Implantación de una plataforma de administración de sistemas en red integrado

Autor: Antonio Picazo Veloso
Tutor: Tomás de Miguel

Índice

1. Introducción

La década de los 80 y primeros años de los 90 ha sido una época de informatización masiva. La mayoría de las empresas tanto públicas como privadas se han estado preocupando de dotarse de la infraestructura necesaria para afrontar esta nueva era tecnológica. Las empresas invertían en servidores, PCs y en software que hacía el trabajo más fácil y efectivo. Además se han ido instalando redes para optimizar la comunicación tanto dentro de la empresa como con el exterior. A principios de los 90 llegó internet y se empezó a complicar aún más el parque tecnológico de las empresas.

Actualmente se sigue invirtiendo dinero en dispositivos que actualizan y aumentan el la infraestructura tecnológica, pero las empresas están empezando a preocuparse más por la gestión de esta gran masa de dispositivos, invirtiendo en herramientas que aseguren la disponibilidad y el óptimo rendimiento de todos estos equipos y aplicaciones.

Debido a este crecimiento del parque informático y la necesidad de mantenerlo siempre a un nivel óptimo de rendimiento, muchas empresas cuentan o con un departamento de Tecnologías de Información (TI) o cada vez son más, las que optan por subcontratarlo (outsourcing).

En este entorno las tareas administrativas cada vez son más complicadas, las redes son más complejas y están formadas por sistemas heterogéneos. Para facilitar este trabajo surgen productos de software de diversos fabricantes como IBM, Hewlett-Packard, Computer Associates, destinados a ayudar a los administradores de TI.

La principal diferencia que existe entre los productos de los diferentes fabricantes es la arquitectura que presentan: modular o solución global. La arquitectura modular (*Building Blocks)* se compone de un conjunto de módulos especializados en diferentes áreas de gestión y donde cada uno puede funcionar independientemente o integrado con el resto. Dentro de este tipo de arquitectura se enmarca la solución *Openview* de *Hewlett-Packard*. Las herramientas que presentan una solución global (arquitectura *FrameWorks*) tienen una interfaz única pero sus componentes no pueden funcionar independientemente. Este tipo de arquitectura es la seguida por la solución *CA-Unicenter* de *Computer Associates* y *Tivoli* de *IBM*.

2. Objetivos

Este proyecto consiste en la definición e implantación de una plataforma de gestión integrada y centralizada a través de la cual se pueda administrar la red que se supervisa desde el centro de cálculo de la Escuela Técnica Superior de Ingenieros de Telecomunicación.

La red está compuesta por sistemas heterogéneos que van desde equipos Unix con Solaris, HP-UX, Red-Hat 5.2 o Irix hasta equipos con Windows NT. Este proyecto tiene una primera fase donde se va a centrar en la gestión de sistemas y aplicaciones y una segunda fase en la que abordará la gestión desde un punto de vista de servicios.

Con la monitorización de sistemas se pretende obtener información que pueda comprometer la disponibilidad de los nodos gestionados. Con esta funcionalidad se podrá vigilar la carga de CPU, el uso de sistemas de ficheros, el uso de la RAM, el estado de procesos vitales... Asimismo también se supervisarán ficheros importantes de log de los que se extraerá información como: mensajes de error de los sistemas operativos, conexiones fallidas, cambios de configuración...

En la gestión de aplicaciones se tendrá que supervisar el estado de los procesos que las mantienen activas y habrá que vigilar los ficheros de log que generen. Una gestión más ambiciosa y potente podría consistir en el envío directo de mensajes al Centro de Gestión desde las propias aplicaciones.

La implantación de esta plataforma se basa en la herramienta de gestión *Openview IT/Operations* de *Hewlett-Packard*.

El alcance de este proyecto no pretende llegar a gestionar el parque de PCs pero gracias a la arquitectura modular de la herramienta se podrá en un futuro integrar con otros productos de la familia *Openview* como *DTA*, especializados en entornos de PCs.

3. Arquitectura de la plataforma de gestión

La plataforma de gestión proporciona un sistema centralizado para presentar y resolver todas las incidencias que ocurran en el entorno de computación, independientemente de que se origen en sistemas, bases de datos o aplicaciones. Se reduce tanto la complejidad de gestionar un entorno distribuido como el tiempo necesario para la resolución de problemas.

La consola de gestión *HP Openview IT/Operations* proporciona un proceso de gestión de problemas consistente, permitiendo a los operadores el uso de técnicas comunes de gestión para todos los objetos gestionados, con lo que se consigue que los operadores se concentres en lo que gestionan, dejando la tarea de cómo hacerlo a la plataforma de gestión.

La plataforma de gestión presenta una arquitectura distribuida cliente/servidor. En el servidor de gestión reside la parte de software encargada de recibir y presentar a los operadores las incidencias que se han producido en el entorno de computación. La parte cliente está constituida por los agentes inteligentes instalados en los nodos gestionados. Estos agentes son autónomos y se dedican a la recolección de eventos y de la notificación al servidor cuando se superen los umbrales definidos. La característica autónoma de los agentes les permite tomar acciones para resolver las incidencias sin necesidad de tener comunicación con el servidor.

La comunicación gestor/agente se realiza mediante *RPC* (Remote Procedure Call). Con la utilización de *RPC* se garantiza que el sistema gestor va a recibir todos los eventos que detecten los agentes sin perder ningún dato a diferencia de *SNMP* que no puede hacerlo. Además mediante el empleo de *DCE* se garantiza una comunicación segura entre agente y servidor

En el proceso de gestión se pueden distinguir cuatro pasos clave: recolección, procesamiento, presentación y acción del operador.

Recolección

Se recogen tantos eventos cómo sea posible de fuentes variadas y distintas en el entorno de computación gestionado. Los eventos son las informaciones que se extraen de los componentes que son objeto de gestión, como por ejemplo, tiempos de utilización de CPU, utilización de discos…

El comportamiento de los agentes viene definido por las plantillas que les son distribuidas desde el servidor de gestor. Estas plantillas contienen toda la información de lo que debe supervisar el agente y de cómo debe hacerlo. La información más relevante que se introduce en la creación de estas plantillas es: la fuente de información, el periodo de supervisión, los umbrales, las acciones automáticas que se van a ejecutar ante la superación de umbrales y las acciones que puede iniciar el operador.

Las fuentes de información a través de las cuales se va a supervisar la disponibilidad y rendimiento de los sistemas y aplicaciones son básicamente tres: ficheros de *log*, programas (scripts) y una interfaz a través de la cual se pueden enviar mensajes al servidor de gestión.

Mediante la vigilancia de los ficheros de *log* se puede supervisar cualquier aplicación que escriba mensajes en estos ficheros. *IT/O* asume que estos ficheros contienen un mensaje por cada línea, pero se puede configurar para ejecutar un programa que prepare los ficheros para que puedan ser leídos. Estos programas de preprocesamiento pueden ser externos a *IT/O* y tienen como función el crear ficheros de texto que tengan por cada línea un mensaje. En las plantillas de este tipo se pueden definir múltiples condiciones que intenten casar diferentes cadenas de caracteres con el fichero objeto de la supervisión y en caso de ocurrir hacer que el agente envíe mensajes con las severidades pertinentes.

Los programas que se ejecutan periódicamente, que los denominaremos a partir de ahora monitores, pueden estar desarrollados en cualquier lenguaje de programación. El único requisito que deben cumplir es que antes de finalizar su ejecución deben hacer una llamada al comando *opcmon* para avisar al agente del resultado del monitor. El agente comparará este valor con los umbrales que tenga definidos y avisará al gestor si es pertinente. Con esta funcionalidad se pueden supervisar partes del sistema como procesos vitales, tamaños de ficheros, sistemas de ficheros, en definitiva, todo lo que el sistema operativo nos permita.

La interfaz que incorpora *IT/O* es un comando que ordena al agente enviar mensajes al servidor gestor. Este comando tiene argumentos como: la severidad, la aplicación que lo origina, el objeto, el texto del mensaje y el grupo de mensajes al que pertenece. La utilidad principal de esta interfaz es la de poder gestionar cualquier aplicación desarrollada a medida. Si combinamos el uso de esta interfaz con el uso de monitores hacemos que la gestión sea mucho más flexible. De esta manera podemos crear ficheros de configuración que contengan umbrales diferentes para cada nodo que queramos gestionar y a través de un monitor creado genéricamente para cualquier nodo comparar los resultados con los umbrales de estos ficheros.

IT/O permite además recibir traps SNMP provenientes de los sistemas y dispositivos de comunicaciones del entorno que estamos gestionando.

Procesamiento

Los eventos pasan por un procesamiento que comprende las siguientes fases:

- Filtrado y registro. En las plantillas se define un conjunto de condiciones que se compara con la información de los eventos, separando así los eventos relevantes de los que no lo son. Estas condiciones son una cadena de caracteres o un valor. Las cadenas de caracteres definen el patrón que hay que buscar en un fichero de log o el formato del mensaje enviado a través del comando *opcmsg*. Los valores definen los umbrales que se comparan con los resultados que devuelven los monitores.

- Conversión en mensajes. Los eventos que han pasado el filtrado se convierten en mensajes para ser enviados al servidor de gestión. En esta conversión se les asigna una prioridad para indicar su importancia y una categoría para poder tener agrupados los mensajes del mismo tipo. Así por ejemplo se pueden definir grupos como: Backup, Rendimiento, Seguridad… Como es lógico estas asignaciones vendrán definidas en las plantillas.

Los mensajes que se envían al servidor pueden tener una acción automática correctiva asociada. En este caso el agente ejecuta dicha acción independientemente del servidor de gestión.

Presentación

Los mensajes enviados al servidor de gestión se presentan de forma gráfica al operador. El operador tiene un conjunto de responsabilidades que le han sido asignadas por el administrador. Las responsabilidades no son más que un conjunto de categorías de mensajes. Así por ejemplo a los operadores de copias de seguridad se les asignará el la categoría de mensajes de Backup.

Cada operador tiene tres ventanas donde ve reflejado la llegada de los mensajes. En una ventana tiene las categorías de los mensajes que le han sido asignadas donde los iconos que las representan van cambiando de color según la prioridad del mensaje. En una segunda ventana tiene los nodos de los que es responsable que van cambiando de color según la prioridad del mensaje. La tercera ventana es una consola donde se representa el mensaje textual con la siguiente información:

- Objeto gestionado, categoría del mensaje, aplicación causante, texto original y texto procesado.
- Información sobre las acciones disponibles y sus anotaciones. Da una información del éxito o no de la ejecución de las acciones. Además en las anotaciones se visualiza el resultado de las acciones ejecutadas.
- Instrucciones específicas del mensaje. En las plantillas se pueden escribir las instrucciones que ha de seguir el operador para que cuando le llegue el mensaje le sirvan de ayuda para resolver el problema.

Los mensajes también se pueden escalar a otros servidores de gestión o se puede una vez recibidos reenviar automáticamente a: sistemas de notificación de incidencias (Trouble Ticket) y servicios de notificación externa como envío de correo electrónico, envió de mensajes cortos a móviles…

Actuación

Finalmente se intentarán resolver las condiciones críticas detectadas antes de que afecten a los usuarios finales.

Como se ha descrito anteriormente si el mensaje tiene asociado una acción automática, ésta se ejecutará sin la intervención de ningún operador. El resultado de esta acción y si ha sido exitosa o no la podrá ver el operador en su consola.

Si con las acciones automáticas no se resuelva la situación entonces el operador cuenta por una parte con acciones asociadas al mensaje y con un conjunto de aplicaciones que le han sido asignadas. El operador tiene una ventana con un conjunto de aplicaciones que le ha concedido el administrador. Estas aplicaciones pueden ser de cualquier tipo, desde scripts hasta aplicaciones gráficas.

Por último hay que destacar un componente muy importante de la plataforma de gestión, el repositorio central. Este repositorio basado en una base de datos Oracle sirve de almacenamiento de:

- Los datos de configuración del entorno de gestión de problemas y operaciones para un dominio de gestión (perfiles de operadores, umbrales, patrones de comparación para filtrado de eventos…)
- La topología de la red que forma el entorno gestionado Openview
- Los datos que identifican a cada objeto gestionado (nombre, direcciones IP, fabricante…)
- El registro de todos los eventos que ha recibido el sistema gestor, tanto históricos como actuales
- El registro de cómo se han resuelto los problemas, resultado de las acciones automáticas y anotaciones realizadas por los operadores

Con toda esta información se pueden usar herramientas proporcionadas por las bases de datos u otras aplicaciones para la generación de informes de cualquier tipo.

4. Diseño de la plataforma de gestión

En este apartado se va a describir cómo se va a realizar la gestión de sistemas y aplicaciones. Debido a que la red está formado por sistemas Unix y NT se va a definir de diferente manera la gestión de ambos tipos de sistemas.

La gestión de sistemas se abordará desde dos puntos de vista:

- Gestión de problemas que se encargará de detectar todas las incidencias producidas en el sistema que comprometan la disponibilidad del mismo.
- Gestión de rendimiento que recogerá el estado del sistema para poder hacer análisis de previsión de problemas.

4.1. Definición de la Gestión de Sistemas Unix

Gestión de problemas

La gestión de problemas en sistemas Unix se basará en la lectura de los ficheros de log y los monitores se desarrollarán en shell scripts.

Abordaremos los principales problemas de disponibilidad que vamos a controlar en nuestro entorno de sistemas Unix.

Carga de la CPU

La disponibilidad de la CPU es un parámetro básico que hay que supervisar. Evitar que la CPU alcance durante determinado tiempo una carga excesiva repercute directamente en el resto de parámetros del sistema que queramos vigilar. Se definirán dos umbrales que ante su superación se informará al operador correspondiente. Estos umbrales serán:

- 85% durante 5 minutos. La superación de este umbral originará el envío de un mensaje con una severidad *Warning*.
- 90% durante 5 minutos. La superación de este umbral supone que el sistema está en una situación crítica y por ello la severidad del mensaje será la de mayor categoría *Critical*.

El mensaje que le llegará al operador tendrá asociado unas anotaciones en las que se visualizará la salida del comando *top* de tal manera que pueda ver los procesos que más están consumiendo la CPU.

Los mensajes generados serán asignados al grupo de mensajes Rendimiento configurado en el entorno de operación.

Uso de los sistemas de ficheros

La vigilancia de los sistemas de ficheros es también muy importante porque cuando se llenan los sistemas de ficheros pueden provocar que las aplicaciones, o no puedan arrancar o que dejen de funcionar por no tener suficiente espacio en disco. Normalmente los sistemas de ficheros se pueden llenar por acumulación de ficheros temporales, de cores o porque no les hayamos asignado suficiente espacio. Con esta vigilancia se pretende avisar al operador para que actúe pertinentemente. En caso de no haber disco suficiente nos es muy útil para poder incorporar discos adicionales antes de que se llene completamente el sistema de ficheros.

Esta supervisión se va a hacer con un monitor que nos vaya comparando el tanto por ciento de uso de cada uno de los sistemas de ficheros que tenga el nodo con los siguientes umbrales:

- 75%. La superación de este umbral enviará una alarma de baja severidad si no hay espacio libre en disco que se le pudiera asignar al sistema de ficheros en un futuro. Con este aviso se pretende que el operador empiece a valorar la posibilidad de tener que añadir discos al sistema. En la ventana de anotaciones se visualizará el uso de cada uno de los sistemas de ficheros con el comando *bdf* o alguno similar según que sistema Unix sea. También vamos a adjuntar los ficheros core que encuentre en este sistema de ficheros.
- 80%. Este umbral ya supone el envío de un mensaje más crítico. Además de adjuntar lo mismos que en el mensaje del 70%, vamos a incluir el espacio libre sin asignar que hay en el sistema. Este mensaje tendrá un acción que podrá iniciar el operador que consistirá en borrar los ficheros temporales y de core que se encuentren en este sistema de ficheros. En la ventana de instrucciones asociada a este mensaje vamos a poner los pasos a seguir para aumentar el espacio del sistema de ficheros.
- 90%. El alcance de este umbral indica que estamos en una situación crítica. Incluiremos lo mismo que en el caso anterior.

Los mensajes serán asignados al grupo de mensajes de Sistema Operativo configurado en el entorno de operación.

Uso de la RAM

La vigilancia del uso de la RAM también es de suma importancia porque nos va a prever situaciones en las que los usuarios pueden notar la lentitud de las aplicaciones. Vamos a definir dos umbrales:

- 85% durante 5 minutos. El mensaje enviado será de alerta y contendrá en la ventana de anotaciones además de la salida del comando *top* la información de *swap*. La información de *swap* la incluimos porque hay sistemas Unix que permiten reservar parte de la memoria RAM al *swap*.
- 90% durante 5 minutos. Este mensaje será de mayor severidad e incluirá lo mismo que en el caso anterior.

Los mensajes serán asignados al grupo de mensajes de Rendimiento configurado en el entorno de operación.

Uso del espacio de SWAP

En la supervisión de del uso de espacio de *swap* definiremos también dos umbrales:

- 90% durante 5 minutos. El mensaje enviado será de alerta y contendrá en la ventana de anotaciones la información de swap.
- 95% durante 5 minutos. Este mensaje tendrá una severidad mayor y en su ventana de anotaciones se incluirá lo mismo que en el caso anterior.

Los mensajes serán asignados al grupo de mensajes de Rendimiento configurado en el entorno de operación.

Estado de procesos vitales

Los procesos que vamos a vigilar estarán enumerados en un fichero de configuración que tendrá cada nodo. El monitor encargado de esta supervisión detectará la caída de alguno de estos procesos y definiremos según el proceso, si decidimos arrancarlo automáticamente o si esperamos a la orden del operador. En ambos casos llegará al servidor un mensaje de severidad que dependerá del proceso caído. En caso de que el arranque automático no funcionase el operador también estaría informado y podrá ver en la ventana de anotaciones la salida del programa que ha intentado arrancarlo.

Estado del cron

El *cron* es una aplicación Unix encargada de la ejecución periódica de tareas. Por lo tanto es muy importante conocer si no están ocurriendo errores. Para ello vamos a leer periódicamente el fichero de *log* del *cron*. En caso de que haya habido algún error se enviará un mensaje al servidor. Asimismo definiremos el *cron* como un proceso vital que será vigilado por el monitor anterior.

Servicio DNS

Los servidores que resuelven los nombres de dominio deben estar funcionando correctamente porque si no muchas de las conexiones resultarán fallidas. El estado de este servicio lo vamos a controlar a través de las entradas producidas en el fichero *syslog.log*. En caso de que se detecte algún error se notificará al servidor gestor. Si es un error de los ficheros de configuración se incluirá en la ventana de anotaciones dichos ficheros.

Servicio FTP

El estado del servicio FTP estará vigilado a través del monitor de procesos vitales. También es importante vigilar el aspecto de seguridad. Para ello vamos a detectar los accesos fallidos y los accesos con el usuario *root* a través de la lectura del fichero de *log syslog.log*.

Ficheros de crecimiento ilimitado

Vamos a vigilar ficheros de *log* que crecen ilimitadamente. En cada nodo definiremos un fichero de configuración, estableciendo cuales son los ficheros y sus respectivos tamaños máximos. La acción automática que vamos a establecer va a consistir en copiar el fichero con extensión *.old* y en vaciar el fichero. Así tendremos una copia por si se quiere analizar su contenido.

Conexiones fallidas

El servidor gestor va a recibir mensajes cada vez que en cada uno de los nodos haya una conexión fallida por fallos en la autenticación de usuarios. Esta supervisión de seguridad se va a realizar a través de la lectura periódica de los ficheros de *log btmp* y *sulog*. También consideramos importante recibir un mensaje cada vez que el usuario *root* acceda al nodo.

Ficheros Críticos

Vamos a vigilar cuándo y qué usuario hace cambios en ficheros que consideremos críticos. En cada nodo tendremos un fichero de configuración donde tengamos los ficheros objeto de esta vigilancia. En cuanto se produzca algún cambio de fecha, tamaño, permisos y/o dueño en estos ficheros se recibirá un mensaje que tendrá asociada una acción que permitirá al operador restaurar el fichero.

Para la resolución de problemas los operadores cuentan con un conjunto de aplicaciones. Asimismo desde la herramienta se podrán conectar remotamente al sistema afectado a través de *telnet* o de conexiones seguras y corregir así los problemas que hayan ocurrido.

Gestión del rendimiento

La gestión de rendimiento pretende recoger información del estado del sistema y almacenarlo en forma histórica. Esta información será fundamental para llevar a cabo medidas preventivas. Esta gestión se realizará a través del agente de *MeasureWare* que se integra con *IT/O* enviando mensajes al servidor gestor ante la superación de umbrales definidos. Este agente MeasureWare también se utilizará en sistemas NT.

Los parámetros del sistema que vamos a estudiar coinciden en gran parte con los considerados en la gestión de disponibilidad, pero en este caso obtendremos un análisis más profundo. En este tipo de gestión sacaremos la evolución de estos parámetros a lo largo de un determinado de tiempo y podremos representar gráficas que nos indiquen esta evolución. Estas gráficas las podemos asociar a los mensajes que nos lleguen por la superación de los umbrales definidos. Principalmente extraeremos información de:

- CPU. Promedio de carga, porcentaje de tiempo de inactividad, consumo del modo usuario y sistema, longitud media de la cola…
- Memoria. Número de fallos de página por segundo, número de lecturas y escrituras por segundo del disco a la caché, número de páginas libres..
- Sistemas de ficheros. Espacio libre en el sistema de ficheros, tanto por ciento de ocupación, inodos libres…
- Discos. Número de peticiones de I/O a disco por segundo, de I/O en cola, de r/w, tiempo de respuesta medio…
- Procesos. Número de procesos activos, a la espera de recursos, zombies.

Los mensajes serán asignados al grupo de mensajes de Rendimiento configurado en el entorno de operación.

El almacenamiento de los datos históricos que se van recolectando se realizará en el propio agente del nodo gestionado. La explotación de estos datos históricos se hará de forma cíclica, es decir, se irán borrando los datos más antiguos para insertar los más modernos. Definiremos un período cíclico de un mes.

4.2. Definición de la gestión de los sistemas NT

La gestión de problemas de los sistemas NT se basará principalmente en la información que se pueda obtener de los ficheros de *log* y del *Performance Monitor* del sistema operativo. Los ficheros de *log* que nos ofrece NT son tres: el de sistema, el de aplicaciones y el de seguridad.

Los monitores que vamos a desarrollar se harán con *Visual Basic Script*, lenguaje de programación sencillo y muy útil para la gestión de sistemas.

La gestión de rendimiento es exactamente igual que en los sistemas Unix puesto que se utilizará el agente de MeasureWare.

Gestión de problemas

Los problemas de disponibilidad que se van a gestionar serán los mismos prácticamente que en Unix. Muchos de los parámetros de disponibilidad se obtendrán del Performance Monitor. Esta herramienta de NT está estructurada en objetos, donde cada uno tiene un conjunto de contadores y donde cada contador tiene un conjunto de instancias. Los objetos son elementos del sistema como Procesador, Memoria, Disco.., los contadores son las características de los objetos y las instancia son el número de objeto de ese tipo en el caso que haya varios.

Vigilancia de la CPU

Se definen los mismos umbrales que en los sistemas Unix. La información se obtiene del objeto del Performance Monitor *Procesador*. El contador que se vigila es el *%de tiempo de Procesador*. Los mensajes se asignan al grupo Rendimiento.

Vigilancia de la RAM

Se definen los mismos umbrales que en los sistemas Unix. El objeto que se monitoriza es *Memoria* y el contador *Bytes disponibles*. Los mensajes también están asignados al grupo Rendimiento.

Vigilancia del fichero Pagefile

En los sistemas NT es muy importante saber el tanto pociento de uso del fichero de paginación *pagefile.sys*. Se definen dos umbrales:

- 85% durante 5 minutos. Mensaje de alerta.
- 90% durante 5 minutos. Mensaje crítico.

Los mensajes están asignados al grupo Sistema Operativo.

Vigilancia de procesos vitales

El monitor encargado de la vigilancia de procesos vitales, estará supervisando el estado de los servicios NT y enviará un mensaje con una severidad que dependerá del servicio caído.

Los servicios que se vigilan son:

- Servicio de publicación FTP
- Servicio de publicación WWW
- Servidor de acceso remoto (RAS)
- Servidor DNS de Microsoft
- Servidor DHCP de Microsoft

Los mensajes están asignados al grupo Sistema Operativo. Estos mensajes tienen asociado una acción automática que intentará volver a arrancar el servicio caído.

Vigilancia de discos locales

El monitor se encarga de supervisar el tanto por ciento de uso de todos los discos lógicos locales que disponga el sistema. Al igual que en los sistemas Unix se definen los mismos umbrales.

Los mensajes están asignados al grupo Sistema Operativo. Además estos mensajes tienen asociados una acción automática que mostrará al operador el contenido de las carpetas temporales.

Vigilancia de Seguridad del sistema

En los sistemas NT que se quiera realizar una vigilancia de seguridad se activará la auditoría de inicio y cierre de sesión. De esta manera cuando algún usuario se conecte se escribirá en el fichero de log de Seguridad de NT. El agente enviará un mensaje de alerta cuando haya dos intentos fallidos de conexión. Igualmente se enviará un mensaje de severidad normal cuando se conecte el administrador.

Vigilancia de Sesiones abiertas

Según las características del sistema NT se definirán dos umbrales. Esta supervisión se realiza a través del contador *Sesiones del servidor* del objeto *Servidor*.

Los mensajes están asociados al grupo Sistema Operativo.

La mayor limitación de los sistemas NT es que su administración remota para corregir los problemas que surgen no es posible debido a que no cuenta con servicios remotos como *telnet* que nos permita conectarnos.