Escrito por Dolores Tomé Cotarelo
Luns, 28 Abril 2003 15:13

There are no translations available.



En este artículo se comenta el programa gratuito Aida32 con el que podemos hacer auditoría de equipos informáticos monitorizando un equipo (o una red) de tal forma que podamos sacarle el máximo partido de la forma más segura.

Objetivo de la Auditoría

Cuando hablamos de auditoría lo primero que nos viene a la cabeza es una pregunta: ¿por qué necesito auditar un ordenador? Son varios los motivos por los que no sólo es importante sino necesario, hacer un seguimiento de los equipos informáticos con los que trabajamos.

La primera razón es para saber qué hardware tenemos instalado. Cuando compramos un equipo sabemos perfectamente lo que tiene, pero en las empresas es habitual que con el uso diario falle algo y se cambie un componente. También es frecuente que para mejorar el rendimiento se añada memoria o un disco duro por ejemplo. Todos estos cambios hacen que con el tiempo, el ordenador inicial que compramos no se parezca en mucho al que actualmente tenemos. Con un buen programa de auditoría se puede conocer el hardware que hay instalado lo que nos facilita la tarea a la hora de planear futuras ampliaciones o mejoras.

Otra razón es conocer los programas que tenemos instalados. A lo largo de la vida de un equipo es frecuente que instalemos y desinstalemos programas. Esto no sólo repercute en el rendimiento del equipo sino que en muchas ocasiones es frecuente que las instalaciones dejen ficheros residentes que no se borran por completo (ocupan espacio y ya no son necesarios).

Con la proliferación de Internet, virus y ataques externos es necesario tener en cuenta una

buena política de seguridad en nuestras máquinas para prevenir y no tener que preocuparnos cuando ya las cosas se han estropeado. En la línea de la prevención también están las auditorías, ya que permiten conocer lo que hay en cada momento en nuestro equipo de tal forma que podamos detectar por ejemplo programas extraños que no hayamos instalado nosotros.

La seguridad no solo consiste en ver los programas que hay instalados. Un buen programa de auditoría permitirá monitorizar una red de ordenadores, de tal forma que podamos averiguar qué equipos forma parte de la red, qué usuarios tienen privilegios de acceso y ciertos parámetros de la configuración de la red. El conjunto de esta información es vital a la hora de proteger nuestros equipos de ataques informáticos y facilita la labor, ya que no hay que ir equipo a equipo mirando estos datos. La mayoría de los programas de auditoría permitirán conocer esta información desde un servidor centralizado.

Finalmente un motivo más para auditar equipos o redes de equipos es la realización de estadísticas que permitan medir el rendimiento haciendo estudios comparativos entre informes.

Hasta ahora se ha explicado por qué es importante monitorizar nuestros ordenadores, pero cómo podemos hacerlo de verdad es otro tema. Una opción es desarrollar un software específico que permita auditar lo que realmente queremos, pero el desarrollo es caro y no suele estar al alcance de todos. Otra opción es adquirir un software que ya esté desarrollado. Si bien no suelen tener todo lo que queremos si suelen ser bastante completos. Aquí proponemos el uso de Aida32, un programa de uso sencillo y que dependiendo del uso que hagamos es gratuito.

Generación de Informes con Aida32

Aida32 es un programa de auditoría muy completo. Si entrar en detalle permite obtener información de un equipo muy variada: resumen de lo que hay en el equipo, detalle de la placa base, sistema operativo, parámetros del servidor, características del monitor, información multimedia, dispositivos de almacenamiento, entrada y resto del hardware, información de las direct x, programas instalados, información de la red, parámetros varios de configuración y una comparativa de la memoria.

Toda esta información se puede mostrar en diversos informes. Aida32 permite generar informes con toda o parte de la información y mostrarlos de diferente forma. Los formatos de salida son los siguientes: texto simple, HTML,MHTML, XML, CSV, MIF, INI, ADO.

Especialmente interesante es el formato ADO. Eligiendo y configurando en las preferencias esa opción se pueden insertar los resultados del informe en una base de datos. Si en un futuro se quieren ampliar los informes del programa con estadísticas que no están se puede hacer estudiando la información que hay en la base de datos. Entre las bases de datos con las que trabaja está Access, Oracle, SQL Server y MySQL, cuyas estructuras vienen incluidas con Aida32.

¿Cómo podemos auditar y obtener estadísticas de una red de ordenadores con Aida32?

Aida32 propone en su documentación dos formas de auditar una red de equipos. Aquí comentaremos la más segura (no es en tiempo real pero el retardo es mínimo y aceptable teniendo en cuenta la seguridad que proporciona).

Lo único que hay que hacer es instalar Aida32 en un equipo y poner la carpeta en la que esté con acceso de solo lectura para todos los equipos de la red que se quieren auditar.

Aquí recomendamos crear otra carpeta con permisos de lectura – escritura , igualmente accesible para todos los equipos de la red a auditar. En esta carpeta se volcarán los informes de auditoría en formato CSV. Si se prefiere se puede prescindir de esta carpeta y volcar los informes a una base de datos de las anteriormente citadas, pero téngase en cuenta que esta opción implicaría mucho más tráfico de red y provocará retrasos en las comunicaciones.

En cada uno de los equipos a auditar se lanzará el siguiente comando desde una ventana del DOS:

servidor carpeta_aida aida32 /

servidor (con doble barra invertida delante) es el nombre de la máquina donde está instalado el programa Aida32;

carpeta_aida es la carpeta con permisos de solo lectura en la que está instalado;

carpeta_informes es la carpeta con permisos de lectura – escritura en la que se dejarán los informes;

nombre_informe es el nombre del informe. Si se quiere que aparezca el nombre de la máquina de la que procede el informe se puede poner $HOSTNAME;

/CSV es el formato de salida del informe. Si se quiere se puede poner /ADO (para bases de datos);

/AUDIT, /SILENT y /SAFE son parámetros necesarios para mantener la seguridad.

Una vez hecho esto se tiene en la carpeta de los informes una lista de ficheros (uno por cada ordenador auditado). Lo único que hay que hacer para ver informes conjuntos es poner en marcha Aida32 y arrastrar todos los ficheros al marco de la izquierda. Inmediatamente aparecerán la lista de equipos que han sido monitorizados.

Una vez hecho esto se tiene en la carpeta de los informes una lista de ficheros (uno por cada ordenador auditado). Lo único que hay que hacer para ver informes conjuntos es poner en marcha Aida32 y arrastrar todos los ficheros al marco de la izquierda. Inmediatamente aparecerán la lista de equipos que han sido monitorizados.

Junto con la lista de equipos aparecen unos informes estadísticos que se han generado automáticamente con la información de la auditoría. Si se añaden más informes de equipos se actualizan estas estadísticas, que entre otras cosas son muy útiles para evaluar el rendimiento de los equipos de forma individual y en el conjunto de la red.

Dónde se puede conseguir el programa

Aida32 para sistemas operativos Windows, se puede descargar desde la página del autor en h
ttp://www.aida32.hu/aida-download?bit=32
. El producto es freeware y no es necesario hacer nada más si es para uso personal. Sin embargo, si es para uso profesional es necesario notificar su uso al autor vía correo electrónico o desde la página web
http://www.aida32.hu/registration
.

Aida32 tiene tres versiones (personal, network y enterprise). Aquí recomendamos la última por ser la más completa y por tener toda la funcionalidad explicada a lo largo del artículo.

Continua leyendo este artículo