tecnim@p Sevilla 2006
30 mayo a 2 junio
060.es
24x7x365

Comunicación

230

MONITORIZACIÓN Y GESTIÓN DE DISPOSITIVOS, SERVICIOS Y APLICACIONES

Eloy Rafael Sanz Tapia
Asesor Técnico - Seguridad
Consejería de Educación - Junta de Andalucía

Lourdes Benítez Sánchez-Cid
Jefa del Servicio de Informática - Secretaría General Técnica
Consejería de Educación - Junta de Andalucía

Juan Almorza Daza
Jefe de Sistemas de Información - Secretaría General Técnica
Consejería de Educación - Junta de Andalucía

Eloy Rafael Sanz Tapia
Lourdes Benítez Sánchez-Cid
Juan Almorza Daza

Palabras clave

Monitorización, sistemas, servicios, aplicaciones.

Resumen de su Comunicación

El conocimiento exacto del estado de los dispositivos (servidores, hardware de red, appliances), los servicios y las aplicaciones gestionados por el Servicio de Informática es necesario para asegurar la disponibilidad, reaccionar inmediatamente ante los problemas y actuar proactivamente para prevenirlos.

Esta comunicación describe los esfuerzos que en este sentido se están realizando por parte del Servicio de Informática de la Consejería de Educación de la Junta de Andalucía, y los planes que se tienen para posibles mejoras.

Eloy Rafael Sanz Tapia
Lourdes Benítez Sánchez-Cid
Juan Almorza Daza

MONITORIZACIÓN Y GESTIÓN DE DISPOSITIVOS, SERVICIOS Y APLICACIONES

1. Introducción

El gran número de servidores y otros dispositivos, servicios y aplicaciones propias que debe gestionar hoy cualquier departamento de informática de un organismo de tamaño medio o grande hace necesario mantener un control sobre su funcionamiento y rendimiento.

Este control o monitorización sirve varios propósitos fundamentales:

- El mantenimiento de la disponibilidad del servicio, gracias a la detección inmediata de problemas.
- El dimensionamiento adecuado de la capacidad (red, almacenamiento, proceso).
- El conocimiento de las pautas y horarios de utilización de los servicios y aplicaciones.
- La detección de usos fuera de lo común, y la consiguiente evitación o respuesta rápida ante incidentes de seguridad.

En el Servicio de Informática de la Consejería de Educación de la Junta de Andalucía, el número de servidores ronda los setenta, sin contar otros dispositivos (routers y switches gestionabes, cortafuegos y sondas de detección de intrusiones). Hay aproximadamente cuarenta aplicaciones servidas, de diferente criticidad y grado de complejidad. Se utilizn herramientas de software libre para monitorizar el rendimiento y el estado de todos estos activos de información. También está en desarrollo una aplicación para mantener la información del sistema y las relaciones entre sus partes.

2. Estructura actual del sistema

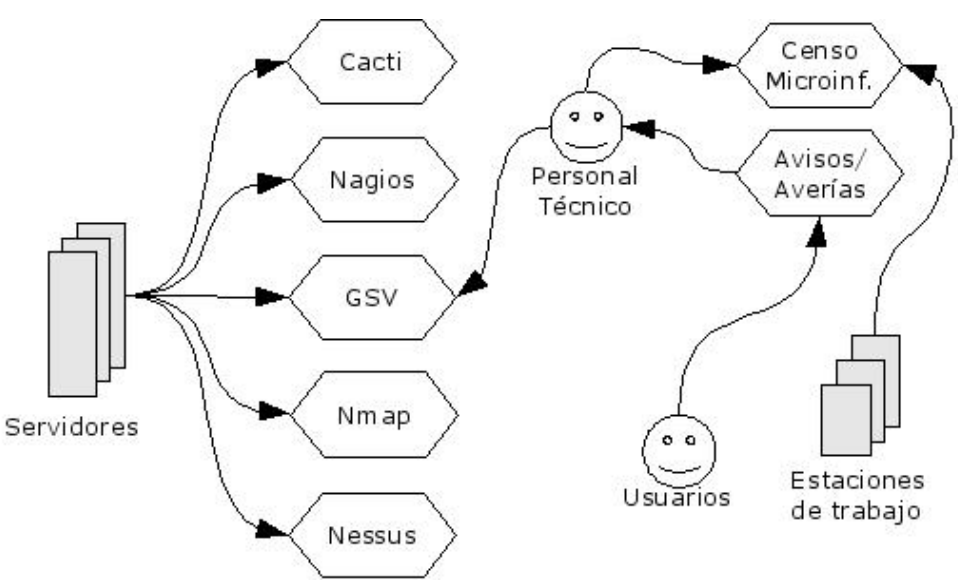

Fig.1: Esquema del sistema actual

Eloy Rafael Sanz Tapia
Lourdes Benítez Sánchez-Cid
Juan Almorza Daza

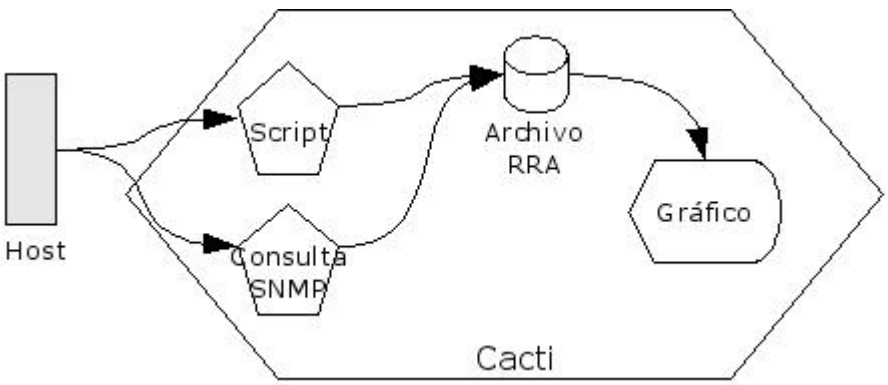

Fig.2: Cacti

Actualmente (ver fig. 1) se monitoriza el estado de los sistemas, servicios y aplicaciones de la siguiente forma:

Cacti

Se utiliza la herramienta Cacti para capturar información cualitativa sobre el estado de los dispositivos. Esta herramienta (fig. 2) accede a cada dispositivo y extrae información sobre su estado actual mediante consultas SNMP (simple network management protocol) o mediante scripts específicos escritos por el personal del Servicio de Informática.

Los agentes SNMP existentes para servidores Solaris, Linux y Windows ofrecen información sobre uso de procesador, número de usuarios conectados, utilización de memoria, espacio libre en particiones de disco, tráfico de red en cada interfaz... Mediante scripts ad-hoc se extrae información sobre número de accesos por segundo al sitio web de la Consejería, estado de los hilos de servicio de la misma web, tiempos de respuesta en servidor y en cliente de la aplicación Séneca, tiempos de respuesta tomados desde servidores externos a la Red Corporativa de la Junta de Andalucía...

La flexibilidad de Cacti permite tener múltiples dispositivos monitorizados, de cada uno de los cuales se extrae información que se almacena en un archivo histórico RRA (round robin archive). A partir de esos archivos se generan gráficos de manera sencilla y reutilizable mediante plantillas (fig. 3).

Nagios

La monitorización cualitativa de los servicios se realiza mediante el sistema Nagios (fig. 4). Nagios es un sistema potente que permite seguir el estado de múltiples servicios de red en múltiples servidores y avisar a personas o grupos de personas responsables de los mismos. En Nagios se permiten escaladas de avisos en función del tiempo de parada y otros parámetros, múltiples métodos de aviso (correo electrónico, SMS...) y presentación gráfica muy práctica del estado actual y del histórico de estados.

Nmap

Cada semana se ejecuta automáticamente una revisión de los puertos de red abiertos en los servidores de la Consejería. La herramienta Nmap permite no solo detectar dichos puertos, sino también descubrir (en muchos casos) el tipo de servicio, el software que lo ofrece y la versión del mismo que se está usando. Esta lista de servicios activos y versiones de software usadas se contrasta con lo esperado y se utiliza en los servicios de seguridad gestionada (principalmente en los de alerta temprana de vulnerabilidades).

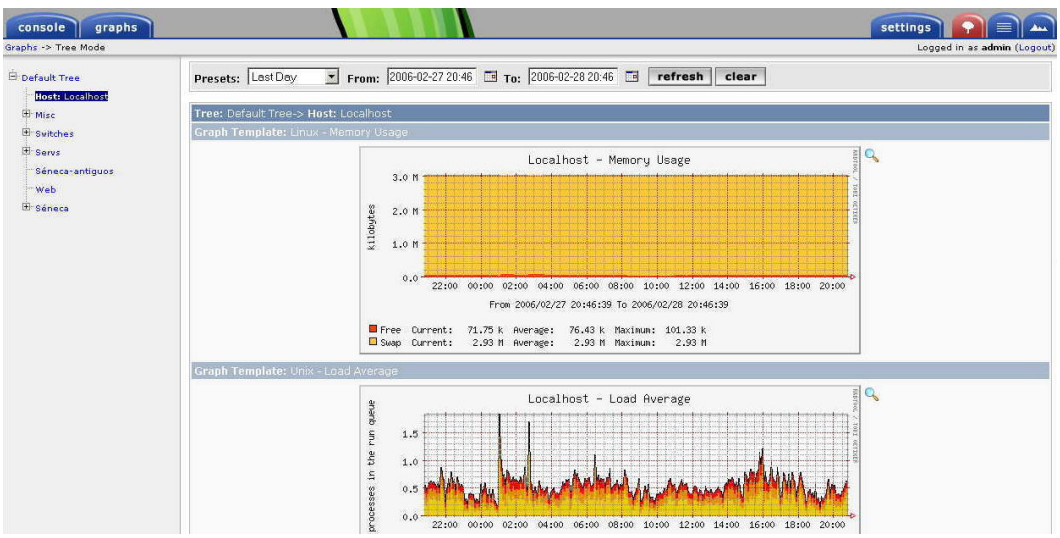

Fig.3: Cacti

Nessus

La herramienta Nessus se ejecuta de forma automática cada dos semanas para obtener un análisis de seguridad de los servidores, a partir de firmas de vulnerabilidad actualizadas antes de la ejecución. Este informe permite detectar vulnerabilidades y ejecutar las acciones correctivas adecuadas (parcheo, reconfiguración de servicios, adición de reglas de cortafuegos...).

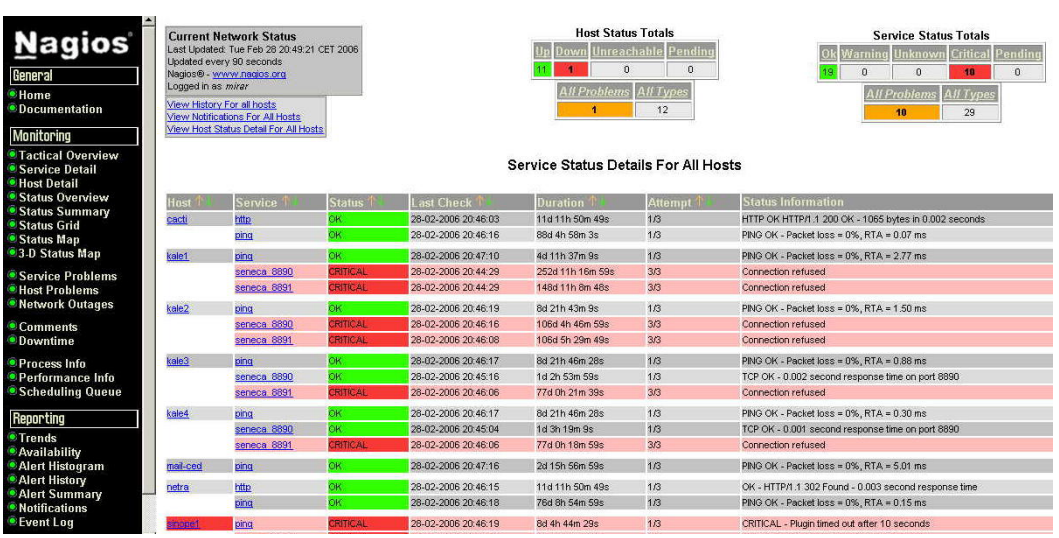

Fig.4: Nagios

GSV

Actualmente se encuentra en desarrollo en el Servicio de Informática una herramienta (temporalmente llamada GSV) para gestionar los activos de proceso de información existentes en el Servicio. Un modelo de datos informal se muestra en la figura 5. Las principales entidades (servidores, servicios, aplicaciones y responsables) se encuentran relacionadas entre sí de forma múltiple. Otra importante entidad es la que representa la actuaciones de diverso tipo que los responsables técnicos del Servicio realizan sobre los servidores y otros dispositivos. La construcción y el uso de esta herramienta están siendo impulsados por

la implantación del Sistema de Gestión de Seguridad de la Información actualmente en curso.

Aunque este documento se centra en servidores, se ha querido incluir por completitud y por la gran aceptación que tienen las dos principales herramientas para la gestión del parque microinformático de la Consejería:

Censo microinformático

Esta aplicación, desarrollada internamente, permite llevar un completo control sobre las características de las estaciones de trabajo en uso en la Consejería. Se incluyen datos sobre sistema operativo instalado, dependencia, número de serie, contacto de mantenimiento...

Avisos de averías

Los usuarios de la Consejería pueden avisar al área de microinformática del Servicio de averías e incidencias mediante esta aplicación, también desarrollada internamente.

3. Futuras mejoras

Actualmente el sistema se encuentra en explotación y mejora continua. Los

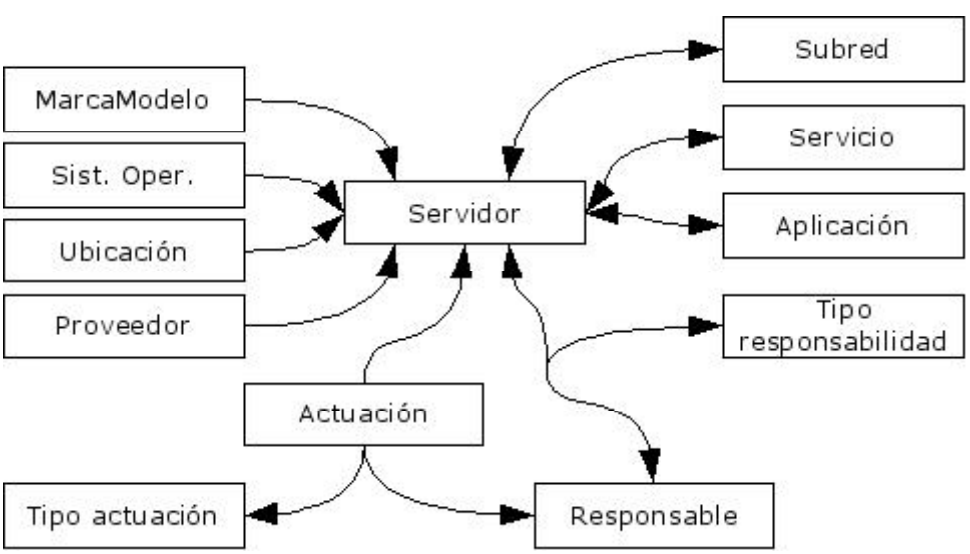

Fig. 5: Aplicación de gestión de servidores

nuevos servidores se integran en los servicios de monitorización y en la aplicación GSV como parte del checklist de instalación.

Algunas posibilidades que se barajan para el futuro incluyen integrar la configuración de las herramientas nessus, nmap, cacti y nagios en la aplicación GSV, de modo que el alta de un servidor nuevo en ésta cause su inclusión en el resto de los subsistemas de monitorización.

En el área de microinformática se ha pensado implantar la herramienta OCS Inventory NG, que permite recopilar de forma automática (en cada arranque) información sobre las estaciones de trabajo (aplicaciones instaladas, sistema operativo y nivel de parcheo, hardware...) y agruparla en una base de datos central con un interfaz de consulta bastante potente.

La centralización de logs y su explotación es uno de los subproyectos que se están acometiendo como parte del Plan Director de Seguridad y la implantación del SGSI. La herramienta Splunk parece ofrecer prometedoras características en este aspecto y está siendo evaluada.

4. Conclusiones

De todas las herramientas utilizadas, todas menos Nessus y Splunk están publicadas bajo licencias libres. Las aplicaciones propias desarrolladas por la Consejería están, de hecho, en proceso de liberación en virtud de la Orden de 21 de febrero de 2005, sobre disponibilidad pública de los programas informáticos de la Administración de la Junta de Andalucía y de sus organismos autónomos.

El Software Libre se plantea claramente como una alternativa válida para la realización de muchas tareas asociadas a los departamentos de Informática, y el Servicio de Informática de la Consejería de Educación cree firmemente en esto y piensa seguir apoyando al Software Libre usándolo y, sobre todo, escribiéndolo.

5. Referencias

Cacti	http://www.cacti.net
SNMP	http://en.wikipedia.org/wiki/Snmp
	http://es.wikipedia.org/wiki/SNMP
Nagios	http://www.nagios.org
Nmap	http://www.insecure.org/nmap
Nessus	http://www.nessus.org
OCS Inventory NG	http://ocsinventory.sourceforge.net
Splunk	http://www.splunk.com

Repositorio de Software Libre de la Junta de Andalucía:
http://www.juntadeandalucia.es/repositorio