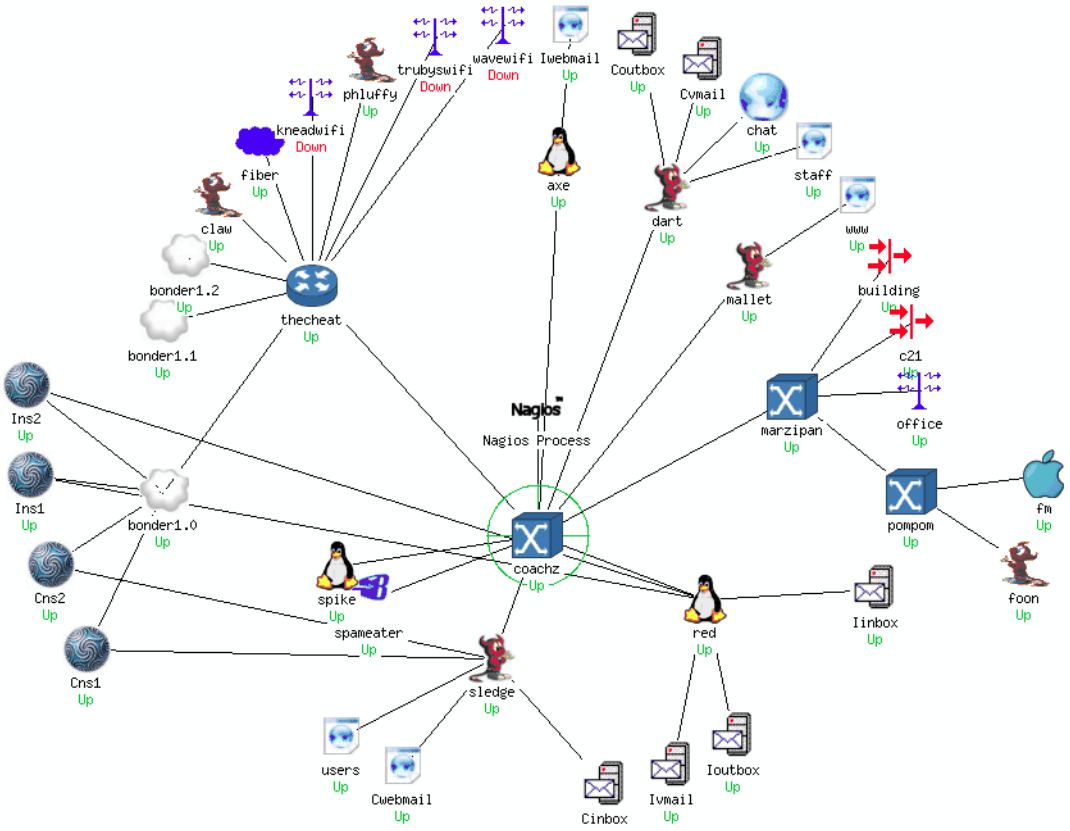
Técnicas de monitorización de red con Nagios.



Nota sobre la obra:

Técnicas de monitorización de redes con nagios por Kamal Majaiti se encuentra bajo una Licencia Creative Commons Atribución-NoComercial-Compartir Igual 3.0 Unported.

Esto quiere decir que:

- No se permiten usos comerciales de la obra.
- Se permitir modificaciones y mejoras de la obra mientras se comparta bajo la misma licencia.
- La Jurisdicción de la licencia es Internacional.

Respecto al autor

La obra está realizada por Kamal Majaiti y queda atribuida a Kamal Majaiti con el cual se puede contactar mediante twitter mediante el siguiente Nick @kamalsenior o a través de la url https://twitter.com/kamalsenior. Ya sea para resolver una duda o cualquier otro interés.

(cc) BY-NC-SA

1. Información Sobre Nagios

1.1 ¿Qué es Nagios?

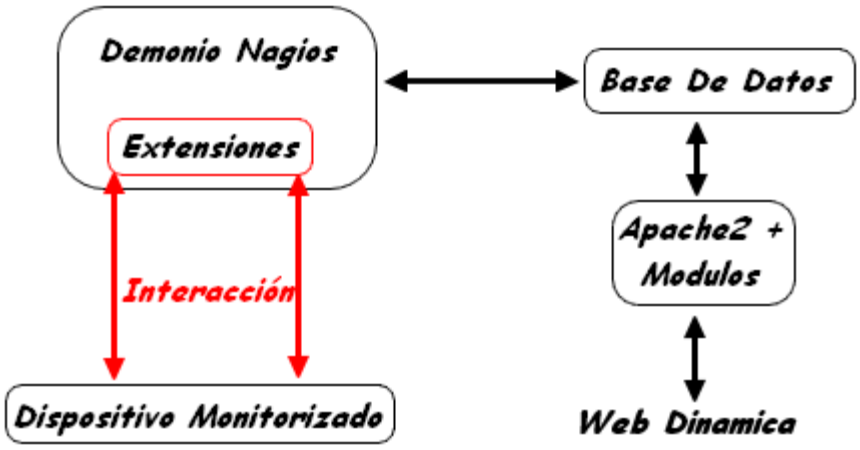
Nagios es un Sistema de Control y Observación de redes, ampliamente utilizado en sistemas Unix y derivados.

1.2 ¿Qué permite Nagios?

-Monitorizar servicios.
-Monitorizar Recursos.
-Notificación de incidencias.
-Cualquier funcionalidad se puede agregar mediante extensiones.

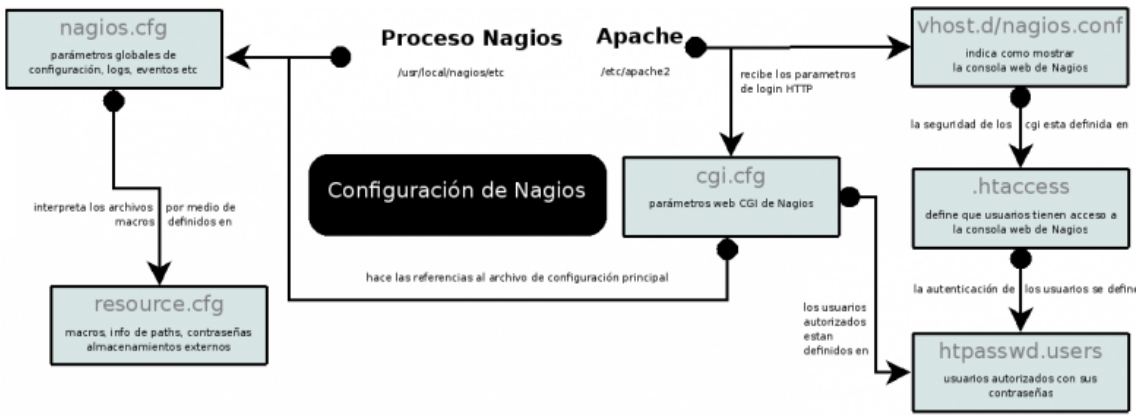
1.3 Funcionamiento de Nagios.

Una imagen vale más que mil palabras.



Núcleo: Es un demonio que realiza las operaciones lógicas y controla las extensiones.
Extensiones: Son pequeños programas que añaden funcionalidad al núcleo.

1.4 Archivos de configuración de Nagios.



Los archivos más importantes son:
/etc/nagios3/nagios.cfg
Contiene los parámetros globales de configuración de Nagios.

(cc) BY-NC-SA

/etc/nagios3/cgi.cfg
Contiene los parámetros de Seguridad CGI **permisos** de escritura y lectura así como ejecución de scripts.

/etc/nagios3/apache2.conf
Contiene los parámetros de configuración del host virtual de apache2.

/etc/nagios3/commands.cfg
Contiene las acciones que puede tomar Nagios así como las tareas de mantenimiento.

/etc/nagios3/htpasswd.users
Contiene los usuarios autorizados para acceder a Nagios.

Y dentro de **/etc/nagios3/conf.d/**

```
root@Usrv-sad-kml:/etc/nagios3/conf.d# ls
contacts_nagios2.cfg       generic-service_nagios2.cfg  localhost_nagios2.cfg
extinfo_nagios2.cfg        host-gateway_nagios3.cfg     services_nagios2.cfg
generic-host_nagios2.cfg   hostgroups_nagios2.cfg       timeperiods_nagios2.cfg
root@Usrv-sad-kml:/etc/nagios3/conf.d#
```

Se encuentran los objetos de configuración de Nagios.
Contactos de Administración, Servicios, Dispositivos.

2. Instalación de Nagios.

La instalación se puede realizar de dos formas la primera es compilando el código fuente descargado desde sourceforge y la segunda es la instalación de paquetes binarios desde los repositorios de tu distribución.

2.1 Instalacion de nagios desde el repositorio.

En este caso buscamos los paquetes de nagios. Como se aprecia no son pocos.

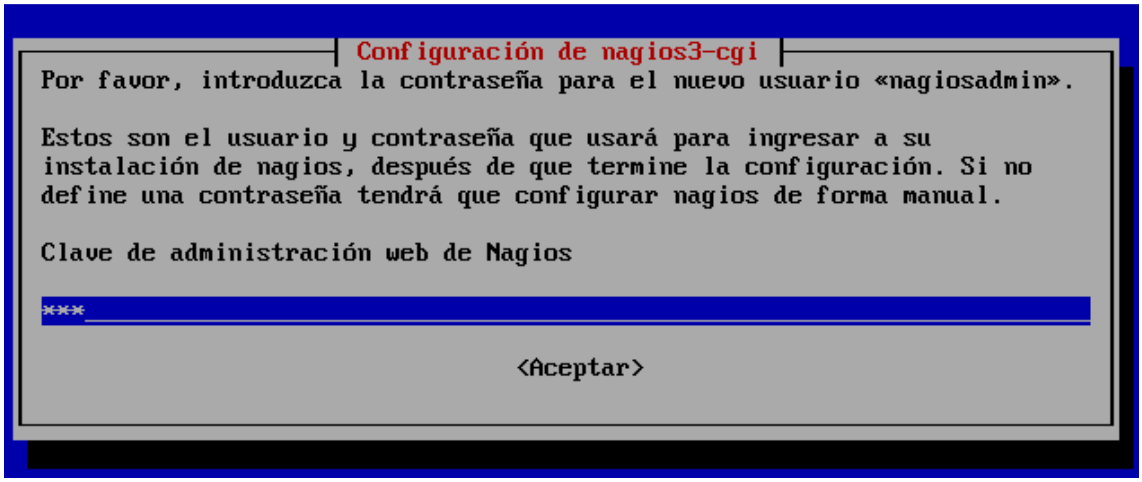
```
root@Usrv-sad-kml:~# aptitude search nagios
p   libnagios-object-perl          - Perl module to parse and represent Nagios
p   libnagios-plugin-perl          - family of perl modules to streamline writi
p   nagios-images                  - Colección de imágenes e iconos parea el si
p   nagios-nrpe-plugin             - Nagios Remote Plugin Executor Plugin
p   nagios-nrpe-server             - Nagios Remote Plugin Executor Server
p   nagios-plugins                 - Complementos para la monitorización de red
p   nagios-plugins-basic           - Complementos para la monitorización de red
p   nagios-plugins-extra           - Plugins for the nagios network monitoring
p   nagios-plugins-standard        - Complementos para la monitorización de red
p   nagios-snmp-plugins            - Complementos SNMP para nagios
p   nagios-statd-client            - Nagios client for monitoring remote system
p   nagios-statd-server            - Nagios server for monitoring remote system
p   nagios3                        - A host/service/network monitoring and mana
p   nagios3-cgi                    - cgi files for nagios3
p   nagios3-common                 - support files for nagios3
p   nagios3-core                   - A host/service/network monitoring and mana
p   nagios3-dbg                    - debugging symbols and debug stuff for nagi
p   nagios3-doc                    - documentation for nagios3
p   nagiosgrapher                  - Charting add-on for Nagios
p   ndoutils-nagios3-mysql         - This provides the NDOUtils for Nagios with
```

La instalación se realiza de la siguiente forma. **Aptitude install nagios3**

(cc) BY-NC-SA

```
root@Usrv-sad-kml:~# aptitude install nagios3
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Leyendo la información de estado extendido
Inicializando el estado de los paquetes... Hecho
Se instalarán los siguiente paquetes NUEVOS:
  apache2{a} apache2-mpm-worker{a} apache2-utils{a} apache2.2-bin{a}
  apache2.2-common{a} bsd-mailx{a} fancontrol{a} gawk{a} libapr1{a}
  libaprutil1{a} libaprutil1-dbd-sqlite3{a} libaprutil1-ldap{a}
  libgd2-noxpm{a} libjpeg62{a} libmysqlclient16{a} libnet-snmp-perl{a}
  libperl5.10{a} libpq5{a} libradius1{a} libsensors4{a} libsnmp-base{a}
  libsnmp15{a} lm-sensors{a} mysql-common{a} nagios-images{a}
  nagios-plugins{a} nagios-plugins-basic{a} nagios-plugins-standard{a}
  nagios3 nagios3-cgi{a} nagios3-common{a} nagios3-core{a} postfix{a}
  radiusclient1{a} smbclient{a} snmp{a}
```

Después le ponemos la contraseña de acceso.



3. Configuracion Basica de nagios (usuarios).

1. *Añadir un usuario con privilegios de Administrador.*

Para añadir un usuario en Nagios debemos añadirlo al archivo de autorización y luego darle privilegios en el archivo cgi.cfg.

Para ello se realiza así:

```
root@Usrv-sad-kml:~# htpasswd /etc/nagios3/htpasswd.users kamal
New password:
Re-type new password:
Adding password for user kamal
root@Usrv-sad-kml:~#
```

Después editamos el archivo de privilegios cgi para poder darle privilegios.

`Archivo: /etc/nagios3/cgi.cfg`

Añadimos las directivas (Clonamos).

Privilegio sobre información de procesos.

```
authorized_for_system_information=nagiosadmin,kamal
```

Privilegio sobre la información de configuración de Nagios.

(cc) BY-NC-SA

```
authorized_for_configuration_information=nagiosadmin,kamal
```

Privilegio para poder ejecutar comandos en la maquina Nagios.

```
authorized_for_system_commands=nagiosadmin,kamal
```

Autorización de acceso desde cualquier servicio.

```
authorized_for_all_services=nagiosadmin,kamal
```

Autorización de acceso desde cualquier equipo /Dirección IP.

```
authorized_for_all_hosts=nagiosadmin,kamal
```

2. Añadir un usuario con privilegios Mínimos.

Quizás al becario u otra persona le interesa saber el estado de la red pero para evitar problemas le damos permisos solo de lectura.

Añadimos al usuario lector.

```
root@Usrv-sad-kml:~# htpasswd /etc/nagios3/htpasswd.users becario
New password:
Re-type new password:
Adding password for user becario
root@Usrv-sad-kml:~#
```

Una vez hecho le damos permisos de lectura.

```
Archivo: /etc/nagios3/cgi.cfg
```

Al final del todo.

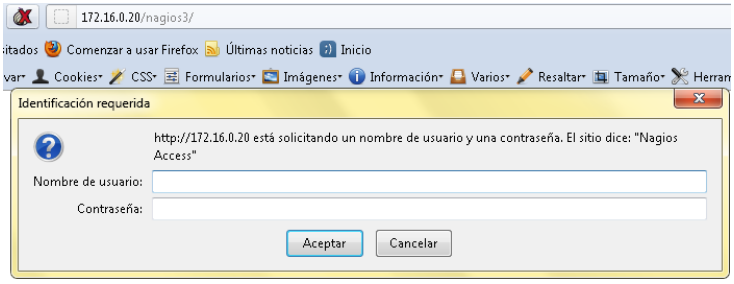
Lo añadimos en la directiva.

```
authorized_for_read_only=becario,empresario
```

3. Deshabilitar al usuario por defecto. (No recomendado)

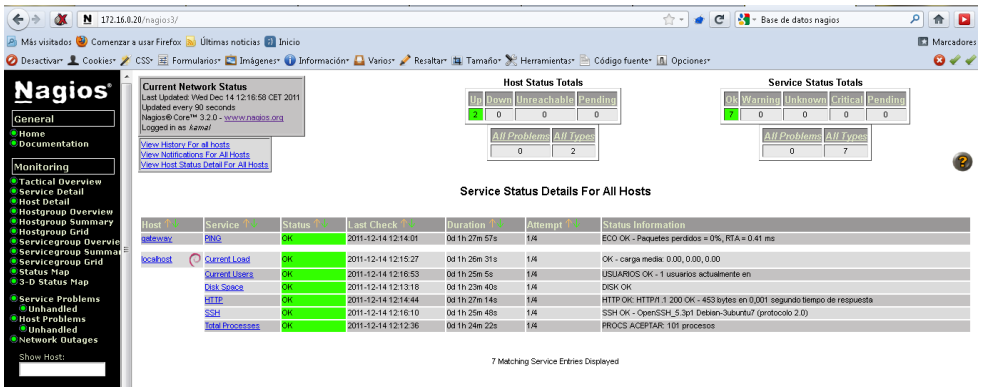
```
  GNU nano 2.2.2      Archivo: /etc/nagios3/htpasswd.users

#nagiosadmin:Rrs5lDdXc4oIM
kamal:UkDscTHh.qVKo
becario:UTA9cmKlmwJr6
```

Una vez hecho esto podemos acceder a Nagios por primera vez. http://**host**/nagios3/



Ponemos nuestras claves de acceso y accedemos.

(cc) BY-NC-SA



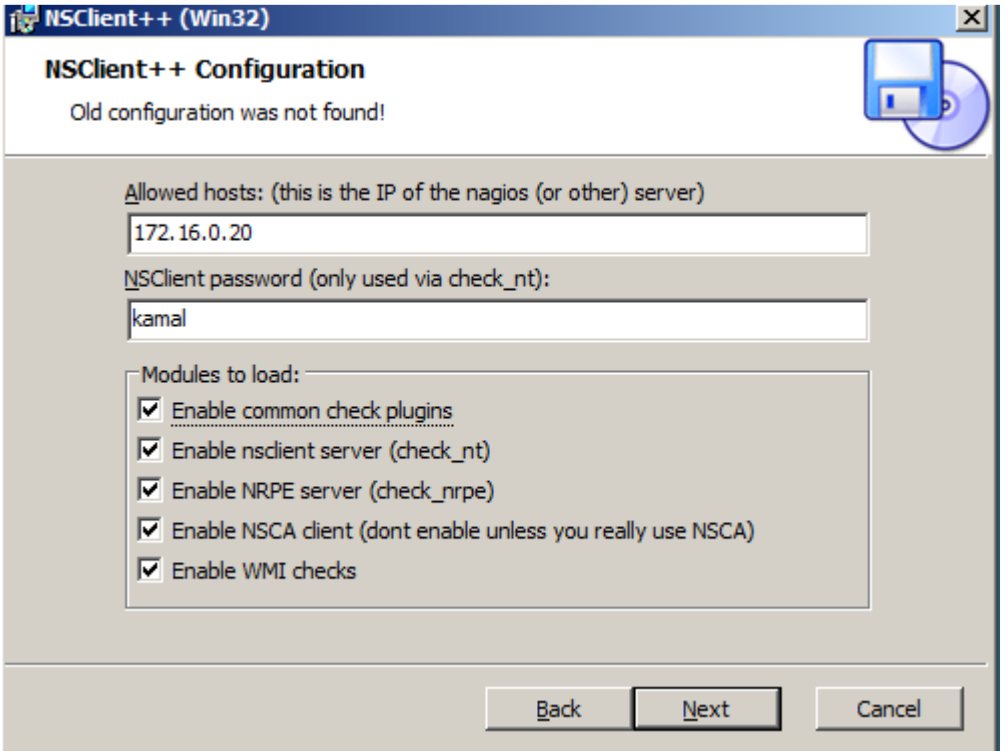
4. Añadir Dispositivos a Nagios.

Monitorización de Servidor Windows.

Primero nos descargamos el cliente de Nagios de la página web.

http://sourceforge.net/projects/nscplus/

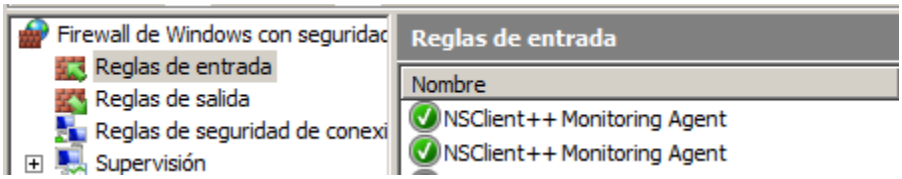
Después en el instalador configuramos los parámetros de monitorización. En mi caso active todas las opciones.



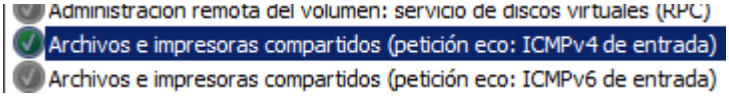
Y por ultimo lo instalamos.

(cc) BY-NC-SA

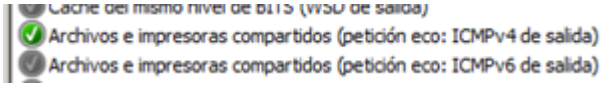
Se aprecia que el instalador modifico el cortafuegos añadiendo sus propias excepciones.



Después permitimos la entrada de eco al servidor.



Y a la salida.



Con esto ya tenemos al equipo preparado ahora toca el servidor Nagios que es algo más tedioso.

1º Buscamos la plantilla de Nagios para Windows.

```
root@Usrv-sad-kml:/etc/nagios3# dpkg -S windows.cfg
nagios3-common: /usr/share/doc/nagios3-common/examples/template-object/windows.c
fg
root@Usrv-sad-kml:/etc/nagios3#
```

2º La copiamos a conf.d dentro de Nagios.

```
root@Usrv-sad-kml:/etc/nagios3/conf.d# cp /usr/share/doc/nagios3-common/examples
/template-object/windows.cfg /etc/nagios3/conf.d/
root@Usrv-sad-kml:/etc/nagios3/conf.d#
```

3º Reiniciamos Nagios.

```
Error: Template 'windows-server' specified in host definition could not be not f
ound (config file '/etc/nagios3/conf.d/windows.cfg', starting on line 25)
   Error processing object config files!
```

Y aparece un error esto quiere decir que falta la plantilla llamada Windows-server que está definida en el archivo.

(cc) BY-NC-SA

```
 GNU nano 2.2.2            Archivo: windows.cfg

##############################################################################
##############################################################################
#
# HOST DEFINITIONS
#
##############################################################################
##############################################################################

# Define a host for the Windows machine we'll be monitoring
# Change the host_name, alias, and address to fit your situation

define host{
        use             windows-server  ; Inherit default values from a template
        host_name       winserver       ; The name we're giving to this host
        alias           My Windows Server       ; A longer name associated with$
        address         192.168.1.2     ; IP address of the host
        }
```

Así que de momento para salir del paso copiamos la plantilla genérica al equipo.

```
root@Usrv-sad-kml:/etc/nagios3/conf.d# cp generic-host_nagios2.cfg windows-serve
r.cfg
root@Usrv-sad-kml:/etc/nagios3/conf.d# _
```

Una vez copiada la editamos y cambiamos el nombre de la plantilla.

```
 GNU nano 2.2.2        Archivo: windows-server.cfg                Modificado

# Generic host definition template - This is NOT a real host, just a template!

define host{
        name                            windows-server    ; The name of this ho$
        notifications_enabled           1       ; Host notifications are enabled
        event_handler_enabled           1       ; Host event handler is enabled
        flap_detection_enabled          1       ; Flap detection is enabled
        failure_prediction_enabled      1       ; Failure prediction is enabled
```

Y si ahora reiniciamos.

```
root@Usrv-sad-kml:/etc/nagios3/conf.d# service nagios3 restart
 * Restarting nagios3 monitoring daemon nagios3
                                                                    [ OK ]
root@Usrv-sad-kml:/etc/nagios3/conf.d#
```

Una vez que funciona le cambiamos la ip y el nombre al equipo.

```
 GNU nano 2.2.2            Archivo: windows.cfg                   Modificado

define host{
        use             windows-server  ; Inherit default values from a template
        host_name       winserver       ; The name we're giving to this host
        alias           WinServ08-SRI   ; A longer name associated with the host
        address         172.16.0.34     ; IP address of the host
        }
```

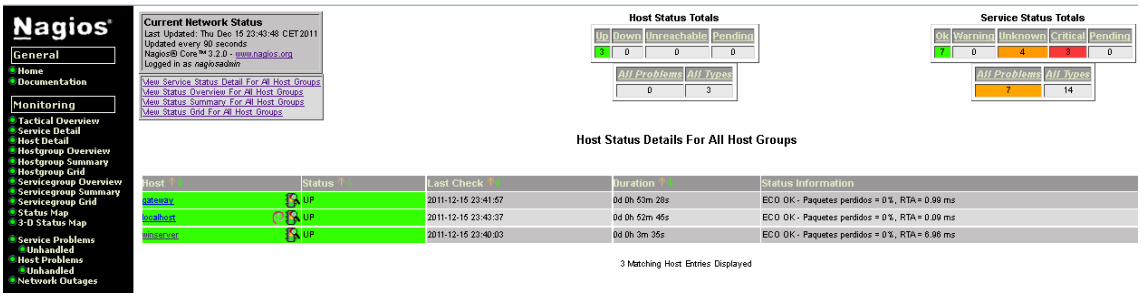
El hostname no lo cambiamos porque si no lo tendríamos que cambiar más abajo en cada fichero.

(cc) BY-NC-SA

Una vez hecho reiniciamos el servicio de Nagios.

```
root@Usrv-sad-kml:/etc/nagios3/conf.d# service nagios3 restart
 * Restarting nagios3 monitoring daemon nagios3
Waiting for nagios3 daemon to die.....
kill: 1: No such process
```

Y miramos el resultado.



Pero si entramos en el Windows Server veremos que tenemos unos errores.

Le damos al semáforo para ver los detalles.

Host	Service	Status	Last Check	Duration
winserver	C:\ Drive Space	UNKNOWN	2011-12-15 23:43:15	0d 0h 14m 48s
	CPU Load	UNKNOWN	2011-12-15 23:41:10	0d 0h 13m 44s
	Explorer	UNKNOWN	2011-12-15 23:42:14	0d 0h 12m 40s
	Memory Usage	CRITICAL	2011-12-15 23:42:11	0d 0h 15m 35s
	NSClient++ Version	CRITICAL	2011-12-15 23:43:15	0d 0h 15m 31s
	Uptime	CRITICAL	2011-12-15 23:44:20	0d 0h 14m 27s
	W3SVC	UNKNOWN	2011-12-15 23:41:32	0d 0h 13m 22s

Y se aprecia que algo funciona mal.

Esto es porque en la instalación le pusimos contraseña al servicio de Nagios así que al cliente hay que indicársela.

Para ello debemos editar el fichero de la extensión se indica en la fotografía.

```
root@Usrv-sad-kml:~# cat /etc/nagios-plugins/config/nt.cfg
# If you are confused about this command definition, cause you was
# reading other suggestions, please have a look into
# /usr/share/doc/nagios-plugins/README.Debian

# 'check_nt' command definition
define command {
        command_name    check_nt
        command_line    /usr/lib/nagios/plugins/check_nt -H '$HOSTADDRESS$' -v '
$ARG1$'
}

# 'check_nscp' command definition
define command {
        command_name    check_nscp
        command_line    /usr/lib/nagios/plugins/check_nt -H '$HOSTADDRESS$' -p 1
2489 -v '$ARG1$'
}
root@Usrv-sad-kml:~#
```


(cc) BY-NC-SA

Si ejecutamos ese comando a por si solo veremos los parámetros de configuración.

```
root@Usrv-sad-kml:~# /usr/lib/nagios/plugins/check_nt --help | grep pas
 -s, --secret=<password>
   Parámetros pasados a la comprobación específica (ver debajo) -d, --display={S
HOWALL}
root@Usrv-sad-kml:~#
```

Como se aprecia debemos editar el fichero para añadir el puerto y la contraseña.

El puerto de escucha es:

Para verlo en Windows ejecutamos el comando.

```
C:\Users\serv08-kml>netstat -ab | more
```

Y lo buscamos.

```
[nsclient++.exe]
  TCP    0.0.0.0:12489          WIN-OQJY6CD3MNS:0      LISTENING
```

Después con los datos obtenidos modificamos los ficheros.

```
# 'check_nt' command definition
define command {
        command_name    check_nt
        command_line    /usr/lib/nagios/plugins/check_nt -H '$HOSTADDRESS$' -v '
$ARG1$' -s kamal -p 12489
}

# 'check_nscp' command definition
define command {
        command_name    check_nscp
        command_line    /usr/lib/nagios/plugins/check_nt -H '$HOSTADDRESS$' -p 1
2489 -v '$ARG1$' -s kamal }
```

Guardamos y reiniciamos Nagios.

```
root@Usrv-sad-kml:~# service nagios3 restart
 * Restarting nagios3 monitoring daemon nagios3
/sbin/start-stop-daemon: warning: failed to kill 12521: No such process
                                                                    [ OK ]
```

Si ahora lo comprobamos

Host	Service	Status	Last Check	Duration	Attempt	Status Information
winserver	C:\ Drive Space	UNKNOWN	2011-12-16 00:08:15	0d 0h 39m 18s	4/4	se perdieron los parÃ¡metros -l
	CPU Load	UNKNOWN	2011-12-16 00:08:55	0d 0h 38m 14s	4/4	se perdieron los parÃ¡metros -l
	Explorer	UNKNOWN	2011-12-16 00:07:14	0d 0h 37m 10s	4/4	No se especificÃ³ el servicio/proceso
	Memory Usage	OK	2011-12-16 00:07:11	0d 0h 12m 13s	1/4	UtilizaciÃ³n de memoria: total:4330,05 Mb - utilizado: 292,77 Mb (7 %) - libre: 4037,28 Mb (93 %)
	NSClient++ \Version	OK	2011-12-16 00:08:15	0d 0h 11m 9s	1/4	NSClient++ 0.3.9.327 2011-08-16
	Uptime	OK	2011-12-16 00:04:20	0d 0h 6m 4s	1/4	Tiempo de funcionamiento del sistema - 0 dÃa(s) 0 hora(s) 5 minuto(s)
	W3SVC	UNKNOWN	2011-12-16 00:04:59	0d 0h 37m 52s	4/4	No se especificÃ³ el servicio/proceso

Vemos que la cosa ya mejora.

Memory Usage	OK	2011-12-16 00:07:11	0d 0h 11m 19s	1/4	UtilizaciÃ³n de memoria: total:4330,05 Mb - utilizado: 292,77 Mb (7 %) - libre: 4037,28 Mb (93 %)
NSClient++ \Version	OK	2011-12-16 00:08:15	0d 0h 10m 15s	1/4	NSClient++ 0.3.9.327 2011-08-16
Uptime	OK	2011-12-16 00:04:20	0d 0h 4m 10s	1/4	Tiempo de funcionamiento del sistema - 0 dÃa(s) 0 hora(s) 5 minuto(s)

(cc) BY-NC-SA

Pero todo el resto es un bug de debían el cual hay que informar así que mandamos un correo notificando del fallo.

https://lists.ubuntu.com/archives/ubuntu-bugsquad/2011-December/003582.html

Después de informar seguimos arreglando el paquete.

Análisis del problema.

El problema reside en que Nagios a leer el fichero de configuración del host Windows.cfg se encuentra con el espacio y piensa que el comando se acabo entonces lo siguiente los descarta quedando el comando cortado en memoria. La solución es poner los parámetros entre comillas simples 'ejemplo' para que los espacios no los tome con final. Y entren en la variable que le pasa a la extensión.

Monitorizar la carga de CPU

El original venia así:

```
define service{
        use                     generic-service
        host_name               winserver
        service_description     CPU Load
        check_command           check_nt!CPULOAD!-l 5,80,90
        }
```

Y hay que meter los parámetros entre comillas simples.

```
# Create a service for monitoring CPU load
# Change the host_name to match the name of the host you defined above

define service{
        use                     generic-service
        host_name               winserver
        service_description     CPU Load
        check_command           check_nt!CPULOAD!'-l 5,80,90'
        }
```

Monitorización del Memoria RAM

```
# Create a service for monitoring memory usage
# Change the host_name to match the name of the host you defined above

define service{
        use                     generic-service
        host_name               winserver
        service_description     Memory Usage
        check_command           check_nt!MEMUSE!'-w 80 -c 90'
        }
```


(cc) BY-NC-SA

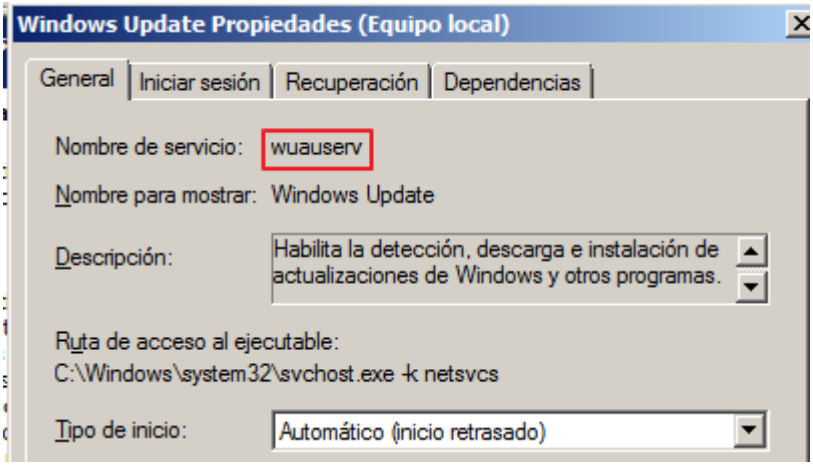
Monitorización de estado de Disco Duro.

```
# Create a service for monitoring C:\ disk usage
# Change the host_name to match the name of the host you defined above

define service{
        use                     generic-service
        host_name               winserver
        service_description     C:\ Drive Space
        check_command           check_nt!USEDDISKSPACE!'-l 5,80,90 c -w 80 -c 90'
        }
```

Había que añadirle las comillas y los parámetros del contador.

Monitorización de un servicio de Windows.

Los servicios de Windows tienen un Nombre identificativo interno para verlo ejecutamos services.msc y vemos el nombre del servicio deseado.



Después en el fichero introducimos los parámetros quedando así:

```
define service{
        use                     generic-service
        host_name               winserver
        service_description     Windows Update
        check_command           check_nt!SERVICESTATE!'-d SHOWALL -l wuauserv '
        }
```

Monitorización de un proceso.

```
define service{
        use                     generic-service
        host_name               winserver
        service_description     Explorer
        check_command           check_nt!PROCSTATE!'-d SHOWALL -l Explorer.exe'
        }
```

Hay que hacer lo mismo poner los parámetros entre comillas.

(cc) BY-NC-SA

Una vez acabado podemos reiniciar el servicio y si nos metemos a la interface web queda así:

Host	Service	Status	Last Check	Duration	Attempt	Status Information
winserver	C:\ Drive Space	UNKNOWN	2011-12-16 03:19:34	0d 0h 9m 29s	4/4	wrong -l argument
	CPU Load	OK	2011-12-16 03:23:20	0d 0h 20m 43s	1/4	CPU Load 0 % (5 min average)
	Explorer	OK	2011-12-16 03:19:52	0d 0h 19m 11s	1/4	Explorer.EXE: Running
	Memory Usage	OK	2011-12-16 03:21:52	0d 0h 42m 11s	1/4	Memory usage: total:4330,05 Mb - used: 308,42 Mb (7 %) - free: 4021,64 Mb (93 %)
	NSClient++ Version	OK	2011-12-16 03:22:38	0d 0h 41m 25s	1/4	NSClient++ 0.3.9.327 2011-08-16
	Uptime	OK	2011-12-16 03:23:24	0d 0h 40m 39s	1/4	System Uptime - 0 day(s) 3 hour(s) 24 minute(s)
	Windows Update	OK	2011-12-16 03:23:02	0d 0h 16m 1s	1/4	wuauserv: Started

7 Matching Service Entries Displayed

Monitorización de un Sistema Linux.

En el caso de un sistema Linux es similar debemos instalar el programa de monitorización de Nagios.

En caso usare backtrack como ordenador que será monitorizado. Para ello debemos instalar el agente de información para Nagios.

```
root@bt:~# aptitude install nagios-nrpe-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
Reading extended state information
Initializing package states... Done
The following NEW packages will be installed:
  libradius1{a} nagios-nrpe-server nagios-plugins{a} nagios-plugins-basic{a} nagios-plugins-standard{a} radiusclient1{a}
0 packages upgraded, 6 newly installed, 0 to remove and 0 not upgraded.
Need to get 996kB of archives. After unpacking 2,998kB will be used.
Do you want to continue? [Y/n/?]
```

Una vez instalado lo iniciamos.

```
root@bt:/etc/nagios# /etc/init.d/nagios-nrpe-server start
 * Starting nagios-nrpe nagios-nrpe
```

Después editamos el fichero de configuración del agente. Y cambiamos la acl del programa.

```
  GNU nano 2.2.2                    File: /etc/nagios/nrpe.cfg

# NRPE GROUP
# This determines the effective group that the NRPE daemon should run as.
# You can either supply a group name or a GID.
#
# NOTE: This option is ignored if NRPE is running under either inetd or xinetd

nrpe_group=nagios



# ALLOWED HOST ADDRESSES
# This is an optional comma-delimited list of IP address or hostnames
# that are allowed to talk to the NRPE daemon.
#
# Note: The daemon only does rudimentary checking of the client's IP
# address.  I would highly recommend adding entries in your /etc/hosts.allow
# file to allow only the specified host to connect to the port
# you are running this daemon on.
#
# NOTE: This option is ignored if NRPE is running under either inetd or xinetd

allowed_hosts=172.16.0.20
```

Siendo 172.16.0.20 la ip del programa. Ahora lo reiniciamos para que se aplique la configuración.

```
root@bt:/etc/nagios# /etc/init.d/nagios-nrpe-server restart
 * Stopping nagios-nrpe nagios-nrpe
 * Starting nagios-nrpe nagios-nrpe
root@bt:/etc/nagios# _
```


(cc) BY-NC-SA

Comprobamos que escucha el agente en el puerto por defecto.

```
root@bt:/etc/nagios# netstat -ltpn
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:5666            0.0.0.0:*               LISTEN      4202/nrpe
```

Ahora en el servidor de monitorización de Nagios debemos instalar la extensión para soportar el agente de Linux.

```
root@nagios:/etc/nagios3/conf.d# aptitude search nrp
p   nagios-nrpe-plugin             - Nagios Remote Plugin Executor Plugin
p   nagios-nrpe-server             - Nagios Remote Plugin Executor Server
p   openrpg                        - client/server application to play RPG over
p   python-transmissionrpc         - Transmission RPC client module for Python
root@nagios:/etc/nagios3/conf.d# aptitude install nagios-nrpe-plugin
Se instalarán los siguiente paquetes NUEVOS:
  nagios-nrpe-plugin
0 paquetes actualizados, 1 nuevos instalados, 0 para eliminar y 0 sin actualizar
.
Necesito descargar 17,8 kB de ficheros. Después de desempaquetar se usarán 98,3
kB.
Err http://ftp.es.debian.org/debian/ squeeze/main nagios-nrpe-plugin i386 2.12-4
  No se pudo resolver «ftp.es.debian.org»
E: Se produjo un fallo al descargar http://ftp.es.debian.org/debian/pool/main/n/
nagios-nrpe/nagios-nrpe-plugin_2.12-4_i386.deb: No se pudo resolver «ftp.es.debi
an.org»
```

Una vez hecho debemos buscar la plantilla. Cosa que no hay pero en la documentación oficial disponemos de plantillas de ejemplo.

http://nagios.sourceforge.net/docs/nrpe/NRPE.pdf

En mi caso creó una parecida en /etc/nagios3/conf.d/Linux.cfg.

```
define host{
use generic-host ; Inherit default values from a template
host_name remotehost ; The name we're giving to this server
alias BackTrack ; A longer name for the server
address 172.16.0.37 ; IP address of the server
}
define service{
use generic-service
host_name remotehost
service_description CPU Load
check_command check_nrpe!check_load
}
define service{
use generic-service
host_name remotehost
service_description Current Users
check_command check_nrpe!check_users
}
define service{
use generic-service
host_name remotehost
service_description /dev/hda1 Free Space
check_command check_nrpe!check_hda1
}
define service{
use generic-service
host_name remotehost
service_description Total Processes
check_command check_nrpe!check_total_procs
}
define service{
use generic-service
host_name remotehost
service_description Zombie Processes
check_command check_nrpe!check_zombie_procs
}
```


BY-NC-SA

Una vez hecho reiniciamos Nagios.

Y aparece así:

Host	Status	Last Check	Duration	Status Information
localhost	UP	2011-12-17 07:12:04	1d 4h 39m 51s	PING OK - Packet loss = 0%, RTA = 0.06 ms
remotehost	UP	2011-12-17 07:13:14	0d 0h 23m 7s	PING OK - Packet loss = 0%, RTA = 0.89 ms

Todo bien pero si vemos los servicios.

Host	Service	Status	Last Check	Duration	Attempt	Status Information
remotehost	/dev/hda1 Free Space	UNKNOWN	2011-12-17 07:16:18	0d 0h 23m 34s	4/4	(No output returned from plugin)
	CPU Load	UNKNOWN	2011-12-17 07:12:08	0d 0h 22m 44s	4/4	(No output returned from plugin)
	Current Users	UNKNOWN	2011-12-17 07:12:58	0d 0h 21m 54s	4/4	(No output returned from plugin)
	Total Processes	UNKNOWN	2011-12-17 07:13:48	0d 0h 21m 4s	4/4	(No output returned from plugin)
	Zombie Processes	UNKNOWN	2011-12-17 07:15:32	0d 0h 20m 14s	4/4	(No output returned from plugin)

Así que lo primero que hacemos el comprobar que funciona la conexión.

Del agente con el plugin de Nagios.

Usando el comando.

/usr/lib/Nagios/plugins/check_nrpe -H 172.16.0.37 -c check_zombie_procs -p 5666

Obtenemos el siguiente resultado.

```
root@nagios:/etc/nagios-plugins/config# /usr/lib/nagios/plugins/check_nrpe -H 17
2.16.0.37 -c check_zombie_procs -p 5666
PROCS OK: 0 processes with STATE = Z
root@nagios:/etc/nagios-plugins/config#
```

Por lo cual descubrimos que el agente funciona correcta mente y el problema reside en el fichero de configuración puesto que está mail o el fichero de configuración del host o el del plugin.

En este caso fue fácil detectar el fallo puesto el problema reside otra vez con la definición de comandos.

```
  GNU nano 2.2.4                    Fichero: /etc/nagios-plugins/config/check_nrpe.cfg

# this command runs a program $ARG1$ with arguments $ARG2$
#define command {
#       command_name    check_nrpe
#       command_line    /usr/lib/nagios/plugins/check_nrpe -H $HOSTADDRESS$ -c $ARG1$  -a $ARG2$
#}

# this command runs a program $ARG1$ with no arguments
define command {
        command_name    check_nrpe
        command_line    /usr/lib/nagios/plugins/check_nrpe -H $HOSTADDRESS$ -c $ARG1$
}
```

En este caso la solución es comentar el cuadrado en rojo (Comando uno) y en el segundo comando cambiarle el nombre a check_nrpe (Rectángulo verde). Una vez hecho reiniciamos Nagios y queda echo. Se ve así☺.

(cc) BY-NC-SA

Otra opción es en el plugin cambiar el nombre del comando al valor que salía antes.

Host	Service	Status	Last Check	Duration	Attempt	Status Information
remotehost	/dev/hda1 Free Space	CRITICAL	2011-12-17 07:21:18	0d 0h 4m 52s	4/4	DISK CRITICAL - /dev/hda1 is not accessible: No such file or directory
	CPU Load	OK	2011-12-17 07:22:08	0d 0h 4m 2s	1/4	OK - load average: 0.00, 0.01, 0.05
	Current Users	OK	2011-12-17 07:22:58	0d 0h 3m 12s	1/4	USERS OK - 1 users currently logged in
	Total Processes	OK	2011-12-17 07:23:48	0d 0h 2m 22s	1/4	PROCS OK: 68 processes
	Zombie Processes	OK	2011-12-17 07:21:29	0d 0h 4m 41s	1/4	PROCS OK: 0 processes with STATE = Z

Pero como se aprecia falla el disco duro.

Esto es debido a que no usamos discos duros IDE lo cuales son llamados hdx en cambio en los discos duros sata/ SCSI son llamados sdx lo cual la solución es fácil.

Editamos el fichero del host y le cambiamos el valor del disco duro.

En mi caso se llama SDA1

```
root@bt:/etc/nagios# df -H
Filesystem             Size   Used  Avail Use% Mounted on
/dev/sda1               11G   7.7G   2.0G  81% /
none                   253M   242k   253M   1% /dev
none                   261M      0   261M   0% /dev/shm
none                   261M    58k   261M   1% /var/run
none                   261M      0   261M   0% /var/lock
none                   261M      0   261M   0% /lib/init/rw
root@bt:/etc/nagios#
```

Por lo cual lo cambiamos en el fichero de configuración del host a SDA 1

Quedando así.

```
define service{
use generic-service
host_name remotehost
service_description /dev/sda1 Free Space
check_command check_nrpe!check_sda1
}
```

Ahora guardamos y reiniciamos Nagios.

```
root@nagios:/etc/nagios-plugins/config# service nagios3 restart
Restarting nagios3 monitoring daemon: nagios3
.
```

Luego en el fichero del agente de Nagios también cambiamos el comando.

```
 GNU nano 2.2.2                    File: /etc/nagios/nrpe.cfg

command[check_users]=/usr/lib/nagios/plugins/check_users -w 5 -c 10
command[check_load]=/usr/lib/nagios/plugins/check_load -w 15,10,5 -c 30,25,20
command[check_sda1]=/usr/lib/nagios/plugins/check_disk -w 20% -c 10% -p /dev/sda1
command[check_zombie_procs]=/usr/lib/nagios/plugins/check_procs -w 5 -c 10 -s Z
command[check_total_procs]=/usr/lib/nagios/plugins/check_procs -w 150 -c 200
```

Al modificarlo toca reiniciar el agente.

(cc) BY-NC-SA

```
root@bt:/etc/nagios# /etc/init.d/nagios-nrpe-server restart
 * Stopping nagios-nrpe nagios-nrpe
 * Starting nagios-nrpe nagios-nrpe
root@bt:/etc/nagios#
```

Y ya por fin lo tenemos funcionando.

Service Status Details For Host 'remotehost'

Host	Service	Status	Last Check	Duration	Attempt	Status Information
remotehost	/dev/sda1 Free Space	WARNING	2011-12-17 07:40:15	0d 0h 1m 14s	4/4	DISK WARNING - free space: / 1816 MB (19% inode=39%):
	CPU Load	OK	2011-12-17 07:37:08	0d 0h 19m 21s	1/4	OK - load average: 0.01, 0.02, 0.05
	Current Users	OK	2011-12-17 07:37:58	0d 0h 18m 31s	1/4	USERS OK - 1 users currently logged in
	Total Processes	OK	2011-12-17 07:38:48	0d 0h 17m 41s	1/4	PROCS OK: 68 processes
	Zombie Processes	OK	2011-12-17 07:36:29	0d 0h 20m 0s	1/4	PROCS OK: 0 processes with STATE = Z

Monitorización de un Router Cisco.

Configuramos el agente SNMP en cisco IOS.

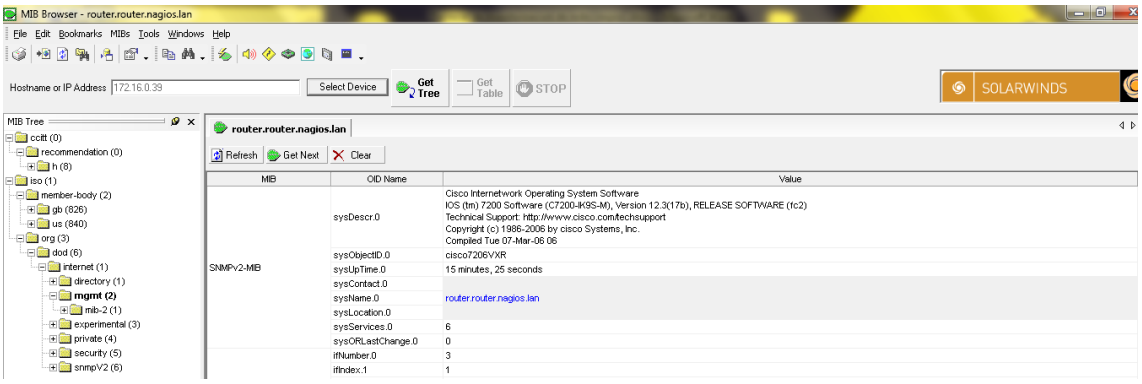
Para ello empezamos creando una ACL para tener algo de seguridad en el agente SNMP aunque use texto plano.

```
router(config)#ip access-list standard 1
router(config-std-nacl)#permit 172.16.0.20
router(config-std-nacl)#permit 172.16.0.1
router(config-std-nacl)#deny any
router(config-std-nacl)#
```

Después habilitamos el servidor SNMP.

```
router(config)#snmp-server community public ro 1
router(config)#
```

Ahora procedemos a enumerar la MIB de cisco en mi caso uso el programa MIB Browser de Solarwinds.



(cc) BY-NC-SA

Una vez enumerada la MIB procedemos a realizar una abstracción de que es lo que necesitamos vigilar en el Router.

En mi caso elijo estos.

Información del sistema.

SNMPv2-MIB	sysObjectID.0	cisco7206VXR
	sysUpTime.0	15 minutes, 25 seconds
	sysContact.0	
	sysName.0	router.router.nagios.lan

Autentificaciones Fallidas para detectar ataques de fuerza bruta.

CISCOTRAP-MIB	authenticationFailure.0	0

Estado de los paquetes de Redirección ICMP para detectar ataques MITM.

IP-MIB	icmpInRedirects.0	0
	icmpOutMsgs.0	0

Y el estado de los interfaces.

IF-MIB	ifAdminStatus.1	up(1)
	ifAdminStatus.2	down(2)
	ifAdminStatus.3	up(1)
	ifOperStatus.1	up(1)
	ifOperStatus.2	down(2)
	ifOperStatus.3	up(1)
	ifLastChange.1	7 seconds
	ifLastChange.2	7 seconds
	ifLastChange.3	0,00 seconds

Una vez que sabemos que es lo que queremos instalamos las extensiones SNMP para Nagios.

```
root@Usrv-sad-kml:~# aptitude install nagios-snmp-plugins
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
```

Y copiamos la plantilla para un dispositivo de red.

```
root@nagios:~# dpkg -S switch.cfg
nagios3-common: /usr/share/doc/nagios3-common/examples/template-object/switch.cf
g
root@nagios:~# cp /usr/share/doc/nagios3-common/examples/template-object/switch.
cfg /etc/nagios3/
root@nagios:~#
```

Ahora procedemos a editarla.

```
root@nagios:~# cd /etc/nagios3/
root@nagios:/etc/nagios3# nano switch.cfg
```


(cc) BY-NC-SA

Obtenemos la ip del Router.

```
router#show ip interface brief
Interface                  IP-Address      OK? Method Status                Prot
ocol
FastEthernet0/0            172.16.0.39     YES DHCP   up                    up

FastEthernet0/1            unassigned      YES NVRAM  administratively down down
```

Y procedemos a modificar la plantilla.

1º Cambiamos los valores de la plantilla para evitar errores. Que son la plantilla del dispositivo, el alias y la dirección.

```
define host{
        use             generic-host            ; Inherit default values from a template
        host_name       linksys-srw224p         ; The name we're giving to this switch
        alias           Router de Kamal         ; A longer name associated with the switch
        address         172.16.0.39             ; IP address of the switch
        }
```

Después borramos todos los comandos menos el del Uptime.

Dejando el comando así.

```
# Monitor uptime via SNMP

define service{
        use                     generic-service ; Inherit values from a template
        host_name               linksys-srw224p
        service_description     Uptime
        check_command           check_snmp!sysUpTime.0
        }
```

Por último nos queda así:

```
  GNU nano 2.2.4                              Fichero: /etc/nagios3/conf.d/switch.cfg

################################################################################
################################################################################
#
# HOST DEFINITIONS
#
################################################################################
################################################################################

# Define the switch that we'll be monitoring

define host{
        use             generic-host            ; Inherit default values from a template
        host_name       linksys-srw224p         ; The name we're giving to this switch
        alias           Router de Kamal         ; A longer name associated with the switch
        address         172.16.0.39             ; IP address of the switch
        }

# Monitor uptime via SNMP

define service{
        use                     generic-service ; Inherit values from a template
        host_name               linksys-srw224p
        service_description     Uptime
        check_command           check_snmp!sysUpTime.0
        }
```


(cc) BY-NC-SA

Ahora en /etc/nagios-plugins/config/snmp.cfg

Añadimos la definición del comando check_snmp.

```
# 'check_snmp' command definition
define command{
command_name check_snmp
command_line $USER1$/check_snmp -H $HOSTADDRESS$ -o  $ARG1$
}
```

Quedando así:

```
  GNU nano 2.2.4                                  Fichero: /etc/nagios-plugins/config/snmp.cfg

# 'check_snmp' command definition
define command{
command_name check_snmp
command_line $USER1$/check_snmp -H $HOSTADDRESS$ -o  $ARG1$
}
```

De esta forma podemos consultar el objeto de cualquier MIB de cualquier HOST con un agente SNMP. Soy partidario de usar protocolos Estándar como este y de no usar los agentes propietarios de Nagios aunque sean openSource pero bueno a veces no queda otra. En este caso solo nos hacen falta 2 cosas en el comando. El identificador del objeto que queremos consultar y su dirección IP.

Y si ya tenemos la lista de objetos que deseamos monitorizar empezamos a introducirlos.

Información de IOS.

```
#Nombre del Host
define service{
        use                     generic-service ; Inherit values from a template
        host_name               linksys-srw224p
        service_description     Informacion de IOS
        check_command           check_snmp!sysDescr.0
        }
```

Nombre del Router.

```
#Nombre del Host
define service{
        use                     generic-service ; Inherit values from a template
        host_name               linksys-srw224p
        service_description     Nombre del router
        check_command           check_snmp!sysName.0
        }
```

Tiempo de actividad.

```
define service{
        use                     generic-service ; Inherit values from a template
        host_name               linksys-srw224p
        service_description     Uptime
        check_command           check_snmp!SNMPv2-MIB::sysUpTime.0
        }
```


(cc) BY-NC-SA

Estado de interfaces de RED 1 y 2.

```
define service{
        use                     generic-service ; Inherit values from a template
        host_name               linksys-srw224p
        service_description     Estado Interfaz 1
        check_command           check_snmp!ifAdminStatus.1,ifOperStatus.1,ifDescr.1
        }

define service{
        use                     generic-service ; Inherit values from a template
        host_name               linksys-srw224p
        service_description     Estado Interfaz 2
        check_command           check_snmp!ifAdminStatus.2,ifOperStatus.2,ifDescr.2
        }
```

Monitorización de la ruta por defecto del router.

```
define service{
        use                     generic-service ; Inherit values from a template
        host_name               linksys-srw224p
        service_description     Ruta por defecto
        check_command           check_snmp!netDefaultGateway.0
        }
```

Ahora una vez hecho lo metemos a conf.d y reiniciamos Nagios.

```
root@nagios:/etc/nagios3# mv switch.cfg conf.d/
root@nagios:/etc/nagios3# service nagios3 restart
Restarting nagios3 monitoring daemon: nagios3
.
root@nagios:/etc/nagios3#
```

Esperamos un rato y al final queda así:

Host	Service	Status	Last Check	Duration	Attempt	Status Information
linksys-srw224p	Estado Interfaz 1	OK	2011-12-23 04:45:33	0d 0h 6m 12s	1/4	SNMP OK - up(1) up(1) FastEthernet0/0
	Estado Interfaz 2	OK	2011-12-23 04:45:28	0d 0h 6m 17s	1/4	SNMP OK - down(2) down(2) FastEthernet0/1
	Informacion de IOS	OK	2011-12-23 04:46:18	0d 0h 5m 27s	1/4	SNMP OK - Cisco Internetwork Operating System Software
	Nombre del router	OK	2011-12-23 04:42:08	0d 0h 9m 37s	1/4	SNMP OK - router.router.nagios.lan
	Ruta por defecto	OK	2011-12-23 04:46:23	0d 0h 0m 22s	1/4	SNMP OK - = IpAddress: 172.16.0.2
	Uptime	OK	2011-12-23 04:42:13	0d 0h 4m 32s	1/4	SNMP OK - Timeticks: (88118) 0:14:41.18

6 Matching Service Entries Displayed

3. 0 Bibliografía.

Estándar SNMP
http://www.snmp.com/protocol/

http://www.pulsewan.com/data101/pdfs/snmp.pdf

Instalación y Administración de Nagios Documentación.
http://nfsv4.bullopensource.org/doc/admin_tools/latex_doc/installNagios.pdf

http://nagios.sourceforge.net/docs/

(cc) BY-NC-SA