UNIVERSITAT OBERTA DE CATALUNYA


# Proyecto Final de Máster en Software Libre

## Creación de red de Sensores para la Autoridad Portuaria de Gijón

**Autor: Nicanor Garcia Álvarez**

**09/06/2014**

**Tutor Externo**: Jorge Álvarez Fernández

**Consultor:** Miguel Martín Mateo

**Especialidad**: Administración de redes y sistemas Operativos

# LICENCIA DE LA PUBLICACIÓN DEL DOCUMENTO

# RESUMEN DEL PROYECTO.

Mediante este trabajo, se ha dotado a la Autoridad Portuaria de Gijón de un sistema de monitorización y control de sus activos tanto hardware como software con una herramienta que permite dar una solución proactiva a los problemas de seguridad y de disponibilidad de sus sistemas y procesos críticos.

Dicha herramienta se ha integrado en el sistema de virtualización de la Autoridad Portuaria de Gijón y, siguiendo las indicaciones del personal de de dirección de la Autoridad Portuaria de Gijón, cuenta con sensores que permiten la monitorización de servidores, electrónica de red y servicios críticos de la red corporativa de la Autoridad Portuaria de Gijón.

Después del estudio correspondiente la herramienta elegida ha sido Nagios. El producto se presenta como una máquina virtual integrada en el sistema de virtualización corporativa de la Autoridad Portuaria y funcionando como una página web interna en la que se visualiza el estado de los sistemas monitorizados.

# TABLA DE CONTENIDO

# TABLA DE ILUSTRACIONES

# INTRODUCCIÓN

Fruto del acuerdo de colaboración entre la Autoridad Portuaria de Gijón y la Universitat Oberta de Catalunya, he tenido la oportunidad de trabajar como becario en prácticas en el Departamento de sistemas de Información de la Autoridad Portuaria y desarrollar así una red de sensores que permitan determinar en tiempo real el estado de los servicios críticos a monitorizar. En el proyecto se han definido, además de dichos servicios críticos, los entregables del proyecto, la documentación y las necesidades de formación al personal técnico.

Se plantea en este primer capítulo los objetivos que se pretende cubrir:

# OBJETIVOS

Los objetivos del proyecto se definieron en las reuniones llevadas a cabo con el personal de sistemas de información, se han descrito los requisitos del sistema y estos han sido los resultados:

El sistema final deberá dotar la APG de los siguientes sistemas de monitorización y/o Control:
El sistema deberá monitorizar el estado del clister de virtualización VMware

El sistema deberá monitorizar el estado del clúster de XenServer, tanto en la parte servidor, con sus dos máquinas físicas, como el estado de las máquinas que lo integran, principalmente de los servidores XenApp virtualizados

El sistema final contará con un mapa de red integrado por los principales dispositivos de red, incluyendo al menos el estado de:

- Core de red
- Switches de conexión de edificios secundarios, cuando sea posible su monitorización
- Sistema de seguridad y firewall
- Impresoras de red

El sistema de monitorización incluirá el estado de los servidores de ficheros corporativos

# ESTADO DEL ARTE

Para la elección de la herramienta final, se han evaluado todas las opciones punteras en ámbito del software libre y se ha estudiado la idoneidad de cada una para cubrir las necesidades del cliente, las opciones evaluadas han sido las siguientes:

## NAGIOS

Nagios [1] es una de las herramientas más extendidas en la monitorización de infraestructuras, con una amplia comunidad de usuarios, y totalmente personalizable, ofrece la posibilidad de crear Plugins personalizados para la monitorización de las infraestructuras, mejoradas recientemente con la liberación el cuatro de marzo de 2014 de la versión 2.0 del Nagios Plugins[2]. Nagios funciona con sitemas de monitorización, alertas, respuestas, informes, mantenimiento y planificación para la gestión proactiva de entornos corporativos como el de la APG.

Nagios se distribuye con licencia GPL

## PANDORA FMS

Pandora [3] es un software de monitorización orientado a todo tipo de entornos cuyo objetivo es ser suficientemente flexible para gestionar y controlar todo tipo de infraestructuras.

Pandora FMS nace de la iniciativa personal de su autor Sancho Lerena en 2003 y se distribuye bajo licencia GLP

Las características principales del producto son las siguientes:

- **Auto descubrimiento**. En local, los plugins "por defecto" de los agentes de Pandora permiten detectar los discos duros, las particiones o las bases de datos en un servidor de base de datos, entre otras muchas cosas.

- **Auto exploración**. En remoto, y usando la red, puede detectar sistemas activos, catalogarlos según su sistema operativo, y dado un perfil empezar a monitorizarlos. Incluso puede detectar la topología de la red y "pintar" un esquema de red basado en su enrutamiento.

[1] http://www.nagios.org/
[2] http://www.nagios.org/news/77-news-announcements/371-nagios-plugins-20-released
[3] http://wiki.pandorafms.com/index.php?title=Main_Page

- **Monitorizar**. Los agentes de Pandora FMS son de los más poderosos del mercado. Pueden obtener información desde la ejecución de un comando, hasta la llamada a más bajo nivel de la API de Windows: eventos, logs, datos numéricos, estados de un proceso, consumo de memoria o de CPU. Pandora dispone de una biblioteca de monitores por defecto, pero lo importante de Pandora FMS es lo **fácil** que es añadir y crear nuevos monitores.

- **Controlar**. Los propios agentes pueden levantar servicios, borrar ficheros temporales o ejecutar procesos. También puede hacerlo de la consola, ejecutando remotamente tareas como parar o arrancar servicios. Incluso puede programar tareas para su ejecución periódica. Además, puede usar Pandora FMS para acceder remotamente a máquinas windows (vía VNC) o a sistemas de red o Unix mediante Telnet o SSH, todo desde un interfaz web.

- **Alertar y notificar**. Tan importante como detectar un fallo es avisar de él. Con Pandora, tiene una variedad casi infinita de formas y formatos de notificación, incluyendo: escalados, correlación de alertas y protección de cascada de eventos.

- **Visualizar y analizar**. Monitorizar no sólo es recibir un trap o visualizar un servicio caído, es presentar informes de tendencias, gráficas resumen de datos correlados durante meses, generar portales de usuarios, delegar informes a terceros o definir sus propias gráficas y tablas. Pandora incorpora todo ello desde la interfaz WEB.

- **Inventariar**. Al contrario que otras soluciones donde el concepto de CMDB es la base, para Pandora es opcional. El inventario es flexible y dinámico (se puede auto-descubrir, hacer remotamente, etc). Puede notificar de cambios (p.e: software des-instalado en un equipo) o simplemente ser usado para elaborar listados.

## ZENOSS

Zenoss[4] es una aplicación de código abierto, bajo GLP dotada de interfaz web que permite a los administradores monitorizar la disponibilidad inventario y configuración de eventos en entornos corporativos.

Zenoss se distribuye como una familia de productos: "Zenoss Service Dynamics" que proveen servicios a infraestructuras tanto físicas como virtuales.

Las principales características son las siguientes:

- Gestión de eventos
- Optimización y Análisis
- Gestión de recursos

Zenoss tiene una importante presencia en infraestructuras virtuales y en la nube, con importante presencia para Hyper-V, XenServer, VMware y sistemas "Cloud" como Azure, OpenStack, vCloud y otros.

Es muy destacable también la presencia en la monitorización de Hardware con los principales fabricantes como Dell, HP, IBM, Solaris, Linux, etc. y sistemas de almacenamiento y de red como Cisco, Juniper, CeckPoint y otros fabricantes destacados.

## CACTI

Cacti [5] es una solución para la generación de gráficos de red y de monitorización que se libera bajo licencia GLP.

Se apoya en una herramienta desarrollada en PHP: RRDtool (Round Robin Database Tool) y cuenta con un interfaz de usuario de gran usabilidad.

Como sus competidoras, trabaja principalmente con protocolo SNMP que pemite a los administradores de red supervisar la red a su cargo, resolver problemas y supervisar su rendimiento.

[4] http://www.zenoss.com/
[5] http://cacti.net/

## VALORACIÓN Y ELECCIÓN DE LA HERRAMIENTA ADECUADA

Para valorar las diferentes alternativas y otras existentes[6] hemos consultado diferente literatura y hemos estudiado las posibilidades de ciertas soluciones.

Hay varios productos que cubren las necesidades del cliente, entre ellos los citados en el apartado anterior, pero todos los estudios consultados destacan la potencia de Nagios sobre sus competidores su potencia[7], su consolidación y exhaustiva documentación [8] y su escalabilidad y extensiblidad[9]

Como parte negativa de Nagios, podemos citar su dificultad de integración y de implantación, en comparación con sus competidoras. Dichos problemas los intentaremos salvar en las demás fases del proyecto con el fin de dotar a la APG de la herramienta que mejor se ajuste a sus necesidades.

Nagios, por lo tanto se trata de una alternativa perfectamente viable para dotar a la APG de un sistema de monitorización y control de sus activos críticos y por lo tanto la alternativa recomendada al cliente.

En la decisión de utilizar Nagios, ha tenido peso las siguientes características técnicas [10]

- Monitorización de servicios de red
- Monitorización de los recursos de equipos hardware (carga del procesador, uso de los discos, logs del sistema) en varios sistemas operativos, incluso Microsoft Windows con los plugins
- Monitorización remota, a través de túneles
- Diseño simple de plugins, que permiten a los usuarios desarrollar sus propios chequeos de servicios dependiendo de sus necesidades, usando sus herramientas preferidas
- Chequeo de servicios paralizados.

---

[6] Hemos revisado la lista completa de herramientas de monitorización en esta excelente comparativa:
http://es.wikipedia.org/wiki/Anexo:Comparaci%C3%B3n_de_sistemas_de_monitorizaci%C3%B3n_de_redes

[7] Ver http://pfcmon.wikispaces.com/1.1+Nagios+XI

[8] Ver recomendaciones de Ubuntu en http://doc.ubuntu-es.org/Monitorizaci%C3%B3n/Comparativa

[9] Ver http://www.nagios-cl.org/502

[10] Fuente : http://es.wikipedia.org/wiki/Nagios

- Posibilidad de definir la jerarquía de la red, permitiendo distinguir entre host caídos y host inaccesibles.
- Notificaciones a los contactos cuando ocurren problemas en servicios o hosts, así como cuando son resueltos (a través del correo electrónico, buscapersonas, Jabber, SMS, o cualquier método definido por el usuario junto con su correspondiente complemento).
- Posibilidad de definir manejadores de eventos que ejecuten al ocurrir un evento de un servicio o host para resoluciones de problemas proactivas.
- Rotación automática del archivo de registro.
- Soporte para implementar hosts de monitores redundantes.
- Visualización del estado de la red en tiempo real a través de interfaz web, con la posibilidad de generar informes y gráficas de comportamiento de los sistemas monitorizados, y visualización del listado de notificaciones enviadas, historial de problemas, archivos de registros....

Como dato curioso, decir que Nagios hace referencia a un acrónico recursivo "*Nagios Ain't Gonna Insist On Sainthood*". Es una referencia a la encarnación original del software bajo el nombre de Netsaint, el cual tuvo que ser cambiado por ser supuestamente similar a un nombre comercial. "Agios" significa "santo" en griego.

El proyecto se ha desarrollado en el sistema de virtualización corporativo de la Aturidad Portuaria de Gijón que se integra en una clúster de servidores con esta configuración de la máquina virtual entregada a la Autoridad Portuaria:

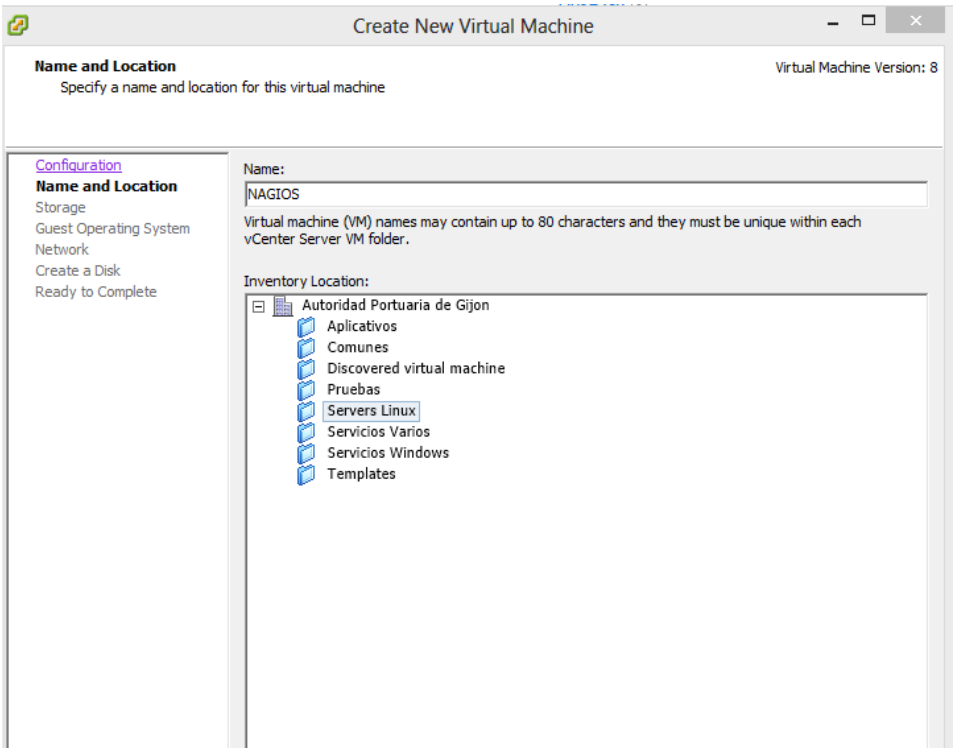



ILUSTRACIÓN 1: CREACIÓN DE MÁQUINA VIRTUAL

Los pasos de la creación han sido Supervisados por el personal técnico de la Autoridad Portuaria y el proceso de Instalación tanto de Nagios como del sistema operativo CentOS se suministra como anexo de esta memoria.

Una vez elegida la herramienta e instalado el Nagios, llegó el momento de cubrir las necesidades descritas por el cliente en las reuniones programadas. El proceso ha sido el siguiente

Accedemos desde cualquier navegador:

Los administradores de sistemas han establecido un alias en el directorio activo que permite acceder por esta dirección

http://nagios/nagios

O bien con la dirección IP de la máquina:

con el usuario nagiosadmin y la contraseña establecida.

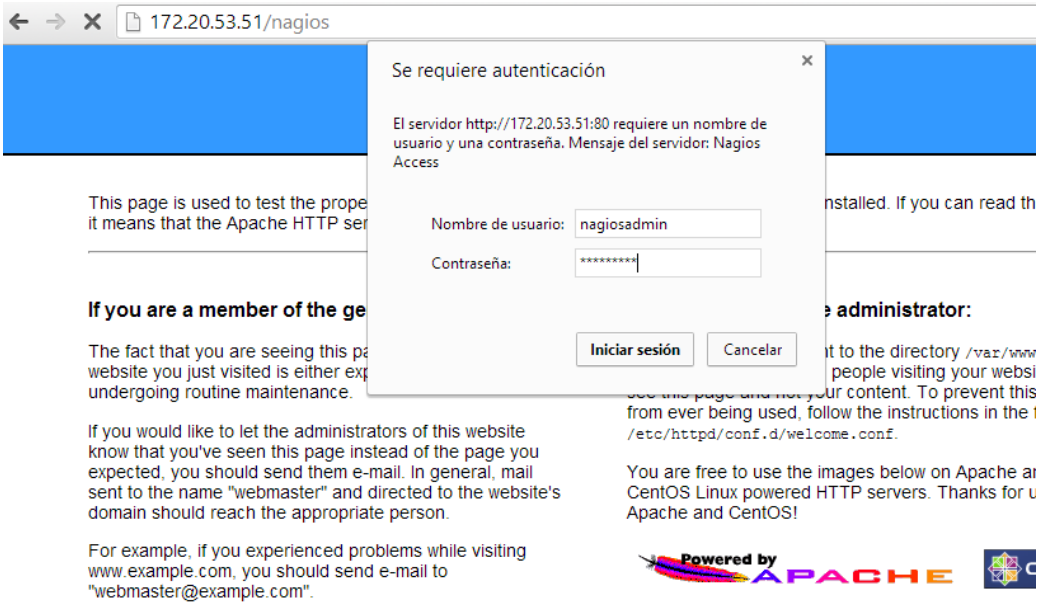



ILUSTRACIÓN 2: PANTALLA DE AUTENTICACIÓN AL SISTEMA

Este es el interfaz de Nagios ya configurado:

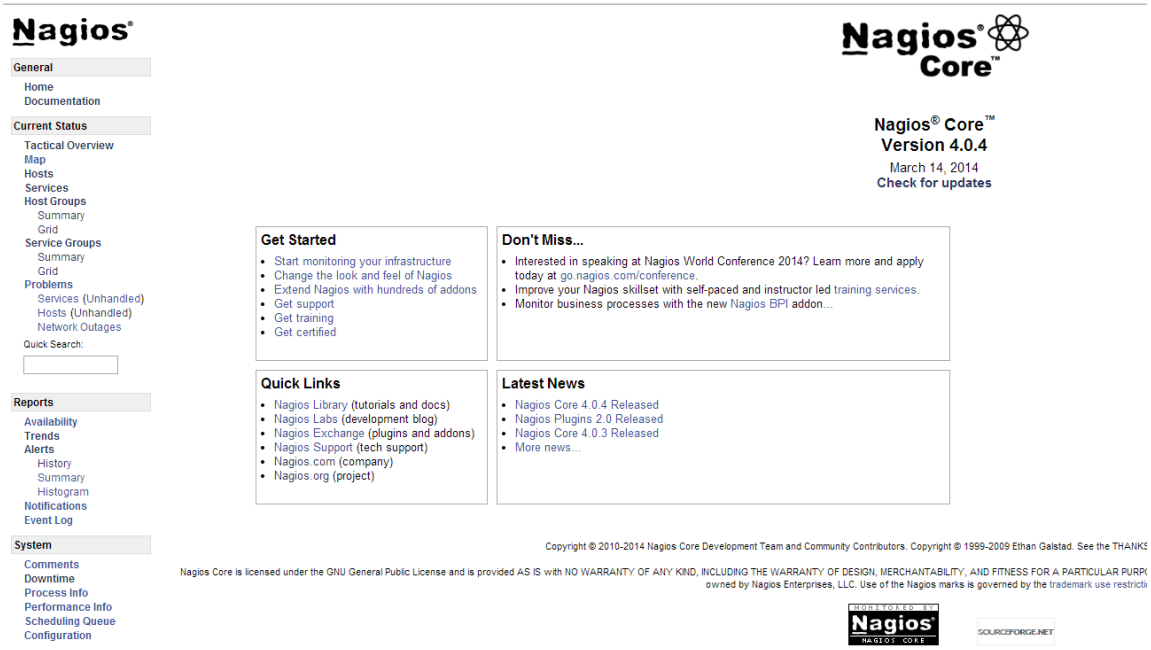



ILUSTRACIÓN 3: PANTALLA PRINCIPAL DE NAGIOS

## MONITORIZANDO SERVIDORES WINDOWS

Una vez descargado el servidor comenzamos la monitorización de los clientes.

En este caso instalaremos un cliente para monitorizar el entorno Citrix, en este caso será el agente nsclient [11]

[11] http://www.nsclient.org/download/0-4-2/

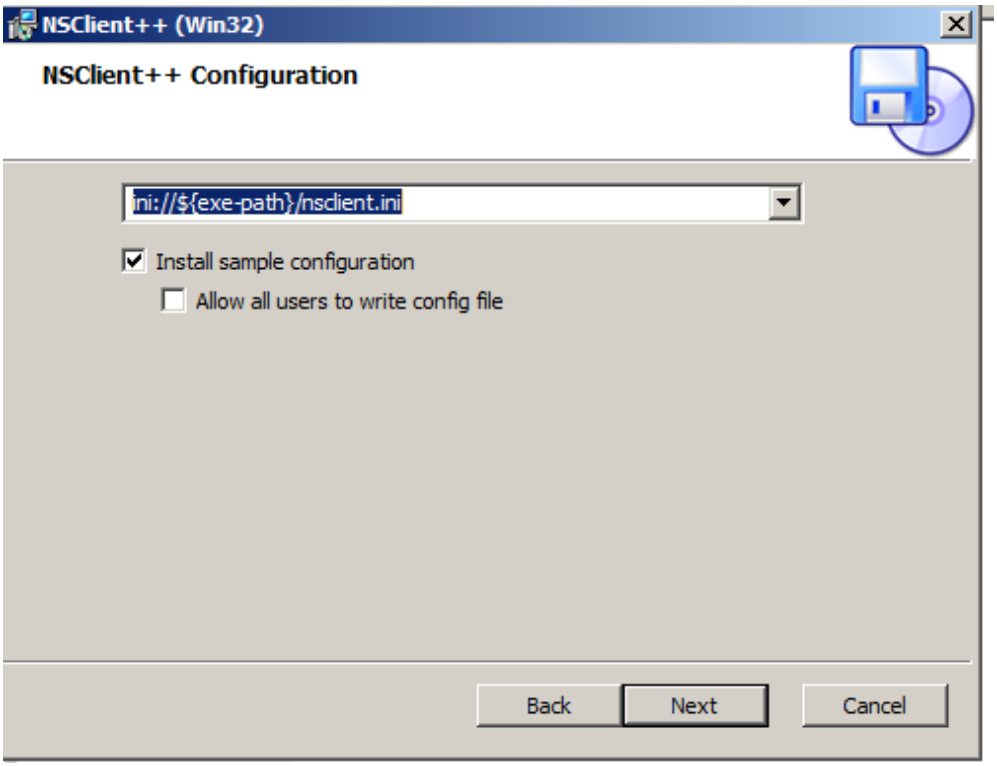



ILUSTRACIÓN 4: INSTALACIÓN DE AGENTES WINDOWS

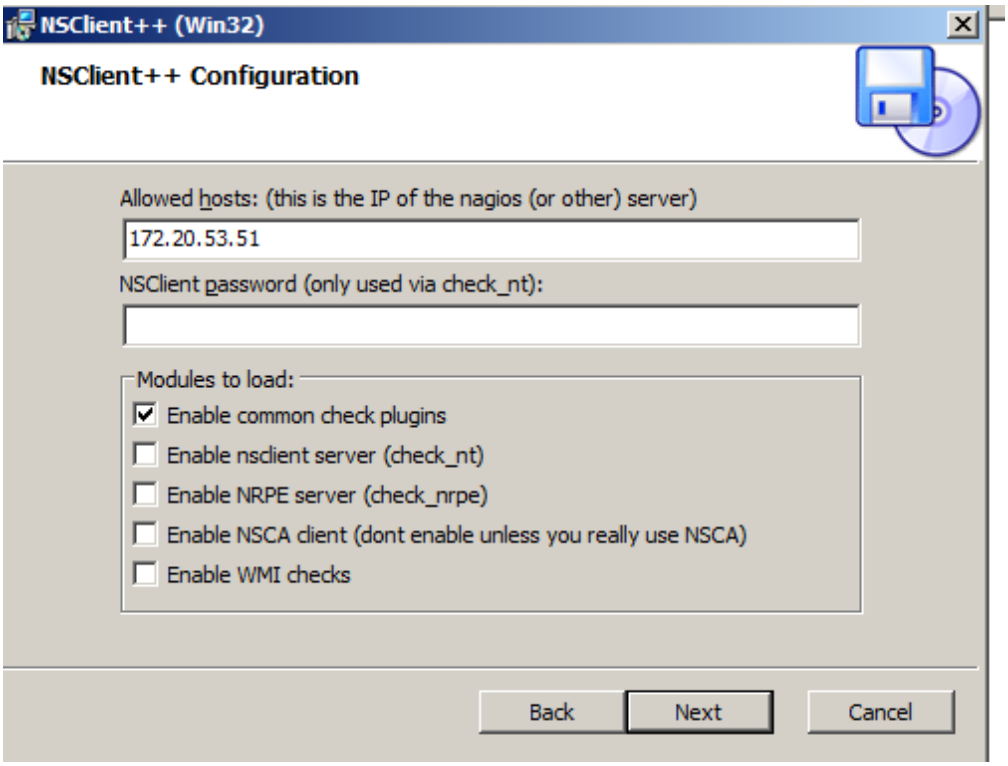



ILUSTRACIÓN 5: PERSONALIZACIÓN DE LOS AGENTES

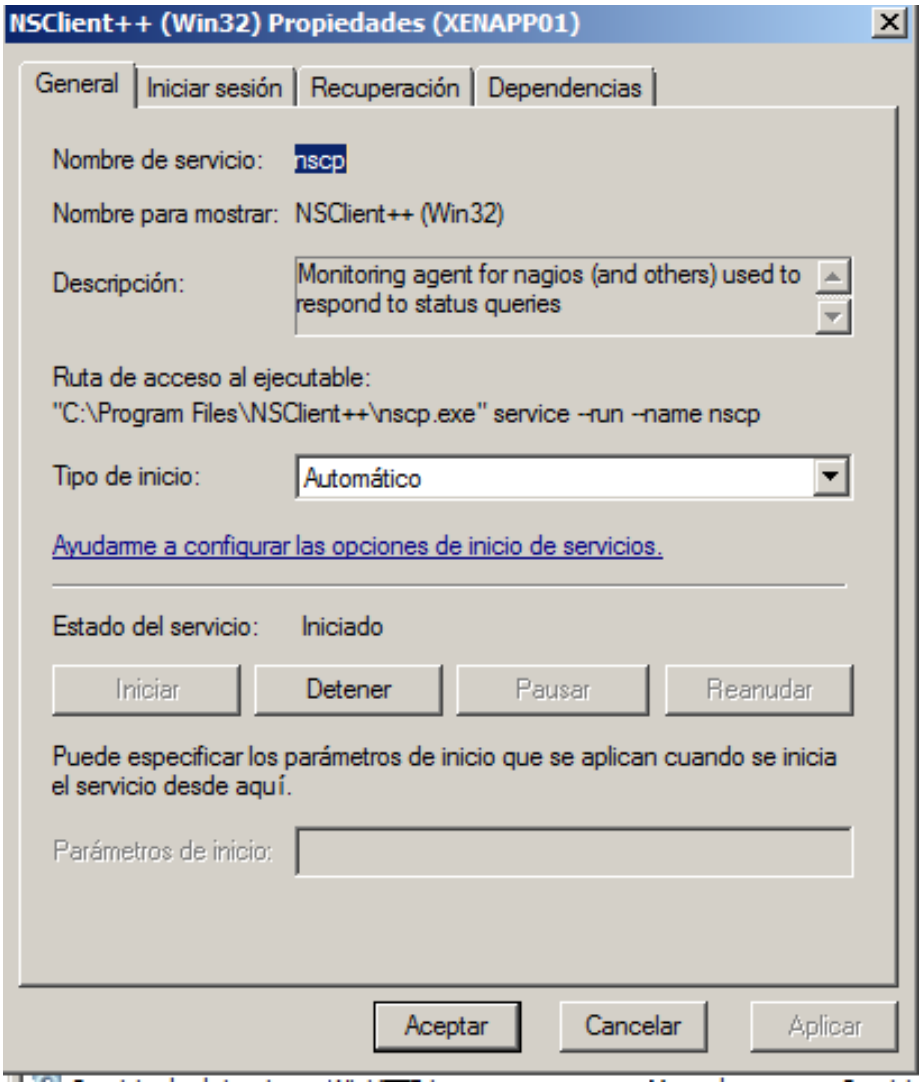



ILUSTRACIÓN 6: SERVICIOS DE AGENTE NAGIOS EN WINDOWS

El proceso de instalación está concluido, pero tenemos que tocar la configuración en la parte Nagios

```
# Definitions for monitoring a Windows machine
cfg_file=/usr/local/nagios/etc/objects/windows.cfg
```

ILUSTRACIÓN 7: ARCHIVO DE CONFIGURACIÓN SISTEMAS WINDOWS

y una vez editado el archivo archivo /usr/local/nagios/etc/objects/windows.cfg se verifica la configuración mediante el siguiente comando

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

y comprobamos en la salida del comando que no existen problemas:

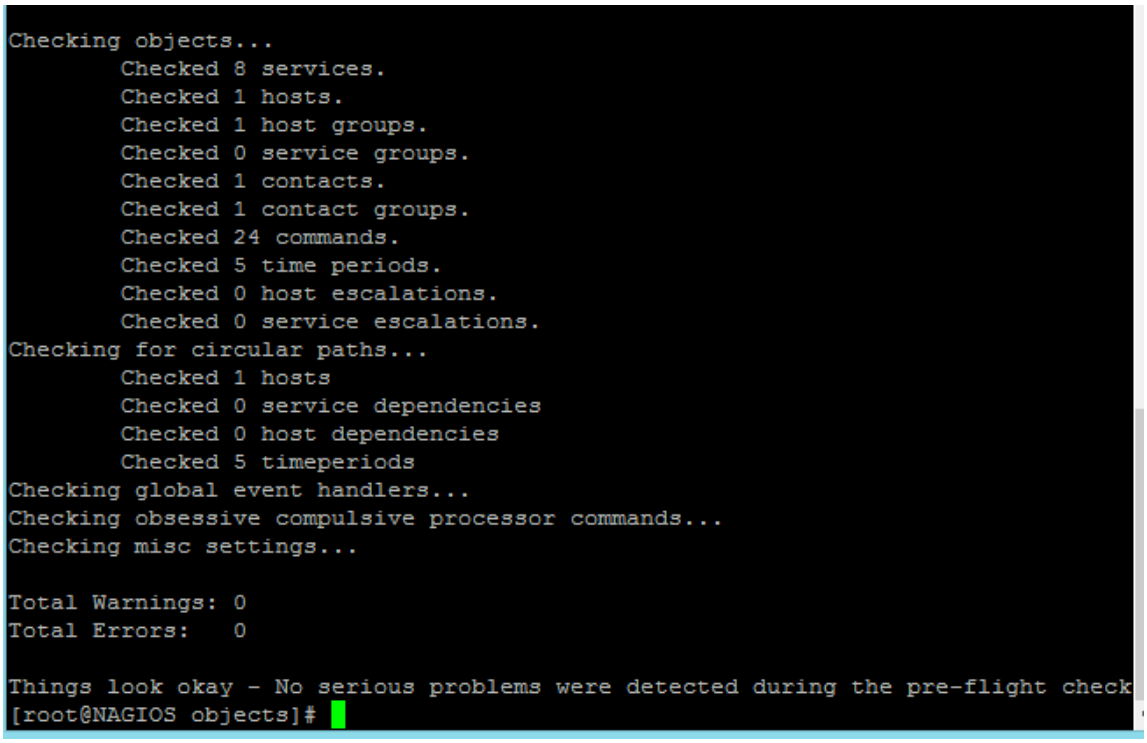



ILUSTRACIÓN 8: COMPROBACIÓN DE SERVICIOS

Reiniciamos ahora los servicios Nagios

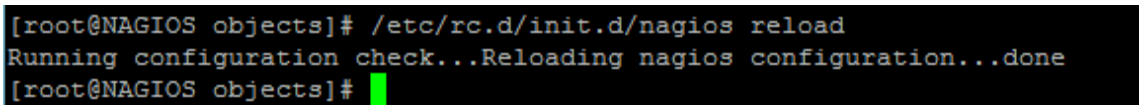



ILUSTRACIÓN 9: REINICIO DE SERVICIO NAGIOS

Comprobamos que el host aparece en el sistema de monitorización de Nagios:

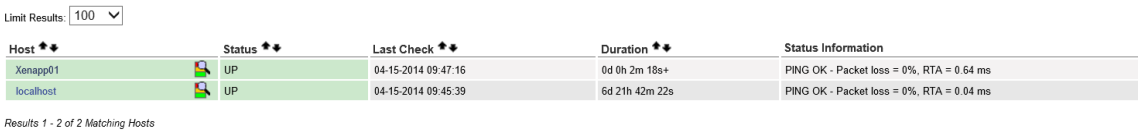



ILUSTRACIÓN 10: HOSTS MONITORIZADOS

Efectivamente la máquina ya está monitorizada y se puede comprobar su estado

## MONITORIZANDO ELECTRÓNICA DE RED

El proceso de monitorización de elementos de electrónica de red es el siguiente:

Para el primer dispositivo, editamos el archivo switch.cfg, añadimos el switch a monitorizar

y editamos los servicios para este host.

No se entregan ilustraciones de este proceso por expreso deseo del cliente.

## MONITORIZACIÓN DE IMPRESORAS DE RED:

Editamos de nuevo el fichero de configuración nagios.cfg quitando la almohadilla inicial de la referencia de la configuración de impresoras

#cfg_file=/usr/local/nagios/etc/objects/printer.cfg
Editamos ahora el fichero

/usr/local/nagios/etc/objects/printer.cfg
Definimos tres impresoras de red

y como siempre verificamos configuración

/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
y reseteamos servicios

Con esto ya comprobamos que se monitorizan las impresoras de red

## PLANIFICACIÓN DE LAS ACTIVIDADES DE INTEGRACIÓN DEL SISTEMA

Las actividades a planificar se alinearán con las descritas en la guía de trabajo y se corresponden a grandes rasgos con las siguientes tareas:

- Elaborar un "Estado del arte" con las herramientas más apropiadas para la monitorización de la Infraestructura de la Autoridad Portuaria y seleccionar la más adecuada a dichos sistemas.
- Instalar una máquina virtual que de soporte a la solución elegida en el paso anterior.
- Definición de los sistemas, servicios y dispositivos de red a monitorizar.
- Configurar los sensores necesarios y los sistemas de monitorización, alertas e informes en el servidor dedicado.
- Creación de mapas de red y alertas visuales para la mejora de la administración
- Documentación del proyecto, formación al personal de la Autoridad Portuaria y revisión con dicho personal del entorno de monitorización. Por motivos de agenda, la formación se reducirá a

una jornada.

Lo que se corresponde gráficamente con la siguiente estimación de planificación:

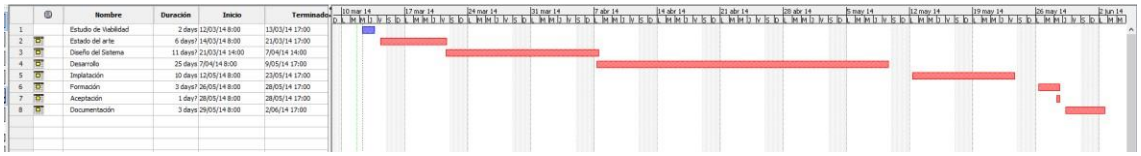


ILUSTRACIÓN 11: DIAGRAMA DE GANTT DEL PROYECTO

O en modo tabla:

| | Nombre | Trabajo | Duración | Inicio |
|---|---|---|---|---|
| 1 | Estudio de Viabilidad | 16 horas | 2 days | 12/03/14 8:00 |
| 2 | Estado del arte | 48 horas | 6 days? | 14/03/14 8:00 |
| 3 | Diseño del Sistema | 88 horas | 11 days? | 21/03/14 14:00 |
| 4 | Desarrollo | 200 horas | 25 days | 7/04/14 8:00 |
| 5 | Implatación | 80 horas | 10 days | 12/05/14 8:00 |
| 6 | Formación | 24 horas | 3 days? | 26/05/14 8:00 |
| 7 | Aceptación | 8 horas | 1 day? | 28/05/14 8:00 |
| 8 | Documentación | 24 horas | 3 days | 29/05/14 8:00 |

ILUSTRACIÓN 12: TABLA DE TAREAS Y PLANIFICACIÓN DEL PROYECTO

Al ofrecerse como opción el mantenimiento de la plataforma, no se incluye dicho mantenimiento en la planificación del proyecto.
Todos las fases del proyecto de esta planificación se han cumplido en tiempo y forma y las tareas programadas se ha desarrollado conforme a la planificación inicial.

## GESTIÓN DE RIESGOS

La gestión de los riesgos siempre supone una parte importante y crítica en un proyecto de este tipo.

En la gestión de este proyecto, hemos seguido las recomendaciones del Inteco[12] .

Según dicha guía, un riesgo de un proyecto se define como:

[12] Guía Avanzada de Gestión de Riesgos http://www.inteco.es/file/TnOIvX7kM5r8OY-S8r9Bmg

*"un evento o condición incierto que, si se produce, tendrá un efecto positivo o negativo sobre al menos un objetivo del proyecto, como tiempo, coste, alcance o calidad, es decir, cuando el objetivo de tiempo de un proyecto es cumplir con el cronograma acordado; cuando el objetivo de coste del proyecto es cumplir con el coste acordado, etc. "*

Las organizaciones perciben los riesgos por su relación con las amenazas al éxito del proyecto o por las oportunidades de mejorar las posibilidades de éxito del proyecto. Los riesgos que son amenazas para el proyecto pueden ser aceptados si el riesgo está en equilibrio con el beneficio que puede obtenerse al tomarlo.

El riesgo está compuesto de tres componentes esenciales:

un evento definible

probabilidad de ocurrencia

consecuencia de la ocurrencia (impacto)

Para la adecuada gestión de los riesgos, se debería establecer un "Plan de gestión de riesgos" y en dicho plan se debería describir los siguientes elementos:

- Una estrategia de gestión de riesgos
- Alcance del esfuerzo en gestión de riesgos
- Cómo se piensa llevar a cabo la identificación de riesgos
- Cómo se va a llevar a cabo el análisis de riesgos (cualitativo, cuantitativo, priorización)
- Cómo se va a llevar a cabo el plan de respuesta (no debe contener los propios planes de respuesta ni tratar riesgos concretos)
- Cómo se va a llevar a cabo la monitorización y control
- Presupuesto de gestión de riesgos
- Calendario de actividades de gestión de riesgos
- Roles y Responsabilidades

Con lo que en la vida útil del proyecto, se debería de cumplir con este ciclo de actividades:

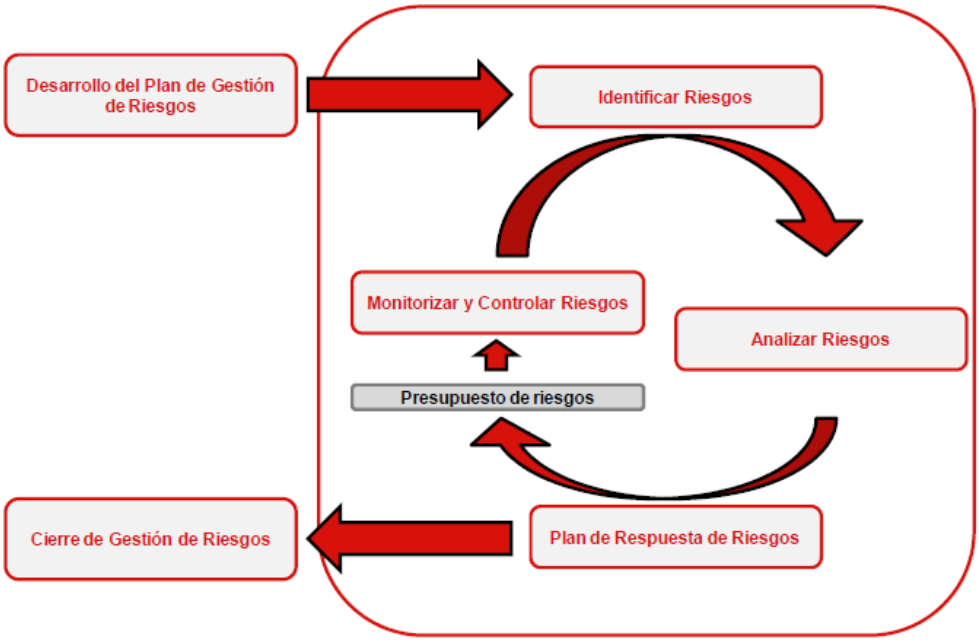



ILUSTRACIÓN 13: ACTIVIDADES DE GESTIÓN DE RIESGOS. (INTECO)

Para realizar un análisis exhaustivo de los riesgos, el jefe del proyecto debería utilizar registros y registrar el estado de cada elemento de riesgo. En dicho registro se debería almacenar información de este tipo:

- Identificador del riesgo
- Estado del riesgo
- Descripción del riesgo
- Probabilidad cualitativa (baja, media, alta, muy alta)
- Impacto cualitativo (bajo, medio, alto, muy alto)
- Impacto de costes
- Categorización de riesgos cualitativa
- Probabilidad cuantitativa (%)
- Impacto cuantitativo (Euros)
- Valor esperado
- Estrategia de respuesta
- Descripción de respuesta

Nuestro modelo es mucho más modesto y se ha identificado los riesgos más importantes del proyecto con estos resultados:

| Riesgo | Fecha Límite | Acción | Estado |
|---|---|---|---|
| **No disponer de la infraestructura adecuada** | 31/03/2014 | Suplir los requisitos hardware como máquina física local | Correcto |
| **Demora de la implantación** | 07/04/2014 | Redefinir necesidades con el cliente | Correcto |
| **Acceso a recursos de APG** | 10/04/2014 | Definir claramente responsabilidades por parte de APG | Correcto |
| **Impacto en la infraestructura de cliente** | Toda la fase de implantación | Ante cualquier impacto aseguraremos siempre un proceso de vuelta atrás del sistema | Correcto |

La herramienta forma parte del sistema de virtualización de la Autoridad Portuaria de Gijón, tal como se ha descrito en los apartados anteriores.

La máquina  entregada es una máquina virtual con las siguientes características:

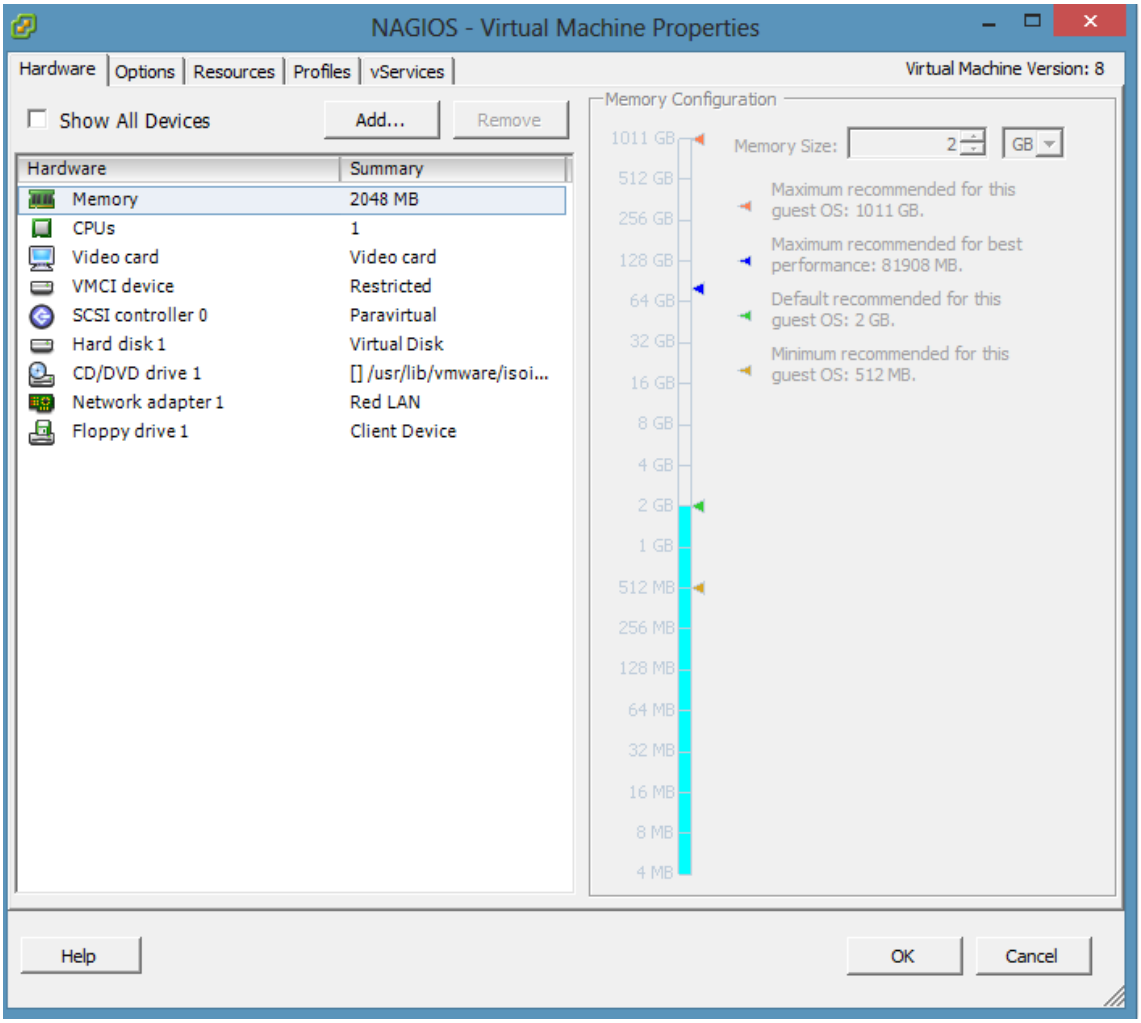



ILUSTRACIÓN 14: CARACTERÍSTICAS DE LA MÁQUINA VIRTUAL

En dicha máquina corre un sistema Nagios cuya página principal es la siguiente

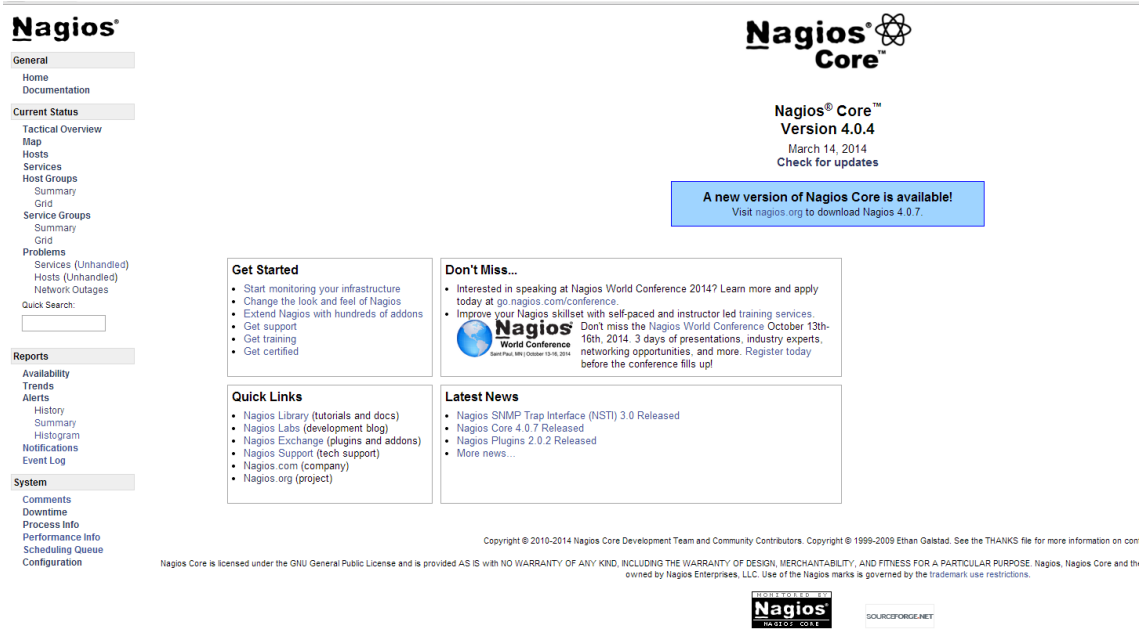



ILUSTRACIÓN 15: PÁGINA PRINCIPAL DEL SISTEMA NAGIOS

El sistema de monitorización Nagios muestra toda su potencia en los entornos descentralizados y heterogéneos como el existente en la red del cliente.

Nos hemos encontrado con Servidores de impresión, Directorio activo, Sistemas colaborativos, servidores de Bases de datos basados en múltiples SGDB's y varios servidores de aplicaciones.

En el ámbito del software libre también contamos con varios servidores basados en distribuciones CentOS.

Aunque el ámbito de la monitorización en una primera fase no abarcaba toda la red corporativa, uno de los ámbitos de mejora es la extensión de los sensores instalados a todos los servicios corporativos, tal como quedará descrito en posteriores apartados.

Desde la interfaz web controlamos de un vistazo la situación general de los sistemas

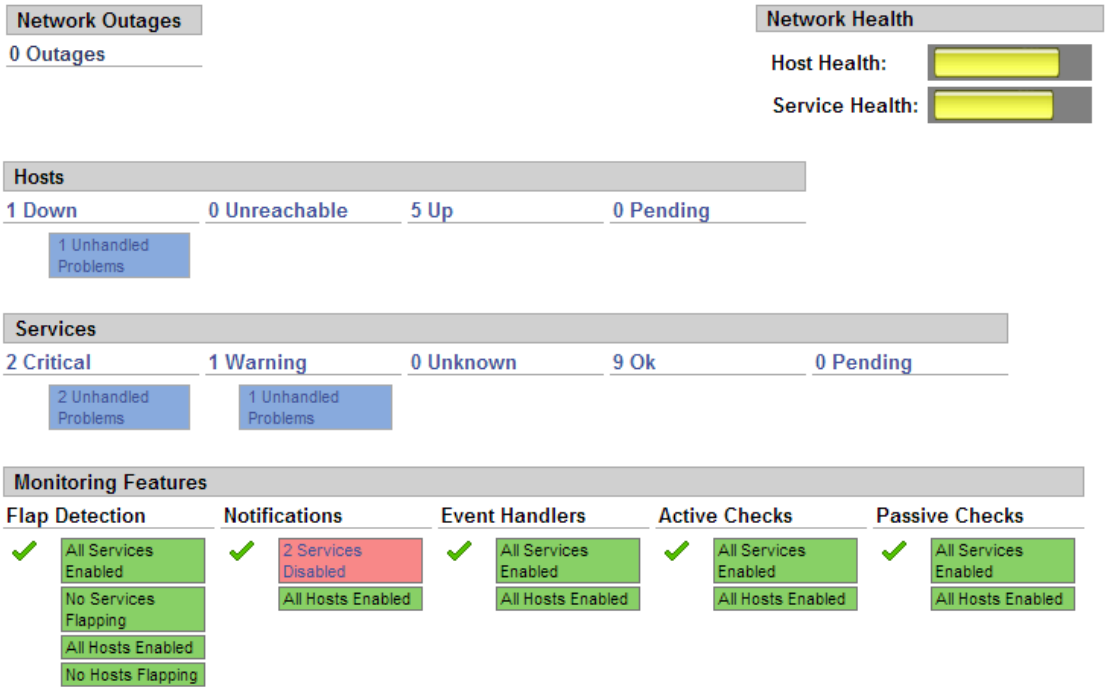



ILUSTRACIÓN 16: SITUACIÓN GENERAL DE LOS SISTEMAS MONITORIZADOS

Como vemos en la ilustración anterior, en esta opción disponemos de una fotografía de nuestros sistemas con las alertas más importantes, como los servicios críticos no disponibles, los servidores que no están dando servicio y las comprobaciones activas y pasivas.

Una de las lecturas más interesantes es el "Monitoring Performance" en el que podemos comprobar latencias y tiempos de ejecución de servicios monitorizados en nuestra red, así como los Servidores activos y otras informaciones de interés como podemos ver en las ilustraciones siguientes:

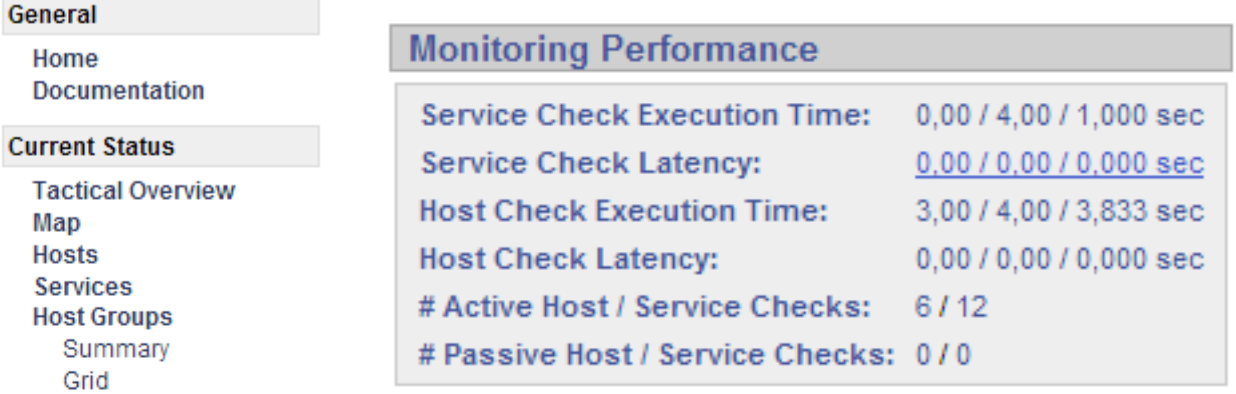



ILUSTRACIÓN 17: MONITORING PERFORMANCE

Podemos establecer mapas de red con ciertos dispositivos monitorizados y accedemos a ellos por el menú General Nagios que vemos en la ilustración siguiente:

Es importante destacar la multitud de opciones de visualización que nos ofrece el menú general de Nagios, en el que podemos tener acceso y en el que caben destacar las vistas de Grupos de servidores y las opciones de resolución de problemas de servicios y servidores, asi como los informes de Disponibilidad y las alertas de eventos y notificaciones.

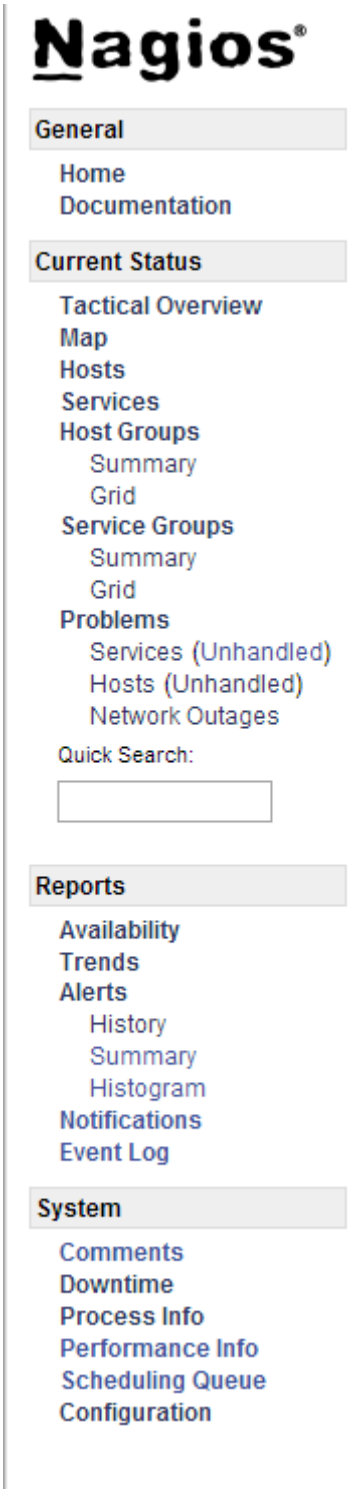



ILUSTRACIÓN 18: MENÚ GENERAL

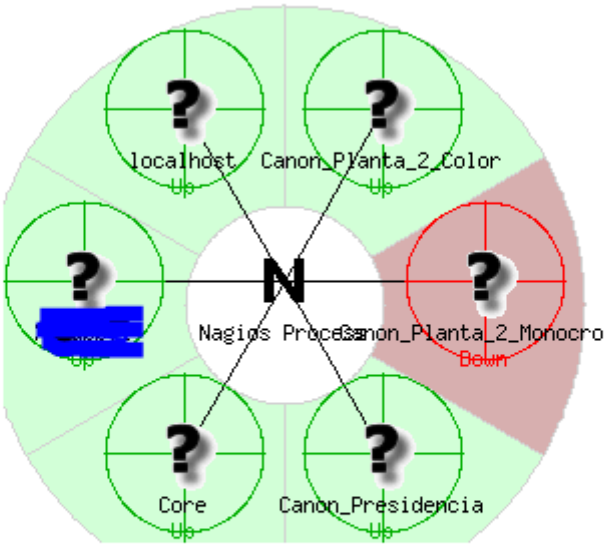



ILUSTRACIÓN 19: EJEMPLO DE MAPA DE RED

Como vemos en la ilustración anterior, es posible monitorizar los sistemas agrupándolos y comprobando con esquemas su disponibilidad

Se puede igualmente establecer grupos para una mejor gestión como vemos en esta figura:

**Status Summary For All Host Groups**

| Host Group | Host Status Summary | Service Status Summary |
|---|---|---|
| Linux Servers (linux-servers) | 1 UP | 7 OK<br>1 WARNING : 1 Unhandled |
| Network Printers (network-printers) | 2 UP<br>1 DOWN : 1 Unhandled | 1 OK<br>1 CRITICAL : 1 Unhandled |
| Network Switches (switches) | 1 UP | 1 OK<br>1 CRITICAL : 1 Unhandled |
| Windows Servers (windows-servers) | 1 UP | No matching services |

ILUSTRACIÓN 20: ESTADO DE LOS ELEMENTOS MONITORIZADOS

Bajando de nivel podemos comprobar el estado de más servicios

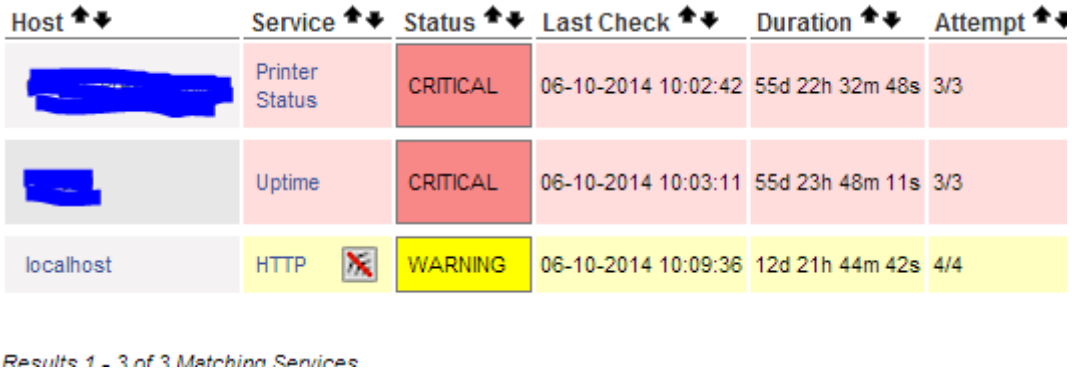
Limit Results: 100

| Host | Service | Status | Last Check | Duration | Attempt |
|---|---|---|---|---|---|
| [redacted] | PING | OK | 06-10-2014 10:02:00 | 21d 17h 55m 52s | 1/3 |
| | Printer Status | CRITICAL | 06-10-2014 10:02:42 | 55d 22h 30m 51s | 3/3 |
| Core | PING | OK | 06-10-2014 10:08:27 | 55d 23h 47m 53s | 1/3 |
| | Uptime | CRITICAL | 06-10-2014 10:03:11 | 55d 23h 46m 14s | 3/3 |
| localhost | Current Load | OK | 06-10-2014 10:04:00 | 56d 0h 31m 30s | 1/4 |
| | Current Users | OK | 06-10-2014 10:06:32 | 62d 22h 1m 0s | 1/4 |
| | HTTP | WARNING | 06-10-2014 10:04:36 | 12d 21h 42m 45s | 4/4 |
| | PING | OK | 06-10-2014 10:07:08 | 62d 21h 59m 45s | 1/4 |
| | Root Partition | OK | 06-10-2014 10:05:16 | 62d 21h 59m 8s | 1/4 |
| | SSH | OK | 06-10-2014 10:05:17 | 62d 21h 58m 30s | 1/4 |
| | Swap Usage | OK | 06-10-2014 10:05:20 | 62d 21h 57m 53s | 1/4 |
| | Total Processes | OK | 06-10-2014 10:06:11 | 62d 21h 57m 15s | 1/4 |

*Results 1 - 12 of 12 Matching Services*

ILUSTRACIÓN 21: EJEMPLO DE MONITORIZACIÓN DE SERVICIOS

Y en el caso de que ciertos elementos no estén activos podemos comprobar su estado en las tablas correspondientes (la siguiente ilustración se corresponde con elementos apagados)



| Host | Service | Status | Last Check | Duration | Attempt |
|---|---|---|---|---|---|
| [redacted] | Printer Status | CRITICAL | 06-10-2014 10:02:42 | 55d 22h 32m 48s | 3/3 |
| [redacted] | Uptime | CRITICAL | 06-10-2014 10:03:11 | 55d 23h 48m 11s | 3/3 |
| localhost | HTTP | WARNING | 06-10-2014 10:09:36 | 12d 21h 44m 42s | 4/4 |

*Results 1 - 3 of 3 Matching Services*

ILUSTRACIÓN 22: ESTADO DE SERVICIOS Y HOSTS

Y en el caso de que se trate de hosts apagados, también podemos comprobar que existe un problema en la vista "Problemas" del menú general

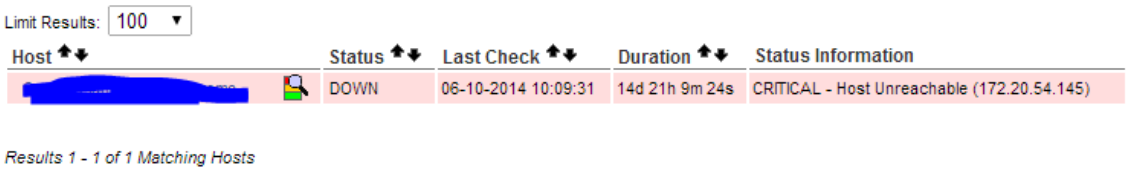



ILUSTRACIÓN 23: PROBLEMAS CON LOS HOSTS MONITORIZADOS

## INFORMES Y ALERTAS

En Nagios existe la posibilidad de realizar informes de alertas y del estado de los sistemas monitorizados en función de un potente motor de búsquedas:

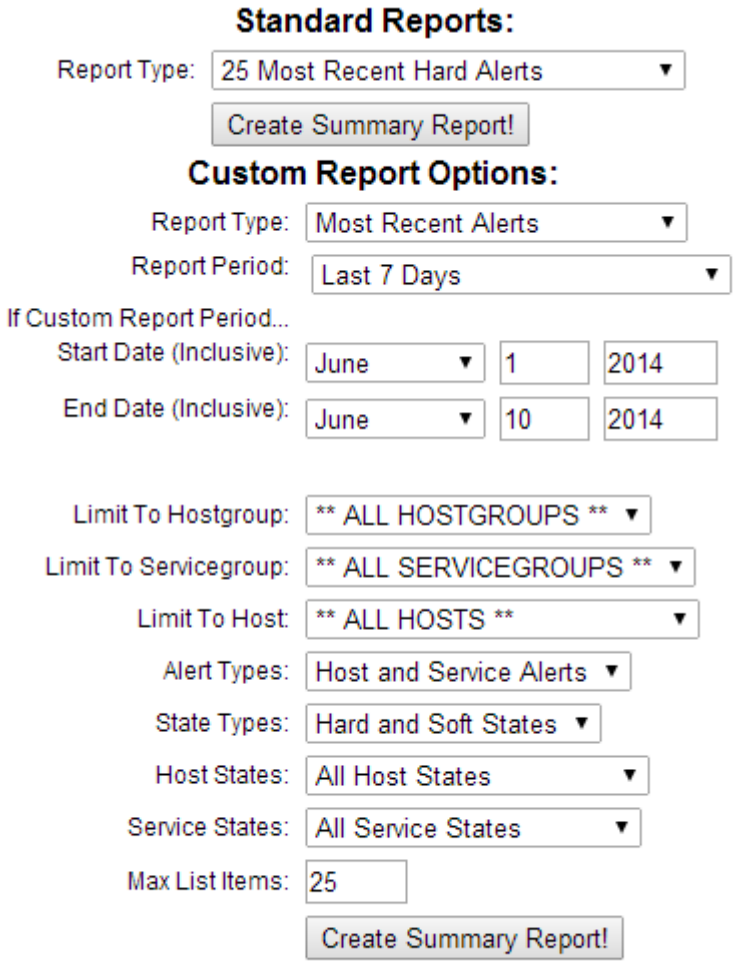



ILUSTRACIÓN 24: CREACIÓN DE INFORMES EN NAGIOS

Como podemos comprobar en la figura anterior, es posible crear todo tipo de informes de los elementos monitorizados, asi como programar alertas asociadas a dichos eventos.

| Time | Alert Type | Host | Service | State | State Type | Information |
|---|---|---|---|---|---|---|
| 06-05-2014 13:19:31 | Host Alert | [redacted] | N/A | UP | SOFT | PING OK - Packet loss = 0%, RTA = 0.67 ms |
| 06-05-2014 13:18:27 | Host Alert | [redacted] | A | DOWN | SOFT | CRITICAL - Host Unreachable (172.20.54.108) |

ILUSTRACIÓN 25: EJEMPLO DE INFORMES DE MONITORIZACIÓN

Las posibilidades de monitorización de los eventos son múltiples y ponen a disposición de los administradores de sistemas la información necesaria

para una gestión efectiva y de alto nivel de los sistemas corporativos.

| Host | Service | Type | Time | Contact | Notification Command | Information |
|---|---|---|---|---|---|---|
| [redacted] | N/A | HOST DOWN | 06-10-2014 10:04:31 | nagiosadmin | notify-host-by-email | CRITICAL - Host Unreachable ([redacted]) |
| [redacted] | Uptime | CRITICAL | 06-10-2014 10:03:11 | nagiosadmin | notify-service-by-email | (No output on stdout) stderr: execvp(/usr/local/nagios/libexec/check_snmp, ...) failed. errno is 2: No such file or directory |
| [redacted] | N/A | HOST DOWN | 06-10-2014 09:34:14 | nagiosadmin | notify-host-by-email | CRITICAL - Host Unreachable ([redacted]) |
| [redacted] | Printer Status | CRITICAL | 06-10-2014 09:22:42 | nagiosadmin | notify-service-by-email | (No output on stdout) stderr: execvp(/usr/local/nagios/libexec/check_hpjd, ...) failed. errno is 2: No such file or directory |
| [redacted] | N/A | HOST DOWN | 06-10-2014 09:03:56 | nagiosadmin | notify-host-by-email | CRITICAL - Host Unreachable ([redacted]) |
| [redacted] | Uptime | CRITICAL | 06-10-2014 09:03:11 | nagiosadmin | notify-service-by-email | (No output on stdout) stderr: execvp(/usr/local/nagios/libexec/check_snmp, ...) failed. errno is 2: No such file or directory |
| [redacted] | Printer Status | CRITICAL | 06-10-2014 08:22:42 | nagiosadmin | notify-service-by-email | (No output on stdout) stderr: execvp(/usr/local/nagios/libexec/check_hpjd, ...) failed. errno is 2: No such file or directory |
| [redacted] | Uptime | CRITICAL | 06-10-2014 08:03:11 | nagiosadmin | notify-service-by-email | (No output on stdout) stderr: execvp(/usr/local/nagios/libexec/check_snmp, ...) failed. errno is 2: No such file or directory |
| [redacted] | Printer Status | CRITICAL | 06-10-2014 07:22:42 | nagiosadmin | notify-service-by-email | (No output on stdout) stderr: execvp(/usr/local/nagios/libexec/check_hpjd, ...) failed. errno is 2: No such file or directory |

ILUSTRACIÓN 26: SISTEMA DE MONITORIZACIÓN DE EVENTOS CRÍTICOS

Se pueden igualmente definir o programar informes de errores o caída de servicios

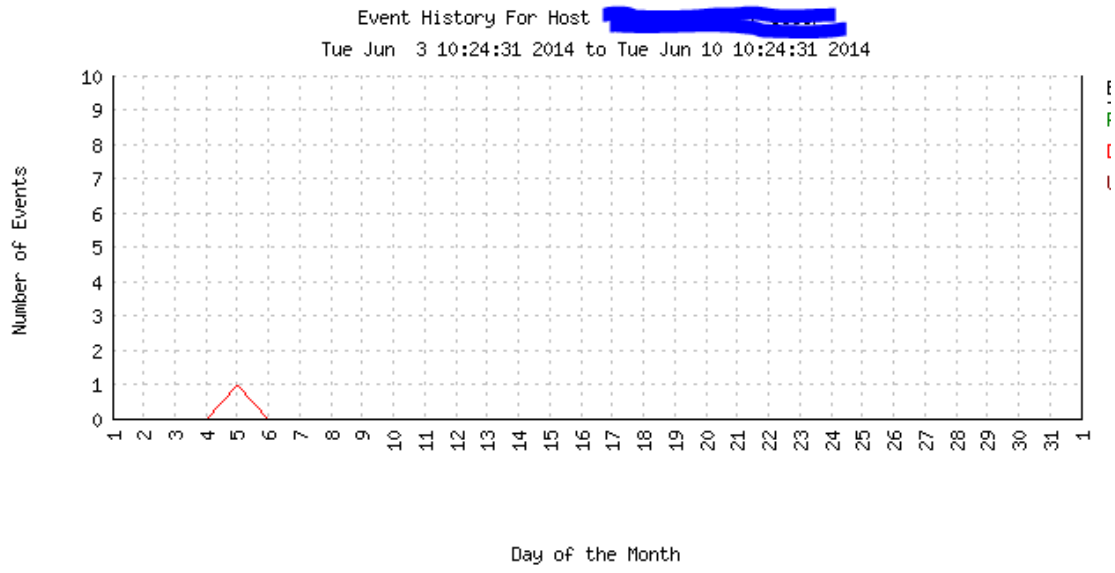



ILUSTRACIÓN 27: HISTORIAL DE EVENTOS CRÍTICOS EN UN SISTEMA MONITORIZADO

Esta opción resulta especialmente interesante en caso de tener que cumplir con acuerdos de nivel de servicios, ya que permite justificar los tiempos de actividad del sistema ante una posible reclamación y establecer umbrales para la comprobación de este tipo de entornos, como los tiempo de baja de

un servicio que es necesario para la actualización de sistemas, los cuales se pueden programar como se puede ver en el siguiente gráfico:

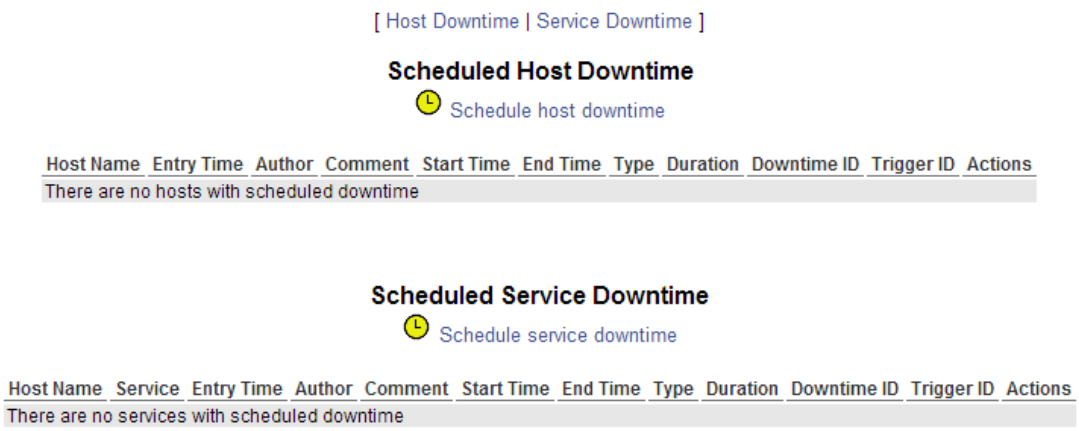



ILUSTRACIÓN 28: PARADAS DE SISTEMA PROGRAMADAS

Los sistemas monitorizados, permiten interactuar con ellos, y con los procesos Nagios, como vemos en la siguiente figura

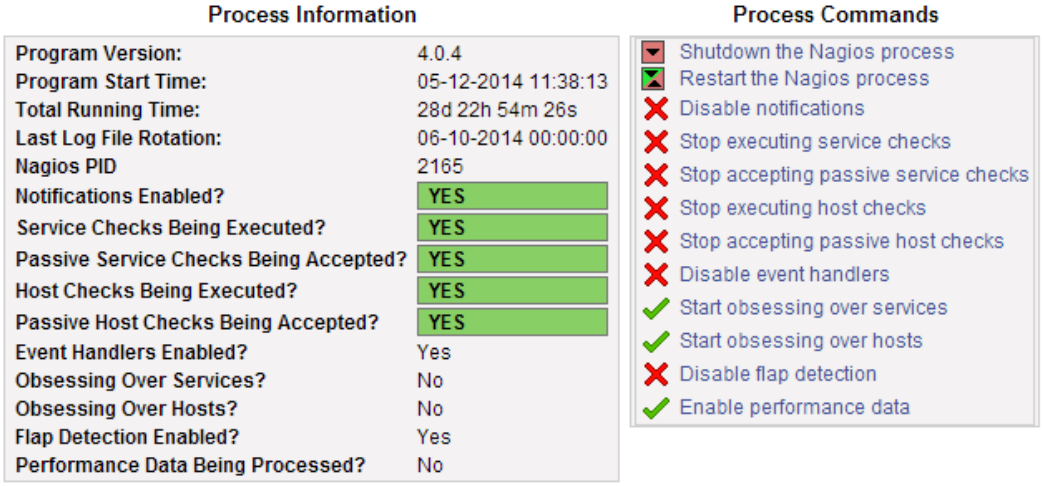



ILUSTRACIÓN 29: INFORMACIÓN DEL PROCESO DE NAGIOS

# CONSIDERACIONES FINALES Y CONCLUSIONES

En este tiempo de uso (tres semanas desde la primera instalación) los administradores de sistemas de la Autoridad Portuaria, han tenido acceso a la consola de administración y nos han trasladado las siguientes opiniones y ámbitos de mejora:

## PUNTOS FUERTES:

- Excelente interfaz de monitorización
- Fácil despliegue de agentes de monitorización tanto en Linux como en Windows
- Información exhaustiva del rendimiento de las máquinas virtuales
- Buena documentación del proyecto y del despliegue en las máquinas existentes
- Buena elección de la herramienta de monitorización con la posibilidad de escalar el producto sin límite de crecimiento para la infraestructura de la Autoridad Portuaria

## ÁMBITOS DE MEJORA

- Diseño de mapas de red personalizados: Se contemplará como ampliación del proyecto ya que el alcance del proyecto inicial sólo contemplaba la monitorización de los servicios críticos identificados por la Autoridad Portuaria.
- Creación de scripts para respuesta a ciertos eventos críticos, y la posibilidad de levantar servicios caídos automáticamente. Dicha posibilidad también se contemplará como ampliación del proyecto inicial.

Como aportación a estas mejoras, estimo que sería muy interesante mejorar los siguientes puntos;

- Extensión de la red de sensores de monitorización a toda la red corporativa.
- Instalación de un sistema de visualización lo suficientemente grande que permita mostrar en pantalla los eventos más críticos o bien con un sistema de rotación que visualice el estado de dichos sistemas y que permita así minimizar el tiempo de reacción ante una incidencia.

# CONCLUSIONES

El proyecto final ha cubierto las expectativas del cliente, aunque en un proyecto de este tipo, desde mi punto de vista es tan importante la implantación como un correcto mantenimiento que permita la explotación del sistema introduciendo procesos de mejora continua que permitan por un lado identificar los procesos críticos, y por otro redefinir continuamente los indicadores en función de las necesidades cambiante de los sistemas.

En un entorno de este tipo es fundamental la implicación de los usuarios finales, en este caso el personal de Innovación y Sistemas de Información de la Autoridad Portuaria, cuyo apoyo, profesionalidad e inmejorable disposición han sido imprescindibles para la correcta finalización de este trabajo.

La herramienta ha quedado activada y en producción dentro de los servidores corporativos, y está sirviendo de ayuda en la resolución de problemas de conectividad al personal técnico.

Quedaría en una segunda fase del proyecto la extensión a todos los servidores corporativos y servicios con posibilidad de monitorización, así como la creación de los scripts y programas necesarios que permitan solucionar los problemas de los sistemas críticos de una manera proactiva.

# BIBLIOGRAFÍA


Cacti. (s.f.). *http://cacti.net/*.

Canonical. (s.f.). *http://doc.ubuntu-es.org/*.

Catalunya, U. O. (s.f.). *www.uoc.edu*.

Inteco. (s.f.). *http://www.inteco.es/file/TnOIvX7kM5r8OY-S8r9Bmg*.

Nagios. (s.f.). *http://www.nagios.org/*.

Nsclient. (s.f.). *http://www.nsclient.org/*.

Pandora. (s.f.). *http://wiki.pandorafms.com*.

PCFMON. (s.f.). *http://pfcmon.wikispaces.com*.

Zenoss. (s.f.). *http://www.zenoss.com/*.