

ApplicationsAgent

VISUAL Message Center Applications Agent

User Guide

1. Contenido

1. Contenido	2
2. Visión General	3
3. ¿Cómo funciona Applications Agent?	4
4. ¿Qué es un Archivo Log?	5
5. Propiedades del Monitor de Archivos Log	6
6. Diálogos del Editor de Inclusión/Exclusión	8
7. Editor de Campos	9
8. Propiedades del Monitor de Archivos de Sistema	11
9. Visión General de la Consola	13
10. Agentes, Monitores, Objetos y Eventos	14
10.1 Perfiles del Agente	15
11. Carpetas	16
12. Funcionamiento de la Consola de Applications Agent	17
13. Menú Principal	18
14. Diálogo de Opciones	20
15. Diálogo de Selección del tipo de Monitor	21
16. Apéndice: Ejemplos de creación de monitores personalizados	22
16.1 Visión General de los Monitores Personalizados	22
16.2 Monitorizando Disponibilidad del Servidor	23
16.3 Monitorizando Puertos TCP Abiertos	27
16.4 Monitorizando Procesos Windows	32
16.5 Monitorizando Servicios Windows.....	37
16.6 Monitorizando Usuarios Inactivos	40
17. Recursos en la Web	46
18. Acerca de Tango/04 Computing Group	47
19. Aviso legal	48

2. Visión General

Applications Agent es un procesador de archivos de texto en tiempo real. La mayoría de aplicaciones de procesamiento de archivos de texto trabajan off-line, una vez la aplicación ha producido el archivo, y generan reportes o algún otro tipo de salida basada en los contenidos del archivo.

Applications Agent procesa archivos mientras estos están siendo rellenos con datos. Esto hace que la información del archivo esté disponible en tiempo real, permitiéndole controlar y monitorizar esta información.

Puede parecer que esta información únicamente es útil si usted dispone de una aplicación que explícitamente genera archivos de textos o de log (como un web server, un servidor de base de datos...), pero, como verá en el apartado Monitores Personalizados, esto no es completamente cierto: Sí, Applications Agent es muy útil si tiene una de estas aplicaciones, pero, también puede ayudarle a controlar prácticamente cualquier aspecto de su sistema.

Existen muchas herramientas de línea de mandatos para administración de sistemas que producen una salida de texto, esta salida puede ser fácilmente volcada a un archivo, y Applications Agent puede monitorizar ese archivo. O usted puede escribir su propia herramienta que vuelque la información que necesita a un archivo, y monitorizarlo con Applications Agent.

Applications Agent puede procesar cualquier tipo de archivo de texto, por favor diríjase al apartado "Cómo funciona Applications Agent" para información más detallada.

Las principales funcionalidades de Applications Agent se resumen a continuación:

- Integración con VISUAL Message Center, a través del Event Log de Windows.
- Procesamiento en tiempo real de archivos de texto locales.
- Procesamiento a intervalos fijos de archivos de texto remotos.
- Avanzado motor de filtrado de textos basado en expresiones habituales.
- Avanzado procesamiento de archivos de formato log con campos de ancho fijo y campos delimitados.
- Formatos de archivos predefinidos para aplicaciones comunes (ISA, Apache, SQL Server,...)
- Reconocimiento automático de campos de tipo Boleano, Entero, Real, Fecha, Hora, Fecha/Hora y cadenas de texto.
- Lenguaje de procesamiento de scripts potente pero sencillo.
- Diseño Multi-threaded para altas cargas de proceso.
- Incluye funcionalidades de monitorización de archivos de simples de sistema.

3. ¿Cómo funciona Applications Agent?

Antes que nada, una aclaración, cada una de las líneas de texto contenidas en un archivo de texto se denomina una **Entrada**.

Application Agent puede procesar cualquier tipo de archivo de texto, pero está ajustado específicamente para archivos de log.

- Si el archivo que desea monitorizar es un archivo de texto plano (lo que significa, que no todas las entradas siguen la misma estructura o patrón), deberá realizar algún tipo de proceso para buscar la información que necesita de la entrada, pero
- Si el archivo que desea monitorizar es un archivo de log, Applications Agent hará la mayor parte del trabajo por usted, extrayendo los diferentes campos de información de la entrada.

Básicamente, Applications Agent no hace nada hasta que cambia el archivo monitorizado. Cuando se detecta un cambio, realiza los siguientes pasos o acciones:

1. **Lectura de la Entrada:** Lee la siguiente entrada no procesada del archivo.
2. **Filtrado de la Entrada:** Acepta o descarta un procesamiento de la entrada dependiendo de ciertos criterios definidos por el usuario.
3. **Extracción de los Campos de la Entrada:** Si el archivo no tiene un formato fijo, o lo que es lo mismo, no es un archivo de log, salta al paso 4, pero si el usuario ha definido un formato de campos de entrada, extrae los diferentes campos de información de la entrada.
4. **Procesamiento de la Entrada:** Ejecuta un script de procesamiento de la entrada, permitiendo extraer, manipular y notificar la información de la entrada.
5. Si existe más entradas no procesadas, salta al paso 1. Si no se mantiene parado hasta que se detecta un nuevo cambio.

Como descubrirá al leer el apartado Monitores Personalizados, este sencillo mecanismo es muy potente, permitiendo una gran variedad de tareas de monitorización.

4. ¿Qué es un Archivo Log?

Existe mucha confusión entre archivos log, archivos trace, archivos de volcado y otros archivos generados por aplicaciones. Todos estos archivos suelen ser archivos basados en texto, pero tienen diferentes propósitos:

- **Archivos Log** Anotan información durante el tiempo de ejecución de la aplicación, con la intención de procesamiento estático tras la ejecución o análisis. Son muy útiles para propósitos de reporte y análisis de uso de la aplicación.
- **Archivos de Volcado** Anotan el estado de la aplicación cuando se detecta un error. Son muy útiles para desarrolladores, ayudándoles a reproducir y solucionar comportamientos anormales.
- **Archivos Trace** Anotan secuencias de acciones o procesos realizados por la aplicación. Son muy útiles para desarrolladores y analistas para localizar y solucionar situaciones anormales de proceso, problemas de rendimiento, errores en la lógica de la aplicación,...

A pesar del propósito de cada uno de estos tipos de archivo, la principal característica de un archivo de log, es el formato del archivo. Applications Agent puede procesar archivos log que:

- Estén realizados con líneas imprimibles de caracteres ASCII.
- Cada línea finaliza por un retorno de carro y/o un carácter de alimentación de línea.
- Cada línea tiene el mismo formato, el mismo tipo de bloques de información.

Lo que esto significa, básicamente, es que el archivo log debe ser similar a una tabla de base de datos o una hoja de cálculo para que Applications Agent sea capaz de extraer los campos de información contenidos en cada entrada, o lo que es lo mismo, los datos deben estar organizados en líneas y columnas:

- Cada línea define una única entrada.
- Cada línea tiene el mismo número de campos (columnas) en el mismo orden.

La mayoría de archivos de log de las aplicaciones cumplen estos requerimientos, ya que el propósito de un archivo log es proporcionar información detallada en un formato que permita un posterior reporte/análisis utilizando aplicaciones Standard de base de datos o hojas de cálculo.

Además, muchas herramientas de línea de mandatos generan un archivo log como salida, por lo que es muy fácil crear un monitor personalizado utilizando un script, y procesar las salidas de la herramienta de línea de mandatos con Applications Agent.

5. Propiedades del Monitor de Archivos Log

Las diferentes propiedades que definen un Monitor de Archivos log se agrupan de la siguiente forma:

- **Archivo Log Monitorizado:** Las propiedades que identifican que archivo o conjunto de archivos desea monitorizar. Estas propiedades son:
 - **Files:** El path a los archivos que desea monitorizar. Puede utilizar genéricos (*, ?) para indicar un conjunto de archivos, lo que significa, que se va a monitorizar más de un archivo.
 - **Update Policy:** Esta es una propiedad importante.. Indica al monitor como añade información al archivo la aplicación que genera el archivo monitorizado:
 - **Overwrite:** Se crea un archivo nuevo cada vez. La información generada por la aplicación no se añade al archivo, sino que se almacena en memoria, y una vez la información ha sido recogida se vuelca al archivo. El archivo se sobrescribe o se reemplaza cada vez.
 - **Update:** La aplicación genera información tal y como se ejecuta y añade esa información al archivo inmediata o periódicamente, con lo cual el archivo se actualiza con nueva información, pero el archivo no se reemplaza. El archivo crece en tamaño hasta que se alcanza algún criterio límite (un cierto tamaño, una archivo por día, un archivo por mes,...) y entonces, se cierra ese archivo y se crea uno nuevo. El archivo antiguo, a veces es movido a una localización o directorio diferente: puede especificarlo en el cuadro de diálogo Terminated Files.
 - **Monitored Entries:** Las Entradas que van a ser procesadas. Son os campos que va a ser extraídos (cuando se define) y el script de procesamiento de eventos que se va a ejecutar en esas entradas. Puede escoger entre los siguientes valores:
 - **All Entries:** se procesarán todas las entradas.
 - **Only Some Entries:** Únicamente se procesarán las entradas especificadas. Pulse el botón Entries para especificar los criterios para que una entrada sea incluida en su selección.
 - **All Entries Except:** Todas las entradas excepto las que se especifiquen serán procesadas. Pulse el botón Entries para especificar los criterios para que una entrada sea excluida de su selección.
 - **Entry Format:** El número y tipo (Booleano, Entero, Real, Fecha, Hora, Fecha/Hora, cadena de texto) de los campos contenidos en cada entrada. Puede seleccionar entre los siguientes valores:
 - **No Format:** Cada entrada será considerada como texto en bruto, es decir, un único campo de tipo cadena de texto.
 - **Delimited Fields:** Los campos contenidos en cada entrada están delimitados por uno o más caracteres especiales (como tabulador, comas, punto y coma,...). Pulse el campo Fields para especificar los delimitadores y para dar un nombre a cada campo.
 - **Fixed Width Fields:** Los campos contenidos en cada entrada tienen un ancho delimitado, y no disponen de ningún delimitador de campos Pulse el campo Fields para especificar el ancho de cada campo y para dar un nombre a cada campo.

- **Monitoring Settings:** Estas propiedades le permiten definir como van a ser monitorizados esos archivos.
 - **Polling Interval:** El intervalo (en segundos) entre chequeos. Si los archivos monitorizados están situados en la misma máquina que Applications Agent, puede ajustar esta propiedad a 0. Esto significa que Applications Agent puede optimizar el proceso de chequeo, indicando al Sistema Operativo que levante el monitor cada vez que cambie el archivo, y que se relice el chequeo sólo cuando cambia el archivo. Si los archivos no son locales, Applications Agent debe chequear los archivos periódicamente, en intervalos tan amplios como se haya indicado en Polling Interval.
 - **Locked File Wait Time:** Aunque Applications Agent sólo requiere acceso de lectura a los archivos que está monitorizando, algunas aplicaciones pueden aplicar un bloqueo exclusivo mientras están escribiendo en el archivo. Esto implica que Applications Agent no puede leer el archivo hasta que la aplicación finalice la escritura. Con esta funcionalidad (Locked File Wait Time) puede especificar el periodo de espera del monitor para que la aplicación le permita el acceso al archivo. Una vez este tiempo ha expirado y no se ha concedido acceso, el monitor informará al operador de esta situación con un mensaje de error.
 - **Process from first entry:** Esta funcionalidad dice al monitor donde debe comenzar el procesamiento del archivo. Si esta propiedad está marcada, empezará desde la primera entrada. Si no, esperará hasta que se añada una nueva entrada al archivo y comenzará desde esta nueva entrada.
 - **Save processing state:** esta funcionalidad hace que el monitor guarde en disco su estado de procesamiento (los archivos que está procesando y la última entrada procesada). Gracias a ello, en caso de un fallo grave (Applications Agent finalice anormalmente, o el sistema operativo se cierre de manera inesperada), el estado de procesamiento puede ser recargado automáticamente y se continúa el procesamiento de los archivos desde la última entrada procesada, sin que se pierdan entradas sin procesar.
- **Event Processing Script:** Este es el script de procesamiento que se ejecutará con cada entrada. Esto le permitirá definir que hacer dependiendo de la entrada. En la parte derecha del campo de entrada dispone de tres botones:
 - Seleccionar un script ya existente.
 - Editar el script seleccionado.
 - Borrar el campo de entrada de script, lo que significa que no se utiliza ningún script.

6. Diálogos del Editor de Inclusión/Exclusión

Los diálogos de Inclusión/Exclusión le permiten definir una lista de criterios para incluir o excluir entradas. Únicamente las entradas incluidas serán procesadas, lo que implica que se extraerán los campos de la entrada, y el script de procesamiento de eventos se ejecutará en la entrada.

Cuando, en el diálogo de Propiedades del Monitor de Archivos Log, se selecciona **Only Some Entries**, se define una lista de inclusión. Sólo las entradas que cumplan cualquiera de los criterios de la lista será procesada.

Cuando, en el diálogo de Propiedades del Monitor de Archivos Log, se selecciona **All Entries Except** e define una lista de exclusión. Todas las entradas excepto las que cumplan cualquiera de los criterios de la lista será procesada.

Un **criterio** no es más que una condición del tipo "contiene la cadena". Por ejemplo, especificando "404" como criterio significa que si la entrada "contiene la cadena 404", el criterio se cumple. De hecho, los criterios que puede definir en el diálogo de Inclusión/Exclusión son más potentes que esto, ya que están basados en expresiones regulares. Las Expresiones Regulares le permiten especificar condiciones tan simples como la que se ha descrito anteriormente, pero también le permite definir condiciones con cadenas muy complejas.

Para definir un nuevo criterio, una nueva expresión regular, simplemente pulse el botón "**New**". Una vez introduzca la nueva expresión regular, las líneas seleccionadas con los criterios definidos se actualizarán en el panel de vista previa en la parte derecha de la pantalla: Las entradas que serán procesadas se muestran en negro, las entradas que serán filtradas (no-procesadas) se muestran en gris claro, con lo que puede verificar rápidamente que la expresión regular introducida coincide con el criterio deseado.

En la lista de expresiones regulares, también tiene dos columnas denominadas **Match** y **Case Sensitive**:

- **Match**: Marcando esta columna indicamos que el criterio se cumple si la entrada coincide con la expresión regular. Si esta columna no está marcada se cumple el criterio si la entrada **NO** coincide con la expresión regular.
- **Case Sensitive**: Marcando esta columna indicamos que la comparación tiene en cuenta las mayúsculas, por lo que los caracteres en mayúsculas se consideran diferentes que los caracteres en minúsculas ('A' <> 'a', 'B' <> 'b',...). Si esta columna no está marcada los caracteres en mayúsculas se consideran iguales a los caracteres en minúsculas ('A' = 'a', 'B' = 'b', ...).

7. Editor de Campos

El editor de campos le permite definir los campos contenidos en cada entrada de un archivo de log. En la parte derecha de la pantalla puede ver el panel de vista previa. Muestra el archivo de log tal y como quedaría si utilizase las actuales definiciones de campos. Se refresca automáticamente cuando edita las definiciones de los campos.

En la parte superior izquierda, puede ver una barra de herramientas con varios botones:

- **Load Format:** Si el archivo de log tienen un formato conocido, o uno que haya guardado anteriormente utilizando el botón **Save Format**, podrá reutilizar ese formato. Pulsando este botón se abre un diálogo desde el que podrá escoger uno de los formatos previamente guardados, y aplicarlo a este archivo de log.
- **Save Format:** Si tienes otros archivos de log que utilizan el mismo formato, no necesita definir el mismo formato de campos para cada uno de los archivos. Simplemente pulse este botón para guardar el actual formato de campos, y reutilizarlo cuando defina los campos para otros archivos.
- **Update Fields:** El diálogo del Editor de Campos actualiza automáticamente los campos cuando están siendo editados. Pero cuando intenta editar un campo en un formato ya definido, espera que se realice cualquier modificación antes de actualizar las definiciones del campo. Si desea actualizar el campo en el archivo abierto pulse este botón.

Bajo la barra de herramientas, hay varios campos de entrada disponibles para definir el formato del campo:

- **Sample Log File:** Un archivo, que coincide con el entrado en las propiedades del monitor de archivos de log, se proporciona por defecto. Si es necesario, se puede seleccionar un archivo diferente para definir el formato del archivo.
- **Header Lines:** Algunos archivos de log tienen líneas al principio del archivo, que realmente no contiene información útil, y no debería ser procesada. Simplemente son títulos, entradas que contienen información sobre el formato del archivo, como la fecha y hora en la que el archivo fue creado.
- **Date/Time Format:** Es una cadena que define cómo se representan los valores de fecha y hora en el archivo. La cadena puede estar compuesta por cualquier carácter, pero hay algunos caracteres especiales utilizados para indicar la localización de la fecha y hora en los datos de fecha/hora.

Y: se utiliza para indicar la parte año de una fecha.

M: se utiliza para indicar la parte mes de una fecha.

D: Se utiliza para indicar la parte día de una fecha.

h: se utiliza para indicar la parte hora de una hora.

m: se utiliza para indicar la parte minutos de una hora.

s: se utiliza para indicar la parte segundos de una hora.

d: se utiliza para indicar las centésimas de segundo de una hora.

Todos estos caracteres son opcionales (su archivo puede tener únicamente campos de fecha, o de hora,...), y en general, una indicación del carácter es suficiente para indicar la posición de la parte fecha/hora en el campo. Se asume que todos los campos son números enteros por defecto, pero algunos caracteres especiales tienen un significado especial cuando se repiten:

- **MMM**: Significa que el mes está representado como una cadena, el nombre abreviado del nombre del mes (Ene para enero, Feb para febrero,...).
- **MMMM**: Significa que el mes está representado como una cadena, el nombre completo del mes (Enero, Febrero,...).
- **DDD**: Significa que el día está representado como una cadena, el nombre abreviado del nombre del día (Lun para lunes, Mar para martes,...).
- **DDDD**: Significa que el día está representado como una cadena, el nombre completo del día (Lunes, Martes,...).

Cualquier otro carácter se considera como un carácter literal, o lo que es lo mismo, debe estar presente en el campo fecha/hora.

- A Continuación se muestra una Lista de Campos. En esta lista podrá ver todos los campos actualmente definidos, pero también podrá editarlos. Es importante dar a los campos un nombre descriptivo, para que puedan ser utilizados posteriormente, en el Script de procesamiento de eventos, como variables. Incluso cuando el tipo de campo es reconocido automáticamente (Booleano, Entero, Real, Fecha, Hora, Fecha/Hora, Cadena de texto), puede cambiarlo desde aquí: simplemente pulse en la columna **Type** del campo del que quiera cambiar el tipo y seleccione un nuevo tipo de la lista. En el momento de ejecución, si el campo extraído del archivo monitorizado no puede ser convertido al tipo definido, será devuelto como un campo de tipo Cadena.
- En la parte inferior de la ventana, puede ver un check box llamado **Show Preview**. Puede seleccionar el ocultar el panel de vista previa de la parte derecha de la ventana, simplemente desmarcando esta opción. En la parte derecha. A la derecha de este check box, también puede ver un campo que le permite definir cuantas entradas desea mostrar en el panel de vista previa: por defecto sólo se muestran diez entradas, pero puede incrementar o disminuir este valor.

Si está editando un Formato de Campo Delimitado, verá otro campo bajo el formato Fecha/Hora:

- **Delimiter Characters**: Aquí puede introducir tantos delimitadores como desee, pero recuerde que se entienden como 'delimitador de caracteres', no como 'delimitador de cadenas', es decir, se toman uno por uno, no como una única cadena. Si necesita introducir el carácter tabulador, abra el menú desplegable en la parte derecha del campo y selecciónelo de la lista mostrada.

Si está editando un Formato de Ancho Fijo, puede pulsar en los títulos de las columnas del panel de vista previa del log. Se mostrará un menú contextual, que le permitirá:

- **Split Field**: (dividir el campo) en dos, justo en la posición donde está situado la flecha del mouse. Podrá cambiar o ajustar posteriormente la anchura del campo en la lista de campos en la columna Width.
- **Merge with Left Field**: Combina los campos seleccionados con el campo de la izquierda (se existe alguno).
- **Merge with Right Field**: Combina los campos seleccionados con el campo de la derecha (se existe alguno).

8. Propiedades del Monitor de Archivos de Sistema

Las diferentes propiedades que definen un monitor de Archivos de Sistema se agrupan de la siguiente manera:

- **Objetos Monitorizados:** Las propiedades que identifican que objetos del sistema (archivos y directorios) desea monitorizar. Sus propiedades son:
 - **Directory:** El path a los objetos del sistema que desea monitorizar.
 - **Objects:** Los objetos que desea monitorizar. Puede utilizar genéricos (*, ?) para indicar un conjunto de objetos. Por ejemplo:
 - *: Seleccionará todos los archivos o directorios.
 - *.*: Seleccionará todos los archivos o directorios con extensión.
 - *.txt: Seleccionará todos los archivos con extensión txt
 - **Include Subdirectories:** Le permite indicar que también serán monitorizados los subdirectorios. Los Archivos que coincidan con los objetos definidos que se encuentren en subdirectorios del directorio también serán monitorizados.
- **Eventos Monitorizados:** Estas propiedades indican el tipo de cambio en los objetos del sistema que desea monitorizar. Seleccionando los correspondientes check box indicará que desea que el monitor procese el evento. Los tipos de cambios disponibles son:
 - **Creation:** Evento generado cuando se crea un objeto que coincide con los objetos definidos.
 - **Deletion:** Evento generado cuando se borra un objeto que coincide con los objetos definidos.
 - **Existence:** Evento generado cada vez que el monitor chequea el directorio y comprueba la existencia de objeto que coincide con los objetos definidos..
 - **Non-Existence:** Evento generado cada vez que el monitor chequea el directorio y comprueba que no existe un objeto que coincida con los objetos definidos.
 - **Change:** Evento generado cuando se cambia un objeto que coincide con los objetos definidos. También puede especificar en que tipos de cambio está interesado:
 - **Creation Time:** La fecha en la que el objeto fué creado.
 - **Access Time:** La fecha en que se accedió al objeto por última vez. Tenga cuidado con esta opción, ya que la fecha de acceso a objetos sólo se actualiza por el sistema operativo cuando se cierra el objeto, no cuando se abre.
 - **Save Time:** La fecha en que el objeto fué cerrado por última vez.
 - **Attributes:** Atributos binarios del objeto (sólo lectura, oculto, etc.)
 - **Size:** Tamaño del objeto.
- **Propiedades de Monitorización:** Estas propiedades le permiten definir Como van a monitorizarse los objetos.
 - **Polling Interval:** El intervalo de tiempo (en segundos) entre chequeos. Si los objetos monitorizados están localizados en la misma máquina que Applications Agent, puede

ajustar esta propiedad a 0. Esto significa que Applications Agent puede optimizar el proceso de chequeo, indicando al Sistema Operativo que levante el monitor cada vez que cambie el objeto, y que se relize el chequeo sólo cuando cambia el objeto. Si los objetos no son locales, Applications Agent debe chequear los objetos periódicamente, en intervalos tan amplios como se haya indicado en Polling Interval.

- **Script de Procesamiento del Evento:** Es el script de procesamiento que se ejecutará en cada evento detectado en el objeto. A la derecha del campo de entrada dispone de tres botones:
 - Seleccionar un script ya existente.
 - Editar el script seleccionado.
 - Borrar el campo de entrada de script, lo que significa que no se utiliza ningún script..

9. Visión General de la Consola

La consola del Agente es el panel de control central del mismo. Le permite gestionar los monitores y organizarlos en carpetas definidas por el usuario. Permite además ver los últimos eventos detectados por cada monitor.

Funciona en base a perfiles: las configuraciones definidas por el usuario (monitores y carpetas del usuario) se guardan con el nombre del perfil de usuario que arrancó el agente. De todas maneras, puede abrir perfiles creados por otros usuarios cuando las políticas del sistema operativo lo permitan.

Diríjase a los siguientes apartados para saber que puede hacer desde la consola del agente:

- Agentes, Monitores, Objetos y Eventos
- Funcionamiento de la Consola de Applications Agent

10. Agentes, Monitores, Objetos y Eventos

Un **Agente**, en el contexto de VISUAL Message Center, es una aplicación que “vigila” un sujeto específico de interés en un entorno de red. Ejemplos de sujetos de interés en la red son: rendimiento, sistema de archivos, colas de mensajes, logs de auditoría, protocolos de comunicaciones, dispositivos SNMP, servidores web, servidores de correo y aplicaciones de negocio (o lo que es lo mismo, cualquier componente de la infraestructura informática, ya sea hardware o software). Cada agente está ajustado para medir el estado de un componente particular de la red. Es capaz de detectar las condiciones específicas del estado del componente y notificarlo a la consola de VISUAL Message Center, desde donde se puede tomar la acción apropiada para corregir un estado anormal, notificar a los operadores y/o alimentar una base de datos con información relacionada.


Cada componente del entorno de red normalmente se compone de subcomponentes, que pueden o no necesitar de su atención. Nos referiremos a esos subcomponentes como Objetos. Ejemplos de objetos pueden ser los siguientes: utilización de CPU en un agente de rendimiento, archivos alterados en un agente de sistemas de archivo, mensajes de error en un agente de colas de mensaje, y/o puertos TCP abiertos en un agente de protocolo de comunicaciones TCP/IP.


Para especificar que objetos requieren atención, el administrador del agente debe definir un monitor. Un **Monitor** es una entidad de software contenida en el agente, que monitoriza (vigila) un objeto específico. El administrador del agente define los objetos de interés a través de esos monitores. La consola del agente muestra estos monitores.


Los cambios en el objeto detectados por el monitor se denominan **Eventos**. Los eventos están compuestos de diferentes propiedades (campos de información) que identifican el estado del objeto monitorizado. El monitor puede ejecutar un **Script** para responder a un evento detectado. Los eventos se muestran por la consola del agente en la lista de eventos.

Cada monitor tiene diferentes **Estados de Actividad** a lo largo del tiempo. El estado de actividad se refleja en la pantalla principal con una bombilla junto al icono del monitor:





Parado: El monitor está configurado, pero está inactivo. Actualmente no está monitorizando los objetos.

 **Suspendido:** El monitor está configurado, está en estado activo, pero no reporta eventos. Los eventos se reportarán cuando el monitor vuelva al estado “En ejecución”.

 **En Ejecución:** El monitor está configurado, está activo y reportará los eventos detectados.

 **Error:** El monitor está configurado, está activo o inactivo, pero se encuentra en estado de error.

El estado de Actividad puede cambiar debido a:

- **Modificación por el usuario:** El usuario puede cambiar manualmente el estado de un monitor, utilizando las siguientes acciones (desde el menú principal de la barra de herramientas)
 -  Reanudar
 -  Suspende
 -  Parar
 -  Limpiar Error
- **Error:** Puede producirlo el monitor en si mismo o el agente.
- **Script:** Ejecutado por el monitor en respuesta a un evento detectado.




10.1 Perfiles del Agente

Un Perfil del agente es un almacenamiento de la configuración del agente. Está asociado al perfil del usuario que definió la configuración. El perfil del agente contiene los ajustes del agente, de los monitores, de las carpetas del usuario y de todas las opciones de la consola del agente.

11. Carpetas

Las carpetas son contenedores que le permiten organizar los monitores de una forma lógica, haciendo fácil de localizar y comprender las relaciones entre ellos. Su propósito es la visualización y la organización, pero no tienen ningún efecto en la manera que el monitor trabaja.

Existen tres tipos de carpetas:

-  **Root Folder:** es el agente en si mismo. Esta carpeta contiene todos los monitores, por lo que al seleccionarlo en la lista de carpetas le permitirá ver todos sus monitores,..
-  **System Folders:** Carpetas virtuales proporcionadas por el agente, que contienen todos los monitores que pertenecen a la misma clase (hay una Carpeta de Sistema para cada tipo de monitor). No podrá borrar, renombrar o crear nuevas carpetas de sistema. Tampoco podrá copiar monitores en estas carpetas.
-  **User Folders:** Las carpetas definidas por el usuario. Puede gestionarlas como desee, creando, borrando o renombrando a su conveniencia. Los monitores pueden copiarse en diferentes carpetas para su organización. Para copiar un monitor a una carpeta de usuario, puede usar copiar y pegar o arrastrar el monitor desde la ventana de contenidos directamente al directorio de usuario deseado.

Las carpetas de usuario son parte del perfil de Agente activo, o lo que es lo mismo, son parte de su configuración, y se almacenan con su perfil.

12. Funcionamiento de la Consola de Applications Agent

En la ventana principal de la consola del agente puede ver:
















- **Menú:** En la parte superior de la ventana. Diríjase al apartado Menú principal para más detalles de las posibilidades que ofrece este menú.
- **Barra de Herramientas:** Se encuentra justo por debajo del Menú, e incluye botones para la mayoría de acciones que ofrece el menú. Una vez sepa que acciones pueden realizarse, podrá seleccionarlas más rápido desde los botones de la barra de herramientas. También existen shortcuts para usuarios avanzados.
- **Barra de Estado:** Se encuentra en la parte inferior de la pantalla. Muestra varios campos de información:
 - Perfil: El nombre del perfil actualmente en uso.
 - Estado: Estado del agente (En ejecución, Parado)
 - Mensajes: Mensajes informativos relacionados con la actividad que está realizando el agente.
- **Páginas de Información:** En la parte inferior de la ventana, justo por encima de la barra de estado, podrá ver las siguientes etiquetas:
 - Monitors: Muestra información relativa a los monitores.
 - Activity Log: muestra los últimos mensajes de actividad, describiendo el histórico de actividad del agente.



En la página monitors, encontrará:

- **Lista de Carpetas:** bajo la barra de herramientas a la izquierda de la pantalla. Muestra la estructura jerárquica de las carpetas. Pulse en cualquier carpeta para ver los contenidos de la misma en la ventana de contenidos. Cuando un monitor se encuentra en estado de error, una bombilla intermitente aparece junto a cada carpeta que contiene dicho monitor, con lo que rápidamente puede detectar problemas en diferentes áreas de negocio.
- **Ventana de Contenidos:** se encuentra bajo la barra de herramientas en la parte derecha de la pantalla. Muestra los contenidos de la carpeta seleccionada en la lista de carpetas. Junto a cada monitor una bombilla coloreada informa del estado del mismo. Cuando un monitor está en estado de error se muestra una bombilla intermitente junto al icono del monitor.
- **Lista de Eventos:** Justo por debajo de la ventana de contenidos. Cuando se selecciona un monitor de la ventana de contenidos, se muestra la lista de eventos generados por ese monitor.

13. Menú Principal

En el Menú de la ventana principal, se encuentra disponibles las siguientes acciones:

- **File:** Acciones relacionadas con el perfil.
 -  Open Profile: Abrir otro perfil.
 -  Save Profile: guardar el perfil actualmente en uso.
 -  Save Profile As: guardar el perfil actualmente en uso con un nombre diferente.
 - Exit: Salir de la consola del agente.
- **Edit:** Acciones relativas a la edición.
 -  Copy: Copiará los elementos seleccionados (monitores y/o carpetas de usuario) al portapapeles.
 -  Paste: Pegar los contenidos del portapapeles . Fíjese que el monitor no se duplica, simplemente se copia una referencia al monitor originalmente definido.
 -  Delete: Borra los elementos seleccionados (monitores y/o carpetas).
- **Folders**
 -  New Folder: Crea una nueva carpeta de usuario.
 -  Rename Folder: Renombra una carpeta de usuario.
- **Monitors**
 -  New Monitor: Crea un nuevo monitor. Si el agente proporciona más de un tipo de monitor, se abre un diálogo para seleccionar la clase de monitor que desea crear.
 -  Monitor Properties: Muestra el diálogo de propiedades del monitor, permitiéndole cambiar estas propiedades.
 -  Resume Monitor: arranca/reanuda la ejecución del monitor.
 -  Suspend Monitor: Suspende la ejecución del monitor.
 -  Stop Monitor: Detiene la ejecución del monitor.
 -  Clear Monitor Error: Limpia la bandera de error del monitor.
- **View**
 -  Contents: Le permite escoger como se muestran los contenidos de las carpetas seleccionadas en la ventana de contenidos:
 - Large Icons:** Muestra los contenidos con iconos grandes.
 - Small Icons:** Muestra los contenidos con iconos pequeños.
 - List:** Muestra los contenidos como una lista con iconos pequeños.
 - Details:** Muestra los contenidos como una lista con iconos pequeños, mostrando además varias propiedades del monitor.
- **Tools**
 - **Options:** Le permite definir varias opciones de la consola con el diálogo de opciones.


- Help
 -  Contents: Muestra la tabla de contenidos de la ayuda en línea.
 -  Search: Le permite buscar información adicional.

14. Diálogo de Opciones

El diálogo de opciones le permite definir varios ajustes del entorno del agente. Dichos ajustes se organizan en diferentes páginas:

- **Errors:** En esta página puede configurar que desea que el agente haga en caso de que ocurra un error (en cualquier monitor o en el agente en si mismo). La acción normal a tomar es enviar el error al Windows Event Log. En ese caso, puede configurar el servidor como aquel en el que quiere que se almacene el log, el tipo de evento y el identificador del evento.
- **Warnings:** En esta página puede configurar que desea que el agente haga en caso de que se produzca un aviso (en cualquier monitor o en el agente en si mismo). La acción normal a tomar es enviar el error al Windows Event Log. En ese caso, puede configurar el servidor como aquel en el que quiere que se almacene el log, el tipo de evento y el identificador del evento.
- **Activity Log:** En esta página puede especificar que tipo de mensajes deben almacenarse en el Activity Log. Los mensajes de error y aviso se almacenan siempre. Pero puede definir si los mensajes de Éxito, Información y/o Trace deben ser también almacenados. También puede definir cuantos mensajes se mostrarán en el Activity Log, pero tenga cuidado con esto, la cantidad de memoria necesaria para mostrar mensajes en el activity log es proporcional al número de mensajes. Si quiere que se muestren más mensajes, necesitará más memoria.
- **Monitors:** En esta página puede definir cuantos eventos serán mostrados en la lista de eventos, pero tenga cuidado con esto, la cantidad de memoria necesaria para mostrar mensajes en la lista de eventos es proporcional al número de mensajes. Si quiere que se muestren más mensajes, necesitará más memoria.

15. Diálogo de Selección del tipo de Monitor

Cuando el usuario selecciona la acción nuevo monitor () , el agente permite definir un nuevo monitor. Si el agente proporciona más de un tipo de monitor, el diálogo de Selección de tipo de Monitor aparece en pantalla. En este diálogo deberá seleccionar el tipo de monitor en el campo clase de monitor.

Bajo este campo, se proporciona una Descripción de cada clase, para que elija exactamente el tipo de monitor apropiado para el objeto que desea monitorizar.

16. Apéndice: Ejemplos de creación de monitores personalizados

16.1 Visión General de los Monitores Personalizados

Decir que Applications Agent puede monitorizar archivos de texto no es totalmente cierto; puede monitorizar los **contenidos** de los archivos de texto. Esto puede ser obvio, pero no lo es: significa que Applications Agent puede monitorizar cualquier cosa que este dentro del archivo de texto. Esto implica, que incluso aunque el objeto monitorizado es un archivo de texto, si el archivo contiene información sobre otro objeto, estamos monitorizando este segundo objeto. Esto es lo que llamamos **Monitor Personalizado**.

Un **Monitor Personalizado** no es más que un monitor de Archivo Log en el cual el archivo log contiene información sobre un objeto de interés para el cliente.

Para poder definir un Monitor Personalizado, necesita disponer de un proceso que genere periódicamente un archivo de log, que contenga información que va a ser monitorizada.

Pero, ¿cómo crear un proceso que genere periódicamente un archivo de log? De hecho se necesitan dos cosas para “generar periódicamente un archivo de log”:

- Un **Programa** que genere el archivo con la información deseada. Esto no significa que siempre necesite crear un programa que genere el archivo: la mayoría de herramientas de Windows NT Administrative Command Line proporcionadas con Windows NT Resource Kit proporcionan información del sistema muy interesante relativa a incidencias de seguridad, usuarios, procesos, servicios,... También puede buscar en internet programas adicionales, existentes miles de ellos.
- Un **Programador** para ejecutar este programa periódicamente. Existen varias opciones disponibles:
 - Definir una Tarea Programada.
 - Crear un Script o Programa que no finalice nunca. La manera más simple es con un programa BATCH.

Visite los siguientes tópicos para ejemplos de monitores personalizados simples pero útiles:

- Monitorizando Disponibilidad del Servidor
- Monitorizando Puertos TCP Abiertos
- Monitorizando Procesos Windows
- Monitorizando Servicios Windows
- Monitorizando Usuarios Inactivos

16.2 Monitorizando Disponibilidad del Servidor

¿Qué es lo que hace para chequear si un servidor, localizado en su LAN local o en Internet, está disponible? Existen varias opciones, pero quizá la más simple y obvia es utilizar el programa de línea de mandatos de **ping**.

Paso 1. Analizar la salida del programa

Primero, intentaremos conectar a un servidor disponible, haciendo ping a un host local (su máquina, que siempre debería estar disponible). Esta es la respuesta que obtenemos del mandato:

```
C:\WINDOWS>ping local host
Pinging ALEX.TANGO [127.0.0.1] with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<10ms TTL=128
Reply from 127.0.0.1: bytes=32 time<10ms TTL=128
Reply from 127.0.0.1: bytes=32 time<10ms TTL=128
Reply from 127.0.0.1: bytes=32 time<10ms TTL=128
Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milliseconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\WINDOWS>
```

Ahora, vamos a intentar conectar a un servidor no disponible, haciendo ping a una dirección IP local no asignada, por ejemplo:

```
C:\WINDOWS>ping 192.168.0.7
Pinging 192.168.0.7 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.0.7:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    Approximate round trip times in milliseconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\WINDOWS>
```

Y vamos a probar una cosa más, hacer ping a un servidor al que no se puede conectar (por ejemplo, desconectando su PC de la red)

```
C:\WINDOWS>ping www.tango04.com  
Unknown host www.tango04.com.
```

Podemos concluir que, cuando la respuesta del mandato ping es algo parecido a "Replay from..." el servidor está disponible, y cuando la respuesta es "Request timed out." o "Unknown host...", no está disponible.

Paso 2. Periodificar el programa


Para planificar la ejecución del mandato ping, por ejemplo, en intervalos de 15 segundos, escribimos el programa BATCH "Server Monitor.BAT" (este programa puede encontrarlo en la carpeta Samples de Applications Agent):

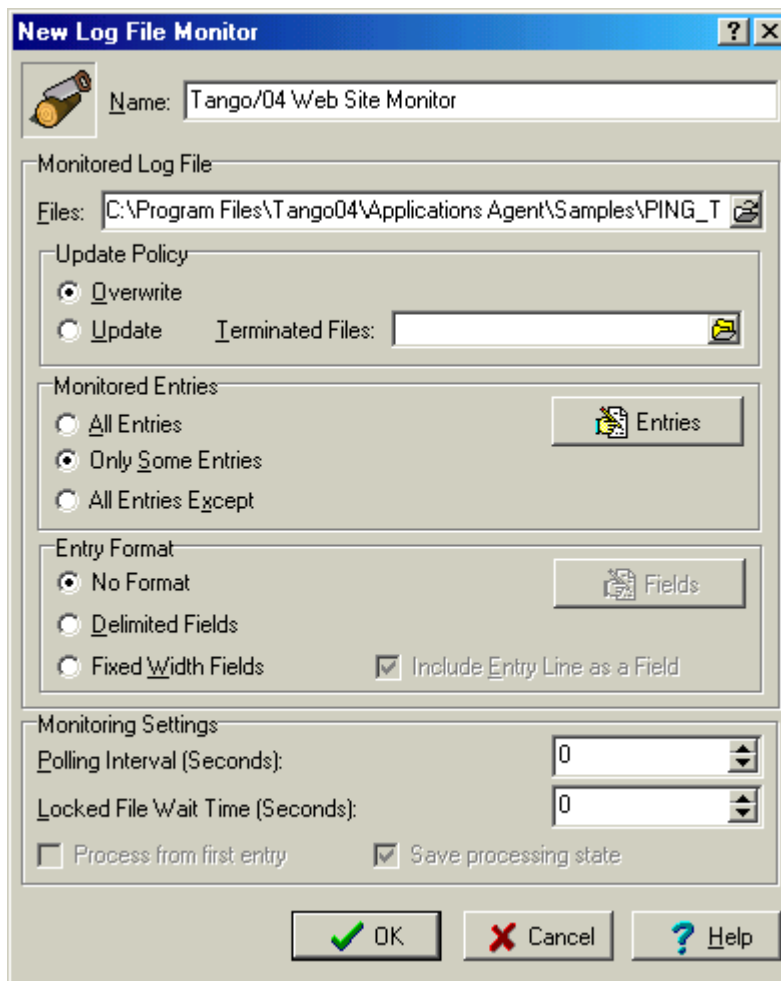
```
:LOOP_START  
PING -n 3 www.tango04.com > PING_TANGO.LOG  
DELAY 15  
GOTO LOOP_START
```

Como puede ver, la respuesta del mandato PING se redirige (utilizando el operador >) a un archivo llamado PING_TANGO.LOG en la sentencia 2. Este es el archivo que monitorizaremos en el Paso siguiente utilizando el Monitor de Archivos Log.

Fíjese también en mandato DELAY de la sentencia 3. Este NO es un mandato proporcionado por Windows, es un pequeño programa instalado con Applications Agent, que simplemente mantiene en estado de espera durante el número de segundos indicados como parámetro. En este caso espera 15 segundos.

Paso 3. Definición del Monitor de Log

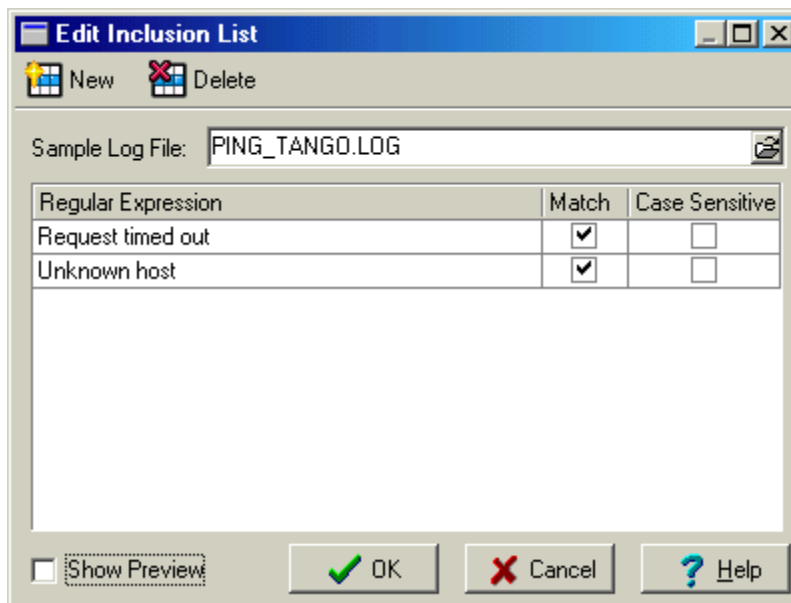
- Pulse en el botón New Monitor () de la barra de herramientas.
- Se mostrará el diálogo Select Monitor Class para que seleccione el tipo de monitor que desea crear. Seleccione "Log File Monitor" en el campo de entrada del tipo de monitor.
- Se abrirá la ventana Log File Monitor Properties para que seleccione la definición del monitor. LA definición debe ser similar a la que se muestra en la siguiente pantalla:



El path **Files** debe apuntar al archivo generado por el programa batch, en este ejemplo:

'C:\Program Files\Tango04\Applications Agent\Samples\PING_TANGO.LOG'

Pulse el botón Entries para ver el diálogo Inclusión/Exclusión y defina que entradas desea monitorizar. Después de indicar las expresiones regulares para las cadenas "Request timed out" y "Unknown host", se mostrará como la siguiente pantalla:





Pulse el botón OK para confirmar la selección, y pulse OK para confirmar el diálogo de Log File Properties.

Paso 4. Definir el Event Processing Script

Se mostrará una pantalla que le pedirá que edite el event processing script. Pulse el botón Yes. Aparecerá el editor de scripts, mostrándole el event processing script por defecto. El event processing script por defecto envía un mensaje de información al Windows Event Log local, diciendo que se ha procesado una entrada de log. Editaremos este script para mandar un mensaje de error diciendo que el Web site de Tango no está disponible, que es mucho más descriptivo:

- Haga doble click en la sentencia "WIN_EVENT_INFORMATION('Log entry processed by...".
- En el diálogo mostrado, sustituya la expresión por la siguiente:

```
WIN_EVENT_ERROR( 'Tango/04 Web Site no está disponible.' )
```

- Pulse el botón OK para cerrar el diálogo y el botón OK para cerrar el editor de scripts.
- Pulse el botón Save () para guardar el perfil.
- Pulse el botón Resume () para iniciar la ejecución del monitor.

16.3 Monitorizando Puertos TCP Abiertos

El mandato **netstat** muestra estadísticas del protocolo TCP/IP y las conexiones TCP/IP actuales. Este mandato es todo lo que necesitamos para monitorizar puertos TCP abiertos.

Paso 1. Analizar la respuesta del programa

Antes que nada, echemos un vistazo a la ayuda del mandato:

```
C:\>netstat /h
Muestra estadísticas del protocolo y conexiones TCP/IP actuales.

NETSTAT [-a] [-e] [-n] [-s] [-p proto] [-r] [intervalo]

-a          Muestra todas las conexiones y puertos escucha.
            (Normalmente, el extremo servidor de las conexiones no
            se muestra).

-e          Muestra estadísticas Ethernet. Se puede combinar con
            la opción -s.

-n          Muestra números de puertos y direcciones en formato
            numérico.

-p proto    Muestra conexiones del protocolo especificado por
            proto; que puede ser tcp o udp. Si se usa con la opción
            -s para mostrar estadísticas por protocolo, proto puede
            ser tcp, udp o ip.

-r          Muestra el contenido de la tabla de rutas.

-s          Muestra estadísticas por protocolo. En forma
            predeterminada, se muestran para TCP, UDP e IP; se puede
            utilizar la opción -p para especificar un subconjunto de
            lo predeterminado.

Intervalo  Vuelve a mostrar las estadísticas seleccionadas,
            haciendo pausas en el intervalo de segundos especificado
            entre cada muestra. Presione Ctrl+C para detener el
            refresco de estadísticas. Si se omite, netstat imprimirá
            la actual información de configuración una vez.
```

Vamos a probar utilizando la opción -a. Esta es la respuesta que obtenemos del mandato:

```
C:\WINDOWS>netstat -a
Active Connections

Proto  Local Address          Foreign Address        State
TCP    ALEX:135              ALEX:0                LISTENING
TCP    ALEX:1026             ALEX:0                LISTENING
TCP    ALEX:nbsession       ALEX:0                LISTENING
TCP    ALEX:nbsession       CPERIS:1190          ESTABLISHED
UDP    ALEX:1151             *:*
```

Como podemos ver, los puertos conocidos (puertos registrados por aplicaciones) se muestran normalmente con un nombre (y no simplemente con un número). Utilizaremos esta funcionalidad para chequear puertos abiertos no conocidos.

Paso 2. Periodificar el programa


Para programar la ejecución del mandato netstat, por ejemplo, en intervalos de 5 segundos, escribiremos el programa BATCH "TCP Ports Monitor.BAT" (este programa puede encontrarlo en la carpeta Samples de Applications Agent):

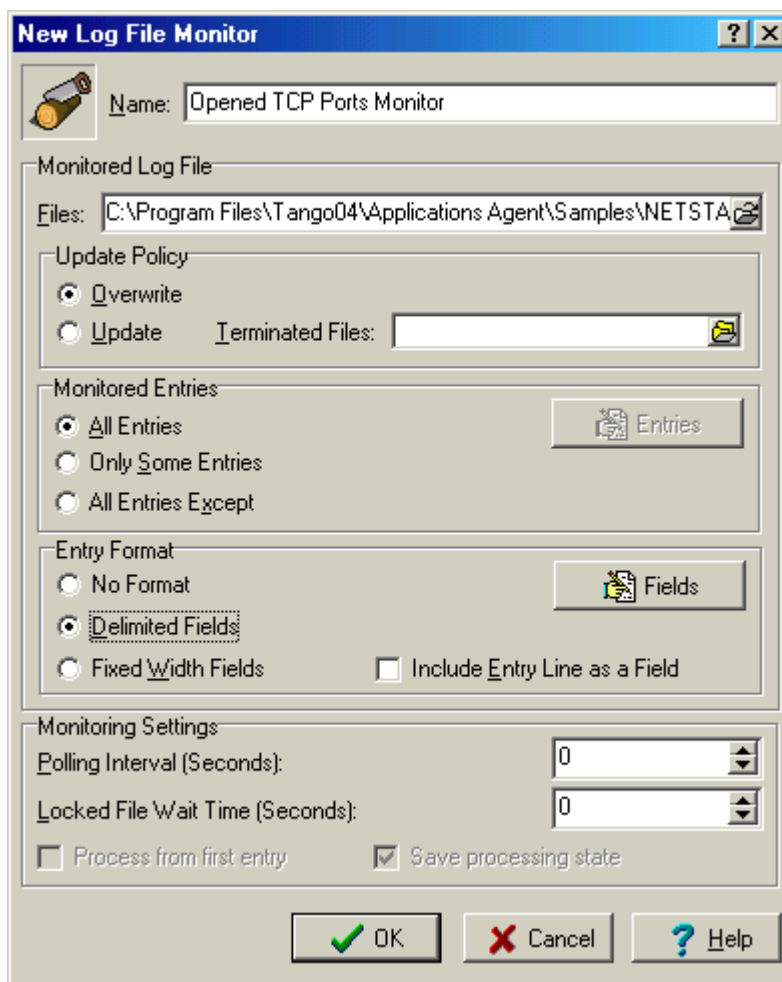
```
:LOOP_START
NETSTAT -a > NETSTAT.LOG
DELAY 5
GOTO LOOP_START
```

Como puede ver, la respuesta del mandato NETSTAT se dirige (utilizando el operador >) a un archivo denominado NETSTAT.LOG en la sentencia 2. Este es el archivo que será monitorizado en el siguiente paso, utilizando un Monitor de archivos Log.

Fíjese también en mandato DELAY de la sentencia 3. Este NO es un mandato proporcionado por Windows, es un pequeño programa instalado con Applications Agent, que simplemente mantiene en estado de espera durante el número de segundos indicados como parámetro. En este caso espera 5 segundos.

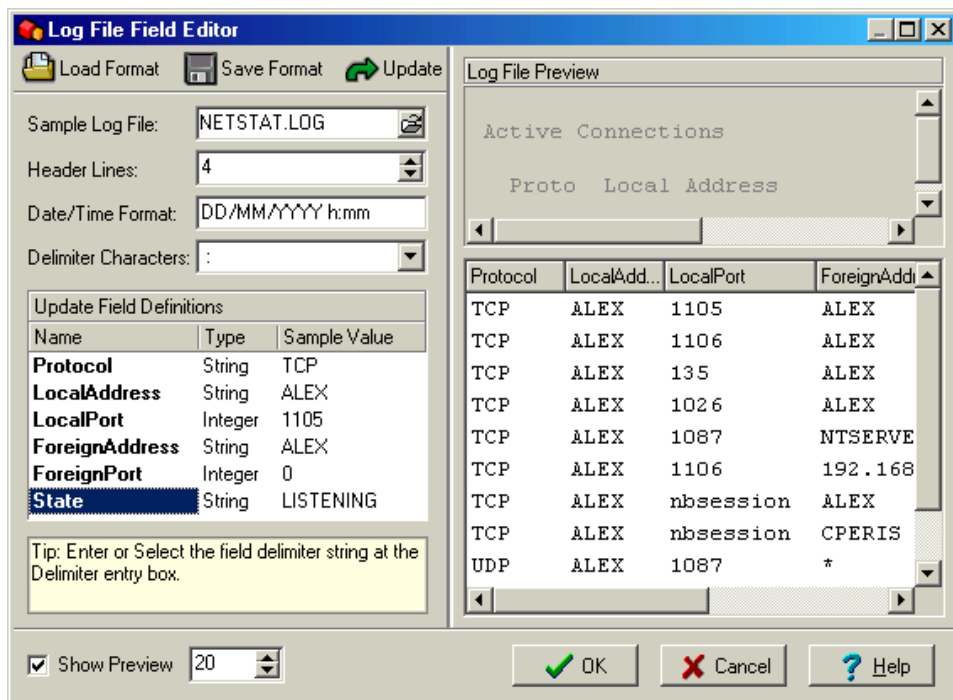
Paso 3. Definición del Monitor de Log

- Pulse el botón New Monitor () en la barra de herramientas.
- Se mostrará el diálogo Select Monitor Class para que seleccione el tipo de monitor que desea crear. Seleccione "Log File Monitor" en el campo de entrada de tipo de monitor.
- Se abrirá la pantalla Log File Monitor Properties para que introduzca la definición del monitor. LA definición debe ser similar a la que se muestra en la siguiente pantalla:



El path **Files** debe apuntar al archivo generado por el programa batch, en este ejemplo 'C:\Program Files\Tango04\Applications Agent\Samples\NETSTAT.LOG'

Pulse el botón Fields para abrir el "Field Editor Dialog": los Caracteres Delimitadores son Espacio y dos puntos (:). Por favor, renombre los nombres de los campos, tal y como se muestra, esto hará más simple el diseño de event processing script.





Pulse el botón OK para confirmar el diálogo, y pulse el botón OK para confirmar la ventana Log File Properties.

Paso 4. Definición del Event Processing Script


Se mostrará una pantalla que le pedirá que edite el event processing script. Pulse el botón Yes. Aparecerá el editor de scripts, mostrándole el event processing script por defecto. Ahora cambiaremos el event processing script por defecto para aplicar un chequeo simple de seguridad:


- Aceptaremos conexiones de puertos conocidos como conexiones seguras.
- Los puertos locales mayores de 1024 en estado LISTENING se considerarán “sospechosos”.
- Los puertos Remotos mayores de 1024 en estado ESTABLISHED se considerarán sospechosos.

Para implementar esta política, siga los siguientes pasos:


- Pulse en la sentencia "WIN_EVENT_INFORMATION('Log entry processed by...'", y bórrala pulsando el botón delete statement () o pulsando la tecla "Supr".
- Pulse el botón Case Statement (), y teclee la siguiente condición:

```
TYPENAME( LocalPort ) = 'STRING'
```


Esta condición sólo será satisfecha cuando el puerto local es un puerto conocido, con lo que se necesitará hacer nada más, simplemente finalizar el script. Pulse el botón Exit () para introducir una sentencia de finalización.

- Seleccione la sentencia, y pulse el botón Decision Statement (), y teclee la siguiente condición:


```
( LocalPort > 1024 ) AND ( State = 'LISTENING' )
```

En este caso, queremos enviar un mensaje de Aviso al Windows Event Log. Para hacerlo, pulse el botón Computation (), e introduzca la siguiente expresión:

```
WIN_EVENT_WARNING( 'Aviso de Seguridad, una aplicación de servidor  
está LISTENING en el puerto local ' + STRING( LocalPort ) )
```

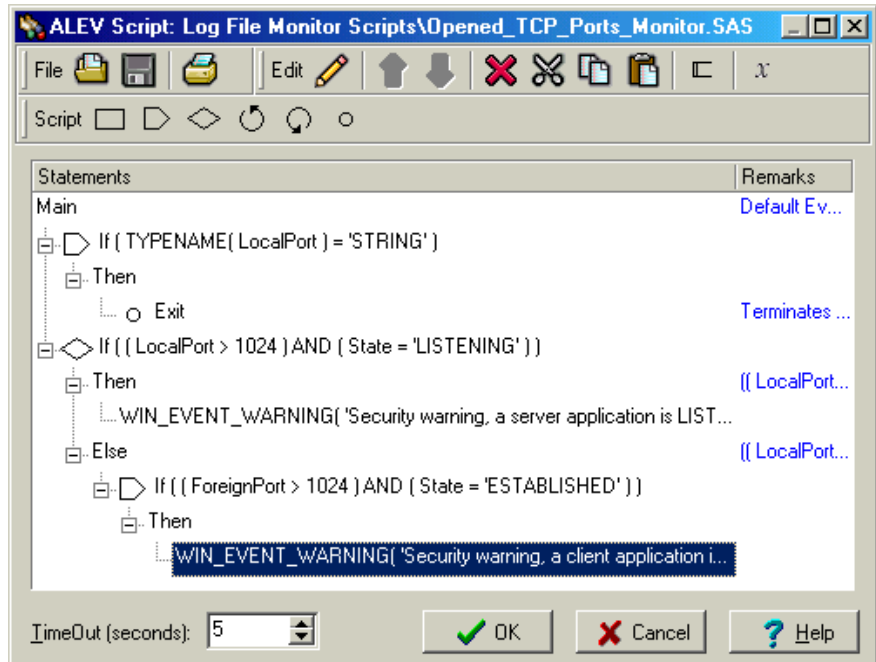
- Seleccione la rama Else en la sentencia de decisión, y pulse el botón Case Statement () para insertar una decisión simple (sin la sentencia Else), y teclee la siguiente condición:



```
( ForeignPort > 1024 ) AND ( State = 'ESTABLISHED' )
```

En este caso, queremos enviar un mensaje de Aviso al Windows Event Log. Para ello, pulse el botón Computation (), e introduzca la siguiente expresión:

```
WIN_EVENT_WARNING( ' Aviso de Seguridad, una aplicación de servidor  
ha ESTABLISHED una conexión a través del puerto ' + STRING(  
ForeignPort ) )
```

El script debería aparecer ahora como en la siguiente imagen:



- Pulse el botón OK para confirmar el diálogo, y pulse OK para confirmar Log File Properties.
- Pulse el botón Save () para guardar el perfil.
- Pulse el botón Resume () para iniciar la ejecución del monitor.

16.4 Monitorizando Procesos Windows

En el directorio Samples de Applications Agent, encontrará un programa denominado **procstat**. Este sencillo programa (alrededor de 200 líneas de código C comentado), utiliza la API Windows EnumProcesses para listar los procesos en ejecución en una máquina Windows NT/2000/XP. En este ejemplo, utilizaremos este programa para monitorizar el uso de memoria y CPU de los procesos en ejecución.

Paso 1. Analizar la salida del programa

Antes que nada, vamos a echar un vistazo a la salida del programa. Como puede ver, el programa muestra una gran cantidad de información para cada proceso: ID del procesos, nombre del proceso, Tipo de Prioridad, Hora de creación, hora Kernel, hora del usuario, %CPU, Faltas de página, Tamaño de Working Set, Pico de Tamaño de Working Set, Uso de Paged Pool, Pico de Uso de Paged Pool, Uso de Non-Paged Poo, Pico de Uso de Non-Paged Pool, Tamaño de Page File, Pico de Tamaño de Page File, Lecturas IO, Escrituras IO, Otros IO, Lectura de Transferencias IO, Escrituras de Transferencias IO, Otras transferencias IO, Objetos GDI y objetos USER.

Las columnas en las que estamos interesado son %CPU (uso de CPU del proceso) y Working Set Size (uso de memoria del proceso)

Paso 2. Periodificar el programa


Para programar la ejecución del mandato procstat, por ejemplo, en intervalos de 15 segundos, escribiremos el programa BATCH "Process Monitor.BAT" (este programa puede encontrarlo en la carpeta Samples de Applications Agent):

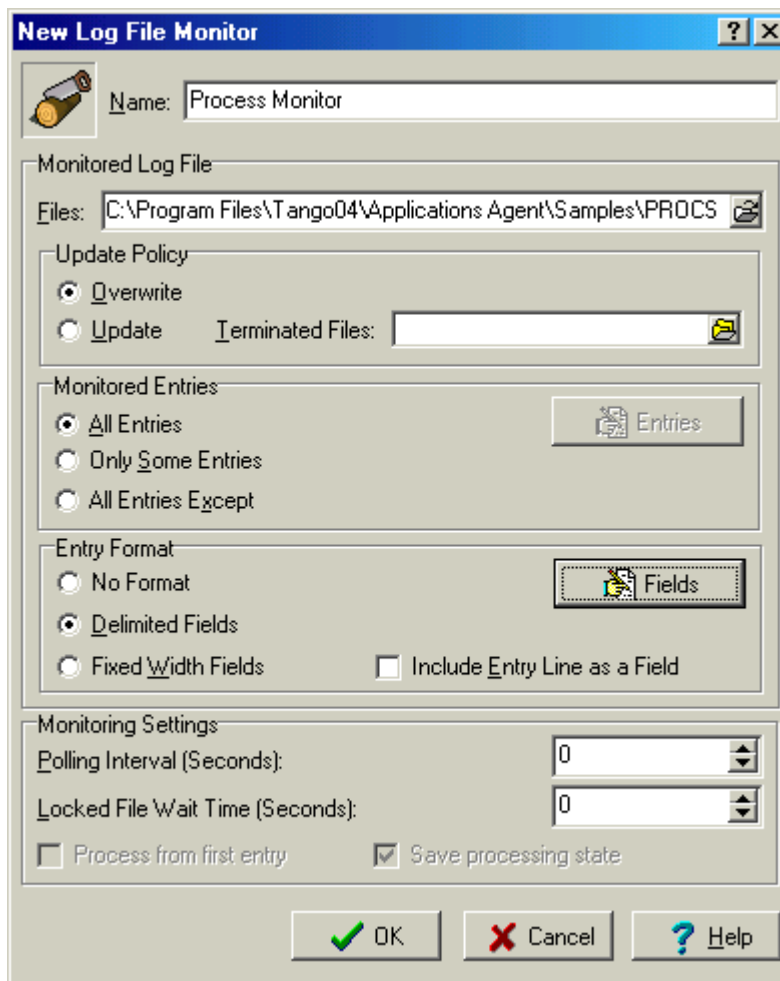
```
: LOOP_START  
PROCSTAT > PROCSTAT.LOG  
DELAY 15  
GOTO LOOP_START
```

Como puede ver, la respuesta del mandato PROCSTAT se redirige (utilizando el operador >) a un archivo denominado PROCSTAT.LOG en la sentencia 2. Este es el archivo que será monitorizado en el siguiente paso, utilizando un Monitor de archivos Log.

Fíjese también en mandato DELAY de la sentencia 3. Este NO es un mandato proporcionado por Windows, es un pequeño programa instalado con Applications Agent, que simplemente mantiene en estado de espera durante el número de segundos indicados como parámetro. En este caso espera 15 segundos.

Paso 3. Definición del Monitor de Log

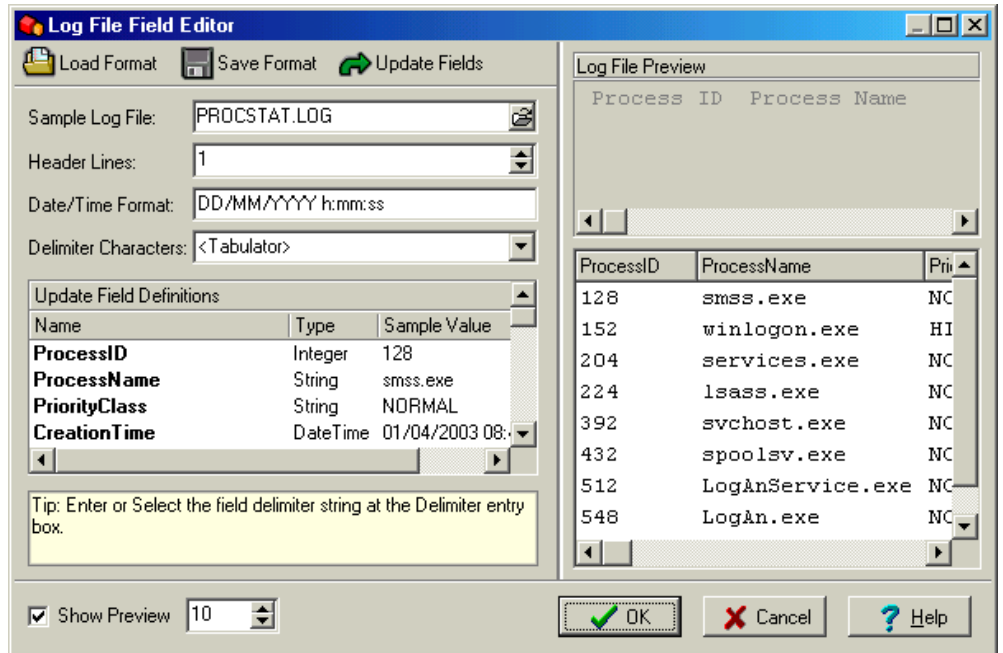
- Pulse el botón New Monitor () en la barra de herramientas.
- Se mostrará el diálogo Select Monitor Class para que seleccione el tipo de monitor que desea crear. Seleccione "**Log File Monitor**" en el campo de entrada de tipo de monitor.
- Se abrirá la pantalla Log File Monitor Properties para que introduzca la definición del monitor. LA definición debe ser similar a la que se muestra en la siguiente pantalla:



El path **Files** debe apuntar al archivo generado por el programa batch, en este ejemplo:

'C:\Program Files\Tango04\Applications Agent\Samples\PROCSTAT.LOG'

Pulse el botón **Fields** para que aparezca la ventana "Field Editor Dialog". Applications Agent proporciona un formato de campos predefinido para el mandato procstat, simplemente pulse el botón **Load Format**, y seleccione 'Command Output Format for PROCSTAT' de la lista mostrada.



Pulse el botón OK para confirmar el diálogo, y pulse OK para confirmar las Log File Properties.

Paso 4. Definición del Event Processing Script

Se mostrará una pantalla que le pedirá que edite el event processing script. Pulse el botón Yes. Aparecerá el editor de scripts, mostrándole el event processing script por defecto. Vamos a cambiar el event processing script por defecto para chequear procesos que utilicen más de un 10% de CPU y más de 15 Mbytes de memoria física.

Para implementar estos chequeos, siga los siguientes pasos:


- Pulse en la sentencia "WIN_EVENT_INFORMATION('Log entry processed by...', y bórrala pulsando el botón delete statement (X) o pulsando la tecla "Supr".
- Pulse el botón Case Statement (D), y teclee la siguiente condición:

CPU > 10

Esta condición será satisfecha cuando el campo CPU, el porcentaje de CPU utilizada por el proceso, es mayor del 10%. Pulse el botón Computation (C), e introduzca la siguiente acción:

```
WIN_EVENT_WARNING( 'El Proceso ' + ProcessName + ' está utilizando el ' + STRING( CPU ) + '% de la capacidad de CPU.' )
```

Esta acción enviará un Evento de Aviso a Windows Event Log informando que un proceso denominado ProcessName utilizad el tanto por ciento CPU de la capacidad de CPU. Vamos ahora al segundo chequeo:

- Seleccione la sentencia y pulse el botón Case Statement () de nuevo. Teclee la siguiente condición:

```
WorkingSet > 15728640
```

El campo WorkingSet, el uso de memoria física del proceso, se proporciona en bytes, pero queremos que chequee si el campo es mayor de 15 Mbytes, por lo que necesitamos expresar ambos valores en las mismas unidades:

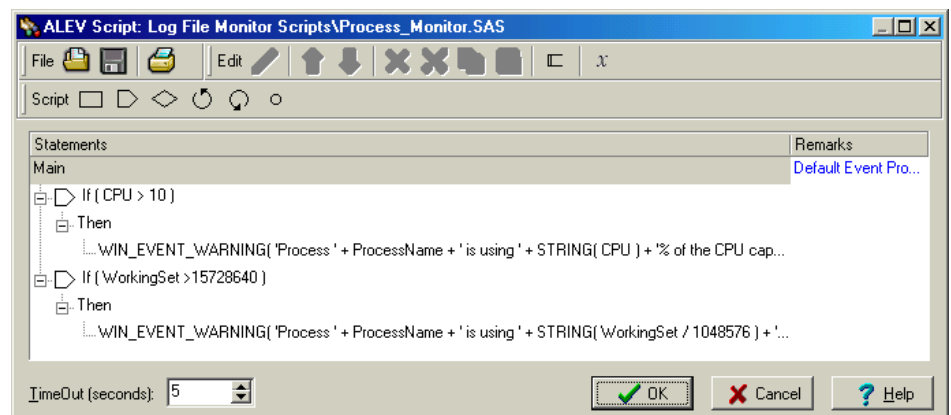
```
15 Mbytes = 15 * 1024 * 1024 Bytes = 15.728.640 Bytes
```



Ahora pulse el botón Computation (), e introduzca la siguiente acción:

```
WIN_EVENT_WARNING( 'El Proceso ' + ProcessName + ' está utilizando ' +  
+ STRING( WorkingSet / 1048576 ) + 'Mbytes de memoria física.' )
```

Esta acción enviará un mensaje de aviso a Windows Event Log informando de que un proceso llamado ProcessName está utilizando WorkingSet / 1048576 Mbytes de memoria física. Recuerde que $1024 * 1024 = 1.048.576$

El script debería aparecer ahora como en la imagen siguiente:



- Pulse el botón OK para confirmar el diálogo, y pulse OK para confirmar Log File Properties.
- Pulse el botón Save () para guardar el perfil.
- Pulse el botón Resume () para iniciar la ejecución del monitor.

16.5 Monitorizando Servicios Windows

En el directorio Samples de Applications Agent, encontrará un programa denominado **srvstat**. Este sencillo programa (alrededor de 200 líneas de código C comentado), utiliza la API Windows EnumServicesStatusEx para listar el estado de los servicios de Windows NT/2000/XP. En este ejemplo, utilizaremos este programa para monitorizar que un proceso específico se está ejecutando.

Paso 1. Analizar la respuesta del programa

Antes que nada, echemos un vistazo a la salida del programa. Como puede ver, el programa muestra mucha información de cada servicio: Nombre del servicio, nombre mostrado, tipo, estado, código de salida de Win32, Código de Salida específico, Check Point, Wait Hint, ID del proceso, y proceso del sistema.

Las columnas en las que estamos interesados son Service Name y State.

Paso 2. Periodificar el programa


Para programar la ejecución del mandato srvstat, por ejemplo, en intervalos de 15 segundos, escribiremos el programa BATCH "Service Monitor.BAT" (este programa puede encontrarlo en la carpeta Samples de Applications Agent):

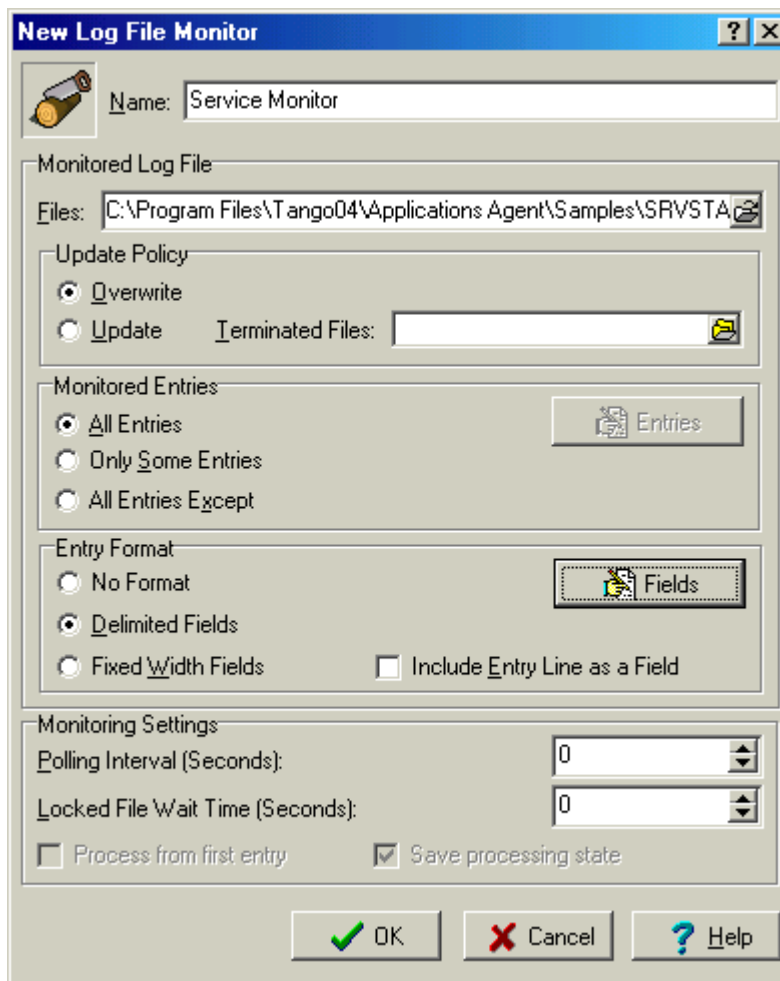
```
:LOOP_START
SRVSTAT > SRVSTAT.LOG
DELAY 15
GOTO LOOP_START
```

Como puede ver, la respuesta del mandato SRVSTAT se redirige (utilizando el operador >) a un archivo denominado SRVSTAT.LOG en la sentencia 2. Este es el archivo que será monitorizado en el siguiente paso, utilizando un Monitor de archivos Log.

Fíjese también en mandato DELAY de la sentencia 3. Este NO es un mandato proporcionado por Windows, es un pequeño programa instalado con Applications Agent, que simplemente mantiene en estado de espera durante el número de segundos indicados como parámetro. En este caso espera 15 segundos.

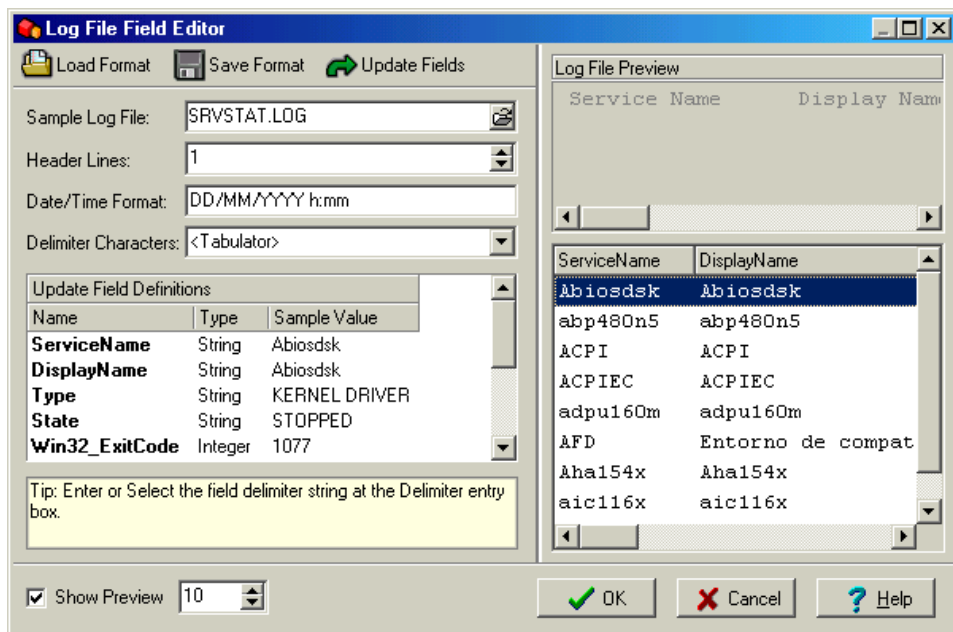
Paso 3. Definición del Monitor de Log

- Pulse el botón New Monitor () en la barra de herramientas.
- Se mostrará el diálogo Select Monitor Class para que seleccione el tipo de monitor que desea crear. Seleccione "**Log File Monitor**" en el campo de entrada de tipo de monitor.
- Se abrirá la pantalla Log File Monitor Properties para que introduzca la definición del monitor. La definición debe ser similar a la que se muestra en la siguiente pantalla:



El path **Files** debe apuntar al archivo generado por el programa batch, en este ejemplo 'C:\Program Files\Tango04\Applications Agent\Samples\SRVSTAT.LOG'

Pulse el botón **Fields** para que aparezca la ventana "Field Editor Dialog". Applications Agent proporciona un formato de campos predefinido para el mandato srvstat, simplemente pulse el botón **Load Format**, y seleccione 'Command Output Format for SRVSTAT' de la lista mostrada.



Pulse el botón OK para confirmar el diálogo, y pulse el botón OK para confirmar la ventana Log File Properties.

Paso 4. Definición del Event Processing Script

Se mostrará una pantalla que le pedirá que edite el event processing script. Pulse el botón Yes. Aparecerá el editor de scripts, mostrándole el event processing script por defecto. Ahora cambiaremos el event processing script por defecto para que verifique que el servicio UPS (Uninterrupted Power-supply System) siempre está en ejecución RUNNING.

Para implementar este tipo de chequeo, siga los siguientes pasos:

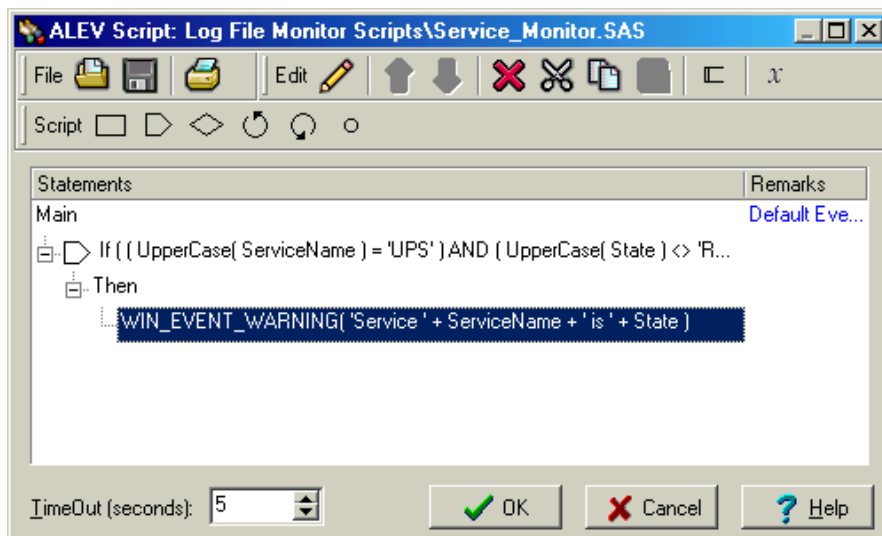
- Seleccione la sentencia "WIN_EVENT_INFORMATION('Log entry processed by...', y bórrala pulsando el botón delete statement () o pulsando la tecla "Supr".
- Pulse el botón Case Statement (), y teclee la siguiente condición:



```
( UpperCase( ServiceName ) = 'UPS' ) AND ( UpperCase( State ) <> 'RUNNING' )
```

Esta condición sólo se cumple cuando el servicio UPS no está en estado RUNNING. En esa situación enviaremos un mensaje de aviso al Windows Event Log. Pulse el botón Computation (), e introduzca la siguiente acción:

```
WIN_EVENT_WARNING( 'El Servicio ' + ServiceName + 'está' + State )
```

El script debería aparecer como:



- Pulse el botón OK para confirmar el diálogo, y pulse OK para confirmar Log File Properties.
- Pulse el botón Save () para guardar el perfil.
- Pulse el botón Resume () para iniciar la ejecución del monitor.

16.6 Monitorizando Usuarios Inactivos

En este ejemplo, utilizaremos el programa **usrstat** para buscar usuarios que no hayan iniciado sesión durante la última semana. Este programa se entrega con Windows NT Server Resource Kit, y muestra nombre de usuarios, nombre completo, y última fecha y hora de conexión para cada usuario del dominio seleccionado.

Paso 1. Analizar la respuesta del programa

Como siempre, echemos un vistazo a la salida del programa (esta es una salida parcial, las entradas no relevantes han sido eliminadas):

```
C:\WINDOWS>usrstat TANGO
Users at \\NTSERVER2
Administrator - - logon: Fri Mar 28 09:41:49 2003
BACKOFFICE - BACKOFFICE - logon: Never
FTP - - logon: Never
Guest - Guest Account - logon: Mon Apr 15 09:33:00 2002
IUSR_NTSERVER - Internet Guest Account - logon: Never
IUSR_NTSERVER2 - Internet Guest Account - logon: Fri Mar 28 11:16:40 2003
IWAM_NTSERVER2 - Web App Manager account - logon: Never
powerlock - - logon: Never
SQLExecCmdExec - SQLExecutiveCmdExec - logon: Never
```

Como podemos ver, la salida del mandato se divide en tres columnas: User Name, Full Name, y last log en fecha y hora.

Paso 2. Periodificar el programa


Para programar la ejecución del mandato usrstat, por ejemplo, una vez al día (1 día = 24 horas = 86400 segundos), escribiremos el programa BATCH "Inactive Users Monitor.BAT" (este programa puede encontrarlo en la carpeta Samples de Applications Agent):

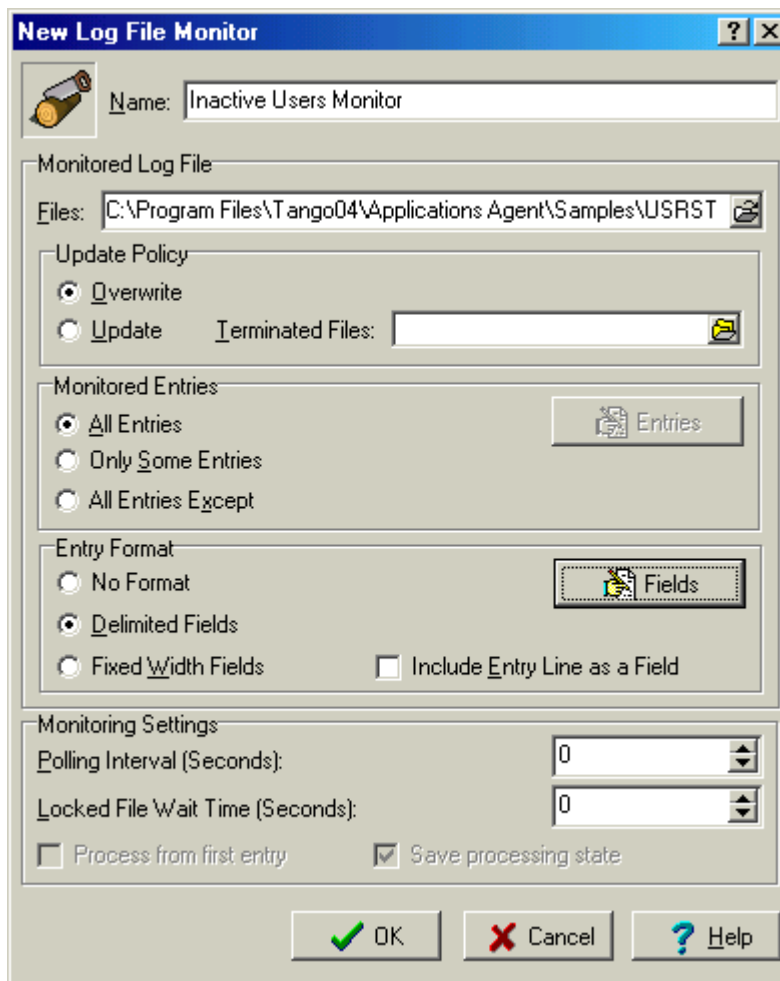
```
: LOOP_START
USRSTAT > USRSTAT.LOG
DELAY 86400
GOTO LOOP_START
```

Como puede ver, la respuesta del mandato USRSTAT se redirige (utilizando el operador >) a un archivo denominado USRSTAT.LOG en la sentencia 2. Este es el archivo que será monitorizado en el siguiente paso, utilizando un Monitor de archivos Log.

Fíjese también en mandato DELAY de la sentencia 3. Este NO es un mandato proporcionado por Windows, es un pequeño programa instalado con Applications Agent, que simplemente mantiene en estado de espera durante el número de segundos indicados como parámetro. En este caso espera 86400 segundos (1 día).

Paso 3. Definición del Monitor de Log

- Pulse el botón New Monitor () en la barra de herramientas.
- Se mostrará el diálogo Select Monitor Class para que seleccione el tipo de monitor que desea crear. Seleccione "**Log File Monitor**" en el campo de entrada de tipo de monitor.
- Se abrirá la pantalla Log File Monitor Properties para que introduzca la definición del monitor. La definición debe ser similar a la que se muestra en la siguiente pantalla:



El path **Files** debe apuntar al archivo generado por el programa batch, en este ejemplo 'C:\Program Files\Tango04\Applications Agent\Samples\USRSTAT.LOG'

Pulse el botón Fields para que aparezca la ventana "Field Editor Dialog".

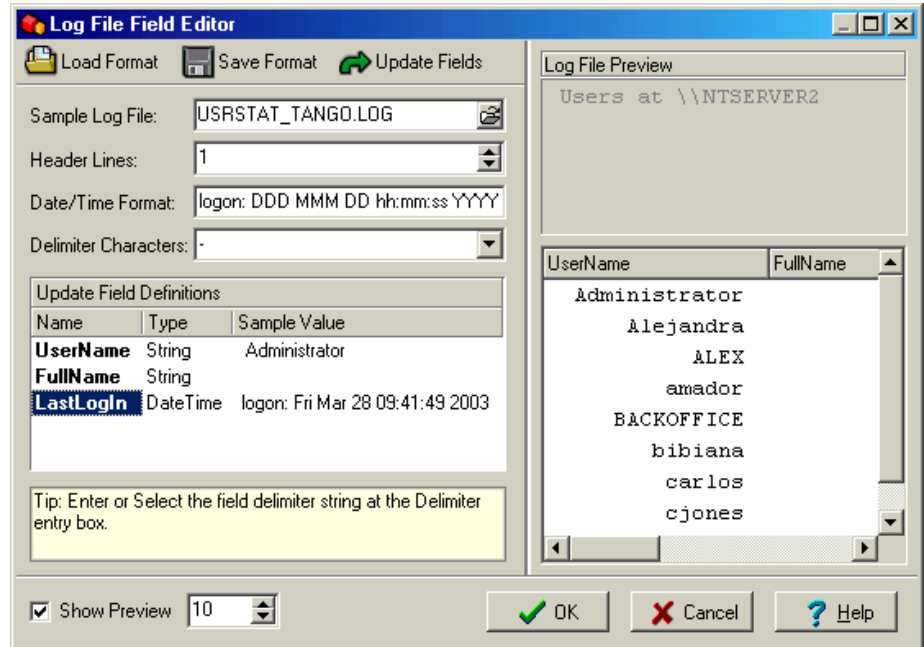
LA primera línea de la salida del mandato es "Users at \\NTSERVER2". Esta línea no nos interesa, es una línea de encabezamiento, por ello debemos introducir 1 en el campo de entrada Header Lines.

Observando la salida del mandato, podemos ver que las tres columnas de información están separadas por el carácter '-' (menos), para separar las columnas teclee '-' en el campo de entrada Delimiter Characters.

Ahora podemos ver las tres columnas correctamente separadas en el Preview Panel, y tres campos en Field List, pero el último campo (last log in date and time) se reconoce como un campo de cadena de texto en lugar de un campo Fecha/Hora. Esto es debido a que el formato de campo Fecha/Hora no ha sido correctamente definido. El formato Fecha/Hora debe definirse como 'logon: DDD MMM DD hh:mm:ss YYYY'.

Pulse en la columna Name de la lista de campos e introduzca nombres con significado para los tres campos.

Ahora, todo está correctamente ajustado, y las definiciones de los campos deberían aparecer como en la siguiente imagen:





Pulse el botón OK para confirmar el diálogo, y pulse el botón OK para confirmar la ventana Log File Properties.

Paso 4. Definición del Event Processing Script


Se mostrará una pantalla que le pedirá que edite el event processing script. Pulse el botón Yes. Aparecerá el editor de scripts, mostrándole el event processing script por defecto. Ahora cambiaremos event processing script por defecto para crear una notificación cuando un usuario no haya iniciado sesión en el dominio durante los últimos siete días.

Importante: Antes de implementar la política de chequeo, debe tener en cuenta lo siguiente. Cuando define el tipo de campo en el Log File Field Editor, Applications Agent intentará convertir el campo a ese tipo. Por ejemplo, en este caso, hemos definido el campo "LastLogIn" para que sea del tipo Fecha/Hora. Esto significa que posteriormente, en tiempo de ejecución, el campo LastLogIn será un valor Fecha/Hora. Pero esto es únicamente válido cuando la conversión tiene éxito, o lo que es lo mismo, cuando el texto encontrado en el archivo puede ser convertido a valor Fecha/Hora con el formato especificado Fecha/Hora. Si el texto encontrado en el archivo no puede ser convertido a valor Fecha/Hora, debido a que el texto no sigue el formato Fecha/Hora, el campo seguirá teniendo formato Cadena de texto. Esto significa que cuando no esté seguro que un campo siempre será del tipo especificado, deberá comprobar el tipo del campo antes de operar con él. Veamos como se aplica esto en la práctica:

- Seleccione la sentencia "WIN_EVENT_INFORMATION('Log entry processed by...', y bórrala pulsando el botón delete statement () o pulsando la tecla "Supr".
- Pulse el botón Selection Statement (), y teclee la siguiente condición:

```
( TYPENAME( LastLogIn ) = 'DATETIME' )
```



La función TYPENAME retorna una cadena con el tipo del parametro variable, LastLogIn en este ejemplo.

En ese caso necesitamos chequear si la variable LastLogIn es más antigua que 7 días o no, para ello pulse el botón Case Statement (), y teclee la siguiente condición:


```
( NOW() - LastLogIn > DAY( 7 ) )
```

La función NOW retorna la fecha y hora actual como un valor Fecha/Hora.

La función DAY, utilizada con un parámetro de tipo entero, retorna un valor Fecha/Hora correspondiente al número de días indicado en el parámetro.

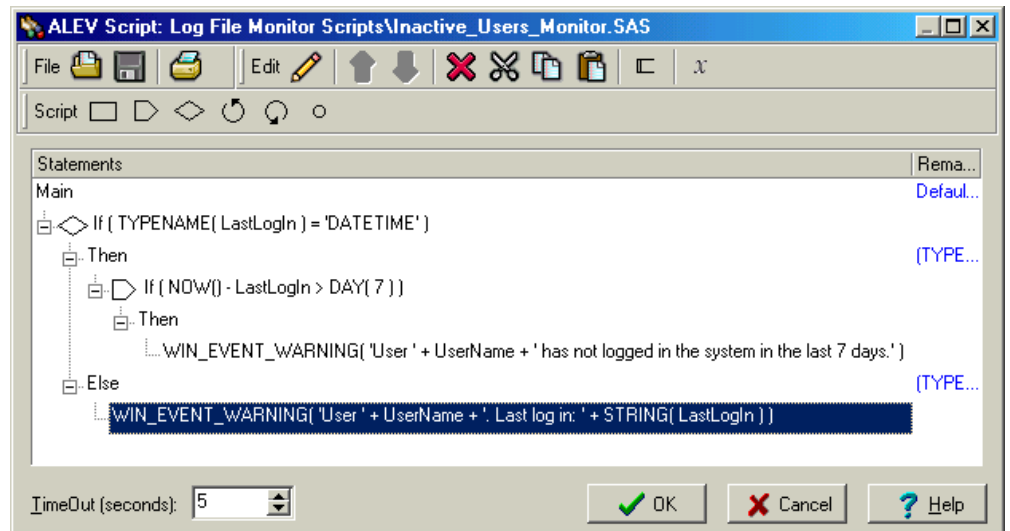
Esta condición se cumplirá cuando hayan pasado más de 7 días entre la Fecha y Hora de LastLogIn y la actual fecha y hora. En esa situación enviaremos un mensaje de Aviso al Event Log. Pulse el botón Computation (), e  duzca la siguiente acción:



```
WIN_EVENT_WARNING( 'El usuario ' + UserName + ' no se ha conectado al sistema durante los últimos 7 días.' )
```

Ahora, seleccione la rama Else de Selection Statement. Esta rama se ejecutará cuando la variable LastLogIn no sea un valor Fecha/Hora. Pulse el botón Computation (), y teclee la siguiente expresión:

```
WIN_EVENT_WARNING( 'Usuario ' + UserName + '. Último log in: ' + STRING( LastLogIn ) )
```

El script deberá aparecer como la siguiente imagen:



- Pulse el botón OK para confirmar el diálogo, y pulse OK para confirmar Log File Properties.
- Pulse el botón Save () para guardar el perfil.
- Pulse el botón Resume () para iniciar la ejecución del monitor.

17. Recursos en la Web

Ha podido ver en este tutorial lo fácil que es ajustar un monitor y ser notificado de eventos que ocurran en áreas administrativas importantes. Puede pensar que la "magia" se hace gracias a programas externos (procstat, srvstat,...), y que probablemente deba escribir sus propios programas para cumplir estas tareas de monitorización. Esto no tiene porque se cierto. Existen muchos recursos en Internet que ofrecen herramientas gratuitas para recuperar y volcar información relativa a administración de sistemas. De cualquier forma, creemos que el primer lugar (y probablemente el mejor) que debería visitar, para buscar las herramientas que necesita es Microsoft TechNet's Script Center: Allí encontrará muchos scripts para la gran mayoría de áreas de interés. Le recomendamos que eche un vistazo.

Microsoft TechNet Script Center

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/scriptcenter/default.asp>

18. Acerca de Tango/04 Computing Group

Tango/04 Computing Group es una de las principales empresas desarrolladoras de software de gestión y automatización de sistemas informáticos. El software de Tango/04 ayuda a las empresas a mantener la salud operativa de sus procesos de negocio, mejorar sus niveles de servicio, incrementar su productividad y reducir costes mediante una gestión inteligente de sus infraestructura informática.

Fundada en 1991 en Barcelona, Tango/04 es IBM Business Partner y miembro de la iniciativa estratégica IBM Autonomic Computing. Además de recibir numerosos reconocimientos de la industria, las soluciones Tango/04 han sido validadas por IBM y tienen la designación IBM ServerProven™. Tango/04 tiene más de mil clientes y mantiene operaciones en todo el mundo a través de una red de 35 Business Partners.

Alianzas



Partnerships

IBM Autonomic Computing Business Partner

IBM PartnerWorld for Developers Advanced Membership

IBM ISV Advantage Agreement

IBM Early code release

IBM Direct Technical Liaison

Microsoft Developer Network

Microsoft Early Code Release

Premios



19. Aviso legal

Este documento y su contenido son propiedad de Tango/04 Computing Group o de sus respectivos propietarios cuando así se indique. Cualquier utilización de este documento con una finalidad distinta de aquella con la cual ha sido creado está prohibida sin la autorización expresa de su propietario. Asimismo queda prohibida la reproducción total o parcial de este documento por cualquier medio físico, óptico, magnético, impreso, telemático, etc., sin la autorización expresa de su propietario.

La información técnica aquí contenida fue obtenida utilizando equipamiento e instalaciones específicas, y su aplicación se limita a esas combinaciones especiales de productos y niveles de versiones de hardware y software. Cualquier referencia en este documento a productos, software o servicios de Tango/04 Computing Group, no implica que Tango/04 Computing Group planea introducir esos productos, software o servicios en cada uno de los países en los que opera o está representada. Cualquier referencia a productos de software, hardware o servicios de Tango/04 Computing Group no está hecha con el propósito de expresar que solamente pueden utilizarse productos o servicios de Tango/04 Computing Group. Cualquier producto o servicio funcionalmente equivalente que no infrinja la propiedad intelectual o condiciones de licenciamiento específicas se podría utilizar en reemplazo de productos, software o servicios de Tango/04 Computing Group.

Tango/04 Computing Group puede tener patentes o estar pendiente de obtención de patentes que cubren asuntos tratados en este documento. La entrega de este documento no otorga ninguna licencia de esas patentes. La información contenida en este documento no ha sido sometida a ningún test formal por Tango/04 Computing Group y se distribuye tal como está. El uso de esta información o la implementación de cualquiera de las técnicas, productos, tecnologías, ideas o servicios explicitados o sugeridos por el presente documento es responsabilidad exclusiva del cliente a quien está dirigido este documento, y es el cliente quien debe evaluar y determinar la aplicabilidad y consecuencias de integrar esas técnicas, productos, tecnologías, ideas o servicios en su entorno operativo.

Si bien cada ítem puede haber sido revisado por Tango/04 Computing Group en cuanto a su exactitud en una situación específica, no existe ni se otorga ninguna garantía de que los mismos o similares resultados puedan ser obtenidos en otras situaciones o instalaciones. Los clientes que intenten adaptar esas técnicas en sus propias instalaciones lo hacen bajo su propia cuenta, responsabilidad y riesgo. Tango/04 Computing Group no será en ningún caso responsable directo o indirecto de cualquier daño o perjuicio causado por el uso de las técnicas explicitadas o sugeridas en este documento, incluso si se han efectuado notificaciones de la posibilidad de esos daños.

Este documento puede contener errores técnicos y/o errores tipográficos. Todas las referencias en esta publicación a entidades externas o sitios web han sido provistas para su comodidad solamente, y en ningún caso implican una validación, garantía o respaldo a esas entidades o sitios.

Las marcas siguientes son propiedad de International Business Machines Corporation en los Estados Unidos y/o otros países: AS/400, AS/400e, iSeries, e (logo)Server, i5, Operating System/400, OS/400, i5/OS.

Microsoft, Windows, Windows NT, Windows XP y el logotipo de Windows son marcas registradas de Microsoft Corporation en los Estados Unidos y/o otros países. Java y todos los logotipos y marcas basadas en Java son propiedad de Sun Microsystems, Inc. en los Estados Unidos y otros países. UNIX es una marca registrada en los Estados Unidos y otros países y se licencia exclusivamente a través de The Open Group. Oracle es una marca registrada de Oracle Corporation. Otras marcas, productos o servicios pueden ser marcas registradas de otras empresas.