Dolores Tomé Cotarelo-k idatzia
Asteartea, 2004(e)ko otsaila(r)en 10-(e)an 18:49etan

There are no translations available.

Este artículo es continuación del artículo Auditoría de equipos informáticos. En esta segunda parte se indica otra forma de hacer una auditoría de equipos conectados en red.

Novedades respecto a la forma anteriormente propuesta

En el primer artículo se proponía una forma de auditar en la que había un ordenador en el que se instalaba Aida32. Conectados en red estaban el resto de equipos que se querían auditar, y lo que hacían era lanzar una petición al ordenador con Aida32 para que generase un informe en formato CSV con esa información.

La petición que había que hacer desde cualquiera de los ordenadores a auditar era:

```
\\serv1dor\carpeta_a1da\a1da32 /R \\serv1dor\carpeta_1nformes\nombre_1nformes
/CSV /AUDIT /SILENT /SAFE
```

Aunque no se dijo en el otro artículo, como se trataba de una ejecución remota del programa desde la línea de comandos, se podría incluir esta orden en una tarea programada del sistema

operativo. Así, se conseguiría automatizar el proceso sin tener que ser realizado de forma manual desde cada uno de los equipos a auditar.

Pero lo que se propone ahora es una forma distinta de auditar: desde un equipo se realizará la auditoría de todos los demás equipos de la red. Dicho equipo hará la auditoría cuando considere conveniente (según las necesidades que marque cada organización). Para hacerlo, se necesita que todos los equipos tengan instalado el Aida32 (y no solo uno como ocurría en la primera propuesta). Otra novedad es que los informes ya no se generan en ficheros con formato CSV, sino que se dejarán en una base de datos.

Una vez instalado Aida32 en todos los equipos y configurado adecuadamente, se podrán hacer auditorías de todos los equipos de la red, controlando el proceso desde un único equipo.

En los siguientes apartados se detalla cada uno de estos pasos a dar antes de proceder a la realización de la auditoría.

Instalación de Aida32 en el equipo auditor

El equipo auditor será aquel que controle todo el proceso de la auditoría. Este equipo tendrá el Aida32 instalado por completo sin restricción alguna. Por tanto lo único que hay que hacer es instalar el programa tal y como se obtiene del distribuidor.

Una vez instalado hay que configurar las preferencias que indican la información que se incluirá en la auditoría. Para hacerlo seleccione Archivo à Preferencias y elija la opción Componentes de auditoría. Ahí, marque cada uno de los elementos que se quiera que aparezcan en los informes de auditoría de los equipos. Esta operación solo hay que hacerla en el equipo que hará las tareas de auditor.

Instalación de Aida32 en los equipos auditados

En el caso de los equipos a auditar sí que hay que establecer una serie de restricciones. Dado que tendrán instalado un Aida32 idéntico al que tendrá el equipo auditor, hay que tomar ciertas medidas de seguridad para que un equipo a auditar no se convierta en un equipo auditor.

Para evitar esto, hay que suprimir una serie de ficheros que sin quitar funcionalidad de la aplicación, sí dificultan que se puedan realizar las tareas que un equipo auditor tendría que hacer. Se mantendrán aquellos archivos necesarios para que desde el equipo auditor se pueda recoger la información del equipo a auditar.

De todos los ficheros de la aplicación, solo hay que dejar los siguientes:

aida32.bin
aida32.dat
aida32.exe
aida32.ini
aida32.mem
aida32.s64
aida32.sys
aida32.vxd
aidaplugin_diskbench.dll
aidaplugin_monitordiag.dll
aidaplugin_netbench.dll
es.lng

El resto de ficheros de pueden borrar sin que se vea afectado el funcionamiento de la aplicación de la forma que nos interesa.

De todos estos ficheros, destaca el **aida32.ini**, que es el que guarda los parámetros de la configuración. En él se detallan datos como el formato de salida de los informes, y como en nuestro caso van a una base de datos, se indicará la configuración de todo lo necesario para establecer las conexiones. En el siguiente apartado se detalla cómo se configuran las preferencias.

Adicionalmente, en los equipos auditados interesa que aida32 se ejecute de forma automática sin que el usuario del equipo auditado tenga que hacerlo de forma manual. Para hacer esto, lo mejor es lanzar un proceso con aida32 como si fuera uno más de los que se arrancan con el inicio de sesión.

Esto se puede hacer modificando la entrada del registro **HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsCurrentVersionRun**
en la que se añadirá la entrada Aida32 y se podrá valor
rutaAida32aida32.exe /hiddenserver /silent /safe
, donde

rutaAida32 es el disco y carpeta donde se ha instalado el programa,

/**hiddenserver** es una opción para el programa se ejecute en segundo plano pero aceptando todas las peticiones que se le manden,

/**silent** es un modo oculto de ejecución del programa de tal forma que el usuario del equipo auditado no se entere de cuándo se le está auditando,

/**safe** es otra opción para ejecutar aida32 en modo seguro, no permitiendo que se lancen dos instancias del programa.

Configuración de las preferencias ADO en los equipos

Como ya se ha indicado en el apartado anterior, los informes de auditoría se guardarán en una base de datos. Esta opción hay que configurarla en Aida32 en todos los equipos a auditar.

Un truco es configurarlo en un equipo y luego copiar el fichero aida32.ini en el resto, ya que este fichero es el que tiene la configuración que se ha puesto en las preferencias.

La configuración se hace en el menú Archivo à Preferencias. Ahí se elige la opción ADO, y se rellenan los parámetros que vienen en la pantalla según sea la base de datos que se utilice.

En caso de ser MySQL (que es gratuita), hay que indicar el servidor en el que reside la base de datos (puede ser el mismo que el de Aida32 u otro). En dicho servidor es necesario que se

haya creado una base de datos que tenga la estructura dada en la distribución del Aida32.

Si se tratase de Microsoft Access, también hay que indicar la ubicación de la base de datos. En este caso, es muy importante utilizar la opción de incremento de identidad automático, ya que si no se marca esta opción los informes no se insertarán correctamente.

En cualquier caso, para comprobar que se han configurado correctamente los parámetros, basta pulsar el botón Test.

Otras preferencias a configurar en equipos auditados y auditores

La forma de auditar que aquí se propone (instalar Aida32 en todos los equipos, sean auditores o auditados) ofrece la posibilidad de controlar desde la máquina auditora ciertas operaciones realizadas sobre las máquinas auditadas.

Así se puede permitir el acceso a los archivos de los equipos auditados, capturar pantallas del escritorio, ejecutar programas remotos, abortar la ejecución de Aida32, o reiniciar el equipo.

Para permitir estos accesos los equipos auditados tendrán que tener señaladas las opciones adecuadas en la ventana Archivo à Preferencias à Servidor.

Si se añaden estas opciones, se puede hacer lo mismo que se dijo en el apartado anterior: configurar un equipo y copiar su fichero aida32.ini en el resto de equipos que se auditarán.

En cualquier caso, un equipo auditor no tendrá opción alguna señalada en este apartado, evitando así que se pudieran realizar estas operaciones sobre él.

Proceso de auditoría

Una vez que se ha instalado Aida32 en los equipos a auditar y en el auditor, y se han configurado según se quiera las opciones de la base de datos, se puede comenzar a auditar

los equipos.

Desde el equipo auditor, se abrirá Aida32 y se elegirá la opción **Informe à Asistente de informe en Red**
Aparecerá una pantalla y se hará lo siguiente:

- En la pantalla de Bienvenida se pulsa **Continuar**.
- A continuación solicita el Perfil, y se elige la opción **Páginas necesarias** para la auditoría. El contenido del informe de la auditoría se habrá elegido en las preferencias cuando se instaló Aida32 en el equipo auditor.

- Lo siguiente que pide es el **Formato del informe**. Aquí se marcará la opción **ADO**.
- El siguiente paso es la elección de los **Ordenadores remotos**. Aparecerá una lista con los últimos ordenadores auditados. De esa lista se elegirán los que se quieren auditar de nevo. Si falta alguno, se puede añadir pulsando el botón
Nuevo
, donde dejará elegir un equipo mediante su dirección IP, o varios equipos dentro de un rango de direcciones IP, rango que se podrá acotar según interese.

- Tras la elección de los equipos a auditar, viene la página en la que se pregunta las **opciones de Salida de informe**
. Si se ha elegido el formato ADO, no es necesario poner nada.

- Una vez rellenado todo se Finaliza y comienza la auditoría de la lista de equipos que se haya indicado.

Como ya se ha dicho, la opción de instalar Aida32 tanto en equipo auditor como en equipos auditados, permitía operaciones adicionales a las de auditoría. Para hacer uso de ellas es necesario establecer en **Archivo à Conexión al servidor Aida32** una comunicación directa entre equipo auditor y auditado. Al hacerlo solicitará la dirección IP del equipo auditado.

Si todo va bien, aparecerá un mensaje confirmando la conexión, y un menú adicional llamado **Cliente**
. En él se tendrán las operaciones disponibles que el equipo auditor puede realizar sobre el equipo auditado. El que una operación esté disponible o no, dependerá de la configuración que se haya hecho en cada uno de los equipos a auditar cuando se instaló Aida32.

Ventajas y desventajas de esta forma de auditoría

En la primera forma propuesta, el informe con el contenido de la auditoría se genera manualmente. Aun cuando se pusiera en una tarea programada, la primera forma supone que la auditoría se hace en un momento fijo de tiempo (cuando se decida en la programación de la tarea). Sin embargo, con el proceso propuesto aquí, la auditoría de los equipos se hace en el momento que el auditor lo desee, controlando el proceso en todo momento.

Con la opción de instalar Aida32 en todos los equipos se puede establecer una conexión con cualquiera de ellos, pudiendo realizar tareas adicionales a las de auditoría, como por ejemplo, lanzar la ejecución de un programa, establecer una conversación mediante mensajes o incluso, copiar archivos en el equipo remoto. Estas operaciones son inviables cuando se opta por la instalación de un único Aida32 como se propuso en el primer artículo.

Con un servidor en cada equipo (auditados y auditores) se consigue otro beneficio: la utilización más eficiente de la red. Al lanzarse la generación del informe desde un equipo central auditor, se decide el número de equipos que se quieren auditar. Si la red está muy cargada, se puede decidir generar un número de informes que no supongan mucho flujo de información. Por contra, si se hace la auditoría en una hora en que haya poco tráfico de red, es posible lanzar la generación de los informes de forma masiva. Sin embargo, si solo tuviéramos un servidor remoto como se proponía en el primer artículo, la generación de los informes hay que programarla de forma muy cuidadosa, tratando de evitar que coincidan muchos en un momento dado ya que eso podría suponer una sobrecarga de la red y el consecuente malestar de los usuarios que la necesitasen para llevar a cabo su trabajo.

Hasta ahora todo parece que son ventajas, pero no es así. Tener un servidor por equipo supone ser vulnerable. Téngase en cuenta que un equipo auditado potencialmente es un equipo auditor ya que tiene instalado el Aida32. Para reducir al máximo este riesgo, es importante seguir cada uno de los pasos propuestos en apartados anteriores, destacando especialmente las opciones /**hiddenserver** /**silent** /**safe**, que evitan que se puedan lanzar dos instancias de Aida32. También es importante que la carpeta donde está Aida32 esté lo más oculta posible para que no sea visible por cualquier usuario. Aun tomando todas estas precauciones, esta forma de auditar es más insegura que la propuesta en el primer artículo.

Otro inconveniente es que la forma de auditar aquí propuesta exige que los equipos estén en red durante todo el proceso de monitorización y/o auditoría. En la otra forma, se pueden

generar los informes cuando se sepa que hay conexión ya que este era un proceso casi manual.

Como conclusión queda decir que una forma no es mejor que la otra. Ambas tienen sus ventajas e inconvenientes. La mejor opción es aquella que tenga en cuenta qué es lo que necesita cada organización. Si sólo interesa auditar sin importar que la información esté actualizada en todo momento es más recomendable la opción de un único servidor remoto. Por el contrario, si interesa tener la mayor información posible de los equipos de la red y que pueda ser obtenida en todo momento, la forma que interesa es la propuesta en este artículo.

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.