8ª Sesión práctica ASRC - 2017/18. Guión de trabajo:

Monitorización de redes con NAGIOS

Sistema de monitorización de redes, de código abierto, que puede vigilar tanto los equipos (hardware) como los servicios (software), que se indiquen, avisando cuando no se comporten de la manera deseada.

Monitoriza, principalmente, servicios de red (tipo SMTP, POP3, HTTP, SNMP …), recursos hardware (carga procesador, uso de discos, memoria, puertos …), con independencia de sistemas operativos, posibilidad de monitorización remota mediante túneles SSL cifrados o SSH, y la posibilidad de programar plugins específicos para nuevos sistemas.

Genera alertas, que pueden ser recibidas por los responsables correspondientes mediante (por ej.) correo electrónico y mensajes SMS, en caso de que estos parámetros exceden de los márgenes definidos por el administrador de red.

Nagios fue originalmente diseñado para ser ejecutado en GNU/Linux, pero también se ejecuta bien en variantes de Unix.

La administración de Nagios se puede volver bastante compleja y enrevesada. Para ello, existe un Front-end que ayuda bastante a esta labor, es el llamado Centreon. Dicho aplicativo, se puede encontrar también en una imagen de VirtualBox llamada FAN (Fully Automated Nagios), que se puede obtener desde http://www.fullyautomatednagios.org/download.
También se puede descargar la imagen en formato .ova desde: https://drive.google.com/open?id=1DZfX3QHdYiGNiKZc-63Ki3n-Y-z2L8In

Dicha distribución es un linux Centos que contiene Nagios junto con una serie de plugins útiles.
Una vez puesta en marcha (previamente importamos el servicio virtualizado desde VBox), lanzaremos un navegador con la ip del servidor Nagios y visualizamos las distintas herramientas que se incluyen en esta distribución:

Básicamente, consisten en :

El núcleo del propio **Nagios**, capaz de realizar monitorización de **servicios** (SMTP, POP3, HTTP, NNTP, ICMP, SNMP, LDAP, etc) y de recursos de servidores y equipos (genéricamente denominados **hosts**) con diferentes sistemas operativos (carga del procesador, uso del disco duro, uso de paginación de memoria, etc), así como la correspondiente configuración y generación de alertas, informes, etc.

Centreon, es una herramienta que presenta los datos de Nagios de forma gráfica y amigable, que puede ser utilizada por cualquier tipo de usuario aunque no sea administrador.

Nagvis, es otro módulo de visualización que permite crear vistas funcionales de la topología de red monitorizada.

Nareto (Nagios Reporting Tools), es un plugin que utiliza la información de Nagios para proporcionar diferentes vistas de los mismos datos para diferentes perfiles de usuario. La información disponible está organizada jerárquicamente y se pueden dar diferentes permisos a cada usuario para diferentes partes de esa jerarquía. Se pueden obtener representaciones visuales en tiempo real, como informes, historiales ó monitorización de alertas.

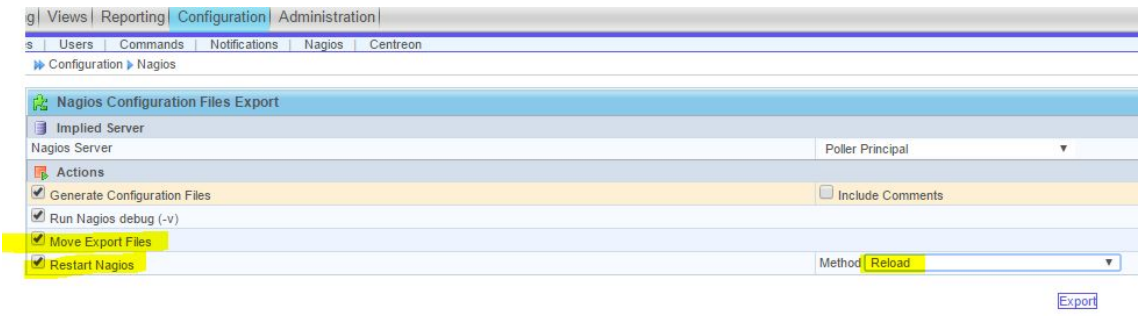
Ciertas tareas de monitorización podrán realizarse sin necesidad de realizar ninguna acción en los sistemas monitorizados (como para saber, por ejemplo, si están respondiendo a un comando ping), mientras otras necesitarán de la instalación o configuración de agentes de monitorización en los equipos que quieran monitorizarse (como, por ejemplo, cuando queramos saber el uso de CPU del equipo remoto).

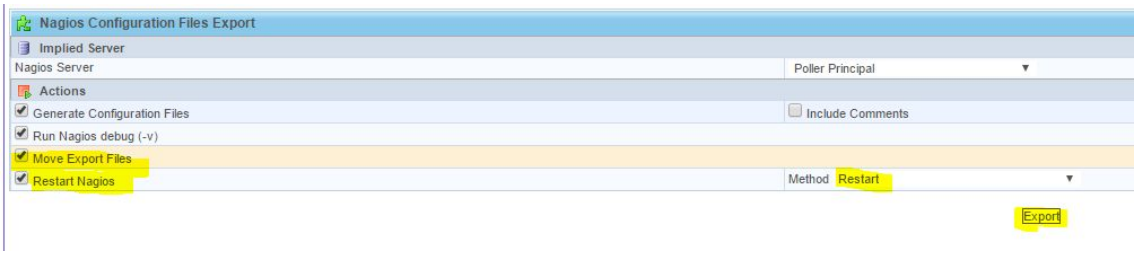
Para comenzar, vamos directamente a usar Centreon, para lo cual, entraremos con el usuario y contraseña por defecto: nagiosadmin/nagiosadmin.

La monitorización gira en torno a 3 conceptos principales, que son el host a monitorizar, el servicio a "vigilar", y el comando que ejecuta esa monitorización del servicio indicado sobre el host.

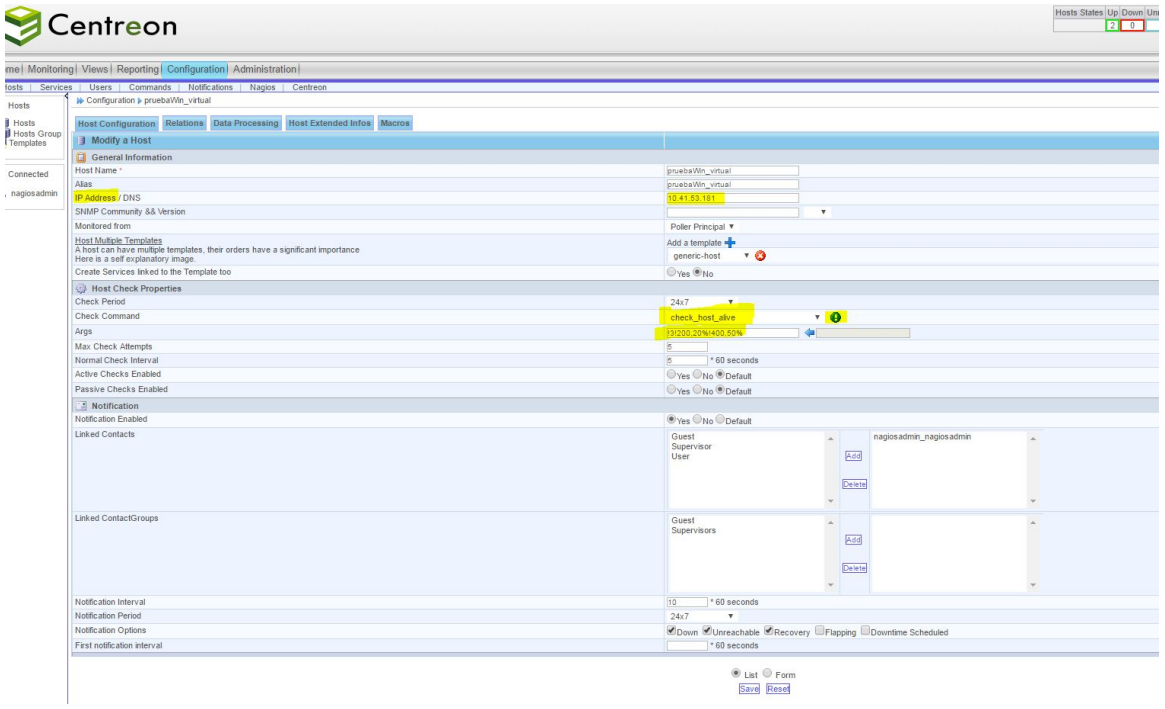
Algunas de las consideraciones importantes a tener en cuenta en determinadas operaciones importantes son estas:

1. Cada vez que añadamos un hosts, hay que actualizarlo en el núcleo, es decir, en Nagios (hay que tener en cuenta que estamos trabajando en el Front-end, Centreon). Para ello, debemos marcar las dos casillas que aparecen en la captura, y hacer un reload. Cuando finalice, repetimos la operación pero seleccionando el método "Restart".

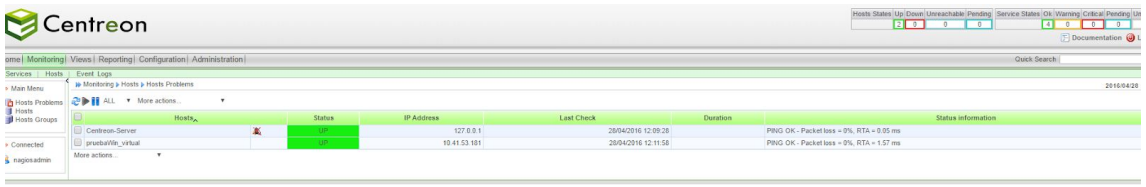




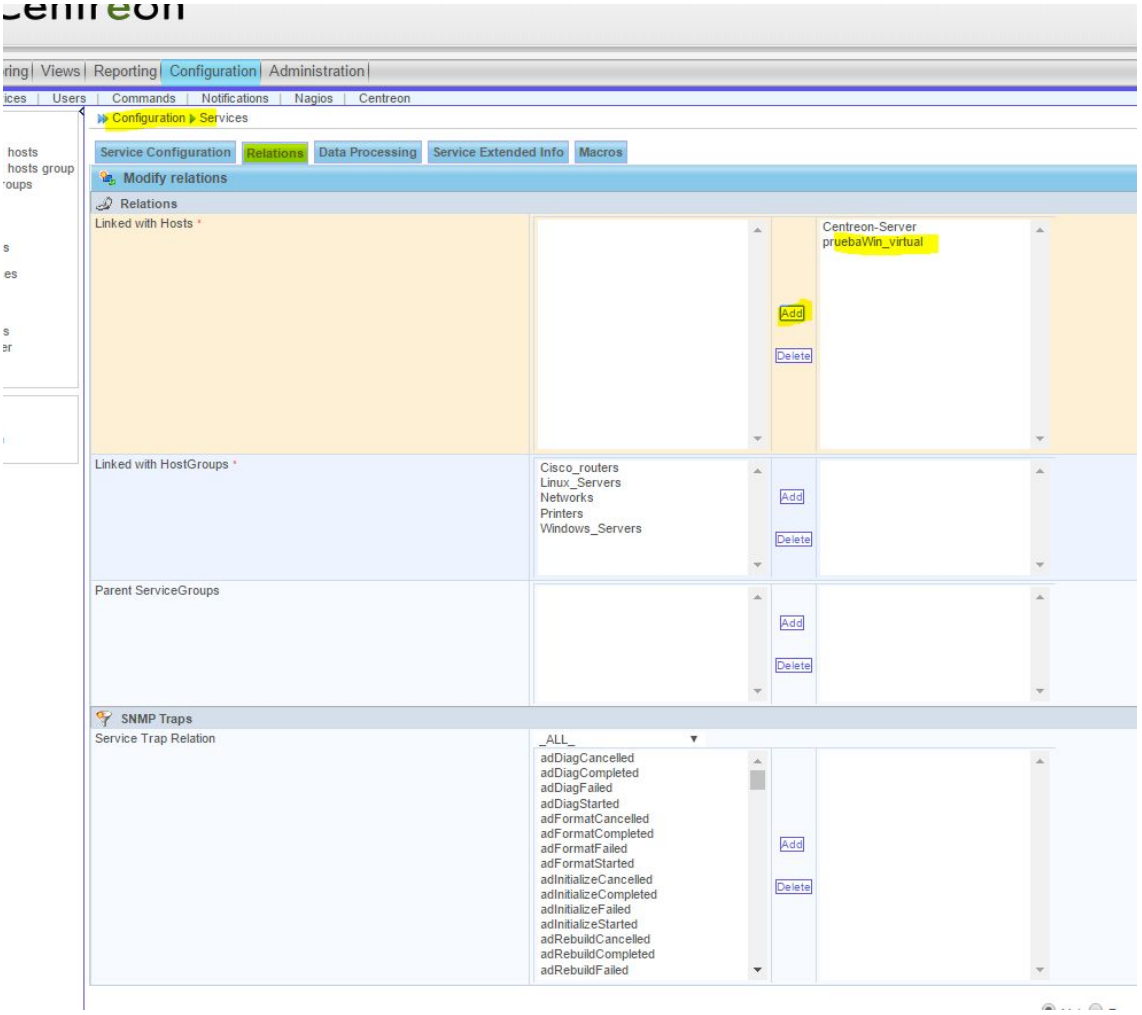
2. Al añadir un host, lo único inicialmente imprescindible es la dirección IP. Se puede, además, añadir un comando que se ejecute sobre dicho host ("Check command"), con la facilidad de usar alguno de los ya predefinidos. Dicho comando tendrá una serie de argumentos con los que trabajar. Pulsando sobre el icono de Información, accedemos a una ayuda donde se explican dichos argumentos:



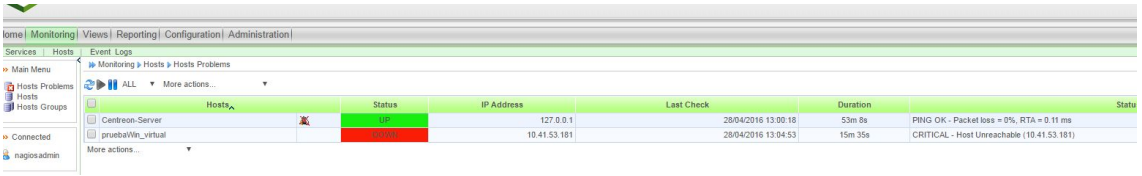
3. Una vez establecidos los comandos a monitorizar, podemos observar el estado de los hosts que tenemos registrados.



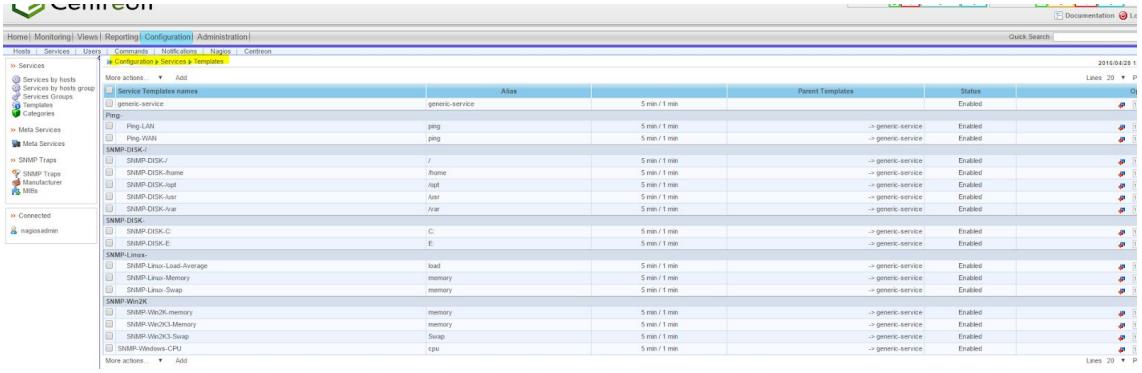
4. Asociar servicio a Hosts. Desde la configuración de los servicios, haciendo clic sobre cualquiera de ellos, y desde la pestaña de "Relations", podemos asociarlo a uno o varios Hosts:



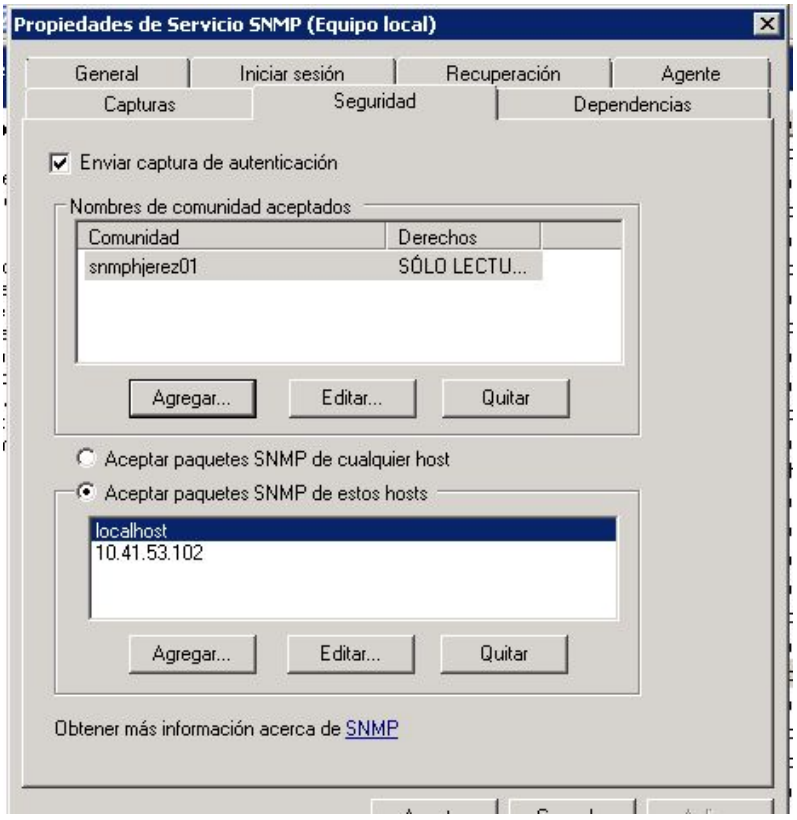
Una vez tengamos asociado el servicio de Ping a algún host, si probamos a apagarlo, al poco tiempo (según se configure el intervalo en el host), veremos algo así:



Podemos destacar, también, la gran cantidad de plantillas de servicios que tiene preconfigurado Nagios, y que podemos usar en nuestras monitorizaciones:



Como hemos podido ver, en un primer momento, no es necesario hacer nada en los clientes, ya que, lo que estamos comprobando es si está levantado o no.
Si deseamos medir otro tipo de eventos, como por ej., la carga de disco, habría que empezar por instalar y activar el servicio SNMP del cliente. En dicho servicio, hay que tener en cuenta dos configuraciones importantes. Por una parte, poner un nombre de comunidad para luego configurarlo como argumento en el comando que se vaya a usar. Así como, también, el tipo de derecho que tendrá dicha comunidad, en nuestro caso, se suficiente con "Sólo Lectura", evitando ciertos riesgos de seguridad que nos produciría la escritura en dicho protocolo de red.
Por otro lado, limitar desde dónde se va a aceptar paquetes SNMP, igualmente, por motivos de seguridad.



Para determinadas monitorizaciones más complejas, sí que sería necesario instalar un cliente propio, como por ej. NSCLIENT++

Tarea a realizar:

1. Crea una monitorización simple, por ejemplo, comprobar si un host está levantado (o si prefieres, puedes probar otra). Luego, dentro de lo posible, aumenta el número de hosts a monitorizar.

2. Habilita en algún host, el protocolo SNMP y haz una monitorización de uso de disco, por ejemplo. (puede encontrar más información al respecto en http://yoadminsis.blogspot.com.es/2010/08/configurar-snmp-para-monitorizar.html)