

- Instalación: Resumen.
 - Instalación de Nagios (bajándose fuentes previamente).
 - Ficheros de configuración.
 - Scripts de arranque y parada.
 - Instalación de plugins (bajándose fuentes previamente).
- Tras la instalación no se puede monitorizar nada aún. Primero hay que diseñar y planificar lo que queremos monitorizar y plasmarlo en los ficheros de configuración.

Instalación y Configuración de Nagios (IV)

- Instalación de Nagios 1.2

```
./configure --prefix=/usr/local/nagios --with-  
  cgiurl=/nagios/cgi-bin --with-htmurl=/nagios --with-nagios-  
  user=nagios --with-nagios-grp=nagios
```

```
make all # Compila todo
```

```
make install-config # Instala ficheros de conf. de ejemplo.
```

```
make install-init # Instala scripts de arranque y parada.
```

```
## Consejo: utilizar valores por defecto ##
```

- Instalación de plugins

```
./configure
```

```
make all
```

```
make install
```

Instalación y Configuración de Nagios (V)

- Instalación: Estructura de directorios
 - bin/ Ejecutable principal de Nagios.
 - etc/ Ficheros de configuración.
 - sbin/ CGIs
 - share/ Ficheros HTML del interfaz web y documentación.
 - var/ Directorio vacío para logs, etc.
 - libexec/ Plugins, ejecutables que realizan los chequeos.

Instalación y Configuración de Nagios (VI)

- ¿Que tenemos ahora? --> Casi nada.
- ¿Qué falta para empezar?
 - Configuración del interfaz web.
 - Configuración básica de Nagios para nuestro caso concreto.
 - Habilitar la ejecución de los CGIs y la autenticación.
 - Habilitar los comandos externos.
- ¿Y qué mas puede hacer?
 - Configuración avanzada, Addons, SNMP, Notificaciones SMS, chequeos pasivos, etc.

Instalación y Configuración de Nagios (VII)

- Configuración del Interfaz Web:
 - Modificaciones en httpd.conf (apache)

```
ScriptAlias /nagios/cgi-bin/ /usr/local/nagios/sbin/  
<Directory "/usr/local/nagios/sbin/">  
    AllowOverride AuthConfig #Para autenticación htpasswd  
    Options ExecCGI  
    Order allow,deny  
    Allow from all  
</Directory>
```

Instalación y Configuración de Nagios (VIII)

- Configuración del Interfaz Web:

```
Alias /nagios/ /usr/local/nagios/share/  
<Directory "/usr/local/nagios/share">  
    Options None  
    AllowOverride AuthConfig # Para autenticación htpasswd  
    Order allow,deny  
    Allow from all  
</Directory>
```

Instalación y Configuración de Nagios (IX)

- Configuración del Interfaz Web:
 - Autenticación mediante htpasswd: para cgis normalmente y opcionalmente para el acceso a los htmls.

```
# htpasswd -c /usr/local/nagios/etc/htpasswd.users USUARIO1
# htpasswd /usr/local/nagios/etc/htpasswd.users USUARIO2
# cat > /usr/local/nagios/sbin/.htaccess    (y a /share/ opcional)
AuthName "Nagios Access"
AuthType Basic
AuthUserFile /usr/local/nagios/etc/htpasswd.users
require valid-user
(CTRL + D)
```

Ficheros de Configuración de Nagios (I)

- Resumen

- `nagios.cfg` --> Fichero de configuración principal; contiene “includes” al resto de ficheros. Opciones de configuración de la aplicación en general.
- `cgi.cfg` --> Fichero de configuración del funcionamiento de los cgis, autenticación, permisos, etc.
- `resource.cfg` --> Definición de variables y macros de Nagios.
- `hosts.cfg`, `hostgroups.cfg`, `services.cfg`, `dependencies.cfg`, `escalations.cfg`, `timeperiods.cfg`, `contacts.cfg`, `contactgroups.cfg`, `checkcommands.cfg`, `miscommands.cfg` --> Objetos de configuración.

Ficheros de Configuración de Nagios (III)

- Ficheros de configuración de objetos:
 - Configuración en ficheros de texto orientada a plantillas (templates). Herencia y sobrescritura de atributos en el uso de plantillas.
 - Atributos para definición y uso de plantillas:
 - name nombre_plantilla: Da un nombre a la plantilla
 - use nombre_plantilla: Indica un nombre de plantilla a utilizar.
 - register [0/1]: Indica si hay que instanciar el objeto o no.

Ficheros de Configuración de Nagios (IV)

- Ficheros de configuración de objetos:
 - Definición de objetos, sintaxis:

```
define tipo_de_objeto {
    atributo1    valor1
    atributo2    valor2
    atributo3    valor31,valor32,valor33,...
    ...
    ...
    use          plantilla_a_utilizar
    register    0 # en este ejemplo
    name        mi_plantilla
}
```

Ficheros de Configuración de Nagios (V)

- hosts.cfg

```
define host{  
    host_name          host_name  
    alias              alias  
    address            address  
    parents            host_names  
    check_command      command_name  
    max_check_attempts #  
    checks_enabled     [0/1]  
    notification_interval #  
    notification_period timeperiod_name  
    notification_options [d,u,r]  
    notifications_enabled [0/1]  
}
```

Ficheros de Configuración de Nagios (VI)

- **services.cfg**

```
define service{
    host_name          host_name
    service_description service_description
    check_command      command_name
    max_check_attempts #
    normal_check_interval #
    retry_check_interval #
    check_period       timeperiod_name
    notification_interval #
    notification_period timeperiod_name
    notification_options [w,u,c,r]
    notifications_enabled [0/1]
    contact_groups     contact_groups
}
```

Ficheros de Configuración de Nagios (VII)

- **contacts.cfg**

```
define contact{  
    contact_name          contact_name  
    alias                 alias  
    host_notification_period    timeperiod_name  
    service_notification_period timeperiod_name  
    host_notification_options  [d,u,r,n]  
    service_notification_options [w,u,c,r,n]  
    host_notification_commands  command_name  
    service_notification_commands command_name  
    email                    email_address  
}
```

Ficheros de Configuración de Nagios (VIII)

- hostgroups.cfg

```
define hostgroup{  
    hostgroup_name    hostgroup_name  
    alias             alias  
    contact_groups    contact_groups  
    members           members  
}
```

Ficheros de Configuración de Nagios (IX)

- **contactgroups.cfg**

```
define contactgroup{  
    contactgroup_name    contactgroup_name  
    alias                 alias  
    members               members  
}
```

Ficheros de Configuración de Nagios (X)

- `timeperiods.cfg`

```
define timeperiod{  
    timeperiod_name timeperiod_name  
    alias            alias  
    sunday          timeranges  
    monday          timeranges  
    tuesday         timeranges  
    wednesday       timeranges  
    thursday        timeranges  
    friday          timeranges  
    saturday        timeranges  
}
```

Ficheros de Configuración de Nagios (XI)

- checkcommands.cfg y misccommands.cfg

```
define command{  
    command_name    command_name  
    command_line    command_line  
}
```

#Ejemplo:

```
define command{  
    command_name    check_pop  
    command_line    /usr/local/nagios/libexec/check_pop  
                   -H $HOSTADDRESS$  
}
```

Ficheros de Configuración de Nagios (XII)

- Trucos para ahorrar tiempo en la configuración
 - Utilizar plantillas y agrupar atributos comunes.
 - Múltiples host o grupos de host en servicios, incluso todos (*)

```
define service {  
    hostgroup_name      grupo1, grupo2  
    service_description NOM_SERVICIO  
    resto atributos...  
}
```

- Para crear un grupo de hosts con todos los hosts podemos utilizar también el '*' en el atributo members.

Arrancando y parando Nagios

- Verificación de la configuración
 - `/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg`
- Iniciar Nagios:
 - `/etc/init.d/nagios start`
- Parar Nagios:
 - `/etc/init.d/nagios stop`

Configuración de CGIs

- Activar la autenticación en los CGIs
 - `use_authentication=1` en `cgi.cfg`
- Diferencias entre contactos autenticados y usuarios autenticados en la implementación de los permisos de ejecución de los CGIs.
- Otros permisos adicionales que se pueden configurar en los CGIs.

Comandos externos

- Habilitar comandos externos:
 - Los comandos externos permiten modificar el comportamiento de nagios desde el interfaz web. Sirven para deshabilitar chequeos de servicios y hosts, solicitar un chequeo instantáneo, planificar una parada de servicio, etc...
 - Modificaciones para habilitar comandos externos (en main.cf):
 - `check_external_commands`
 - `command_check_interval`
 - `command_file` (y asignar permisos en el directorio elegido (/nagios/var/rw)).

Plugins de Nagios (I)

- Los plugins son los encargados de realizar toda la monitorización (chequeos de hosts y de servicios).
- Son ficheros binarios o scripts ejecutables
- Tanto los chequeos como las notificaciones en nagios son realmente ejecutables del sistema. Aquí radica gran parte de la flexibilidad de nagios.
- Los plugins oficiales de nagios son tanto scripts en Perl y Shell como programas escritos en C.
- Sin los plugins no se puede realizar la monitorización.

Plugins de Nagios (II)

- Consejo: Aprender a utilizar cada uno de los plugins. Es la forma de conocer los límites de la monitorización.

- Ejemplos:

```
nagios:/usr/local/nagios/libexec# ./check_snmp_storage.pl --help
```

```
nagios:/usr/local/nagios/libexec# ./check_http --help
```

- Siempre podremos escribir nuestros propios plugins. Para ello leer la especificación de como escribirlos.

Plugins de Nagios (II)

- Plugins oficiales de Nagios:
 - Versión 1.3.1 (Julio 2003)
 - Versión 1.4 (Febrero 2005)
- Plugins “Patrick's Proy” (SNMP)
 - <http://www.manubulon.com/nagios/>
- Otros extras, addons y otros plugins:
 - <http://www.nagios.org/download/extras.php>

Interfaz Web de Nagios (I)

- Con la consola web de monitorización de Nagios podemos, desde cualquier lugar:
 - Acceder a la documentación online de Nagios.
 - Obtener un resumen general del estado del sistema.
 - Conocer el estado actual de todos los servicios y hosts chequeados.
 - Visualizar un mapa de estado con todos los hosts.
 - Visualizar un mapa en 3D (cliente vrml en el navegador).
 - Obtener un resumen de todos los problemas.
 - Añadir comentarios a diferentes situaciones, hosts y servicios.

Interfaz Web de Nagios (II)

- Obtener estadísticas de disponibilidad y estado de los diferentes hosts y servicios.
- Obtener listados del histórico de alertas.
- Obtener listados de notificaciones enviadas.
- Ver los ficheros de configuración y el log de eventos.
- Deshabilitar los chequeos que creamos oportunos.
- Deshabilitar los manejadores de eventos.
- Solicitar chequeo inmediato de un servicio o host.
- Planificar paradas de servicio.

Nagios Extras y Addons (I)

- Existen numerosas aplicaciones desarrolladas por la comunidad que complementan la funcionalidad de Nagios. La mayoría de ellas se publican en la propia página web de Nagios
 - <http://www.nagios.org/download/extras.php>
- Tenemos desde interfaces web para realizar configuración de nagios hasta demonios encargados de enviar notificaciones por ICQ.

Nagios Extras y Addons (II)

- Entre ellos destacamos:
 - NAGAT: Interfaz web escrito en php para realizar la configuración de Nagios (services, hosts, contacts, etc.).
 - APAN: Integración de Nagios con RRD-tool para generar mejores gráficos y estadísticas.
 - NRPE y NRPE_NT: Demonio para ejecutar los plugins de nagios en hosts remotos. De esta forma podemos controlar la carga del sistema, espacio de filesystems, etc sobre hosts remotos. NOTA: Los plugins deben estar instalados en cada máquina de destino.
 - NSCLient: Permite a Nagios obtener información importante sobre hosts Windows NT/2000/XP.
 - Plugins SNMP: Muy útiles. Intercambian información gracias a SNMP. Normalmente son independientes de la plataforma de destino.

Configuración Avanzada

- Otros aspectos de Nagios a tener en cuenta:
 - EventHandlers.
 - Escalations y Dependencies.
 - Passive Checks.
 - Hostextinfo y serviceextinfo.
 - Alarmas SMS con gnokii.

Otras aplicaciones libres de monitorización

- Just For Fun Network Management System
- Angel Network Monitor
- Sysmon
- Mars

Referencias

- <http://www.nagios.org>
- <http://www.totkat.org/>
- <http://dag.wieers.com/packages/nagios-nrpe/>
- <http://www.gnokii.org>
- <http://www.jffnms.com>
- <http://www.manubulon.com/nagios/>
- <http://www.altara.org/mars.html>

Licencia

Copyright 2005. Eduardo González de la Herrán

Copyleft 2005. Eduardo González de la Herrán

Se permite la copia, distribución, uso y realización de la obra, siempre y cuando se reconozca la autoría y no se use la obra con fines comerciales --a no ser que se obtenga permiso expreso del autor--. El autor permite distribuir obras derivadas de esta sólo si mantienen la misma licencia que esta obra.

Esta nota no es la licencia completa de la obra sino una traducción de la nota orientativa de la licencia original completa (jurídicamente válida), que puede encontrarse en:
<http://creativecommons.org/licenses/by-nc-sa/1.0/legalcode>

Para la realización de la obra se ha utilizado la documentación oficial de Nagios 1.2 escrita por Ethan Galstad.