

TCP/IP **Services Agent**

VISUAL Message Center **TCP/IP Services Agent** Guía de Introducción

1. Tabla de Contenidos

1. Tabla de Contenidos.....	2
2. Guía de Introducción a TCP/IP Services Agent.....	3
2.1 Instalación	3
2.2 Activación del Producto	3
2.3 Arrancando la Aplicación.....	4
2.4 ¿Como funciona?	4
3. Antes de Comenzar	6
3.1 Configuración de Servidores	6
3.2 Añadiendo Chequeos - Ping	10
3.3 Reglas Lógicas del Mensaje.....	11
3.4 Arrancar Chequeos	15
3.5 Diferentes Tipos de Chequeo.....	16
3.5.1 Chequeo de Puerto.....	17
3.5.2 Chequeo POP3.....	18
3.5.3 Chequeo SMTP	21
3.5.4 Loop Email: POP3 y SMTP.....	23
3.6 SNMP.....	24
3.7 Receptor de Traps SNMP	26
4. Opciones de Configuración generales	28
4.1 Integración con VISUAL Message Center: Redireccionar Mensajes al Event Log de Windows:	28
4.2 Ejecutar chequeos automáticamente	29
4.3 Ejecutar TCP/IP Services Agent como un Servicio	29
5. Apéndice A: Utilizando el nuevo agente SNMP	30
5.1 Conceptos Básicos.....	30
5.2 Traps	31
5.2.1 Recuperación de datos SNMP.....	31
5.2.2 Valores Delta	33
5.2.3 Recepción de Traps SNMP	34
6. Acerca de Tango/04 Computing Group	35
7. Aviso legal.....	36

2. Guía de Introducción a TCP/IP Services Agent

El Agente de Servicios TCP/IP le permite monitorizar constantemente el estado de todos sus servicios y dispositivos de red, detectando problemas, lentitud de respuestas y midiendo el tiempo de indisponibilidad total.

El agente comprueba de manera continua la salud de los servidores email POP3 y SMTP, además de realizar “pings” comprobando la disponibilidad de los puertos de cualquier dispositivo de red, localmente o a través de internet.

Incluso puede recuperar mensajes nuevos de una cuenta POP3 (esto es útil para detectar errores en dispositivos que envían emails para comunicar problemas operativos).

Los mensajes del estado operativo pueden visualizarse desde la consola Java del Agente de Servicios TCP/IP o pueden ser gestionados desde la consola de VISUAL Message Center, que le proporciona completas funcionalidades de alarmas y automatización.

2.1 Instalación

Deberá instalar el producto desde el CD de productos o desde un archivo descargado desde nuestra página web.

El producto se instala en una estación de trabajo cliente, normalmente un servidor Windows NT/2000/XP.

El producto es una aplicación Java, y corre usando Java 2 Runtime Environment, version 1.3.1. Este entorno se instala automáticamente con la aplicación. El TCP/IP Services Agent lo utilizará independientemente de que tenga o no otras máquinas Java virtuales instaladas en su sistema.

Para ejecutar el programa de instalación, haga doble click en “setup.exe”. Se le pedirá que especifique el directorio de instalación.

Una vez instalado verá el siguiente directorio: C:\Program Files\Tango04\TCPIP Services Agent. Dentro de este directorio están los archivos de programa. También existe un directorio denominado “jre” donde se ha instalado Java Runtime Environment.

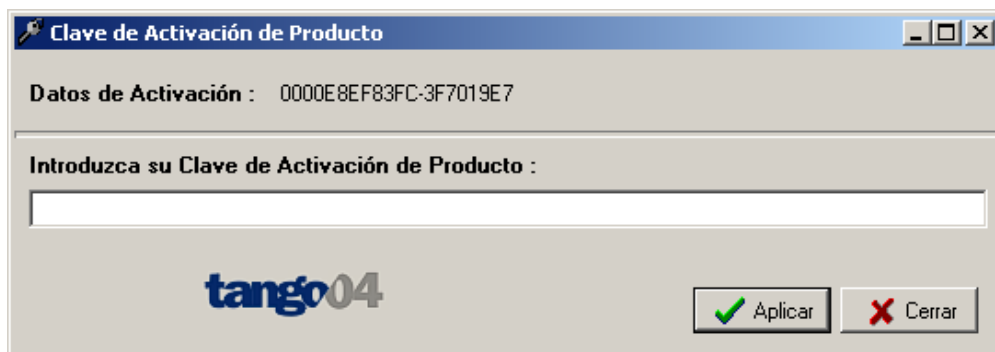
El TCP/IP Services Agent tiene su propio menú de producto: Inicio-Programas-TCPIP Services Agent.

El proceso de instalación es simple y probablemente familiar para usted. Si tiene algún problema con el proceso de instalación, por favor contacte con Tango/04 o un distribuidor autorizado.

2.2 Activación del Producto

Puede activar el producto con una clave de activación desde la opción del menú “Clave de Activación del Producto”. Aquí deberá introducir la clave que le ha proporcionado Tango/04.

Si necesita pedir una clave, por favor contacte con su representante comercial de Tango/04 o un distribuidor autorizado, y especifique los datos de activación mostrados en este diálogo, como se muestra a continuación:



También puede utilizar el middleware de Tango/04 NiceLink para aplicar automáticamente la clave para el TCP/IP Services Agent y cualquier otro producto Tango/04. Consulte la Guía de Ayuda de NiceLink para más información.

2.3 Arrancando la Aplicación

Cuando tenga el producto correctamente instalado y haya introducido un código de autorización válido podrá arrancar la aplicación seleccionando la opción del menú "Visor Log TCP/IP Agent".

2.4 ¿Como funciona?

El TCP/IP Services Agent utiliza "**chequeos**" para monitorizar el estado de sus servicios TCP/IP. Una vez los chequeos se han configurado se activarán periódicamente. Los resultados del chequeo se muestran en la consola del producto, y pueden ser enviados al Visor de Sucesos de Windows del sistema en el que el producto está instalado.

Puede utilizar el Windows Server Agent de VISUAL Message Center para monitorizar el Visor de Sucesos, para poder trabajar con los mensajes dentro de la SmartConsole de VISUAL Message Center.

En esta versión del producto, puede ejecutar cualquier número de chequeos de servicios en **redes locales o internet**, incluyendo:

- Chequear cualquier tipo de servidor – independientemente del sistema operativo o tipo de dispositivo
- Utilizar direcciones IP o DNS indistintamente, por ejemplo: mail.tango04.com o 127.0.0.0
- Servidores de email POP3:
 - Chequear la disponibilidad y tiempos de respuesta

- Chequear los accesos a cuentas de correo, perfiles de usuario y contraseñas
- Chequear el tamaño de las cuentas de correo, en Kb o número de mensajes
- Descargar Mensajes (redireccionándolos a la consola de VISUAL Message Center)
- Servidores de email SMTP:
 - Chequear la disponibilidad y tiempos de respuesta
 - Chequearlos accesos a cuentas de correo, perfiles de usuarios y contraseñas
 - Chequear el envío de mensajes para comprobar que el servicio SMTP funciona correctamente.
- Ciclo Completo
 - Envía mensaje utilizando SMTP
 - Recibe ese mensaje en POP3
- Comprobación de servicios de red, puertos y tiempos de respuesta en:
 - Servidores web (HTTP)
 - FTP
 - Telnet
 - Client Access
 - Aplicaciones de terceros (ERP, CRM,...)
- Realizar pings automáticamente a dispositivos de red como:
 - Impresoras
 - Routers
 - Subsistemas de disco
 - Almacenamiento SAN,...
 - Chequear disponibilidad, tiempos de respuesta,...
- Chequeo SNMP
 - Retorna cualquier variable SNMP de cualquier dispositivo que soporte SNMP
- Recepción de Tramas SNMP
 - Recepción de tramas SNMP desde cualquier dispositivo de red generador de Tramas

Para más información sobre SNMP, diríjase al apéndice A de este documento.

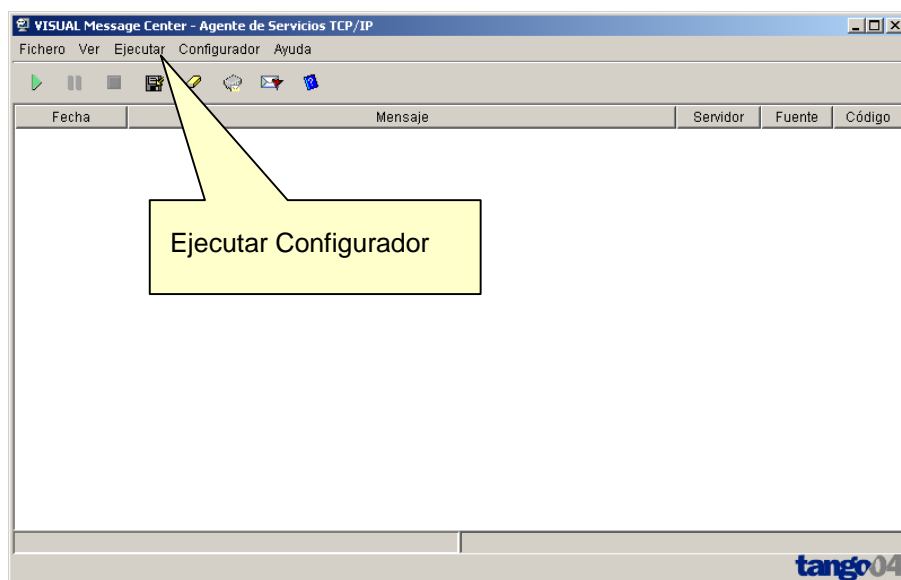
Cuando configura un chequeo, primero debe seleccionar el **servidor** que se va a chequear, y posteriormente definir el **tipo de chequeo** que quiere ejecutar en ese servidor.

3. Antes de Comenzar

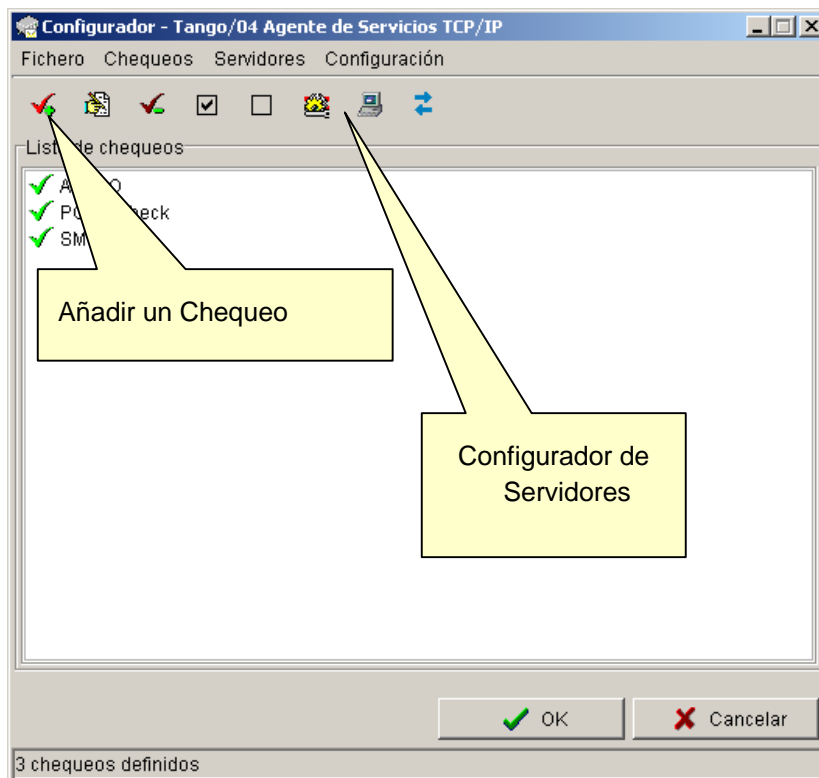
Deberá trabajar desde una consola (normalmente un PC Windows) con una conexión Internet o LAN. Si desea monitorizar dispositivos basados en Internet deberá trabajar con una conexión directa a Internet, por ejemplo, no podrá trabajar a través de un proxy. Debe ser capaz de hacer ping directo al dispositivo que desee monitorizar. Si tiene cualquier duda sobre la naturaleza de su acceso Internet o LAN consulte con su administrador de red.

3.1 Configuración de Servidores

En primer lugar seleccione **Ejecutar Configurator**.



Verá la siguiente pantalla:

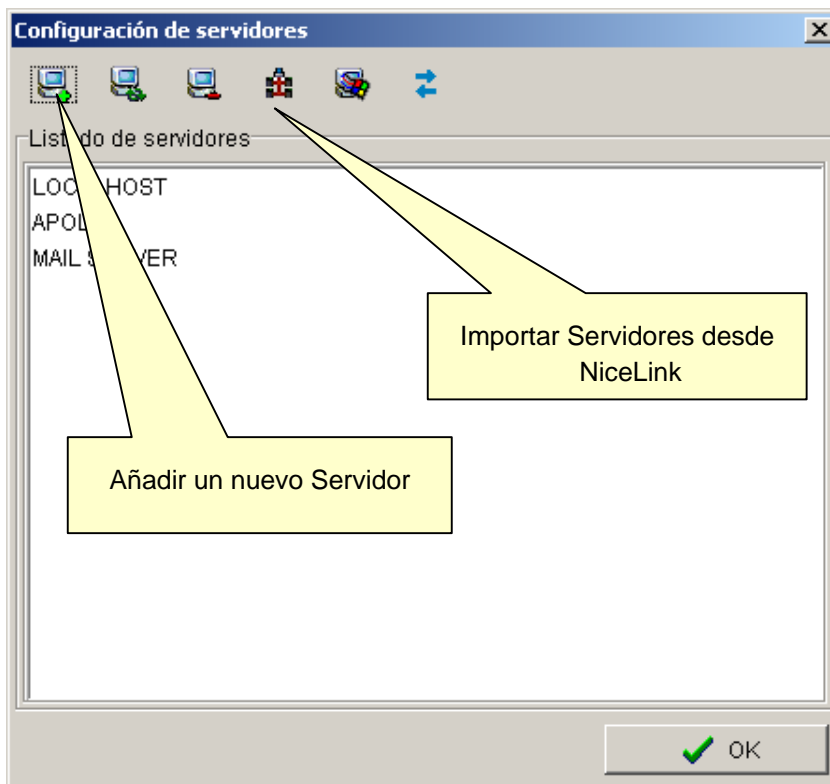


Seleccione la opción **Servidores**.

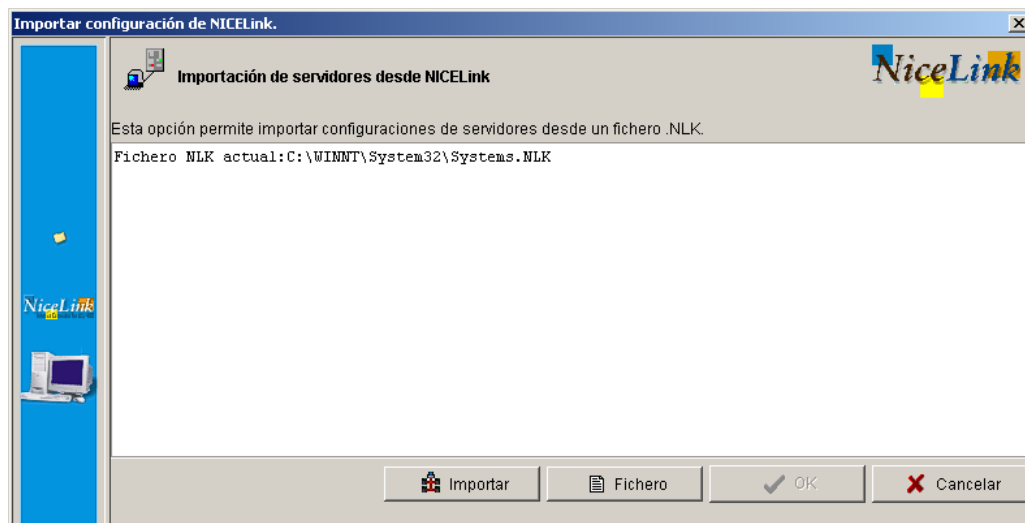
Aquí tiene tres opciones:

- Puede entrar los servidores manualmente
- Importar Servidores desde un archivo de definición de servidores de Windows
- Si ya tiene servidores configurados en NiceLink para trabajar con otros productos Tango/04, puede recuperarlos desde su archivo de configuración de NiceLink.

NOTA: TCP/IP SERVICES AGENT LE PERMITE CHEQUEAR CUALQUIER TIPO DE SERVIDOR INDEPENDIENTEMENTE DE LA PLATAFORMA O EL SISTEMA OPERATIVO.

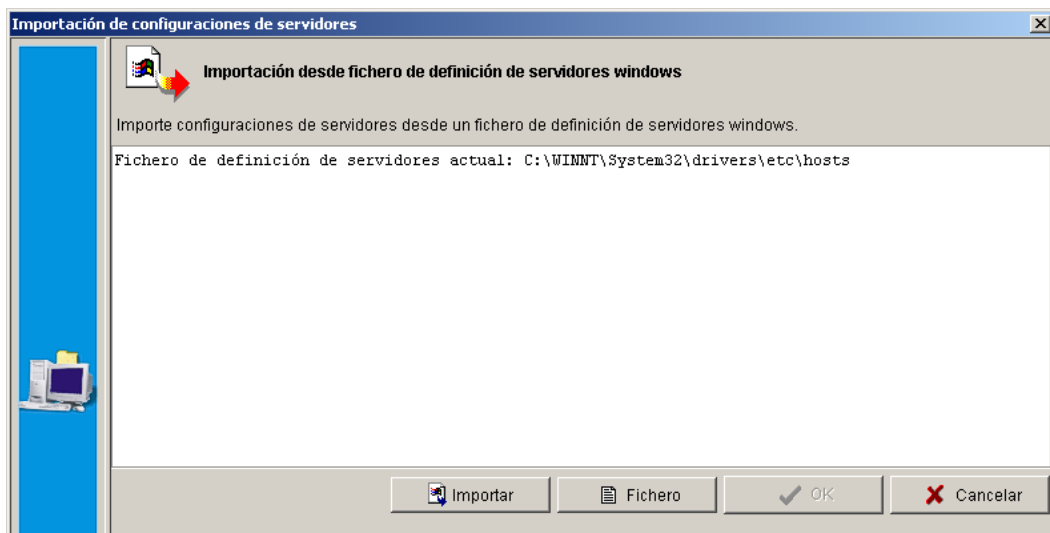


Importar desde NiceLink: pulse sobre el icono de NiceLink. Verá una pantalla como esta.



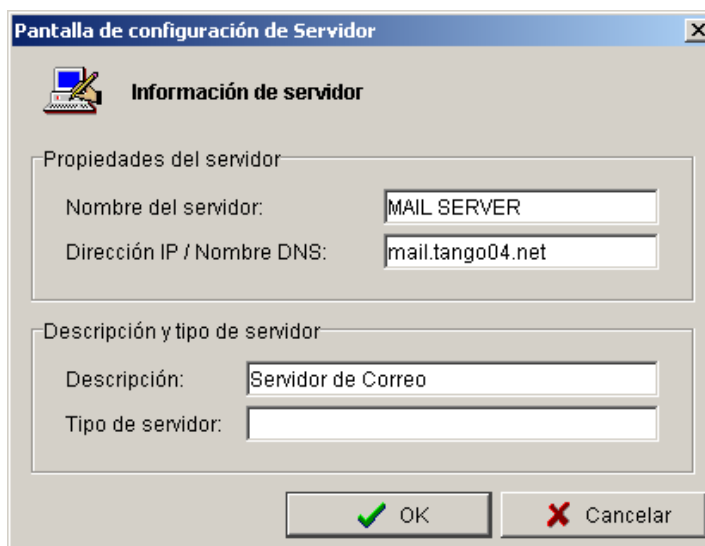
Se muestra el archivo de configuración de NiceLink por defecto. Si es correcto pulse "Importar". El estado de importación será mostrado. Si se descubren servidores duplicados, por ejemplo direcciones IP repetidas, será informado y no se importarán. Una vez que la importación se ha completado, tendrá todos los servidores configurados en NiceLink, con el nombre que tienen en NiceLink y la dirección IP o el nombre DNS. Pulse "OK" para salir.

Importar desde un archivo de definición de servidores Windows: pulse sobre el icono de Windows. Verá una pantalla como esta.



Se mostrará el archivo de definición de Servidores Windows por defecto. Es similar a la función de importación desde NiceLink; si el archivo mostrado es el correcto pulse "Importar".

Añadiendo nuevos servidores: puede añadir manualmente nuevos servidores. Entre el nombre del servidor (puede ser cualquier nombre que usted desee – utilícelo para identificar fácilmente el servidor), la dirección IP o nombre DNS, y una descripción del tipo de Servidor.

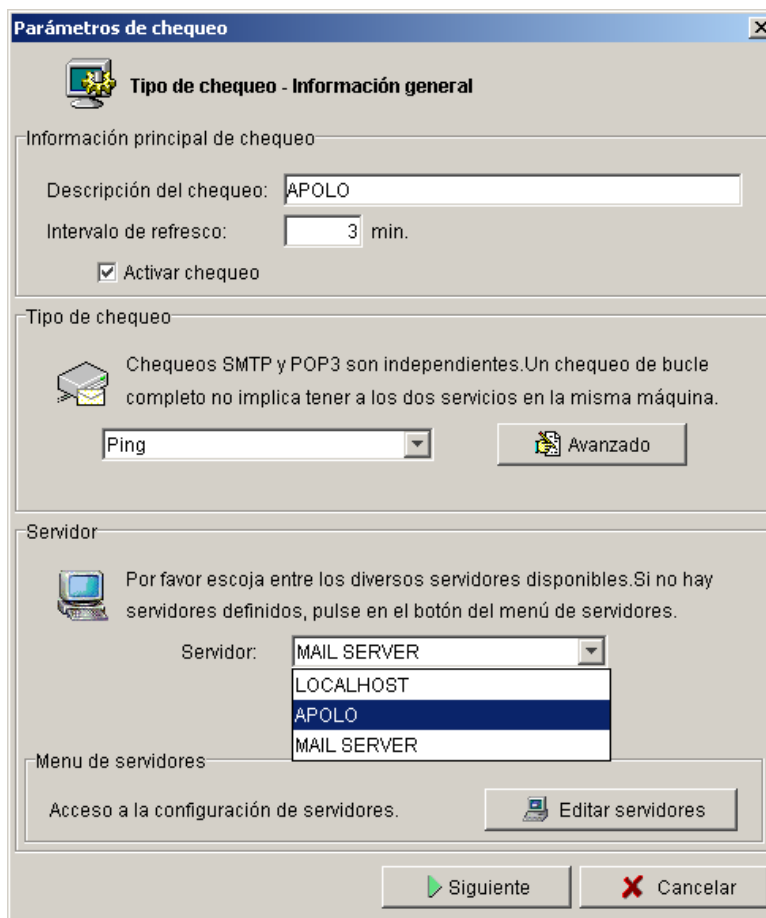


Pulse OK para salir de la **Configuración de Servidores** y regresar a la pantalla de Configuración.

3.2 Añadiendo Chequeos - Ping

Ya hemos descrito los diferentes tipos de chequeos que podemos ejecutar. Vamos a echar un vistazo a como configurar un chequeo.

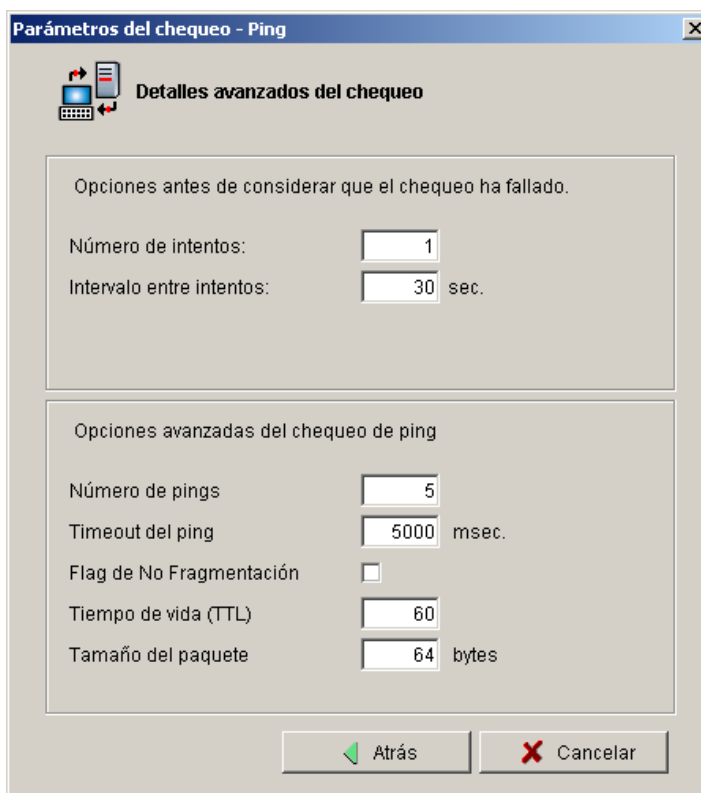
Pules el icono **Añadir nuevo chequeo**. Aparecerá el diálogo de parámetros de chequeo.



En este ejemplo simplemente vamos a ejecutar un ping en un dispositivo de nuestra red para asegurarnos que está disponible y para comprobar el tiempo de respuesta.

Vea en el ejemplo anterior que damos al chequeo un nombre para identificarlo, en este caso "Apolo". El intervalo de refresco es la frecuencia con la que ejecutaremos la acción de ping en Apolo.

A continuación seleccionamos el tipo de chequeo. En este ejemplo seleccionamos Ping. Veremos el resto de chequeos más adelante. Pulsando el botón **Avanzado** tenemos más opciones:



Mientras ejecutamos un ping, quizá queramos ajustar alguna tolerancia a fallos para el reporte de errores. En este caso, si detectamos un error, por ejemplo, no respuesta al ping, determinados que se vuelva a intentar tras 30 segundos. Sólo si se vuelve a producir el error tras el reintento reportará el error. Si desea recibir todos los errores sin reintentar, introduzca número de intentos = 0. Podemos configurar información más detallada del ping, como el número de pings, el timeout, tamaño del paquete y TTL si lo deseamos. De momento déjelo como está y pulse **Atrás**.

Ahora seleccione su Servidor desde la **lista de servidores**. También puede editar los servidores desde aquí. Seleccionamos el sistema Apolo que ya teníamos configurado.

3.3 Reglas Lógicas del Mensaje

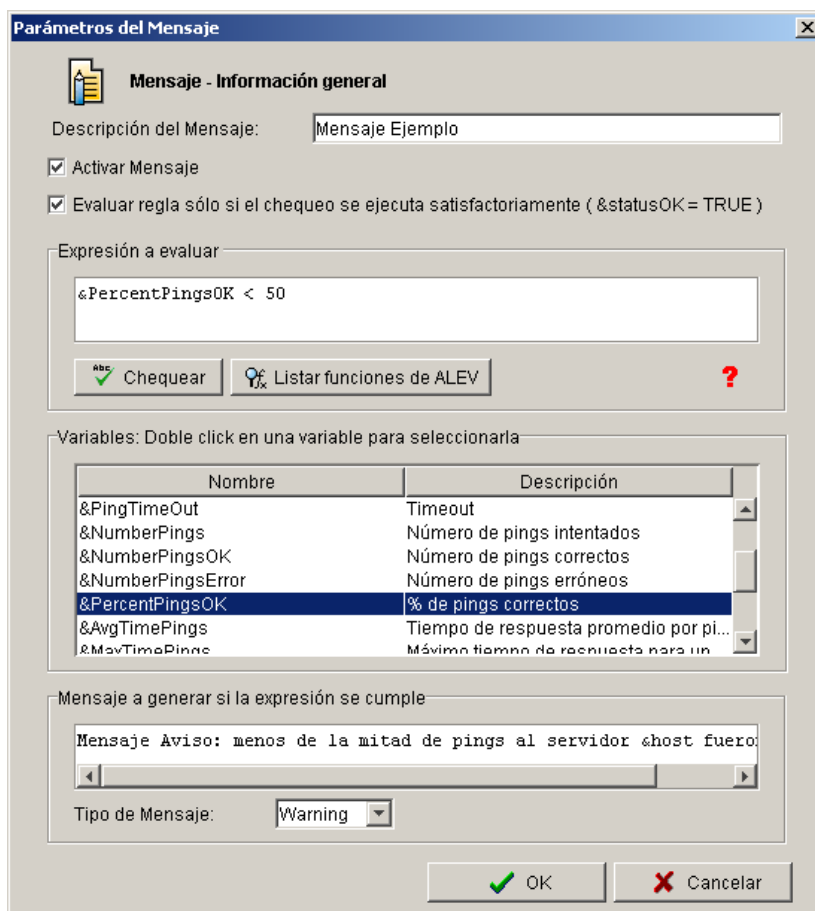
El botón **Avanzado**, no es la única opción disponible para configurar chequeos. También puede insertar condiciones lógicas contra las que se comparan la información procedente del chequeo, creando chequeos altamente específicos. Los mensajes resultantes pueden ser filtrados y actuar con mayor precisión en la consola VISUAL Message Center.

Para hacerlo, pulse **Siguiente**. Esto abrirá una pantalla que le proporciona información sobre la configuración de las condiciones de éxito o error de este chequeo. Una vez haya leído esta información, pulse el botón **Editar Expresiones** para abrir la pantalla de **Lista de Mensajes**:



Aquí puede configurar reglas de éxito o error para los mensajes ping, así como mensajes informativos para comunicarle si su servicio cumple los niveles de SLA. De esta manera, los mensajes son más fáciles de manejar en la consola de VISUAL Message Center para crear con precisión filtros de Business Views, Alarmas y Acciones. Estos tres mensajes aparecen por defecto: de cualquier forma, puede añadir, eliminar o editar reglas/mensajes desde esta pantalla, para que cumplan sus requisitos.

Por ejemplo, imagine que desea recibir un mensaje de Aviso si menos de la mitad de los pings son correctos. Puede crear reglas específicas que a cambio creen un mensaje específico en respuesta a un evento específico.



Para definir las condiciones y parámetros de sus mensajes Informativos, de Error, o de Éxito, necesita crear una expresión lógica contra la que se comparará el chequeo. Utilice el evaluador de expresiones lógicas ALEV para hacerlo. Pulse el icono de interrogación para más información sobre como crear expresiones lógicas en ALEV.

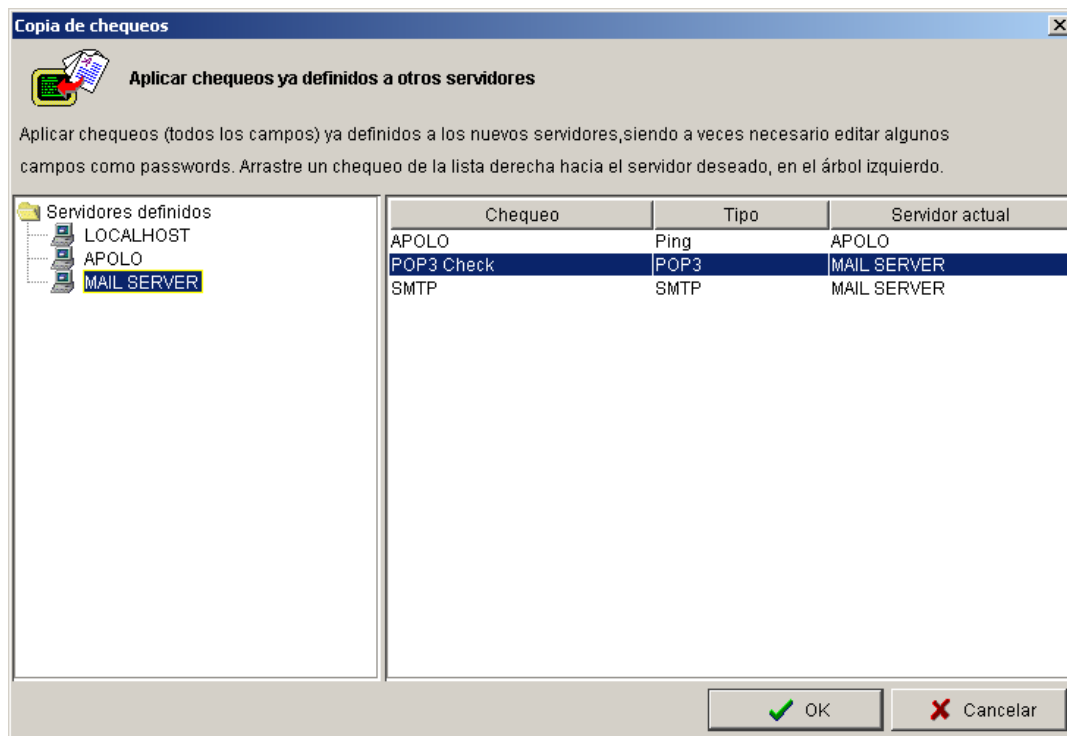
Puede utilizar las variables listadas y las funciones ALEV pulsando el botón Listar funciones de ALEV para crear la expresión lógica exacta que encaje con sus requerimientos. La expresión que encontrará por defecto en la pantalla de Ping SLA es la siguiente:

&PercentPingsOK < 50

Esto significa que si el tiempo promedio para Ping está por encima de tres segundos (3000 milisegundos) o menos de la mitad de ellos tienen éxito, recibirá un mensaje de aviso. Pulse el icono de interrogación para más información sobre como crear expresiones lógicas en ALEV.

Una vez que haya finalizado y comprobado la expresión para asegurarse que la sintaxis es la correcta, pulse **OK** en todas las pantallas para regresar a la pantalla de configuración. Allí podrá ver el nuevo chequeo en la lista.

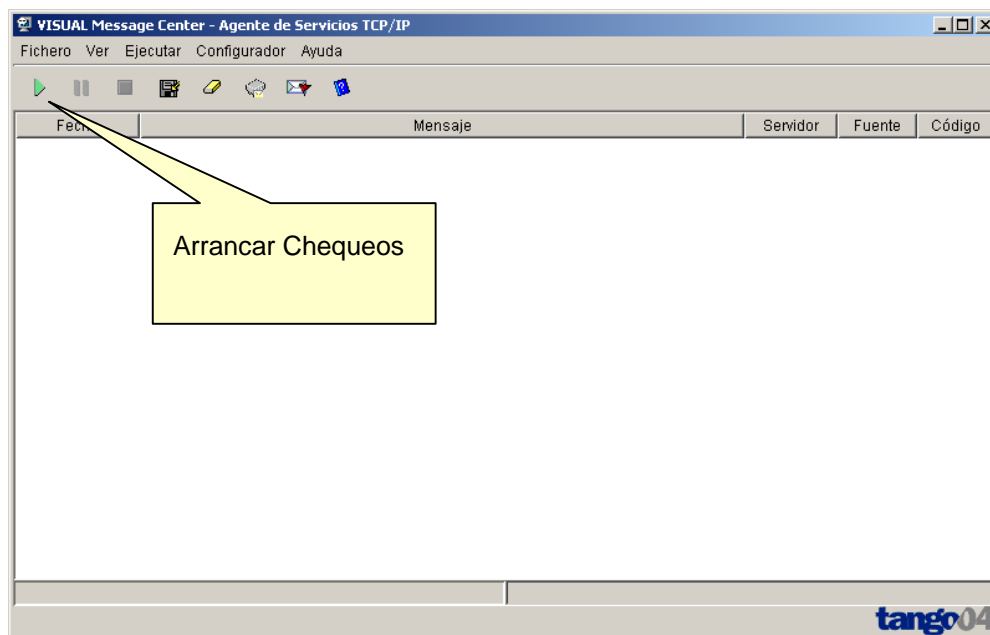
Desde aquí también podrá copiar el chequeo a cualquier Servidor configurado en su TCP/IP Service Agent. Simplemente pulse en el icono **Copiar Chequeos entre Servidores** para abrir la siguiente pantalla:



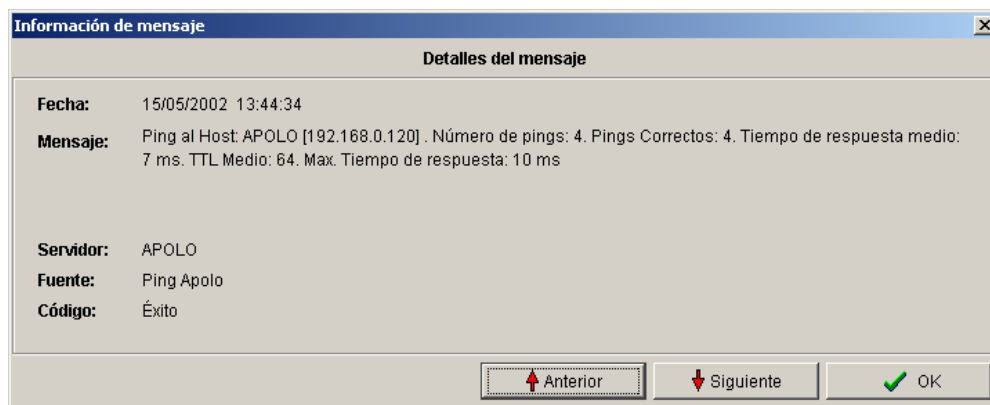
Para copiar el chequeo a otros servidores, seleccione el chequeo y arrástrelo al servidor que desee. Puede editar el chequeo con doble clic sobre él en el árbol de Servidores. Pulse **OK** para configurar la configuración.

Ahora está preparado para ver como trabaja el chequeo.

3.4 Arrancar Chequeos



El botón Play arranca los chequeos activados. El archivo de configuración se activa y comienza el chequeo, de acuerdo con los intervalos de refresco que haya configurado. Los mensajes recibidos por esos chequeos se muestran en la consola. Haga doble click en los mensajes para más información. Este es un ejemplo de ping con éxito. Fijese en la información del tiempo de respuesta:



En la consola, los mensajes se colorean de acuerdo con su tipo: informativo, éxito o error.

Puede seleccionar que tipo de mensajes desea ver en la consola seleccionando **Mostrar/Ocultar Mensajes** en el menú principal, o pulsando el icono **Seleccionar tipo de mensajes a mostrar**.

También puede seleccionar que tipo de mensajes deben ser redireccionados al Windows Event Log en **Configuración/Propiedades/Output**. Vea el apartado **Opciones Generales de Configuración** para más información.

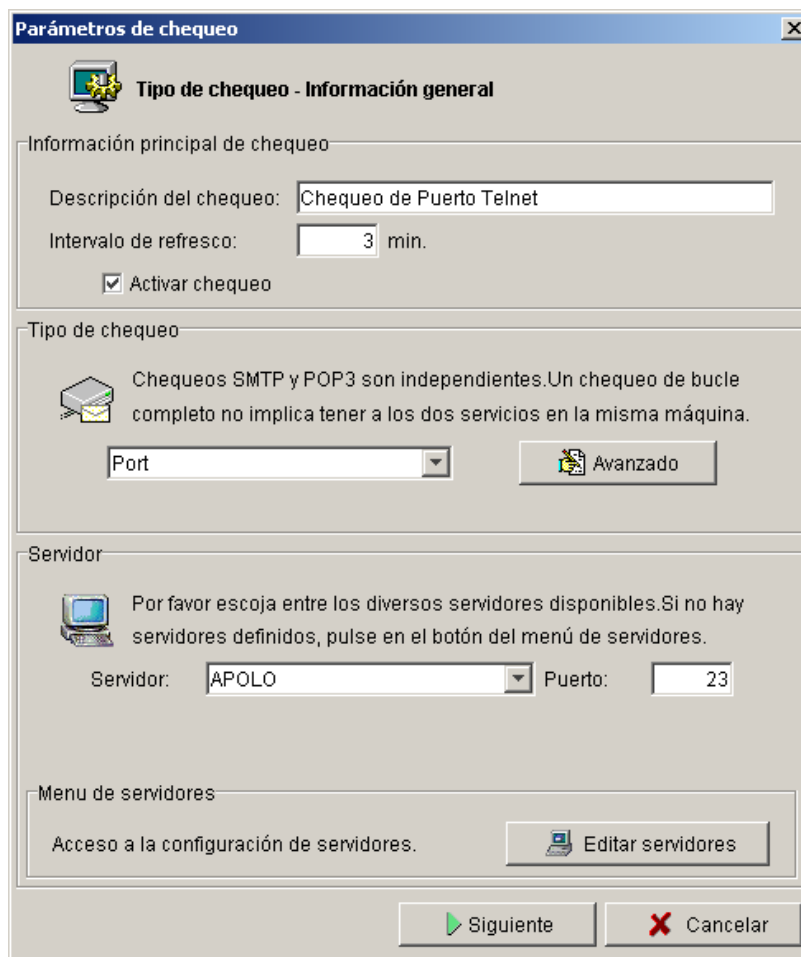
Ha podido ver como configurar un proceso ping sencillo, para hacer ping periódicamente a uno o más servidores y ha visto que la gran cantidad de posibilidades disponibles utilizando ALEV. Puede detener el chequeo en cualquier momento utilizando el botón Stop de la consola.

3.5 Diferentes Tipos de Chequeo

Ahora podemos comenzar a examinar el resto de tipos de chequeo. Ya hemos visto el chequeo de ping. El resto de funciones de chequeo disponibles son:

- Chequeo de puerto
- POP3
- SMTP
- Loop Email (Ciclo Completo de email)
- SNMP
- Traps SNMP

3.5.1 Chequeo de Puerto



La función de chequeo de puerto va un paso más allá que un Ping – actualmente le permite chequear que un puerto específico en un servidor concreto está disponible.

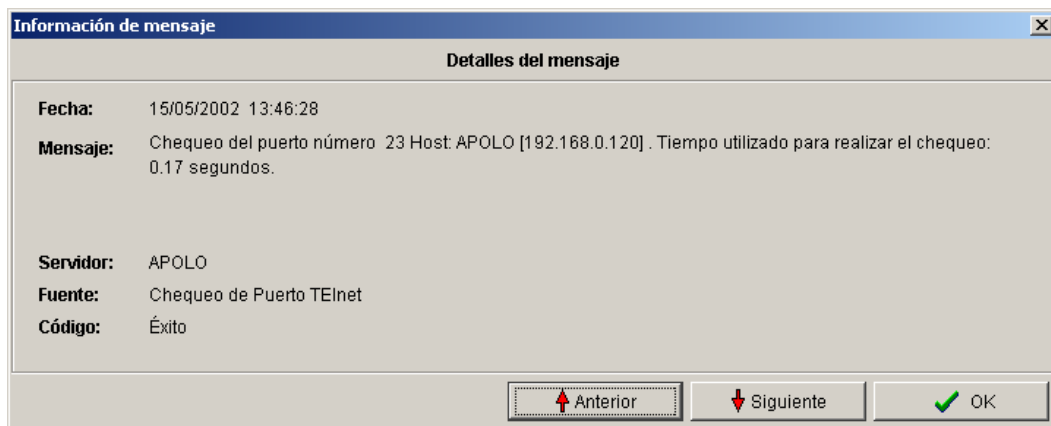
La configuración es simple, escoja el intervalo de refresco, seleccione el tipo chequeo “Puerto” y especifique el servidor y el número de puerto a chequear. Cada chequeo puede chequear un puerto.

En el ejemplo anterior estamos chequeando el puerto Telnet: 23, pero puede chequear cualquier puerto, por ejemplo, FTP: 21; HTTP: 80; Client Access sign-on server: 8476; Client Access server mapper: 449... Si tiene alguna duda sobre un número de puerto usado por un servicio específico TCP/IP consulte con su administrador de red.

Una vez haya realizado la configuración, puede pulsar **Finalizar**. Volviendo a la consola, lo que le permitirá arrancar este chequeo...aunque haya chequeos actualmente en ejecución, este nuevo chequeo se añadirá automáticamente al ciclo de chequeo sin necesidad de parar y arrancar de nuevo.

A continuación puede ver un mensaje de chequeo de puerto. Este es un mensaje de “Éxito”. Fíjese en la información del tiempo de respuesta. Esta puede ser

utilizada dentro de la consola de VISUAL Message Center para desarrollar alarmas de umbral, o puede generar mensajes de aviso o error cuando el Tiempo de Respuesta es mayor que el especificado.



También puede chequear puertos que no deben ser abiertos y hacer saltar alarmas si son abiertos, configurando `&statusOK = TRUE` como condición lógica del mensaje de error.

3.5.2 Chequeo POP3

Ahora seleccione un chequeo POP3. Esto nos permitirá controlar la disponibilidad, operatividad y contenido de cualquier buzón de correo POP3.

Seleccione el chequeo POP3:

The screenshot shows a Windows-style dialog box titled "Parámetros de chequeo" with a close button (X) in the top right corner. The main title is "Tipo de chequeo - Información general".

Información principal de chequeo

Descripción del chequeo:

Intervalo de refresco: min.

Activar chequeo

Tipo de chequeo

Chequeos SMTP y POP3 son independientes. Un chequeo de bucle completo no implica tener a los dos servicios en la misma máquina.

Servidor

Por favor escoja entre los diversos servidores disponibles. Si no hay servidores definidos, pulse en el botón del menú de servidores.

Servidor: Puerto:

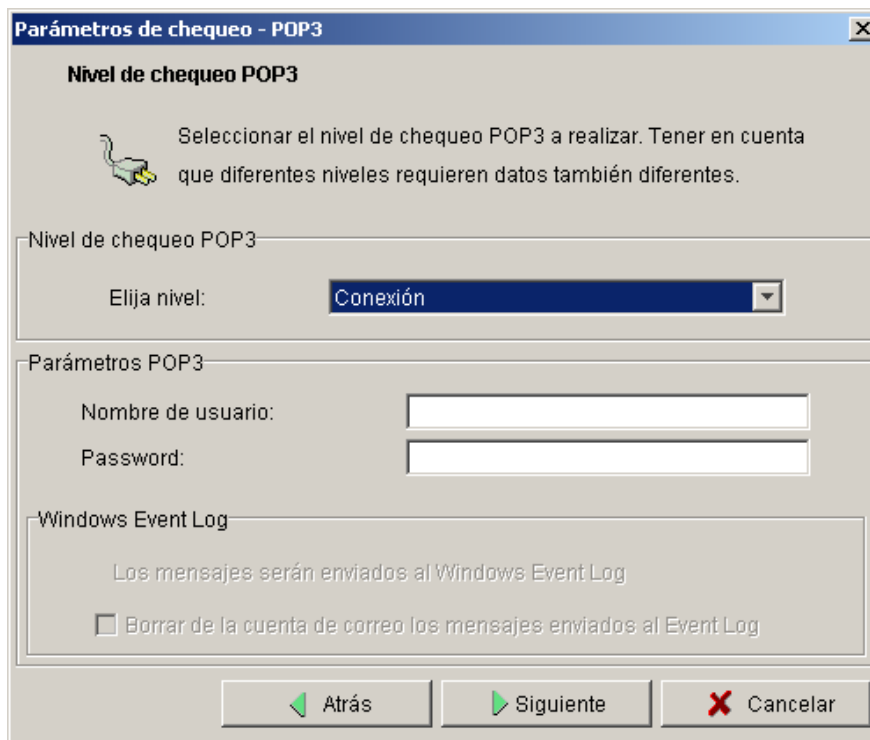
Menu de servidores

Acceso a la configuración de servidores.

At the bottom, there are two buttons: and .

Asegúrese que selecciona un servidor que es un servidor de correo POP3. Puede usar una dirección IP o un nombre DNS.

Fíjese que aparece la opción "Siguiete". Pulse sobre el botón para ir a opciones avanzadas de configuración.



Aquí puede determinar el nivel de chequeo:

- Conexión: chequea disponibilidad y tiempos de respuesta
- Chequear acceso a la cuenta de correo: perfil de usuario y contraseña
- Redirigir mensajes al Event Log: y en consecuencia a la consola de VMC

Las opciones en la parte inferior estarán disponibles o no dependiendo de la opción escogida.

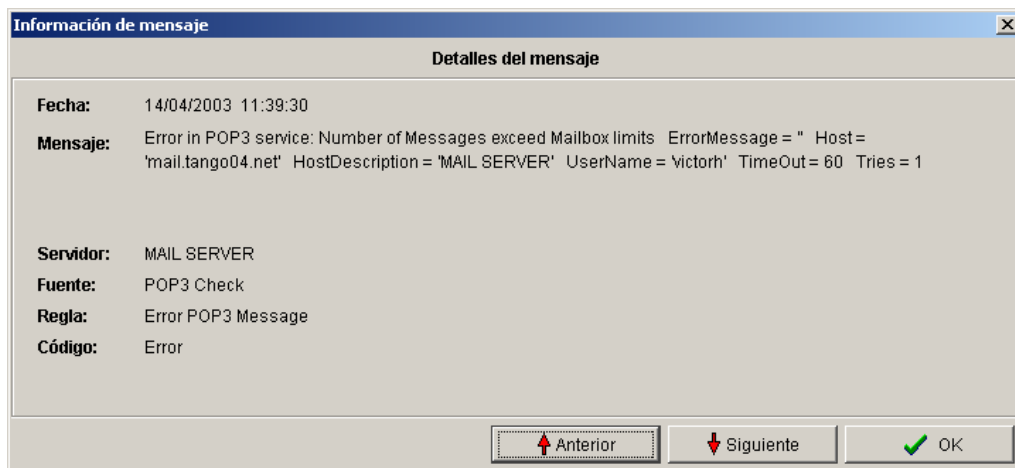
Para comprobar la conexión, no necesita entrar ningún campo más. Simplemente chequea el acceso al buzón de correo y le indica el tiempo de respuesta.

Cuando chequea el acceso a la cuenta de correo, deberá entrar el nombre de usuario y la contraseña de la cuenta de email. Esto chequeará que ese usuario es válido, que el servidor mail válida los perfiles de usuario correctamente y le dirá el tamaño del buzón y el número de mensajes, retornando estos valores como variables. También recibirá información del tiempo de respuesta.

Para redirigir mensajes al Event Log, seleccione la opción **Redirigir Mensajes al Event Log**. Esto descarga el texto de todos los mensajes en el buzón y los envía al Event log de Windows como el texto de un evento. Estos mensajes pueden ser controlados utilizando VISUAL Message Center Windows Agent. Esta característica es útil si tiene algún dispositivo que envía email para notificar eventos. Cada vez un mayor número de dispositivos en el mercado desde routers hasta impresoras, utilizan el email para reportar eventos. Esta característica le permite controlar esos dispositivos utilizando VISUAL Message Center.

Pulsando Siguiente, entrará en el área de configuración de condiciones lógicas ALEV. Aquí podrá definir reglas para chequear, por ejemplo, el tamaño del buzón de correo y el número de mensajes. Por ejemplo, puede definir la siguiente regla para un mensaje de Error:

Si TCP/IP Services Agent detecta que hay más de 500 mensajes en el buzón de correo, mostrará los mensajes de reporte como "Error". A continuación puede ver un ejemplo de un mensaje de chequeo de tamaño de cuenta de correo:



3.5.3 Chequeo SMTP

El chequeo SMTP le permite asegurarse que su servidor SMTP le permite enviar mensajes de email. Las opciones disponibles son:

- Chequeo de conexión: simplemente chequea que el puerto SMTP está disponible
- Conexión y Acceso a la cuenta de correo: chequea que el puerto está disponible y accede utilizando un perfil de usuario y una contraseña (si es aplicable)
- Chequeo Completo (enviar mensaje) – Envía un mensaje de prueba y comprueba si se ha enviado correctamente

Todas las opciones dan información del tiempo de respuesta. A continuación puede ver un ejemplo de Chequeo Completo:

Parámetros de chequeo - SMTP

Nivel de chequeo SMTP

Seleccionar el nivel en que el chequeo SMTP se realizará. Tener en cuenta que diferentes niveles requieren datos diferentes.

Nivel de chequeo SMTP

Elija nivel: Chequeo completo (enviar mensaje)

Parámetros SMTP

Nombre de usuario: test

Password: *****

Nombre del remitente: Victor

Dirección del remitente: test@tango04.net

Enviar mensaje a: test@tango04.net

Opciones del mensaje

Atrás Siguiente Cancelar

El nombre de usuario y la contraseña son aquellos necesarios para enviar el mensaje. El nombre y dirección del remitente son los que aparecerán en el email de prueba enviado. Enviar mensaje a es la cuenta a la que se envía el mail de prueba. Es recomendable crear una cuenta de prueba si desea hacer este chequeo.

Seleccione Opciones del Mensaje para introducir el asunto y el cuerpo del mensaje:

Opciones del mensaje

Opciones del mensaje

Propiedades del mensaje que usa el chequeo SMTP para comprobar si el servicio está funcionando correctamente.

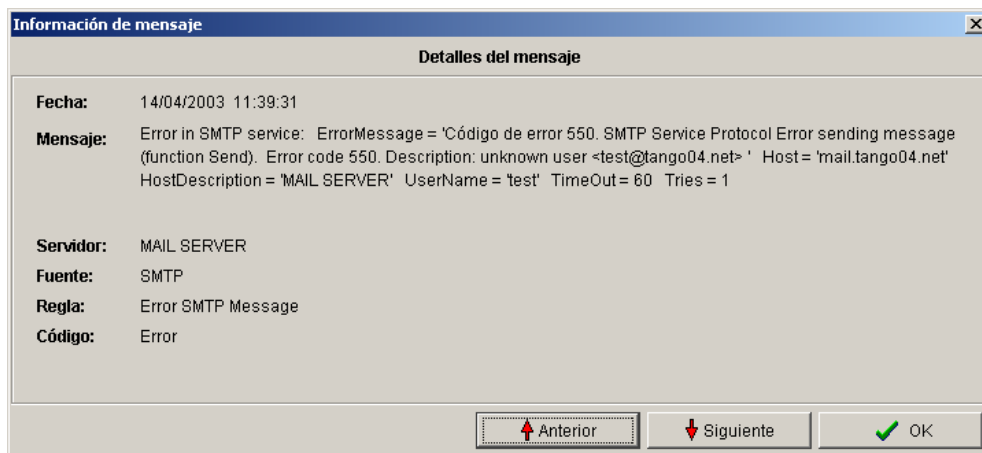
Asunto y cuerpo

Asunto: Test SMTP

Cuerpo: Este mensaje comprueba la operatividad de nuestro servidor SMTP

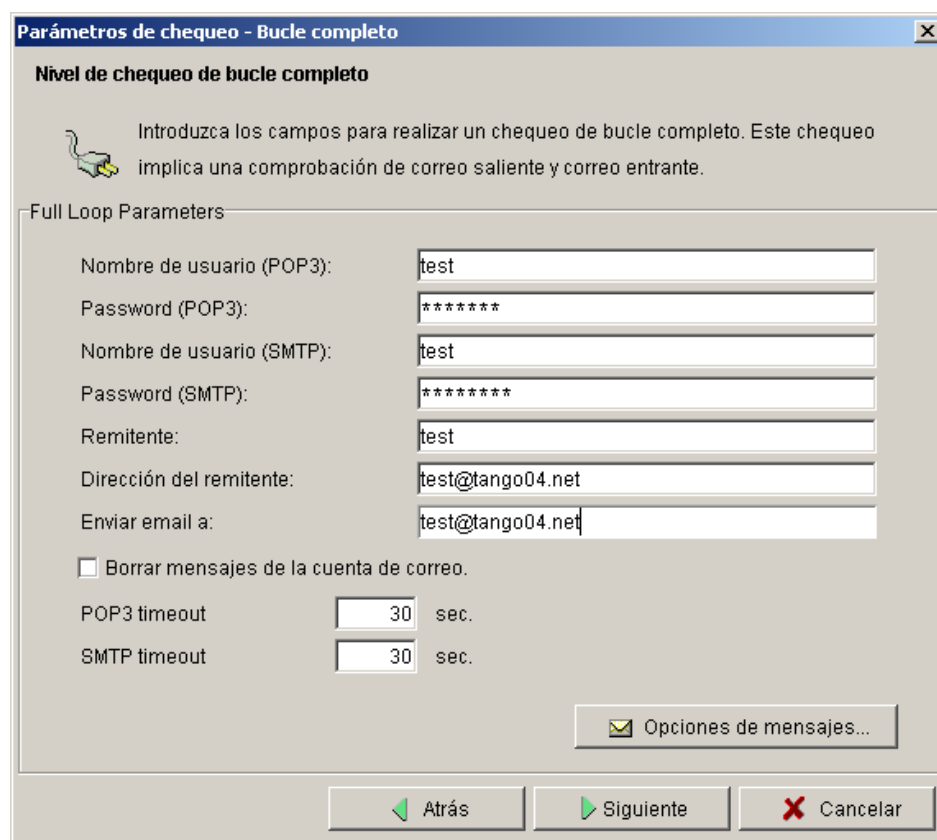
OK

Este mensaje será enviado periódicamente a la dirección de correo especificada. Si el mensaje no puede ser enviado correctamente aparecerá un mensaje de error similar a este:



3.5.4 Loop Email: POP3 y SMTP

La opción loop email combina los chequeo POP3 y SMTP, permitiéndole chequear un ciclo completo de envío / recepción de email.



El chequeo loop email, enviará y recibirá un mensaje de email desde una cuenta de correo. Fíjese que puede seleccionar el borrado de los mensajes de la cuenta de correo – esto asegura que su buzón no se llene con los mensajes de prueba. El resto de opciones son las mismas que en los chequeos POP3 o SMTP.

Un chequeo loop email es recomendable para probar su servicio de email, ya que permite tener información completa de respuesta tanto del envío como de la recepción. A partir de ahora podrá conocer al instante si existe una ralentización del servicio de email en su empresa.

3.6 SNMP

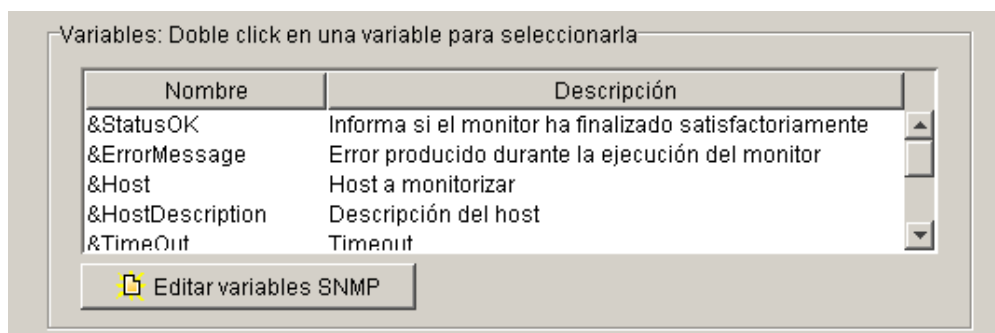
TCP/IP Services Agent permite la creación de monitores SNMP que retornan simples variables desde cualquier dispositivo que soporte SNMP (como routers, servidores y muchos otros). Por defecto, cuando configura un nuevo monitor SNMP, se crea una regla que chequea si el dispositivo está ejecutando el servicio SNMP y que retorna la variable Nombre del Sistema (que corresponde al número OID 1.3.6.1.2.1.1.5.0).

Normalmente, no es suficiente para saber si SNMP está funcionando, sino que necesita recuperar también algunos valores SNMP del dispositivo. Este protocolo tiene unas características particulares (especialmente los OID) con las que deberá familiarizarse antes de configurar chequeos. Si desconoce el funcionamiento de SNMP y Tramas SNMP, por favor, diríjase al Apéndice A de este documento, y después continúe con esta sección.

Cuando selecciona un chequeo SNMP, la ventana cambiará para permitirle seleccionar el servidor, puerto SNMP y SNMP community. Si su dispositivo SNMP utiliza una community con un valor distinto del Standard "public", introdúzcalo aquí para que las comunicaciones con TCP/IP Services Agent tengan éxito.

Pulsando **Siguiente** llegará a la configuración de Reglas de Mensaje ALEV, ofreciendo la extensión de protocolo de comunicaciones SNMP (p.e. puede recibir cualquier información que desee desde dispositivos si están correctamente configurados). El uso efectivo de ALEV en los chequeos SNMP es muy importante. Tiene posibilidades ilimitadas de enriquecer sus mensajes con información del estado del dispositivo, pero necesitará configurar sus mensajes para que organicen esta información de una manera accesible.

ALEV le permite hacerlo. Cuando selecciona una de las reglas (Error, Éxito o Información) o crea su propia regla, verá que bajo la lista de variables aparece el botón **Editar Variables SNMP**.



Pulsando el botón se abre una ventana que contiene una lista de las variables que ha creado de acuerdo a sus configuraciones SNMP. Para crear una nueva variable, pulse **añadir** para abrir la ventana Añadir Nueva Variable SNMP:

Añadir variable SNMP

Añadir nueva variable SNMP

Nombre

Descripción

Introduzca el OID en su forma simbólica (textual) o en su forma numérica.
Recuerde que si quiere usar un OID textual, el MIB donde esté definido debe estar en el directorio /MIBS.

Oid

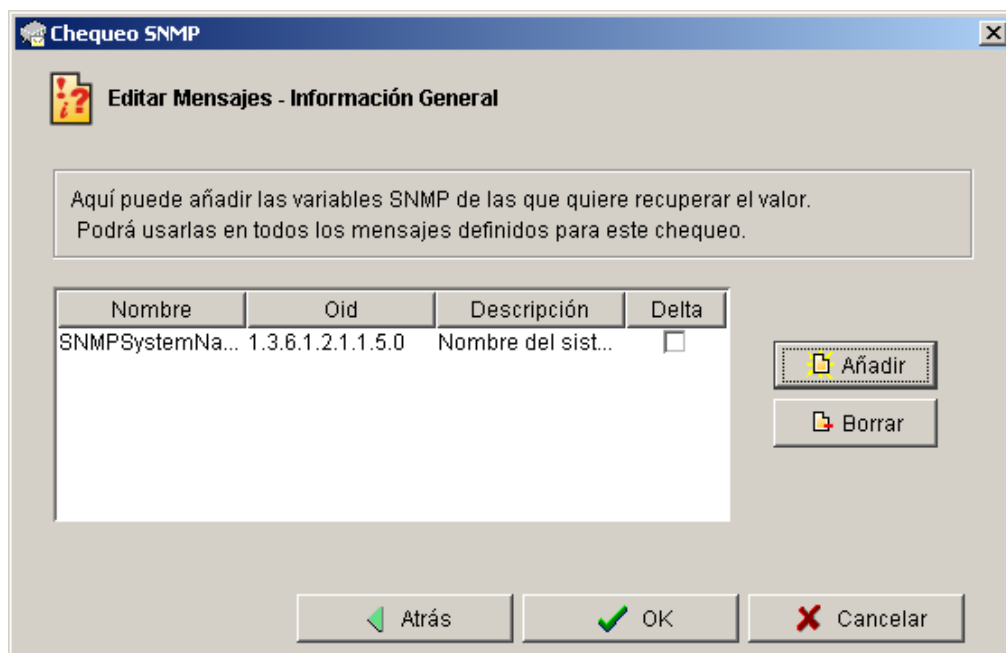
Índice (Use 0 para valores escalares)

En esta pantalla, se puede añadir una variable SNMP definiendo su nombre, su descripción y su OID (el “identificador de objetos” en el protocolo SNMP). El OID puede especificarse numéricamente (1.3.6.1.2.1.3.1.5.0) o mnemónicamente: *iso.org.dod.internet.mgmt.sysName.0*. Sabemos que el OID correspondiente es “1.3.6.1.2.1.25.2.2”, por lo que lo introducimos, junto a una explicación de que es lo que hace.

El OID puede introducirse como texto o como cadena numérica. Puede acceder a la biblioteca de referencia de OIDs pulsando el botón **Ver MIBS definidos**, que abre un buscador que le dice que MIBS están precargados en la memoria y le permite ver la descripción de un OID específico. Diríjase al Apéndice A para más información sobre OIDs definidos.

Si está entrando un valor OID cuyo archivo MIB no se encuentra en los archivos del agente, necesitará introducir el OID numéricamente. Si desea introducirlo como texto, primero deberá copiar el archivo de texto MIB en el subdirectorio “MIBS” para que el producto pueda traducir el texto a un OID numérico.

Una vez haya completado los campos de esta ventana, pulse **OK** para regresar a la ventana de Información General de variables SNMP.



Aquí aparecerán todas las variables SNMP personalizadas.

Seleccionando la opción **Delta** podrá comparar diferentes resultados SNMP, creando un mensaje basado en el estado actual del dispositivo comparado con el estado previo. Delta sólo funciona variables de tipo "contador". Esto es útil, por ejemplo, si queremos medir el número de bytes recibidos por un dispositivo. Un valor sencillo puede decirnos cuantos bytes han sido enviados desde que la máquina se arrancó, mientras que el valor Delta puede darnos información más relevante sobre los datos intercambiados desde la última medición.

Pulse **OK** cuando haya finalizado para regresar a la pantalla ALEV.

Una vez en ella, puede utilizar las nuevas variables para crear mensajes sobre sus dispositivos. Y gracias a la potencia de SNMP para comunicar prácticamente cualquier cosa a su servidor, ahora puede extraer información que desee de sus dispositivos y procesarla con la consola de VISUAL Message Center.

3.7 Receptor de Traps SNMP

La opción Traps SNMP le permite recibir y procesar Traps en TCP/IP Service Agent y redirigirlas a VISUAL Message Center.

Las SNMP Traps son alarmas enviadas desde un dispositivo a un servidor receptor utilizando protocolo SNMP. Para utilizar traps SNMP, primero deberá configurar sus dispositivos para enviar traps al TCP/IP Services Agent a la dirección IP en la que está instalado el Agente. El Agente podrá entonces, convertir cualquier Trap enviada desde un dispositivo a un mensaje de texto que podrá ser procesado en la consola de VISUAL Message Center.

Cuando selecciona Receptor de Traps SNMP, podrá seleccionar Traps desde todos los servidores o simplemente desde un servidor específico. Pulsando **Siguiente** llegará a la siguiente pantalla:

Parámetros de chequeo - SNMP Trap

Configuración de Trap SNMP

Seleccione el tipo de trap que quiere recibir. Si selecciona CUALQUIER trap, recibirá de todos los tipos.

- ColdStart (0) - Enviado cuando el agente SNMP se inicia.
- WarmStart (1) - Enviado cuando el agente SNMP se reinicia.
- LinkDown (2) - Enviado cuando el agente SNMP detecta un fallo en alguno de sus links de comunicación.
- LinkUp (3) - Enviado cuando el agente SNMP verifica que alguno de sus links de comunicación se ha restablecido.
- AuthenticationFailure (4) - Enviado cuando el agente SNMP recibe una comunidad inválida en un mensaje SNMP.
- EgpNeighborLoss (5) - Enviado cuando el agente SNMP detecta se ha perdido la conexión con un vecino EGP.
- EnterpriseSpecific (6) - Designa un trap específico de una empresa.

Recibir cualquier trap

Tipo de trap que quiere recibir

Recibir cualquier "enterprise trap"

Oid del trap que quiere recibir

Esta pantalla muestra seis Traps SNMP pre-configurados, y la opción **EnterpriseSpecific**, que es probablemente la que le resultará de mayor interés. Las traps EnterpriseSpecific son aquellas que haya configurado particularmente entre su servidor y sus dispositivos. Introduciendo aquí su OID, creará un chequeo para sus traps específicas. De nuevo, esto significa que pueden ser procesadas y utilizadas por la consola de VISUAL Message Center, con lo que sus traps se convierten en algo más que un simple aviso: ahora pueden utilizarse para que se ejecute un proceso automático para resolver un problema.

Desde luego, puede crear chequeos de traps SNMP genéricos simplemente seleccionando **Recibir cualquier trap**. Una vez haya completado esta ventana, pulse **Siguiente** para regresar a la ventana Editar Mensajes, y desde allí configure las condiciones lógicas de su chequeo de trap SNMP. Como con todos los demás chequeos, dispone de un mensaje de Éxito y de Error, pero puede editar o añadir los que necesite.

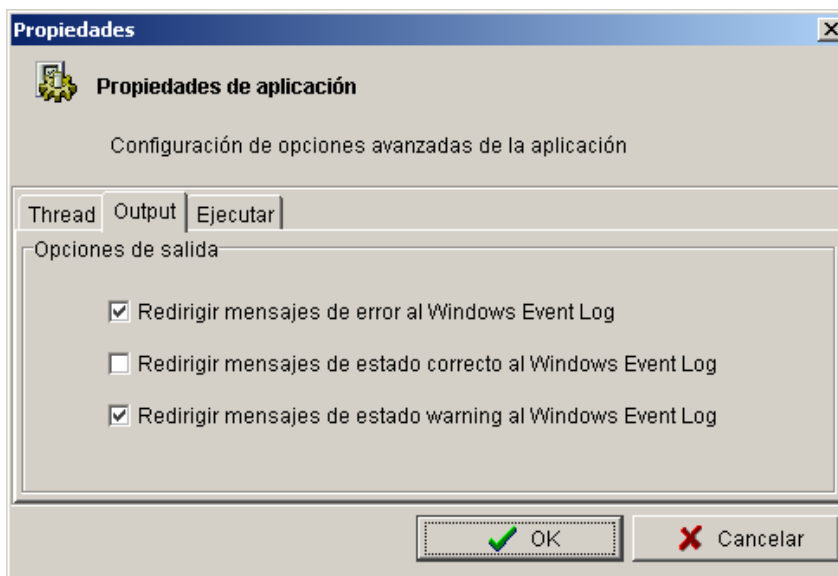
4. Opciones de Configuración generales

4.1 Integración con VISUAL Message Center: Redireccionar Mensajes al Event Log de Windows:

Todos los errores generados por el TCP/IP Services Agent pueden ser redirigidos al Event Log de Windows, con lo que pueden ser leídos por otras aplicaciones, incluyendo la consola de VISUAL Message Center. Cuando redirecciona mensajes al Event Log de Windows, se enriquecen con variables extra, algunas de las cuales no son visibles en el Event Log, y sólo son accesibles cuando los mensajes llegan a VISUAL Message Center. Las variables son:

- VAR1: El mensaje que aparece en el Event Log
- VAR2: El sistema origen que originó el mensaje
- VAR3: El nombre/identificador del chequeo que produjo el mensaje
- VAR4: Nombre de la regla que generó el mensaje

Para configurar esta opción, vaya al **configurador de Chequeos**, seleccione el menú de **Configuración** y la opción **Propiedades**.



La pestaña Output le ofrece la opción de seleccionar que tipo de mensajes redirigir al Event log de Windows. Una vez marque los que desea, todos los mensajes de ese tipo serán enviados al Event Log del sistema en el que tenga instalado el producto.

Ahora podrá utilizar el Windows Agent para monitorizar el Event log y ver esos mensajes desde la consola de VISUAL Message Center. Podrá usar todas las funcionalidades de alarmas y automatización, para mantenerse informado y reaccionar rápidamente a problemas en sus servicios TCP/IP.

4.2 Ejecutar chequeos automáticamente

Puede seleccionar que TCP/IP Services Agent ejecute todos los chequeos automáticamente cuando se arranca el producto. Para ello vaya a **Configuración – Propiedades** y seleccione la opción que aparece en la pestaña **Ejecutar**.

4.3 Ejecutar TCP/IP Services Agent como un Servicio

Puede configurar TCP/IP Services Agent para que se ejecute como un servicio Windows con lo que podrá automatizar la monitorización de servicios de red. Para ello, desde el menú Inicio de su escritorio, vaya a **Programas – TCP/IP Services Agent – Servicio**. Aquí tiene la opción **Instalar TCP/IP Services Agent como Servicio de Windows**. El agente se ejecutará como un servicio a partir de la próxima vez que la máquina se reinicie o el agente se vuelva a arrancar.

También existe la posibilidad de ejecutar TCP/IP Services Agent como un servicio sin necesidad de abrir la consola una vez que esté completamente configurada, automatizando de forma efectiva el proceso completo de monitorización. Para ello, desde Servicios, pulse el botón derecho en TCP/IP Services Agent como Servicio de Windows y seleccione **Deseleccionar – Conectar - Permitir al Servicio Interactuar con el Escritorio**. El Agente se ejecutará automáticamente, aunque si desea cambiar cualquier parte de la configuración, deberá lanzar la consola de forma normal desde el menú **Inicio – Programas**.

NOTA: NECESITARÁ WINDOWS 2000 O POSTERIOR INSTALADO COMO SISTEMA OPERATIVO DE SU PC PARA EJECUTAR ESTA OPCIÓN CORRECTAMENTE.

5. Apéndice A: Utilizando el nuevo agente SNMP

El Agente SNMP es más complejo que el resto de agentes de TCP/IP que son auto-explicatorios. Mientras que la Guía de configuración de TCP/IP Services Agent se centra en cómo configurar el agente SNMP, este apéndice entra más al detalle respecto a la funcionalidad y a la utilidad del SNMP.

5.1 Conceptos Básicos

En esta sección, usted aprenderá lo que hace el agente SNMP y comprenderá cómo trabaja. El protocolo SNMP está diseñado para centrarse en la monitorización básica de dispositivos de red.

El protocolo SNMP permite al usuario:

- Recuperar ciertos valores de un dispositivo (get).
- Modificar Valores SNMP en el host: se utiliza para la configuración remota (set). La configuración de muchos de estos dispositivos se puede cambiar con la alteración de ciertos valores usando SNMP.
- Generación/recepción de Traps (generación/recepción de traps de alarma: alarmas que llega de forma asíncrona del dispositivo monitorizado y que se envían a uno o varios gestores SNMP).

Hay varias versiones de SNMP. La más común es la versión 1, no obstante. Ésta sólo define un tipo de "contraseña" llamada "comunidad" en la terminología SNMP. Por defecto tiene el ajuste "público" para permitir la lectura de datos (get) y "privado" para la escritura (set).

En general, el puerto TCP/UDP 161 se utiliza por el servidor SNMP en la máquina monitorizada y el puerto TCP/UDP 162 se utiliza en el receptor de la trap.

La información recuperable se organiza jerárquicamente utilizando Management Information Bases (MIBs). Las descripciones de las MIBs se guardan en archivos de texto, que incluyen información sobre los campos (tales como nombre, tipo, y localización). Generalmente, la extensión para un archivo MIB es .mib.

Hay MIBs para muchos valores estándar, no obstante SNMP permite la incorporación de definiciones propietarias que le permiten aumentar infinitamente la cantidad de datos a recuperar. Para asegurarse de que las extensiones funcionan, la máquina monitorizada solamente tiene que tener la "extensión" instalada, de modo que sepa cómo recuperar los nuevos datos. Cuando una empresa necesita definir una nueva estructura dentro del árbol de MIBs, solicita un "nodo" del árbol jerárquico de IANA (Internet Assigned Numbers Authority), y a partir de ese momento en el nodo puede ser utilizado como raíz para todos los nuevos datos que sean requeridos por esa empresa.

Cada uno de los posibles valores en el árbol de MIBs es identificado empezando desde el nodo raíz hacia abajo por el árbol. En el siguiente ejemplo, usted continuaría hacia abajo por el árbol hasta llegar al nodo que contiene el valor que se quiere monitorizar:

```
iso(1).org(3).dod(6).internet(1).mgmt(2)...
```

Esta identificación se llama un OID (identificador del objeto) y se puede expresar tanto en numérico (1.3.6...) como formato de texto (iso.org.dod...). En realidad, el OID se envía siempre al dispositivo monitorizado en formato numérico; utilizar el formato de texto simplemente lo hace más legible para el usuario. Otra incidencia de menor importancia con OIDs en formato de texto es poder traducir el texto a formato numérico, el agente de TCP/IP debe tener acceso a las definiciones del MIB de los OIDs que necesitan ser accedidas. Normalmente puede hacerlo preprocesando los MIBs necesarios (en archivos de texto) para crear el árbol SNMP en memoria. Muchas aplicaciones llaman a esto "compilación del MIB."

5.2 Traps

La recuperación de traps es similar a pedir información SNMP, sin embargo cuando recibimos traps los frames SNMP se reciben de forma asíncrona. Cuando un dispositivo se configura para generar una alarma SNMP cuando ocurre algo importante, envía una "trap" a uno o los varios gestores de traps SNMP que están configurados en el dispositivo como receptores de traps SNMP. La información contenida en la trap es simplemente un grupo de OIDs que, como otros OIDs, se definen en un archivo MIB.

En TCP/IP Agent de Tango/04, hay dos agentes SNMP:

- **Recuperador de datos SNMP (función get):** el usuario define los OIDs y el intervalo para la recuperación de datos y el agente TCP/IP lo recoge conectando con el dispositivo SNMP monitorizado, pidiendo los OIDs requeridos.
- **Receptor de Traps:** El agente de TCP/IP monitoriza el puerto de traps SNMP, leyendo y analizando cualquier variable (OID) que llegue, convirtiéndola en un mensaje de texto.

5.2.1 Recuperación de datos SNMP

Primero, debe encontrar los valores SNMP (grupos MIB) que son soportados por el dispositivo que usted desea supervisar. Los grupos MIB soportados varían según el dispositivo y dependen del sistema operativo o del software que usted ha instalado en ese dispositivo o computadora. La configuración de dispositivo o documentación de soporte deben contener los OIDs o MIBs soportados por el dispositivo.

Una vez que sepa qué valores SNMP soporta el dispositivo, puede utilizar el agente TCP/IP para solicitar la información. En este ejemplo, usted intentará obtener el OID que corresponde a la cantidad de memoria (en KBs) en el dispositivo. El OID es "1.3.6.1.2.1.25.2.2" (que es `iso.org.dod.internet.mgmt.mib-2.host.hrStorage.hrMemorySize` en formato texto).

En el agente TCP/IP, puede utilizar siempre el OID numérico porque la petición se envía siempre al dispositivo en formato numérico. Si desea utilizar formato de texto, el agente TCP/IP debe saber cómo convertir esta secuencia en el OID numérico a través de los archivos de texto que describen el MIB donde se define el OID. Para ello, debe obtener y copiar el archivo de texto que describe el MIB en el directorio MIB que se encuentra donde se instaló el agente TCP/IP. El agente TCP/IP incluye las definiciones MIB más comunes.

Para probar la recuperación de datos SNMP, debe tener un sistema con el servicio SNMP instalado. Si está utilizando un PC, por defecto no está instalado con Windows 2000, pero algunos ordenadores lo tienen. Si usted desea monitorizar un iSeries AS/400, debe configurar el servicio SNMP y arrancarlo utilizando el siguiente mandato:

```
TRTCPSVR SERVER(*SNMP)
```

En el servidor SNMP, puede configurarse un número de parámetros importantes, por ejemplo la comunidad, una lista de servidores en cada comunidad que pueda hacer peticiones, etc. De todas maneras, por defecto, "público" debe ser correcto en todos los casos.

Hay un número infinito de valores SNMP recuperables, sin embargo, los valores más importantes dependen del dispositivo que es supervisado.

Aquí tiene dos ejemplos de OIDs a recuperar:

1. **Descripción del sistema:** obtenido por acceso al OID número 1.3.6.1.2.1.1.1.0 (`iso.org.dod.internet.mgmt.mib-2.system.sysDescr.0` en formato texto).
2. **Cantidad de memoria (en KB) en el host:** obtenido por acceso al OID número 1.3.6.1.2.1.25.2.2.0 (`iso.org.dod.internet.mgmt.mib-2.host.hrStorage.hrMemorySize.0` como secuencia de texto). El MIB que define este valor se encuentra en HOST-RESOURCES-MIB.txt.

Si usted utiliza la secuencia OID sin tener el archivo HOST-RESOURCES-MIB.txt en el directorio MIB, del agente TCP/IP aparecerá el error "error parsing OID" porque no puede obtener el OID numérico de la secuencia. Si este archivo se copia en el directorio, no debe haber ningún problema. Por supuesto, cuando trabaja con el OID numérico, la recuperación de valores no debe ser un problema (asumiendo que existen en el dispositivo monitorizado).

IMPORTANTE: CUANDO SE ACCEDE A LA TABLA DE ÍNDICES, ASÍ COMO AL ACCEDER A UN SOLO VALOR OID, LOS VALORES DEBEN ESPECIFICAR EL ÍNDICE (UN NÚMERO TAL COMO LOS "0" EN LOS EJEMPLOS).

5.2.2 Valores Delta

Con los valores Delta, se consigue el diferencial entre dos medidas en vez del valor total desde que el dispositivo fue arrancado. En el ejemplo siguiente, el valor que representa el número de datagramas IP recibidos de un dispositivo:

NOTA: TRABAJA SOLAMENTE CON VARIABLES "DE CONTADOR".

Name: ipInReceives

Type: OBJECT-TYPE

OID: 1.3.6.1.2.1.4.3

Full path: iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).ip(4).ipInReceives

Module: RFC1213-MIB

Parent: ip

Prev sibling: ipDefaultTTL

Next sibling: ipInHdrErrors

Numeric syntax: Counter (32 bit)

Base syntax: Counter

Composed syntax: Counter

Status: mandatory

Max access: read-only

Descripción: El número total de datagramas de entrada recibidos de interfaces, incluyendo los recibidos en error.

En el ejemplo anterior, el número total de datagramas enviados desde que el dispositivo fue arrancado es menos útil que el número de datagramas enviados desde la última medida. En este caso, tendría sentido de definir la variable como "delta" en el agente TCP/IP.

5.2.3 Recepción de Traps SNMP

Para probar la recepción de traps SNMP en el agente TCP/IP tiene dos opciones:

- **Configurar un dispositivo capaz de generar traps SNMP.** Debe configurar este dispositivo para enviar las traps al PC que ejecuta TCP/IP Services Agent. El problema con esta solución es que, en general, es difícil forzar un dispositivo para generar una trap específica, porque, por la definición, una trap es asíncrona y se ejecuta cuando algo "serio" sucede en el dispositivo. Por lo tanto, es a veces más fácil utilizar un programa que simule la generación de traps según lo explicado en la siguiente opción.
- **Utilizar un software de generación de traps en un PC.** Hay muchos programas disponibles en Internet que pueden simular una trap y enviarla a una dirección IP predefinida con una lista de los valores OID asociados. El software de Tango/04 incluye un pequeño generador de traps como parte del soporte de traps SNMP en alarmas de VCW/VMC. Para instalar el generador de traps SNMP de Tango/04, debe ejecutar AlarmTrap.exe en el directorio de producto de VCW/VMC. El soporte para SNMP será instalado en "\Archivos de Programa\Tango04\SNMP". Encontrará las instrucciones de uso en el documento "Soporte de Alarmas usando SNMP traps.doc" en el mismo directorio.

NOTA: ANTES DE PODER UTILIZAR EL GENERADOR DE TRAPS DE TANGO/04'S, DEBE INSTALAR Y CONFIGURAR EL SERVICIO SNMP DE WINDOWS (NO INCLUIDO EN LA INSTALACIÓN DE WINDOWS POR DEFECTO).

6. 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



7. 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 planee 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.