Novell® sentinel™

5.1.3

www.novell.com

Volumen III: GUÍA DEL USUARIO DEL ASISTENTE DE SENTINEL

7 de julio de 2006

Novell®

Aviso legal

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
EE.UU.
www.novell.com

Documentación en línea: Para acceder a la documentación en línea de este y otros productos de Novell y obtener actualizaciones, consulte www.novell.com/documentation.

Marcas comerciales de Novell

Para obtener información sobre marcas comerciales de Novell, consulte la lista de marcas comerciales y de marcas de servicio de Novell (http://www.novell.com/company/legal/trademarks/tmlist.html).

Materiales de otros fabricantes

Todas las marcas comerciales de otros fabricantes son propiedad de sus respectivos propietarios.

Avisos legales de otros fabricantes

Sentinel 5 contiene tecnologías de otros fabricantes:

- Apache Axis y Apache Tomcat, Copyright © de 1999 a 2005, Apache Software Foundation. Para obtener más información y consultar las restricciones y renuncias, visite http://www.apache.org/licenses/
- ANTLR. Para obtener más información y consultar las restricciones y renuncias, visite http://www.antlr.org/
- Boost, Copyright © 1999, Boost.org.
- Bouncy Castle, Copyright © 2000-2004, the Legion of Bouncy Castle. Para obtener más información y consultar las restricciones y renuncias, visite http://www.bouncycastle.org/.
- Checkpoint. Copyright © Check Point Software Technologies Ltd.
- Concurrent, paquete de utilidades. Copyright © Doug Lea. Se utiliza sin las clases CopyOnWriteArrayList ni ConcurrentReaderHashMap.
- Crypto++ Compilation. Copyright © 1995-2003, Wei Dai, que incorpora los siguientes trabajos sujetos a copyright: mars.cpp de Brian Gladman y Sean Woods. Para obtener más información y consultar las restricciones y renuncias, visite http://www.eskimo.com/~weidai/License.txt.
- Crystal Reports Developer y Crystal Reports Server. Copyright © 2004 Business Objects Software Limited.
- DataDirect Technologies Corp. Copyright © 1991-2003.
- edpFTPj, con licencia Lesser GNU Public License. Para obtener más información y consultar las restricciones y renuncias, visite http://www.enterprisedt.com/products/edtftpj/purchase.html.
- Enhydra Shark, con licencia Lesser General Public License disponible en: http://shark.objectweb.org/license.html.
- ICEsoft ICEbrowser. ICEsoft Technologies, Inc. Copyright © 2003-2004.
- ILOG, Inc. Copyright © 1999-2004.
- Installshield Universal. Copyright © de 1996 a 2005, Macrovision Corporation y/o Macrovision Europe Ltd.
- Java 2 Platform, Standard Edition. Copyright © Sun Microsystems, Inc. Para obtener más información y consultar las restricciones y renuncias, visite http://java.sun.com/j2se/1.4.2/j2re-1_4_2_10-license.txt.

  La plataforma Java 2 también contiene los siguientes productos de otros fabricantes:

  - CoolServlets © 1999
  - DES y 3xDES © 2000 de Jef Poskanzer
  - Crimson © 1999-2000 The Apache Software Foundation
  - Xalan J2 © 1999-2000 The Apache Software Foundation
  - NSIS 1.0j © 1999-2000 Nullsoft, Inc.
  - Eastman Kodak Company © 1992
  - Lucinda, marca comercial o marca comercial registrada de Bigelow and Holmes

- Taligent, Inc.
- IBM, algunas partes se encuentran disponibles en: http://oss.software.ibm.com/icu4j/

Para obtener más información acerca de estas tecnologías de otros fabricantes y consultar las restricciones y renuncias de responsabilidad relacionadas, visite: http://java.sun.com/j2se/1.4.2/j2se-1_4_2-thirdpartylicensereadme.txt.

- JavaBeans Activation Framework (JAF). Copyright © Sun Microsystems, Inc. Para obtener más información y consultar las restricciones y renuncias, visite http://www.java.sun.com/products/javabeans/glasgow/jaf.html y haga clic en download > license.
- JavaMail. Copyright © Sun Microsystems, Inc. Para obtener más información y consultar las restricciones y renuncias, visite http://www.java.sun.com/products/javamail/downloads/index.html y haga clic en download > license.
- Java Ace, de Douglas C. Schmidt y su grupo de investigación de la Universidad de Washington y Tao (con empaquetadores ACE) de Douglas C. Schmidt y su grupo de investigación en las universidades de Washington, California, Irvine y Vanderbilt. Copyright © de 1993 a 2005. Para obtener más información y consultar las restricciones y renuncias, visite http://www.cs.wustl.edu/~schmidt/ACE-copying.html y http://www.cs.wustl.edu/~pjain/java/ace/JACE-copying.html
- Módulos Java de servicios de autorización y autenticación, con licencia Lesser General Public License. Para obtener más información y consultar las restricciones y renuncias, visite http://free.tagish.net/jaas/index.jsp
- Java Network Launching Protocol (JNLP). Copyright © Sun Microsystems, Inc. Para obtener más información y consultar las restricciones y renuncias, visite http://www.java.sun.com/products/javawebstart/download-jnlp.html y haga clic en download > license.
- Java Service Wrapper. Copyright de partes como se indica a continuación: Copyright © 1999, 2004 Tanuki Software y Copyright © 2001 Silver Egg Technology. Para obtener más información y consultar las restricciones y renuncias, visite http://wrapper.tanukisoftware.org/doc/english/license.html.
- JIDE. Copyright © de 2002 a 2005, JIDE Software, Inc.
- jTDS con licencia Lesser GNU Public License. Para obtener más información y consultar las restricciones y renuncias, visite http://jtds.sourceforge.net/.
- MDateSelector. Copyright © 2005, Martin Newstead, con licencia de Lesser General Public License. Para obtener más información y consultar las restricciones y renuncias, visite http://web.ukonline.co.uk/mseries.
- Monarch Charts. Copyright © 2005, Singleton Labs.
- Net-SNMP. Partes del código están sujetas a copyright de varias entidades, las cuales se reservan todos los derechos. Copyright © 1989, 1991, 1992 de Carnegie Mellon University; Copyright © 1996, de 1998 a 2000, Junta de regentes de la Universidad de California; Copyright © de 2001 a 2003 Networks Associates Technology, Inc.; Copyright © de 2001 a 2003, Cambridge Broadband, Ltd.; Copyright © 2003 Sun Microsystems, Inc. y Copyright © de 2003 a 2004, Sparta, Inc. Para obtener más información y consultar las restricciones y renuncias, visite http://net-snmp.sourceforge.net.
- The OpenSSL Project. Copyright © 1998-2004. the Open SSL Project. Para obtener más información y consultar las restricciones y renuncias, visite http://www.openssl.org.
- Oracle Help for Java. Copyright © 1994-2006, Oracle Corporation.
- RoboHELP Office. Copyright © Adobe Systems Incorporated, antes conocido como Macromedia.
- Skin Look and Feel (SkinLF). Copyright © 2000-2006 L2FProd.com. Con licencia de Apache Software License. Para obtener más información y consultar las restricciones y renuncias, visite https://skinlf.dev.java.net/.
- Sonic Software Corporation. Copyright © 2003-2004. El software de SSC contiene software de seguridad con licencia de RSA Security, Inc.
- Tinyxml. Para obtener más información y consultar las restricciones y renuncias, visite http://grinninglizard.com/tinyxmldocs/index.html.

- SecurityNexus. Copyright © de 2003 a 2006. SecurityNexus, LLC. Reservados todos los derechos.
- Xalan y Xerces, ambos se otorgan bajo licencia de Apache Software Foundation Copyright © de 1999 a 2004. Para obtener más información y consultar las restricciones y renuncias, visite http://xml.apache.org/dist/LICENSE.txt.
- yWorks. Copyright © de 2003 a 2006, yWorks.

NOTA: A fecha de publicación de este documento, los enlaces indicados anteriormente están activos. En caso de que alguno de los enlaces anteriores esté roto o la página a la que enlace esté inactiva, póngase en contacto con Novell, en la dirección Inc., 404 Wyman Street, Suite 500, Waltham, MA 02451 EE.UU.

Contenido

Prólogo

La documentación técnica de Sentinel es una guía de referencia en la que se describen las funciones más generales. Esta documentación va dirigida a profesionales en seguridad de la información. El texto de esta documentación pretende servir como fuente de referencia para el sistema de gestión de seguridad empresarial de Sentinel. Existe documentación adicional en el portal Web de Sentinel.

La documentación técnica de Sentinel se divide en cinco volúmenes distintos. Son los siguientes:

- Volumen I: Guía de instalación de Sentinel™ 5
- Volumen II: Guía del usuario de Sentinel™ 5
- Volumen III: Guía del usuario del asistente de Sentinel™ 5
- Volumen IV: Guía de referencia del usuario de Sentinel™ 5
- Volumen V: Guía de integración de productos de otros fabricantes en Sentinel™

Volumen I: Guía de instalación de Sentinel

En esta guía se describe cómo instalar los componentes siguientes:

- Servidor de Sentinel
- Consola de Sentinel
- Motor de correlación de Sentinel
- Crystal Reports de Sentinel
- Generador de recopiladores del asistente
- Gestor de recopiladores del asistente
- Asesor

Volumen II: Guía del usuario de Sentinel

En esta guía se tratan los temas siguientes:

- Funcionamiento de la consola de Sentinel
- Funciones de Sentinel
- Arquitectura de Sentinel
- Comunicación de Sentinel
- Apagado/inicio de Sentinel
- Valoración de vulnerabilidades
- Monitorización de eventos
- Filtrado de eventos
- Correlación de eventos
- Gestor de datos de Sentinel
- Configuración de eventos para relevancia empresarial
- Servicio de asignación
- Informes históricos
- Gestión del host del asistente
- Incidencias
- Casos
- Gestión de usuarios
- Flujo de trabajo

Volumen III: Guía del usuario del asistente

En esta guía se tratan los temas siguientes:

- Funcionamiento del Generador de recopiladores del asistente
- Gestor de recopiladores del asistente
- Recopiladores
- Gestión del host del asistente
- Generación y mantenimiento de los recopiladores

Volumen IV: Guía de referencia del usuario de Sentinel

En esta guía se tratan los temas siguientes:

- Lenguaje de los guiones del asistente
- Comandos de análisis del asistente
- Funciones de administrador del asistente
- Meta-etiquetas de Sentinel y del asistente
- Motor de correlación de Sentinel
- Permisos del usuario
- Opciones de línea de comando de correlaciones
- Esquema de la base de datos de Sentinel

Volumen V: Guía de integración de productos de otros fabricantes en Sentinel

- Remedy
- HP OpenView Operations
- HP Service Desk

1 Introducción al asistente

NOTA: El término Agente puede intercambiarse con Recopilador. En adelante, los agentes se denominarán recopiladores.

La guía de usuario del asistente es la introducción al funcionamiento del asistente de Novell. Esta guía le explicará cada componente y su funcionamiento.

En esta guía se supone que está familiarizado con la seguridad de red, la administración de la bases de datos y los sistemas operativos Windows y UNIX.

Contenido

En esta guía se incluyen los capítulos siguientes:

- Capítulo 1 – Introducción al asistente
- Capítulo 2 – Gestión de los hosts del asistente
- Capítulo 3 – Generación y mantenimiento de los recopiladores
- Apéndice A – Conector syslog
- Apéndice B – Servidor de zócalo
- Apéndice C – Información sobre copyright

Convenciones usadas

Notas y precauciones

NOTA: Las notas proporcionan información adicional que puede resultar útil.

PRECAUCIÓN: Las precauciones proporcionan información adicional que puede ayudarle a evitar daños o pérdida de datos en su equipo.

Comandos

La fuente de los comandos es Courier. Por ejemplo:

```
useradd -g dba -d /export/home/oracle -m -s /bin/csh
   oracle
```

Asistente

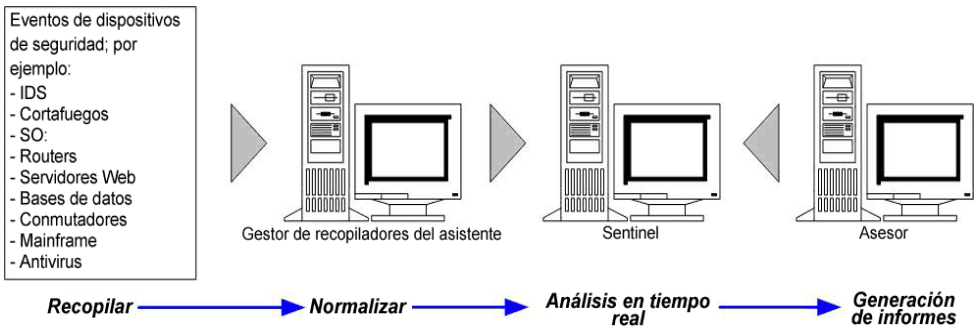
El asistente permite generar, configurar y controlar recopiladores. Los recopiladores se utilizan para recolectar y normalizar los eventos en los dispositivos y programas de seguridad. Estos eventos normalizados se envían a Sentinel para utilizarlos en la correlación de análisis, generación de informes y respuesta en caso de incidencia en tiempo real.

NOTA: Aunque no es un requisito, se recomienda que, en una configuración de Generador de recopiladores del asistente múltiple, se designe un Generador de recopiladores como el Generador de recopiladores primario. Así, esta máquina se utiliza para almacenar, desarrollar o modificar recopiladores y configurar puertos.

El asistente está constituido por los siguientes componentes:

- El Generador de recopiladores es la interfaz de usuario del asistente que le permite generar, configurar, distribuir y controlar los recopiladores. Además de ejecutar los recopiladores localmente, el Generador de recopiladores se puede usar para cargar, descargar y controlar los recopiladores en sistemas remotos.
- El gestor de recopiladores es el módulo subyacente del Asistente que gestiona los recopiladores y los mensajes de estado del sistema y que realiza el filtrado global de eventos.

Un recopilador es el receptor que recopila y normaliza los eventos sin formato de los dispositivos y programas de seguridad y que devuelve los eventos normalizados que se pueden correlacionar, informar y utilizar en caso de repuesta a incidencias. El software de Sentinel incluye recopiladores de nivel 1. Para descargar recopiladores adicionales visite el portal del cliente de Sentinel en la dirección http://www.esecurityinc.com/.



Recopiladores

Los recopiladores se usan para filtrar y transformar los datos de eventos importantes a un formato normalizado para que Sentinel pueda procesarlo. Existen tres niveles de recopiladores:

- Recopiladores admitidos (T1). Estos recopiladores:
  - tienen documentación
  - tienen metadatos
  - están disponibles para todos los clientes
  - Asistencia técnica de Novell
- Recopiladores con documentación (T2). Estos recopiladores:
  - están destinados a la biblioteca de recopiladores
  - tienen documentación

    - tienen metadatos
    - están basados en las plantillas estándar de Sentinel
    - Asistencia técnica limitada
- Recopiladores de muestra (T3). Estos recopiladores:
    - tienen prueba de concepto
    - están desarrollados para un cliente específico
    - pueden no tener metadatos o documentación admitida
    - Asistencia técnica limitada

Los recopiladores le permiten acceder a datos de eventos desde muchos orígenes, entre los que se incluyen:

- Sistemas de detección de intrusos (hosts)
- Sistemas de detección de intrusos (red)
- Cortafuegos
- Sistemas operativos
- Monitorización directivas
- Autenticación
- Routers y conmutadores
- VPN
- Antivirus
- Servidores Web
- Bases de datos
- Mainframe
- Valoración de vulnerabilidades
- Servicios de directorio
- Gestión de redes
- Sistemas registrados

Los recopiladores constan de

- Archivos de plantilla
- Archivos de parámetro
- Archivos de búsqueda
- Archivos de asignación
- Archivos de descripción de parámetro y archivos de manifiesto

El archivo de plantilla y su archivo de parámetro asociado se fusionan en diferentes archivos de guión cuando se genera el guión del recopilador.

Cada archivo de guión se nombra con el nombre de la columna del conjunto de valores en el archivo de parámetros. Los archivos de guión se agrupan en una secuencia ordenada en secuencias de inicio y de restitución.

Las secuencias de inicio y de restitución se asignan a un puerto que ejecuta las series de guiones que contiene cuando se inicia o detiene. Se debe incluir un guión en la secuencia de inicio o restitución para que el puerto lo pueda utilizar. Los puertos permiten al recopilador ubicar los hosts del asistente en la red a través de la dirección IP y del nombre de archivo del host. También proporcionan a Sentinel información sobre la ubicación de los sensores y del recopilador que se utiliza para gestionar datos para esos sensores. Las siguientes opciones son configurables para puertos:

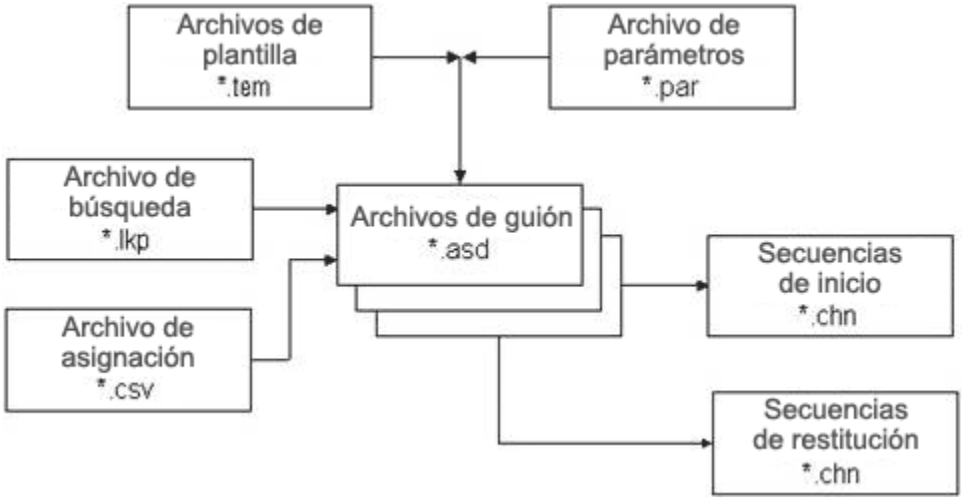
- Tipo de conexión
    - Serie: datos leídos de un puerto en serie RS-232C
    - Zócalo: una conexión por zócalo TPC
    - Nuevo en archivo: lee sólo datos de eventos de seguridad que se añaden a un archivo después de que el guión se haya iniciado (lee desde el final del archivo).
    - Todo en archivo: lee todos los datos de eventos de seguridad en un archivo.
    - Proceso persistente: lanza un proceso persistente cuando se inicia el puerto, se comunica con el recopilador asignado a ese puerto y a una aplicación externa a través de estados de recepción y transmisión y continúa en ejecución durante la vida activa del puerto.

- Proceso transitorio: comunica al Recopilador asignado con el puerto y con la aplicación externa a través de estados de recepción y de transmisión. El proceso transitorio puede iniciarse en varias ocasiones.
- SNMP: recibe mensajes de alerta SNMP v1, v2 y v3.
- Ninguna

- Nombre del recopilador: puede renombrar, copiar y añadir recopiladores.

Cuando una plantilla utiliza el comando de análisis LOOKUP() se busca el archivo de búsqueda apropiado para que se ejecute un bloque específico de comandos de análisis.

Cuando una plantilla usa el comando de análisis TRANSLATE , el comando descarga un archivo de asignación que permite la búsqueda rápida de entradas clave.



Archivos de plantillas

Le permite crear y añadir estados y editar y eliminar plantillas. Las plantillas determinan cómo se procesarán los registros. La mayoría de las decisiones sobre plantillas se centran en los tipos de registros con los que está trabajando y su formato. Existe un archivo de plantilla equivalente con la extensión. tem. Están ubicados en %WORKBENCH_HOME%\elements\<Nombre del recopilador>.

Los archivos de plantillas están basados en estados. Un estado es un punto de decisión en el flujo lógico o en la ruta de una plantilla. Cada punto (estado) contiene información sobre el proceso que se va a realizar. Los estados incluyen una referencia a los parámetros; cuando una plantilla se fusiona con un archivo de parámetros, los parámetros reemplazan a valores específicos. Cuando los parámetros se reemplazan por valores específicos, se crea uno o más de un archivo de guión.

Cuando se inserta un estado a una plantilla, se asigna un número que permanece con él aunque la plantilla cambie de ubicación. Existen tres grupos de estados.

- Los estados de transmisión, recepción, decisión y análisis se enumeran en el orden en el que se insertan en la plantilla.
  - Estado de transmisión (Tx): transmite una cadena a un puerto definido.
  - Estado de recepción (Rx) : define si el asistente recibe o no información de una aplicación de seguridad en un buffer. La información se toma de la definición del puerto.

    - Estado de decisión: utiliza una cadena de datos o una variable para determinar a qué estado pasar.
    - Estado de análisis: : utiliza los comandos de análisis para crear plantillas para procesar la información recogida en el buffer de recepción.
- Los estados Siguiente e Ir a se identifican con el número del estado al que indican.
    - Estado Siguiente: indica a qué estado saltar en el siguiente guión.
    - Estado Ir: se usa para ir a un estado anterior dentro del guión actual.
- Estado Detener es siempre el número cero. Indica cuándo detener el procesamiento en un puerto.

Estado de transmisión

El estado de transmisión envía una cadena o una variable (según el tipo de datos seleccionado) al tipo de conexión configurado para ese recopilador. Si la conexión está interrumpida al entrar a un estado de transmisión y se introduce un valor en el recuadro Valor Rx/Tx del panel puerto de información de la plantilla, se produce el siguiente evento y se intenta restablecer la conexión hasta que se consigue una reconexión satisfactoria.

Existe un retraso de intercarácter que especifica el número de milisegundos (ms) entre el envío de cada byte de datos.

Estado de recepción

El estado de recepción especifica el método que utiliza el asistente para determinar cuándo el recopilador ha recibido los datos. En el estado de recepción se especifica:

- Tipo de recepción
- Bytes mínimos
- Cadena de decisión del delimitador

Si la conexión está interrumpida al entrar a un estado de transmisión y se introduce un valor en el recuadro Valor Rx/Tx del panel puerto de información de la plantilla, se produce el siguiente evento y se intenta restablecer la conexión hasta que se consigue una reconexión satisfactoria.

Después del estado de recepción del RxBuffer, automáticamente se incorporan dos variables con los resultados del estado de recepción.

- s_RXBufferString contiene el texto recibido por el RxBuffer
- i_RXBufferLength contiene la longitud del s_RXBufferString

Esto equivale a ejecutar el siguiente código de guión después de un estado de recepción:

- COPY(s_RXBufferString:)
- LENGTH(i_RXBufferLength,s_RXBufferString)

Estas variables incorporadas automáticamente permiten una comparación fácil en un estado de decisión sobre si el estado de recepción ha excedido su tiempo o no. También permiten la utilización directa del RXbuffer a través de la variable s_RXBufferString.

Tipos de recepción: existen cuatro tipos de recepción disponibles en el editor de plantillas. Son los siguientes:

- Tiempo límite: permite a un guión continuar el proceso si no se reciben datos en un periodo específico de tiempo. La selección del límite de tiempo permite al asistente recibir datos hasta que se alcanza el periodo de tiempo límite, como lo define la variable _TIMEOUT_DELAY.

- Tiempo de espera: se usa principalmente cuando se reciben mensajes de eventos no solicitados. El asistente esperará durante la duración de tiempo límite hasta que se reciban los datos.

  NOTA: Para los tipos de recepción tiempo límite y de espera, el procesamiento en el guión no continuará hasta que se haya recibido el número mínimo de bytes o cuando se alcance el tiempo límite en el caso de la primera opción.

- Tiempo límite delimitado: utiliza un guión de caracteres predefinido para indicar al asistente que se han recibido los datos. Los datos en el recuadro de la cadena de decisión del delimitador se verifican con los datos en el buffer de recepción a medida que se recibe cada byte.
- Tiempo de espera delimitado: se utiliza cuando se esperan mensajes no solicitados. Una cadena de caracteres definida por el usuario indica al asistente que se han recibido los datos. El asistente utiliza los datos en el recuadro de la cadena de decisión del delimitador para verificar los datos de recepción a medida que se recibe cada byte. El parámetro RX_TIMEOUT_DELAY no realiza ninguna acción mientras se utiliza la opción tiempo de espera delimitado.

  NOTA: Para los tipos de recepción tiempo límite delimitado y tiempo de espera delimitado, el procesamiento en el guión no continuará hasta que la cadena de decisión de delimitador no lo valide y se haya recibido el número mínimo de bytes o cuando se alcance el tiempo límite en el caso de la primera opción.

Bytes Mínimos: el número mínimo de bytes es el número de bytes que se debe recibir antes de que el asistente agote el periodo de tiempo límite predeterminado o que continúe con el proceso. El procesamiento en el guión no continuará hasta que se haya recibido el número mínimo de bytes.

Delimitador cadena de decisión: El delimitador cadena de decisión se completa cuando el tipo de recepción es tiempo límite delimitado o tiempo de espera delimitado. El procesamiento del recopilador no pasará al siguiente estado hasta que el delimitador cadena de decisión no concuerde con los datos leídos y se haya recibido el número mínimo de bytes.

El delimitador cadena de decisión es una expresión regular compatible con POSIX 1003.2.

Escenarios de tipos de recepción: existen cuatro tipos de escenarios de tipos de recepción: Son los siguientes:

- Escenario de tiempo límite: después de haberse iniciado el estado de recepción, el procesamiento se detiene hasta que se leen los bytes mínimos o pasan los segundos de RX_TIMEOUT_DELAY. Después de que el asistente haya recibido el número mínimo de bytes especificado o cuando se haya superado el tiempo límite, el procesamiento del puerto del recopilador pasa al siguiente estado del guión.
- Escenario de tiempo de espera: el tipo de estado de recepción de espera aguarda hasta que el recopilador del asistente recibe el número mínimo de bytes en el recuadro de bytes mínimos. Después de la recepción por parte del asistente de un número mayor que el número mínimo de bytes especificado en el recuadro de bytes mínimos, el procesamiento del puerto del recopilador pasa al siguiente estado del guión. Si no se recibe el número mínimo de bytes, el procesamiento del puerto del recopilador nunca alcanza su tiempo límite.

- Escenario de tiempo de espera delimitado: si se encuentra la cadena de decisión de delimitador después de recibir la posición mínima de bytes establecida en el recuadro de bytes mínimos, se guardan los datos hasta e incluyendo el delimitador en el Buffer Rx. Si no se encuentra el guión de decisión del delimitador, no se transfieren datos al buffer de recepción y el procesamiento del puerto del recopilador alcanza su tiempo límite dentro del periodo de tiempo límite predeterminado.
- Escenario de tiempo de espera delimitado: si se encuentra el guión de decisión de delimitador después de recibir el número mínimo de bytes establecido en el recuadro de bytes mínimos, el procesamiento del puerto del recopilador continúa y se procesan los datos. Si no se encuentra el guión de decisión del delimitador, no se transfieren datos al buffer de recepción y el puerto no excede su tiempo límite. Si no se encuentra el guión de decisión del delimitador, el procesamiento del puerto del recopilador nunca alcanza su tiempo límite. Además, si se encuentra el guión de decisión del delimitador pero no se reciben los bytes mínimos, el procesamiento del puerto del recopilador nunca alcanza su tiempo límite.

Estado de decisión

El estado de decisión evalúa el contenido del buffer de recepción o la variable para determinar la acción que se va a realizar. Si la información del buffer de recepción contiene el tipo de decisión seleccionado, el Gestor de recopiladores procesa el comando como verdadero y se sigue la ruta afirmativa. Si el buffer de recepción no contiene el tipo de decisión seleccionado, el Gestor de recopiladores procesa la decisión como falsa y se sigue la ruta negativa.

El buffer de recepción (tamaño Rxbuffer) es un parámetro editable ubicado en:

```
$WORKBENCH_HOME/config/wizard.properties/
   system.max_receive_buffer_size
```

Este parámetro le permite configurar el buffer de recepción del Gestor de recopiladores (Rx buffer). El número de eventos predeterminado es 50.000. El número mínimo de eventos es 5.000. Cuando el buffer Rx alcanza su tamaño máximo, se abandonan nuevos eventos a medida que se reciben porque están en pausa.

Existen cuatro tipos de decisión: Son los siguientes:

- Cadena: compara la cadena de decisión definida por un usuario con el contenido del buffer de recepción. El contenido de la cadena de decisión se verifica con el contenido del buffer de recepción, o con una variable, para determinar qué ruta de decisión procesar. El guión de decisión es una expresión regular compatible con POSIX 1003.2. Una variable admite cadenas, números enteros y de coma flotante.
- Verdadera: impone una evaluación positiva, el Gestor de recopiladores sigue la ruta afirmativa.
- Falsa: impone una evaluación negativa, el Gestor de recopiladores sigue la ruta negativa.
- Datos: compara la cadena de decisión definida por un usuario con otra cadena o con el valor de una variable.

Estado de análisis

El estado de Análisis se utiliza para desarrollar los guiones que se ejecutan en los puertos. Los comandos de análisis pueden incluir parámetros que se fusionan con la plantilla cuando se crean los guiones. Existen un editor visual y un editor de texto disponibles para definir los comandos de análisis.

El estado de análisis se utiliza también para insertar comandos de análisis en una plantilla. Los comandos de análisis pueden incluir parámetros, que se reemplazan por valores específicos cuando la plantilla se fusiona con un archivo de parámetro en el proceso de generación del guión. La fusión de una plantilla y de un archivo de parámetro puede devolver múltiples guiones para ejecutar en los puertos.

Archivos de parámetros

Los parámetros son equivalentes a las variables. Los archivos de parámetros (archivos. par) son tablas que se utilizan para definir nombres de variables en los archivos de guiones de ejecución asociados. Se utilizan cuando se hace referencia a ellos en el código de análisis. Los parámetros se almacenan como cadenas. Cualquier valor numérico tiene que convertirse en una cadena para su manipulación. Cuando se introducen nuevos valores para los parámetros, éstos se activan después de generar el guión. Se fusionan con el archivo de plantilla cuando se crea el guión.

Los nombres de los archivos de guiones de ejecución se muestran en la primera fila de la tabla y los nombres y niveles de los parámetros se muestran en la primera columna de la tabla. La segunda fila de la tabla se utiliza para definir los iconos que aparecen en el árbol del recopilador. La fila restante define las variables o los valores de los parámetros que se utilizan para el parámetro ya que la fila está relacionada con un guión en concreto.

Los valores dentro del archivo de parámetro son:

- Meta-etiquetas, información y comentarios; existen más de 200 meta-etiquetas disponibles, de las cuales 100 son configurables por el usuario y el resto están reservadas.
- Regla: los nombres de los archivos configurados aparecen en la fila del encabezado de la tabla, mientras que los parámetros aparecen en la primera columna de la tabla.
- Mapa de bits: la segunda fila de la tabla define el mapa de bits utilizado para ese archivo. El mapa de bits aparecerá en la lista de recopiladores.

Archivos de búsqueda

Los archivos de búsqueda son tablas opcionales (archivos. lkp) que se comparan con los valores recibidos para determinar qué acciones realizar, en su caso, como respuesta a eventos de seguridad. Los archivos de búsqueda contienen cláusulas de concordancia que se utilizan para comparar cadenas individuales. El comando LOOKUP determinará si la cadena de búsqueda se encuentra o no basándose en las cláusulas de un archivo de búsqueda específico y en los datos recibidos de los dispositivos de origen.

De manera opcional, los comandos de análisis pueden estar asociados a la cadena de concordancia. Los comandos de análisis se ejecutan si se encuentra una concordancia.

Archivos de asignación

Los archivos de asignación son archivos opcionales (.csv) que permiten la búsqueda rápida de entradas clave. El archivo csv es una ruta relativa desde un directorio de guión del recopilador. La edición de estos archivos no está disponible actualmente en el Generador de recopiladores, pero se pueden editar los textos con Excel.

Ejemplo de un posible archivo de asignación:

```
~Mes~      ~Número~
Ene                1
Feb                2
Mar                3
Apr                4
May                5
Jun                6
Jul                7
Ago                8
Sep                9
Oct               10
Nov               11
Dic               12
```

Las entradas pueden ser un número variable de variables de guión (cadena, variable o número de coma flotante) que se utilizan para indicar con qué variables almacenar los datos. Este ejemplo particular se utiliza para traducir (asignar) un Mes por un Número (p. ej. Ene. por 1).

Archivos de manifiesto

Los archivos de manifiesto diferencian a los recopiladores de la versión 5 de recopiladores de versiones anteriores. Los archivos de manifiesto admiten la implantación de recopiladores desde la consola de Sentinel y el control de versiones de recopiladores. El análisis de recopiladores se define en el archivo agent.lkp. Los casos de búsqueda son:

- Setup: configuración de una vez de variables y parámetros
- Check_Setup: comprobación de una vez de esas variables y parámetros
- Initialize_Vars: el principio de cada bucle, donde las variables se inicializan una vez por cada análisis.
- Parse: el lugar donde se realiza el análisis.

Esto permite conectar el nuevo análisis del recopilador en plantillas existentes. Además, proporciona la posibilidad de superponer nuevas versiones del recopilador para actualizar el código. Ésta es una lista de archivos de manifiesto y de su contenido para la versión 5.0:

- agent.nfo
  - product,Snort
  - product.vendor,GNU
  - product.version,2.0
  - product.security.type,IDS
  - product.sensor.type,N
  - product.name,IDSx_GNUx_SNRT
  - file.version,1

Otros materiales de consulta de Sentinel

Los manuales siguientes están disponibles en los CD de instalación de Sentinel.

- Guía de instalación de Sentinel™
- Guía del usuario de Sentinel™
- Guía del usuario del asistente de Sentinel™
- Guía de referencia del usuario de Sentinel™
- Guía de integración de productos de otros fabricantes con Sentinel™
- Notas de la versión

Cómo ponerse en contacto con Novell

- Sitio Web: http://www.novell.com
- Asistencia técnica de Novell: http://www.novell.com/support/index.html
- Asistencia técnica internacional de Novell: http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup
- Self Support (Autoasistencia técnica): http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog
- Para obtener asistencia técnica las 24 horas del día los 7 días de la semana, , llame al número 800-858-4000 (sólo para EE.UU.).

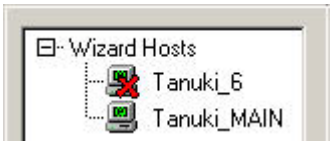
2 Gestión de los hosts del asistente

> **NOTA:** El término Agente puede intercambiarse con Recopilador. En adelante, los agentes se denominarán recopiladores.

Los hosts del asistente son equipos que tienen instalado el Gestor de recopiladores. Dichos hosts interactúan con las máquinas del Generador de recopiladores y Sentinel en la red. Así, los recopiladores reciben y analizan los datos y, basándose en éstos, los hosts enviarán alertas a Sentinel.

El asistente detecta automáticamente los hosts en la red y los añade a la lista de la pestaña de los hosts del asistente. No es posible añadir hosts de forma manual, pero es posible renombrar los que ya existen y suprimir los que ya no estén presentes físicamente y no establezcan comunicación alguna.

El Generador de recopiladores recopila los mensajes sobre la actividad en hosts. Si un host no responde con un mensaje sobre la actividad, el host mostrará una X roja en el árbol Hosts del asistente. Es posible eliminar un host con una X roja, pero si el Generador de recopiladores detecta que hay comunicaciones desde ese host, el host reaparecerá en el árbol Hosts del asistente. Del mismo modo, si se elimina un host que ya está comunicándose, el mensaje sobre la actividad volverá a aparecer en el árbol Hosts del asistente.



Una vez que se ha detectado un host, se asigna le un número de identificación.

Los últimos recopiladores se pueden encontrar en el CD del Service Pack Para obtener más información, consulte las Notas de la versión de Service Pack.

> **NOTA:** Para obtener más información relacionada con la configuración de los recopiladores de demostración, consulte en la Guía de instalación de Sentinel, el apartado Realización de pruebas en la instalación.

Recolección de datos por parte de un host del asistente

Para que un hosts del asistente, máquina con un gestor de recopilación instalado, reciba los datos de un recopilador, se tiene que cargar el recopilador de una máquina generadora de recopiladores a través de un puerto que se haya configurado en el generador de recopiladores. Una vez que se ha cargado un recopilador en un host, el host ya puede recibir datos de dicho recopilador.

Cada host del asistente se puede conectar a varios puertos y monitorizar datos procedentes de varios recopiladores. Un host del asistente puede tener puertos con recopiladores que conecten con distintos tipos de datos de origen, Los recopiladores individuales del host del puerto del asistente se debe cargar para que se pueda ejecutar y, además, los puertos proporcionan al Gestor de recopiladores información sobre la ubicación de los datos de origen.

Permiso del hosts del asistente

El permiso del host del asistente se administra a través de la pestaña Admin del Centro de control de Sentinel. Los permisos del usuario del host del asistente son:

Nombre del permiso	Descripción
Ver recopiladores	▪ Permite ver la pestaña 'Recopiladores' del Centro de control de Sentinel. ▪ Permite ver la pestaña 'Hosts del asistente' en el Generador de recopiladores.
Controlar recopiladores	▪ Incluye las mismas capacidades que el permiso 'Ver recopiladores'. ▪ Permitido para el comando y el control de recopiladores desde el Centro de control de Sentinel ▪ Permite la ejecución y el control de recopiladores desde el Generador de recopiladores del asistente.
Administración del recopilador	▪ Incluye las mismas capacidades que el permiso 'Ejecutar recopiladores'. ▪ En el Generador de recopiladores, permite editar e implantar recopiladores. ▪ En el Generador de recopiladores, permite crear, editar, compilar y depurar recopiladores. ▪ En el Generador de recopiladores, permite cargar y descargar recopiladores. ▪ En el Generador de recopiladores, permite exportar hosts del asistente. ▪ En el Generador de recopiladores, permite añadir, editar y suprimir puertos. ▪ En el Generador de recopiladores, permite definir las opciones del puerto.

La ejecución y el control incluyen:

- Iniciar/detener los puertos individuales
- Iniciar/detener todos los puertos
- Reiniciar hosts
- Renombrar hosts

Gestión del host del asistente

En este capítulo, se tratan los temas siguientes:

Inicio y detención del Gestor de recopiladores

NOTA: La primera vez que se ejecuta el Generador de recopiladores del asistente, aparece el mensaje siguiente: “El directorio 'Recopiladores' no existe. Se creará automáticamente. Es posible que se haya perdido parte de la información.” Seleccione Aceptar. El directorio se creará y se lanzará el Generador de recopiladores del asistente. Si el mensaje se mostrase en las siguientes ejecuciones del Generador de recopiladores, es posible que el directorio Recopilador se haya suprimido accidentalmente, por lo que deberá comprobar si se ha perdido información.

Inicio o detención del Servicio del Gestor de recopiladores para Windows

Inicio o detención del Servicio del Gestor de recopiladores para Windows

1. Haga clic en *Inicio* > *Configuración* > *Panel de control.*
2. En el *Panel de control,* haga doble clic en *Herramientas administrativas* y haga clic en *Servicios*.
3. En el recuadro de texto Servicios, haga clic con el botón derecho en el *Gestor de recopiladores* y haga clic en *Iniciar* o *Detener*.

Inicio del Servicio del Gestor de recopiladores para Windows (línea de comando) .

1. Vaya a %WORKBENCH_HOME%
2. Para iniciar el Gestor de recopiladores:
   - ./agent-manager start
   - ./agent-manager restart: inicia el guión del Gestor de recopiladores en segundo plano y automáticamente se inicia el proceso del Gestor de recopiladores si se ha detenido. Si el proceso del gestor de agentes ya está ejecutándose, se detendrá y se reiniciará.
   - ./agent-manager.sh console: inicia el proceso del Gestor de recopiladores en primer plano.

NOTA: En el modo de consola, compruebe que sólo se ejecute una instancia del Gestor de recopiladores en el equipo.

Detención del Servicio del Gestor de recopiladores para Windows (línea de comando)

1. Vaya a %WORKBENCH_HOME%
2. Para detener el Gestor de recopiladores:

```
./agent-manager stop
```

Inicio del Gestor de recopiladores para UNIX (modo normal y de consola)

Inicio del Gestor de recopiladores para UNIX

1. Como usuario esecadm, vaya a

```
$WORKBENCH_HOME
```

2. Escriba el comando siguiente:

```
./agent-manager.sh start
```

   - ./agent-manager restart: inicia el guión del Gestor de recopiladores en segundo plano e inicia de forma automática el proceso del Gestor de recopiladores si se ha detenido. Si el proceso del Gestor de recopiladores ya está ejecutándose, se detendrá y se reiniciará.
   - ./agent-manager.sh console: inicia el proceso del Gestor de recopiladores en primer plano.

Detención del Gestor de recopiladores para UNIX

Detención del Gestor de recopiladores para UNIX

1. Como usuario esecadm, vaya a

```
$WORKBENCH_HOME
```

2. Escriba el comando siguiente:

```
./agent-manager.sh stop
```

Administración del Gestor de recopiladores

Existe un archivo ejecutable del Gestor de recopiladores (para Windows) y un guión (para UNIX) que permiten:

- Instalar el Servicio del Gestor de recopiladores para Windows (sólo para Windows)
- Eliminar dicho servicio (sólo para Windows)
- Definir el Servicio del Gestor de recopiladores
- Imprimir gran cantidad de información de depuración.
- Mostrar la versión de prototipo
- Mostrar la ayuda

Instalación del Servicio del Gestor de recopiladores para Windows (sólo para Windows)

Instalación del Servicio del Gestor de recopiladores para Windows (sólo para Windows)

1. En el indicador de comandos, vaya a. %workbench_home%.
2. Escriba el comando siguiente:

   ```
   agent-manager.bat -install
   ```

3. Para iniciar el servicio, realice una de las operaciones siguientes:
   - En el indicador de comandos, escriba:

     ```
     net start "agent manager"
     ```

   - Haga clic en *Inicio* > *Configuración* > *Panel de control*. Haga doble clic en *Servicios* y seleccione *Gestor de recopiladores*. Inicie el Servicio del *Gestor de recopiladores.*

NOTA: Si la ventana Servicios ya está abierta, haga clic en *Acción* > *Actualizar* e inicie el Servicio del *Gestor de recopiladores*.

Eliminación del Servicio del Gestor de recopiladores (para Windows)

Eliminación del Servicio del Gestor de recopiladores (Windows).

1. Cierre el Servicio del Gestor de recopiladores como se indica a continuación
   - En el indicador de comandos, escriba:

     ```
     net stop "agent manager"
     ```

   - Haga clic en *Inicio* > *Configuración* > *Panel de control.* Haga doble clic en *Servicios* y seleccione *Gestor de recopiladores*. Detenga el Servicio del *Gestor de recopiladores*. Cierre la ventana Servicios.
2. En el indicador de comandos, vaya a. %workbench_home%.
3. Escriba el comando siguiente:

   ```
   agent-manager.bat -remove
   ```

Cambio de la contraseña del Gestor de recopiladores para Windows

NOTA: Con el fin de cumplir las restrictas configuraciones de seguridad requeridas por la certificación de criterios comunes, es muy recomendable utilizar una contraseña segura con las características siguientes:

1. Elija contraseñas con una longitud mínima de 8 caracteres y que incluyan al menos un carácter en MAYÚSCULA, uno en minúscula, un símbolo especial (!@#$%^&*()_+) y un número (de 0 a 9).

2. La contraseña no puede contener el nombre del correo electrónico ni ninguna parte del nombre completo del usuario.

3. La contraseña no debe ser una palabra común, es decir, no es conveniente que sea una palabra que aparezca en el diccionario o que sea una palabra de uso común.

4. La contraseña no debe contener palabras de ningún idioma, ya que existen varios programas ilícitos de obtención de contraseñas que pueden procesar millones de combinaciones de palabras en tan sólo unos segundos.

5. Se debe elegir una contraseña que sea compleja, pero que a la vez, se pueda recordar.. Por ejemplo, Mht5!As (Mi hijo tiene cinco años) o bien HveCdh5#As (He vivido en California desde hace cinco años).

Cambio de la contraseña del Gestor de recopiladores para Windows.

1. En el indicador de comandos, vaya a. %workbench_home%.
2. Escriba el comando siguiente:

PRECAUCIÓN: El sistema no le solicitará que confirme la contraseña ni le solicitará la contraseña antigua.

```
agent-manager.bat –password <nueva contraseña>
```

3. Para que la nueva contraseña se active:
   - En el indicador de comandos, escriba:

     ```
     net stop "agent manager"
     net start "agent manager"
     ```

   - O bien, en el Generador de recopiladores, haga clic con el botón derecho del equipo host y seleccione la opción de reiniciar el host.
   - Haga clic en *Inicio* > *Configuración* > *Panel de control*. Haga doble clic en *Servicios* y seleccione *Gestor de agentes*. Detenga e inicie el servicio del Gestor de agentes.

Cambio de la contraseña del Gestor de recopiladores para UNIX.

NOTA: Con el fin de cumplir las restrictas configuraciones de seguridad requeridas por la certificación de criterios comunes, es muy recomendable utilizar una contraseña segura con las características siguientes:

1. Elija contraseñas con una longitud mínima de 8 caracteres y que incluyan al menos un carácter en MAYÚSCULA, uno en minúscula, un símbolo especial (!@#$%^&*()_+) y un número (de 0 a 9).

2. La contraseña no puede contener el nombre del correo electrónico ni ninguna parte del nombre completo del usuario.

3. La contraseña no debe ser una palabra común, es decir, no es conveniente que sea una palabra que aparezca en el diccionario o que sea una palabra de uso común.

4. La contraseña no debe contener palabras de ningún idioma, ya que existen varios programas ilícitos de obtención de contraseñas que pueden procesar millones de combinaciones de palabras en tan solo unos segundos.

5. Se debe elegir una contraseña que sea compleja, pero que a la vez, se pueda recordar.. Por ejemplo, Mht5!As (Mi hijo tiene cinco años) o bien HveCdh5#As (He vivido en California desde hace cinco años).

Cambio de la contraseña del Gestor de recopiladores para UNIX

1. Como usuario esecadm, vaya a $WORKBENCH_HOME.
2. Escriba el comando siguiente:

   PRECAUCIÓN: El sistema no le solicitará que confirme la contraseña o le solicitará la contraseña antigua.

   ```
   ./agent-manager.sh -password <nueva contraseña>
   ```

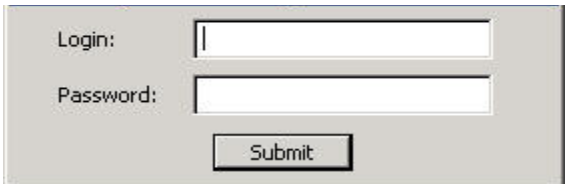
3. Para que la contraseña se active, vaya a /usr/local/bin y escriba el comando siguiente:

   ```
   ./agent-manager.sh -restart
   ```

Inicio del Generador de recopiladores

Inicio del Generador de recopiladores

1. Haga clic en *Inicio* > *Programas* > *Sentinel* > *Generador de recopiladores*, o bien haga doble clic en el icono *Generador de recopiladores* del escritorio.
2. Según la instalación, entre a la sesión como esecadedm o con el nombre de usuario de la autenticación de Windows.



Renombrado de un host del asistente

Renombrado de un host del asistente

1. En el Generador de recopiladores (el asistente), haga clic en la pestaña Hosts del asistente para abrir el panel del árbol correspondiente.
2. En el árbol Hosts del asistente, haga clic con el botón derecho en el host que desea renombrar y haga clic en *Renombrar* host. Sólo se puede renombrar un host que esté activo.
3. Escriba el nuevo nombre del host y pulse Intro.

   NOTA: El hecho de renombrar un host no cambia el número de ID que se asigna al host del asistente durante la instalación. Esta información se almacena en %WORKBENCH_HOME%\wizard\agents\names.dat.

Supresión de un host del asistente

Para suprimir un host, en primer lugar, éste se debe suprimir de la red, ya que los hosts que se están comunicando en la red no se pueden suprimir. Si un host se encuentra en la red pero no se está comunicando, dicho host aparecerá con una X roja sobre el icono de host en el árbol Hosts del asistente.

Supresión de un host del asistente

1. Haga clic en la pestaña *Hosts del asistente* para abrir el panel del árbol Hosts del asistente.
2. En dicho árbol, haga clic con el botón derecho en el host.
3. Haga clic en *Suprimir host.*

Reinicio de un host del asistente

Reinicio de un host del asistente

1. Haga clic en la pestaña *Hosts del asistente* para abrir el panel del árbol Hosts del asistente y seleccione un host.
2. Haga clic con el botón derecho en un host y seleccione *Iniciar el puerto*. Sólo se puede reiniciar un host del asistente que esté activo.

Exportación de un host del asistente

Exportación de un host del asistente

1. Haga clic en la pestaña Hosts del asistente para abrir el panel del árbol Hosts del asistente. Seleccione un host.
2. Haga clic en *Archivo* > *Exportar host* Se creará el subdirectorio siguiente:

   ```
   %WORKBENCH_HOME%\upload_<nombre del host>
   ```

   Este subdirectorio se puede mover a un equipo remoto mediante un shell de seguridad (SSH) o un disco. Una vez que el subdirectorio esté en el equipo remoto, ejecute el comando uploadhost. Éste copia todos los archivos necesarios en los directorios adecuados.

NOTA: Si se cambia la configuración de SNMP, el Generador de recopiladores no se podrá comunicar con el equipo remoto desde que se hace clic en el botón Exportar hasta que los archivos exportados del recopilador no se hayan cargado.

Visualización de las propiedades del host del asistente

Visualización de las propiedades del host del asistente

1. Haga clic en la pestaña Hosts del asistente para abrir el panel del árbol Hosts del asistente.
2. En el árbol Hosts del asistente, haga clic con el botón derecho en el host y haga clic en *Propiedades*. La ventana de propiedades del asistente muestra la información siguiente:
   - Nombre
   - ID
   - Nombre del host
   - Dirección IP
   - Versión
   - Tiempo de actividad
3. Haga clic en *Aceptar* para cerrar la ventana de propiedades.

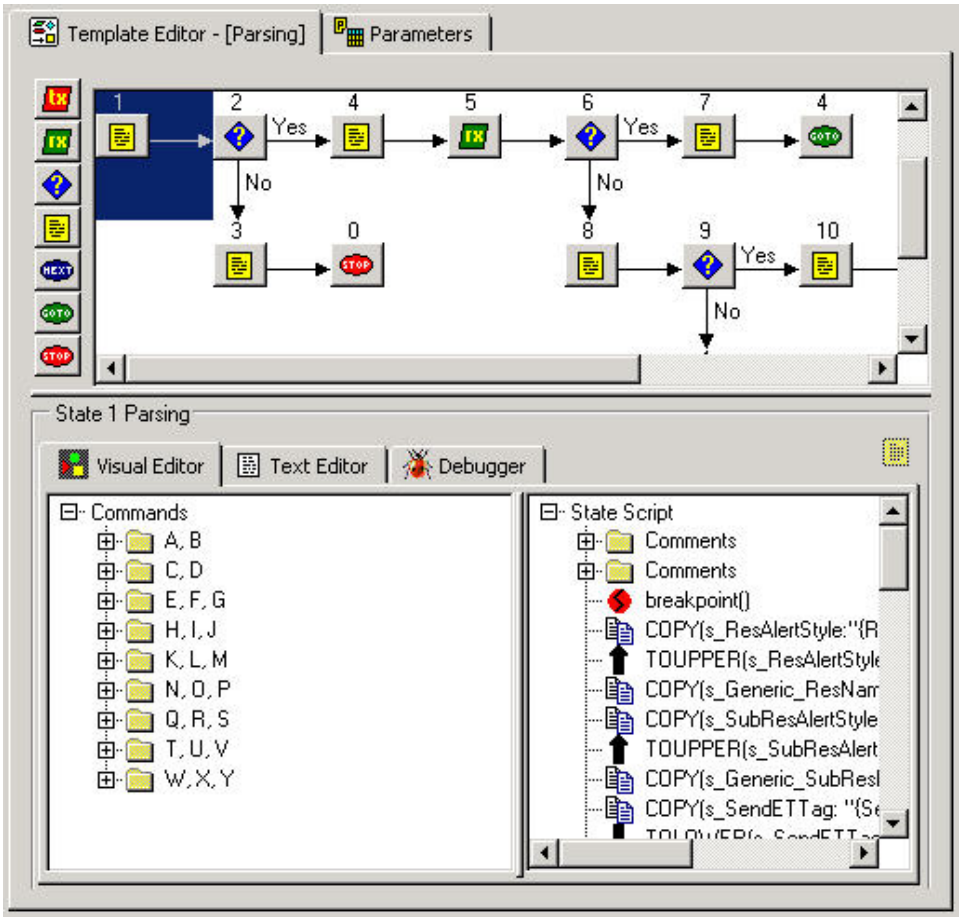
NOTA: Si el host no está ejecutándose, se mostrará una ventana de no respuesta cuando seleccione Propiedades.

Edición de un archivo de plantilla

Edición de un archivo de plantilla

1. Haga clic en la pestaña Recopiladores para abrir el panel del árbol Recopiladores.
2. En el árbol de recopiladores, haga clic en la plantilla y, después, en la pestaña Editor de plantillas de la derecha.

3. En el Editor de plantillas, haga clic en el estado que desea editar y realice los cambios deseados. Para editar un estado puede utilizar el editor visual o bien el editor de textos. Para obtener más información sobre los análisis de comandos, consulte la Guía de referencia del usuario de Sentinel.



Supresión de un archivo de plantilla

Supresión de un archivo de plantilla

1. Haga clic en la pestaña *Recopiladores* para abrir el panel del árbol Recopiladores.
2. En el árbol Recopiladores, haga clic con el botón derecho en una plantilla y, después, en *Suprimir la plantilla.*

Renombrado de un archivo de búsqueda

Renombrado de un archivo de búsqueda

1. Haga clic en la pestaña *Recopiladores* para abrir el panel del árbol Recopiladores.
2. Haga clic con el botón derecho en el archivo de búsqueda y haga clic en *Renombrar archivo de búsqueda*.
3. Escriba el nuevo nombre y pulse *Intro*.

Supresión de un archivo de búsqueda

Supresión de un archivo de búsqueda

1. Haga clic en la pestaña *Recopiladores* para abrir el panel del árbol Recopiladores.
2. Haga clic con el botón derecho en el archivo de búsqueda y haga clic en *Suprimir archivo de búsqueda*.

Supresión de un guión

Supresión de un guión

1. Existen dos métodos para suprimir un guión.
   - En el árbol Recopiladores, haga clic con el botón derecho en un guión y, después, haga clic en *Suprimir*.
   - Haga clic con el botón derecho en el guión en la columna Guiones de inicio o Guiones de sustitución y seleccione Suprimir guión.

Supresión de una secuencia de inicio

Supresión de una secuencia de inicio

1. En el panel Guiones de inicio, seleccione la secuencia de inicio del menú desplegable para que el nombre de la secuencia aparezca en el recuadro Guiones de inicio.
2. Haga clic con el botón derecho en el guión del árbol Recopiladores y seleccione Suprimir secuencia de inicio actual. De este modo, la secuencia de inicio se suprimirá de la lista de secuencias de inicio.

NOTA: Si se suprime la secuencia de inicio por defecto, todos los guiones asignados a la secuencia de inicio por defecto se eliminarán de la columna Guiones de inicio, pero, por defecto, todavía aparecerán en el menú Secuencias de inicio.

Puertos del asistente

En este apartado se describe la detención, inicio, edición, supresión y depuración de un puerto del asistente.

Inicio y detención de un puerto del asistente: GUI

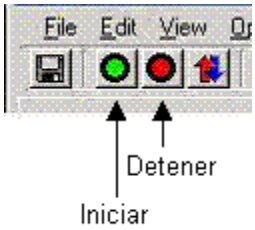
Cuando un recopilador se inicia o se detiene, los botones Iniciar o Detener en la columna Iniciar/Detener, cambiarán una vez que el recopilador se inicie o se detenga. Si se trabaja con un recopilador remoto, el cambio puede ser más lento, ya que se tarda un poco más en recibir el estado del recopilador.

Al iniciar o detener un puerto se ejecutan los guiones de inicio y los guiones de restitución seleccionados.

Al iniciar todos los puertos, un puerto sólo se iniciará si el recuadro Ejecutar puerto durante el inicio está seleccionado en Otras opciones del puerto del menú Opciones.

Inicio y detención de todos los puertos del asistente

1. En la ventana del asistente:
   - Para detener todos los puertos, haga clic en el botón Detener de la barra de herramientas.
   - Para iniciar todos los puertos, haga clic en el botón Iniciar de la barra de herramientas.



Inicio y detención de un puerto del asistente

1. En la ventana del asistente:
   - Para detener un puerto, haga clic en el botón Detener situado en la columna Iniciar/Detener que corresponde al puerto.
   - Para iniciar un puerto, haga clic en el botón Iniciar situado en la columna Iniciar/Detener que corresponde al puerto.

Edición de un puerto d el asistente

Si se editan los valores de configuración de un puerto mientras éste se encuentra en ejecución, dicho puerto se detendrá. Para evitar la pérdida de datos, detenga el puerto de forma manual antes de editar su configuración.

Edición de un puerto de un asistente

1. Para el host adecuado, detenga el puerto.
2. Siga los pasos para crear un puerto del asistente del capítulo 3: La nueva configuración sobrescribirá la configuración existente cuando guarde o cargue el puerto.

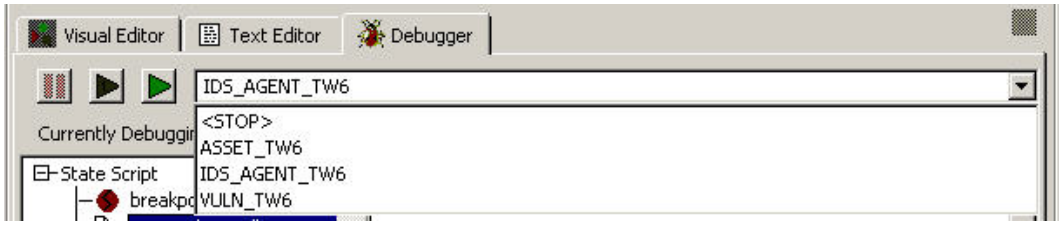
Supresión de un puerto del asistente

Supresión de un puerto del asistente

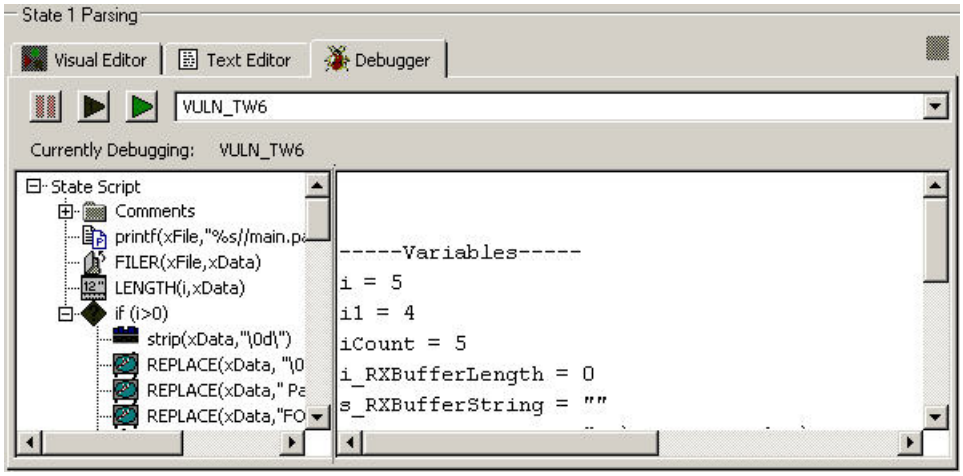
1. Detenga el puerto.
2. En el panel de información del puerto del Generador de recopiladores, haga clic con botón derecho en el nombre del puerto y seleccione Suprimir puerto. Todos los puertos que estén bajo el puerto seleccionado se detendrán automáticamente.
3. Si realiza la supresión desde:
   - Host local: haga clic en *Archivo* > *Guardar* y seleccione Información del puerto.
   - Host remoto: haga clic en *Archivo* > *Cargar/Descargar*.

Depuración de un puerto del asistente

El depurador permite solucionar problemas de ejecución del código del recopilador en un puerto. En el lado izquierdo del panel del depurador se muestra el guión de estado, mientras que en el derecho se muestran los guiones y las variables RX_Buffer, que pueden contener nombres de hasta 32 caracteres.



Para que el depurador esté activo, se debe tener un estado de Análisis como el primer estado y comandos Breakpoint().



Además, mientras está depurando, se debe esperar a la actualización de Rx Buffer antes de realizar otra función.

NOTA: Si el host del Gestor de recopiladores ha perdido la conexión (), no se podrá depurar un puerto de ese host del Gestor de recopiladores.

Depuración de un puerto del asistente

1. En el Editor de plantillas, seleccione la pestaña Depurador en el panel de edición para acceder al depurador. En el panel en blanco que aparece, podrá seleccionar el puerto del asistente que desee depurar de la lista desplegable.

   Si hace clic en la pestaña Hosts del asistente, el puerto que se está depurando indicará que está en modo de depuración.

VULN_TW6	File All	C:\workarea\vuln_inf	DemoVulnerabilityUploa	Stop	Debug
ASSET_TW6	File All	c:\workarea\asset_o	T1_GNUx_NMAP_035	Start	Off

2. En la lista desplegable, seleccione un puerto para iniciar el proceso de depuración. Para depurar el puerto, utilice uno de los métodos siguientes:
   - Pulse F6 para pasar por los comandos de uno en uno o haga clic en el botón Ejecutar un comando

     Vuelva a hacer clic en el botón o pulse F6 para reanudar la ejecución del guión.
   - Pulse F7 para pasar por los comandos o haga clic en el botón Reanudar la ejecución del comando.

     Pulse F5 para que se detenga o haga clic en el botón Poner en pausa la ejecución del comando.

     Así se mantendrá en pausa hasta que se pulse F5 de nuevo o el botón Reanudar la ejecución del comando.

   El depurador se detiene en todos los puntos de límite, pero continúa en ejecución. El estado del puerto es “activo”.

   Durante el modo de depuración, no se envía ningún evento durante las pausas.

   Cuando se sale del analizador, los botones se atenúan y la lista de selección muestra “No se está depurando ningún puerto”.

   El depurador no cancelará la pausa, por tanto, si va a depurar un analizador que ha ejecutado un comando de pausa, el botón Detener o el botón Paso a paso no llevarán a cabo ninguna acción hasta que la pausa se complete.

Carga y descarga de recopiladores y hosts

En la ventana Cargar/Descargar, existen las tres pestañas siguientes:

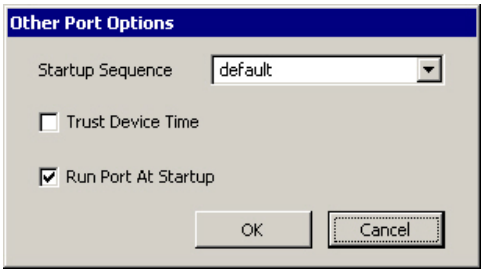
- Hosts: permite cargar la configuración de cada puerto individual y la colección de recopiladores en cada uno de los hosts especificados. Cada uno de los hosts continuará manteniendo su propia configuración del puerto y la colección de recopiladores.
- Recopiladores: permiten cargar los recopiladores individuales.
- Incluir datos en la red: permite cargar la configuración o los agentes del puerto de un único host especificado en todos los hosts seleccionados. De este modo, todos los hosts seleccionados tendrán la misma configuración del puerto y la colección de recopiladores que el host de origen.

Durante la descarga, la configuración del puerto de un recopilador remoto aparecerá en el host que elija para descargar y todos los recopiladores del host remoto con el mismo nombre que el host local se sobrescribirán.

Carga de un recopilador en un único host

Carga de un recopilador en un único host

1. Si el recopilador ya está configurado correctamente y ha generado el guión, puede omitir los pasos del 2 al 11.
2. Haga clic en la pestaña Hosts del asistente y seleccione un host.
3. En la columna Nombre del puerto, haga doble clic en *Nuevo...* y escriba el nombre que desee.
4. En la columna Recopiladores, seleccione un recopilador.
5. Configure el recopilador, como se indica en la documentación correspondiente (`%WORKBENCH_HOME%\Elements\<nombre del recopilador>\docs\<nombre del archivo>.pdf`).
6. Haga clic en la pestaña *Recopiladores*, expanda el recopilador y resalte el archivo de plantilla.
7. En la parte derecha, haga clic en la pestaña *Parámetros*.
8. Defina los valores de los parámetros como se indica en la documentación del recopilador.
9. (opcional) Si desea que el recopilador no arranque al iniciar o que confíe en la hora del dispositivo, haga clic en la pestaña *Hosts del asistente*, haga clic con el botón derecho en el nombre del puerto del asistente, seleccione *Opciones de otros puertos* y deseleccione *Ejecutar puerto durante el inicio,* o haga clic en *Confiar en la hora del dispositivo*. Haga clic en *Aceptar*.



10. Haga clic en *Guardar*.
11. Haga clic en la pestaña *Recopiladores*; con el botón derecho del ratón, haga clic en el archivo de plantilla y seleccione *Generar guiones.*
12. Haga clic en:
    - *Archivo* > *Cargar/Descargar.*
    - Haga clic con el botón derecho en *Recopilador* y haga clic en *Cargar recopilador.*
    - Haga clic en el botón *Cargar/Descargar* 

    Se abrirá la ventana *Cargar/Descargar*.
13. En la ventana *Cargar/Descargar*, haga clic en la pestaña *Recopiladores*.

14. En la lista desplegable, seleccione el *recopilador* que desea cargar.
15. Haga clic en *Cargar*. La primera vez que lleve a cabo esta tarea, el sistema le solicitará una contraseña del *Gestor de recopiladores*, incluso para un host del asistente local. Se abrirá la ventana de curso de la transferencia, en la que se muestra el curso de ésta.

NOTA: La ventana de curso de la transferencia se puede utilizar para reiniciar los hosts tras una transferencia.

Carga de un recopilador en varios hosts

Carga de un recopilador en varios hosts

PRECAUCIÓN: Si se carga un host que tiene un recopilador con el mismo nombre que uno ya existente en el host local, el recopilador del host remoto se sobrescribirá sin previo aviso.

1. Si el recopilador ya está configurado correctamente y ha generado el guión, puede omitir los pasos del 2 al 11.
2. Haga clic en la pestaña *Hosts del asistente* y seleccione un host.
3. En la columna Nombre del puerto, haga doble clic en *Nuevo*... y escriba el nombre que desee.
4. En la columna *Recopiladores*, seleccione un recopilador.
5. Configure el recopilador, como se indica en la documentación correspondiente (`%WORKBENCH_HOME%\Elements\<nombre del recopilador>\docs\<nombre del archivo>.pdf`).
6. Haga clic en la pestaña *Recopiladores*, expanda el recopilador y resalte el archivo de plantilla.
7. En la parte derecha, haga clic en la pestaña *Parámetros*.
8. Defina los valores de los parámetros como se indica en la documentación del recopilador.
9. (opcional) Si desea que el recopilador no arranque al iniciar o que confíe en la hora del dispositivo, haga clic en la pestaña *Hosts del asistente*, haga clic con el botón derecho en el nombre del puerto del asistente, seleccione Opciones de otros puertos y deseleccione Ejecutar puerto durante el inicio, o haga clic en Confiar en la hora del dispositivo. Haga clic en Aceptar.
10. Haga clic en Guardar.
11. Haga clic en la pestaña Recopiladores para abrir el panel del árbol Recopiladores.
12. Haga clic en un recopilador.
13. Haga clic en:
    - Archivo > Cargar/Descargar.
    - Haga clic en Recopiladores y seleccione Cargar recopilador.
    - Haga clic en el botón Cargar/Descargar 

    Se abrirá la ventana de Cargar/Descargar.

14. En la ventana Cargar/Descargar, haga clic en la pestaña Hosts y seleccione o deseleccione la casilla de verificación Cargar recopiladores al cargar.

    Si ha seleccionado esta casilla de verificación, los recopiladores seleccionados en la pestaña Recopiladores se cargarán. Esta casilla de verificación está seleccionada por defecto. Esta opción no tiene ningún efecto al descargar recopiladores desde un host.

15. En la lista, seleccione los hosts del asistente en los que desee cargar los recopiladores.

    Todos los hosts del asistente de la red del asistente se incluirán automáticamente en la lista. Los botones indican si el equipo host está conectado o no.

    Haga clic en Seleccionar todo para seleccionar todos los hosts del asistente de la lista. Haga clic en No seleccionar ninguno para deseleccionar todos los hosts del asistente de la lista.

16. Haga clic en Cargar para cargar los recopiladores seleccionados en los hosts seleccionados. La primera vez que lleve a cabo esta tarea, el sistema le solicitará una contraseña de Gestor de recopiladores, incluso para un host del asistente local.

Descarga de un host

Descarga de un host

PRECAUCIÓN: Si descarga un host que tiene un recopilador con el mismo nombre que uno ya existente en el host local, el recopilador del host local se sobrescribirá sin previo aviso.

1. Haga clic en la pestaña Hosts del asistente para abrir el panel del árbol Hosts
2. En el árbol del asistente Hosts del asistente, haga clic en el host que desee descargar.
3. Haga clic en:
   - Archivo > Cargar/Descargar.
   - Haga clic en Recopiladores y seleccione Cargar recopilador.
   - Haga clic en el botón Cargar/Descargar 

   Se abrirá la ventana de Cargar/Descargar. El recopilador que ha seleccionado se selecciona por defecto.
4. Haga clic en Descargar. La primera vez que lleve a cabo esta tarea, el sistema le solicitará una contraseña de Gestor de recopiladores, incluso para un host del asistente local. El host se descargará y se añadirá al árbol Hosts del asistente. Se abrirá la ventana de curso de la transferencia, en la que se muestra el curso de ésta.

NOTA: La ventana de curso de la transferencia se puede utilizar para reiniciar los hosts tras una transferencia.

NOTA: Sólo puede descargarse un host a la vez. Si se selecciona más de un host, las descargas no se llevarán a cabo.

Descarga de recopiladores desde un único host

Descarga de recopiladores desde un único host

1. Haga clic en:
   - Archivo > Cargar/Descargar.
   - Haga clic en el botón Cargar/Descargar 

   Se abrirá la ventana de Cargar/Descargar.
2. En la lista, seleccione el host del asistente desde el que desee descargar los recopiladores,

   Todos los hosts del asistente de la red del asistente se incluirán automáticamente en la lista. Los botones indican si el equipo host está conectado o no.

   Haga clic en Seleccionar todo para seleccionar todos los hosts del asistente de la lista. Haga clic en No seleccionar ninguno para deseleccionar todos los hosts del asistente de la lista.
3. Haga clic en Descargar para descargar los recopiladores seleccionados desde el host seleccionado.

Carga de puertos en varios hosts

Carga de puertos en varios hosts

1. Haga clic en:
   - Archivo > Cargar/Descargar.
   - Haga clic en el botón Cargar/Descargar 
2. Se abrirá la ventana de Cargar/Descargar.
3. En la ventana Cargar/Descargar, haga clic en la pestaña Incluir datos en la red.
4. En la lista denominada 'Seleccione los recopiladores y la configuración del puerto del host que desea cargar', seleccione el host del que desea cargar los valores de configuración del puerto y los recopiladores.
5. En la lista denominada 'Seleccione los hosts en los que desea cargar esta configuración' seleccione el host del que desea cargar la configuración seleccionada.

   Todos los hosts del asistente de la red del asistente se incluirán automáticamente en la lista. Los botones indican si el equipo host está conectado o no.

   Haga clic en Seleccionar todo para seleccionar todos los hosts del asistente de la lista. Haga clic en No seleccionar ninguno para deseleccionar todos los hosts del asistente de la lista.

Carga de varios recopiladores en una red

Carga de varios recopiladores en una red

1. Desde la ventana principal del asistente, seleccione un recopilador en el árbol Recopiladores.
2. Haga clic en:
   - Archivo > Cargar/Descargar.
   - Haga clic en Recopiladores y seleccione Cargar recopilador.
   - Haga clic en el botón Cargar/Descargar 
3. Seleccione la pestaña Incluir datos en la red.
4. En el primer recuadro de selección del menú desplegable, seleccione los recopiladores y la configuración del puerto del host que desea cargar.
5. En el segundo recuadro de selección del menú desplegable, seleccione en qué hosts desea cargar la configuración.

   NOTA: Al menos debe seleccionarse una opción de las anteriores para poder cargar la configuración correspondiente.

   Es posible seleccionar un recopilador distinto en cada recuadro desplegable. Cada recopilador seleccionado en la lista principal adquirirá la configuración del puerto y los recopiladores del host seleccionado en el recuadro denominado:

   "Seleccione los recopiladores y la configuración del puerto del host que desea cargar" a menos que Ninguno esté seleccionado.
6. Una vez que haya completado la configuración de la red, seleccione el botón Cargar para que comience el proceso de carga.

Actualización de los recopiladores

Actualización de los recopiladores

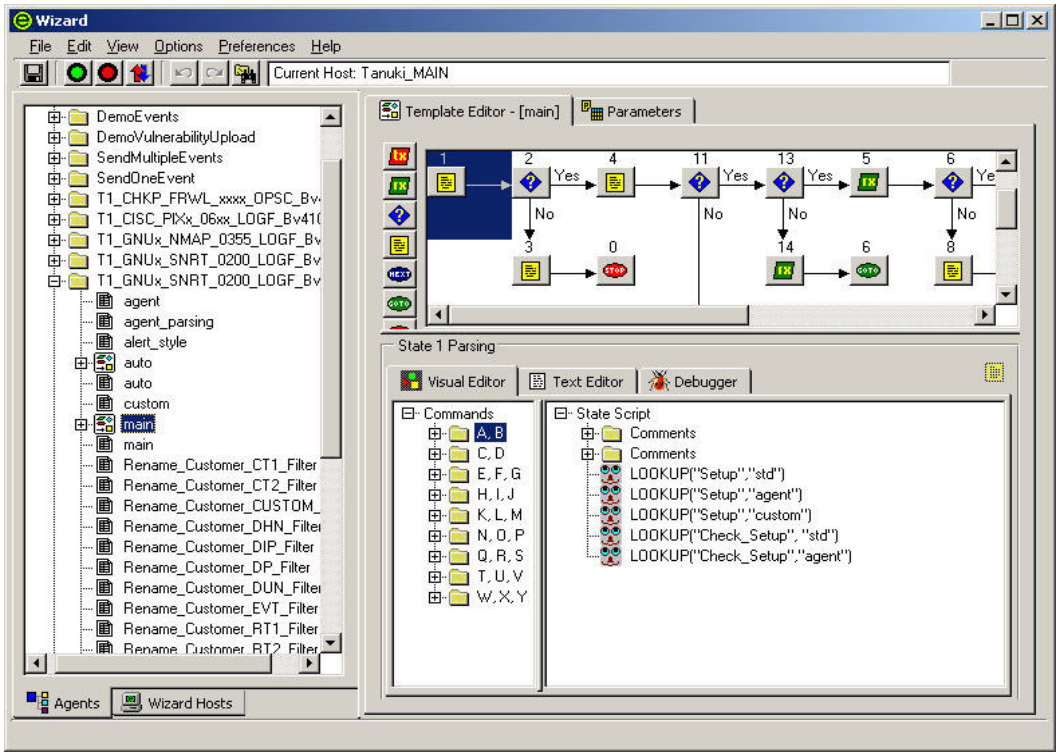
1. Lea la documentación que se adjunta con el nuevo recopilador, en la que se explican los cambios.
2. Coloque la nueva versión del recopilador en el directorio %workbench_home%Elements del PC que es el principal del recopilador.
3. Abra el archivo de parámetros del recopilador que se está sustituyendo, corte y pegue los parámetros que concuerden en el nuevo recopilador.
4. Si es necesario, para suprimir o añadir nuevas variables de parámetros siga las instrucciones de la documentación del nuevo recopilador. Si va a añadir nuevas variables de parámetros, rellene la variable con datos.
5. Guarde el archivo de parámetros en el nuevo recopilador.
6. Genere el nuevo recopilador.
7. Edite la información de configuración del puerto que utilizar el nuevo recopilador.
8. Guarde la información de configuración del puerto:
9. Guarde la configuración del puerto y el nuevo recopilador:
10. Reinicie el puerto

3 Generación y mantenimiento de recopiladores

NOTA: El término Agente puede intercambiarse con Recopilador. En adelante, los agentes se denominarán recopiladores.

NOTA: Para los usuarios de MS SQL 2000, el tamaño del evento no puede ser superior a 8 KB.

Un recopilador es el responsable de analizar los datos de un origen de eventos de seguridad y enviar los eventos a Sentinel. Los recopiladores se generan, activan y mantienen a través del Generador de recopiladores del asistente. Haga clic en la pestaña *Recopiladores* para visualizar el árbol Recopiladores y ver todos los recopiladores y sus componentes en el sistema Sentinel.



El Gestor de recopiladores permite realizar las operaciones siguientes:

- Generación de recopiladores
  - Creación y configuración de archivos de plantilla
  - Creación de archivos de parámetros
  - Creación de archivos de búsqueda
  - Generación de guiones
  - Creación de un puerto del asistente

Aspectos básicos en la generación de recopiladores

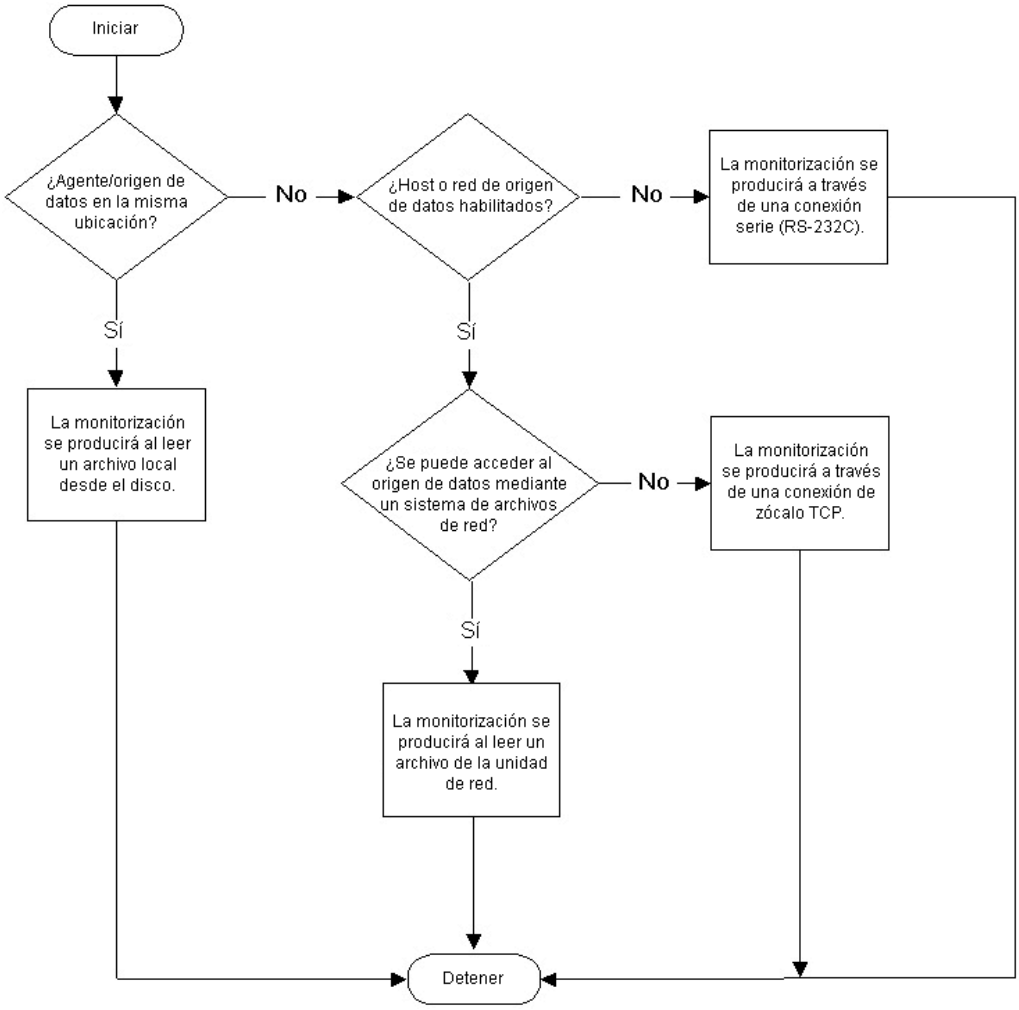
Los pasos básicos para la generación de recopiladores son:

- Crearción y configuración de un archivo de plantillas, incluyendo los puntos de decisión basados en cómo aplicar estados
- Creación y configuración de archivos de parámetros
- Creación y configuración de archivos de parámetros (opcional)
- Generación de guiones
- Asignación de una secuencia de inicio
- Creación de un puerto, asignación de un recopilador al puerto e inicio del puerto

Pasos básicos para la implementación de recopiladores

A continuación se enumeran los pasos básicos para implementar un recopilador:

- Determinar qué desea monitorizar.
- Determinar cómo monitorizar los datos.
- Determinar el sistema operativo del producto.
  - Si el host y el producto se encuentran en la misma ubicación, el modo más lógico de obtener los datos es leerlos del archivo de registro del producto.
  - Si el host y el producto no se encuentran en la misma máquina, los datos necesarios se pueden obtener a través de una configuración del sistema de archivos de red (como recurso compartido NFS, Samba o SMB), una conexión por zócalo TCP/IP o una conexión en serie.
- Generar los recopiladores e iniciar los puertos.
- Si se utilizan hosts remotos, cargue los archivos de recopiladores en los hosts remotos. Inicie el puerto para ejecutar los guiones de inicio; la información recopilada se notificará a través del sistema Sentinel.



Generación de un recopilador

Como se menciona más arriba, la generación de un recopilador requiere crear:

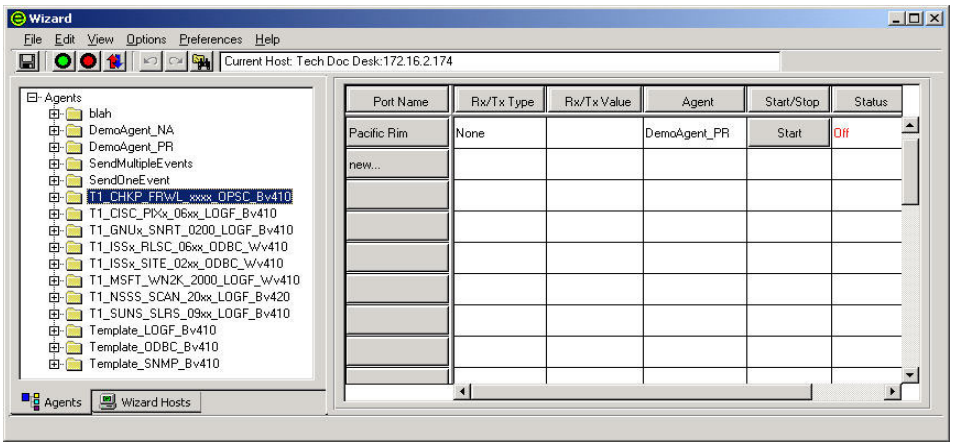
- Archivos de plantilla
- Archivos de parámetros
- Archivos de búsqueda (opcional)
- Guiones
- Asignación de un nombre de puerto del asistente a un recopilador

Creación y configuración de archivos de plantilla

Creación y configuración de archivos de plantilla

1. Inicie el Generador de recopiladores.
2. Haga clic en la pestaña *Recopiladores* para abrir el panel del árbol Recopiladores.
3. En el árbol Recopiladores, haga clic con el botón derecho del ratón en *Recopiladores* y haga clic en *Recopilador nuevo*.

4. Introduzca el nombre del nuevo recopilador en el espacio disponible y pulse Intro.
5. Haga clic con el botón derecho del ratón en el recopilador nuevo y haga clic en *Plantilla nueva.*



6. En el recuadro Plantilla nueva del árbol Recopiladores, escriba un nombre nuevo para la plantilla y pulse Intro.
7. Seleccione la nueva plantilla y haga clic en la pestaña *Editor de plantillas*.
8. En el panel *Editor de plantillas*, arrastre y suelte los estados hasta el área de edición con los botones de estado de la parte izquierda del panel. Para obtener información sobre cómo añadir estados a una plantilla, consulte Añadir estados a una plantilla.
9. Haga clic en *Guardar*.

Adición de un estado a un archivo de plantilla

Todos los recopiladores empiezan el procesamiento en el estado 1, independientemente del lugar del estado 1 en la plantilla. Si se supone que el estado 1 es un estado de procesamiento, inserte el nuevo estado a continuación del estado 1.

El Generador de recopiladores asigna automáticamente al primer estado el número de estado 1. Se recomienda que este primer estado contenga sólo un comando de análisis BREAKPOINT(). Al incorporar sólo un punto de límite después del estado 1, se facilita la depuración. Durante la depuración, el analizador se detendrá automáticamente en el estado siguiente.

Cuando genere una plantilla, comience con un estado de análisis de “sólo punto de límite”. A continuación, añada el estado de Trabajo (estado de Recepción, estado de Análisis, etc.) en el estado 2. Si necesita añadir un estado al principio de la plantilla, insértelo después del estado sólo punto de límite.

No suprima el estado de Análisis de sólo punto de límite a menos que sea necesario para añadir otro estado al principio de la plantilla. De manera opcional, puede introducir comentarios sobre las funciones de la plantilla en este sólo punto de límite.

Cómo añadir un estado a una plantilla

1. Haga clic en la pestaña *Recopiladores* para abrir el panel del árbol Recopiladores.
2. En el árbol Recopiladores, seleccione una plantilla para mostrar el editor de plantillas en el panel derecho.
3. Haga clic en *Opciones > Añadir estado > Estados de Transmisión, Recepción, Decisión, Análisis, Siguiente, Ir o Detener*, según el caso, o haga clic en los botones correspondientes.
   -  Transmisión
   -  Recepción
   -  Decisión
   -  Análisis
   -  Siguiente
   -  Ir
   -  Detener
4. Mediante los paneles de edición de la parte inferior del panel Editor de plantillas, inserte el código nuevo en cada estado a medida que lo añade.

   Otro método consiste en arrastrar y soltar un botón de estado de Análisis desde la parte de la izquierda del editor de plantillas hasta el área de edición.

NOTA: No utilice las dobles comillas como parte de una cadena de decisión ni en un estado de Recepción (para que coincida el delimitador en un archivo de registro, por ejemplo) ni en un estado de Decisión, de lo contrario, aparecerá el mensaje de error siguiente:

```
***ERROR: Leyendo archivo de plantilla..."
```

Cuando se introducen una o más comillas en la cadena de decisión o del delimitador, se produce una incoherencia de comillas como se muestra a continuación:

```
CadenadeDecisióndeEstado: "test"123"
```

La solución es utilizar \22\ en lugar de una comilla (“).

NOTA: Si selecciona otro elemento de la pestaña Recopiladores (incluso en el mismo recopilador) y después vuelve a la plantilla afectada, el Generador de recopiladores mostrará un mensaje de error y no mostrará ninguna parte ni estados de la plantilla. El error se produce porque el carácter de comilla (") se utiliza para delimitar los valores de campo en un archivo .tem. Por ejemplo:

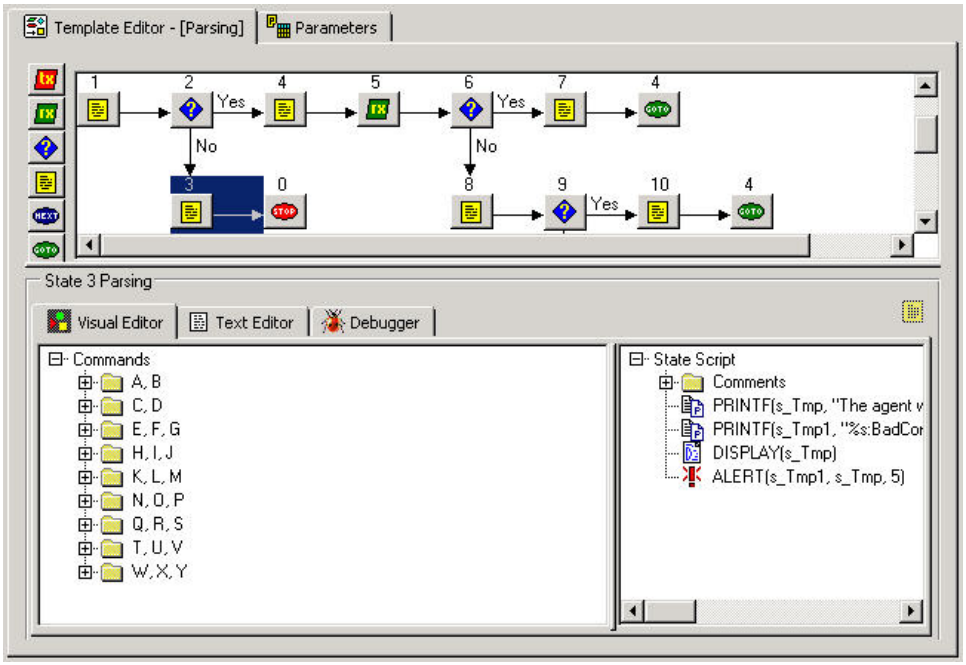
```
CadenadeDecisióndeEstado: "test"123"
CadenadeDelimitadordeEstado "123"
```

Introducción de un comando de análisis mediante el editor visual

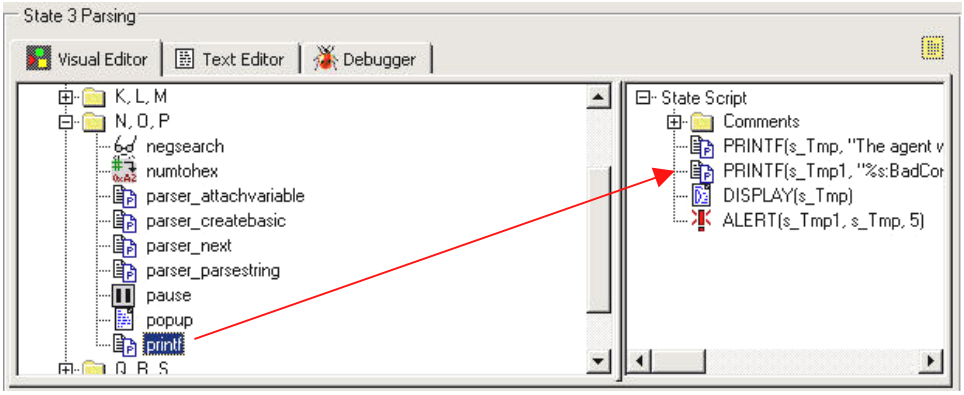
Existen dos métodos para introducir un comando de análisis: mediante el editor visual o mediante el editor de textos. Limite los comandos a un valor inferior a 4096.

Introducción de un comando de análisis mediante el editor visual

1. En el editor de plantillas, seleccione un estado de Análisis. La pestaña Editor visual se abre por defecto cuando se hace clic en una plantilla para abrirla.



2. En el editor visual, arrastre los comandos de análisis hacia la derecha del panel.



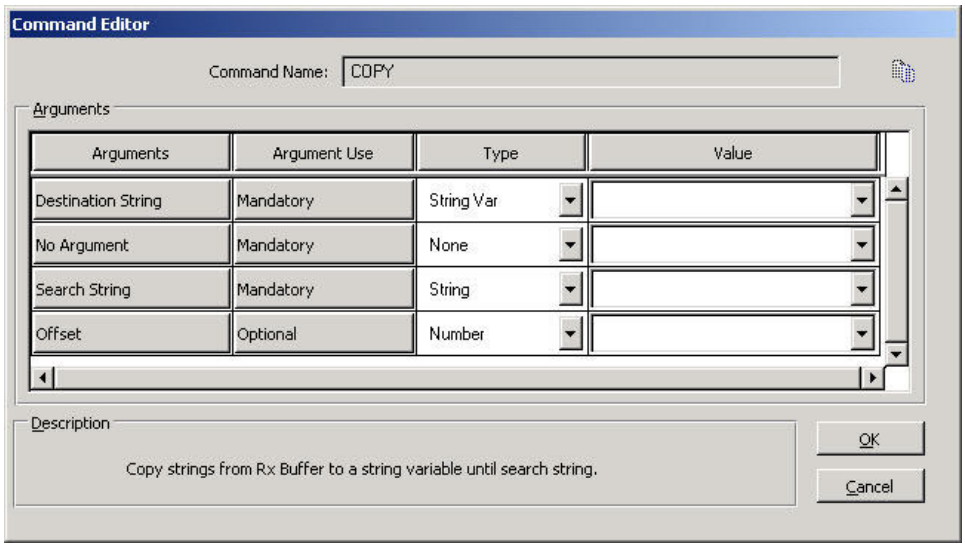
3. Introduzca los valores de argumento en la ventana Editor de comandos emergentes.
   - Seleccione un tipo: los tipos de cada comando de análisis se describen en la Guía de referencia del usuario de Sentinel.
   - Especifique un valor: los valores se definen para una aplicación específica. En la Guía de referencia del usuario de Sentinel se incluyen ejemplos de valores para cada comando de análisis.

Introducción de un comando de análisis mediante el editor de textos

1. En el editor de plantillas, haga clic en la pestaña *Editor de texto*.
2. Introduzca manualmente los comandos de análisis.

   Utilice la tecla de tabulación del teclado para alinear el texto cuando utilice una fuente fija. Las opciones para copiar, cortar y pegar funcionan del mismo modo que en un editor de textos estándar.

Edición de un comando de análisis



- Argumentos: incluye todos los argumentos posibles para el comando de análisis seleccionado en el editor visual.
- Uso de argumento: determina si el argumento es obligatorio u opcional.
- Tipo: determina el tipo de variable; por ejemplo, cadenas, variables de cadena, números, variables de números, valores flotantes, variables de valores flotantes o variables predefinidas.
- Valor: valor que se define para la variable que se nombra en la columna Tipo.

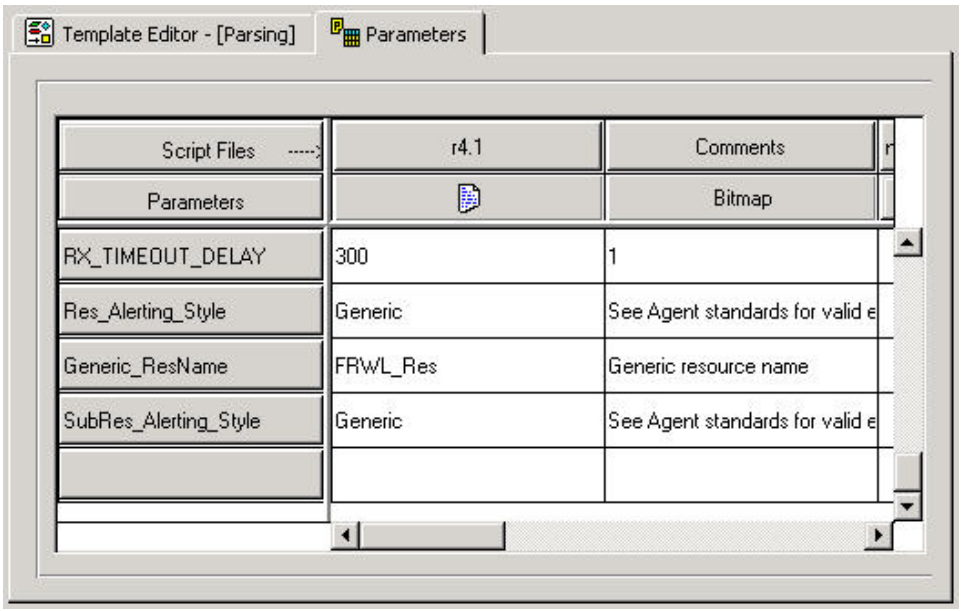
Edición de un comando de análisis

1. En el editor visual, realice una de las operaciones siguientes:
   - Haga clic con el botón derecho del ratón en el comando de análisis y elija *Añadir a la lista de análisis de estado*.
   - Haga doble clic en un comando de análisis y se abrirá el editor de comandos.
2. Rellene los recuadros Tipo y Valor para completar la edición. Consulte la Guía de referencia del usuario de Sentinel para obtener más información sobre las descripciones de los comandos de análisis.

Creación y configuración de archivos de parámetros

Creación y configuración de archivos de parámetros

1. Haga clic en la pestaña *Recopiladores*.
2. Seleccione una plantilla y haga clic en la pestaña *Parámetros* de la parte de la derecha del panel.



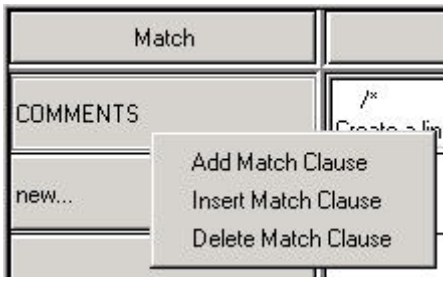
3. Haga doble clic en el botón *Nuevo*… de la primera columna de la tabla Parámetros.
4. Introduzca el nombre del nuevo parámetro (éste es el nombre del guión, por ejemplo r4.1) y pulse Intro.
5. (Opcional) Haga clic con el botón derecho en el botón *Mapa de bits* (segunda columna/segunda fila) y haga clic en *Asignar mapa de bits*. En el recuadro de diálogo Asignación de mapa de bits, seleccione el botón *Mapa de bits*.
6. Haga doble clic en cada uno de los recuadros de parámetros nuevos e introduzca los valores adecuados.
7. Una vez definidos todos los valores, el parámetro y el archivo de plantilla deben compilarse para crear un guión. Vaya a la sección Generación de guiones

Creación y configuración de archivos de búsqueda

Este procedimiento es opcional.

Creación y configuración de archivos de búsqueda

1. Haga clic en la pestaña *Recopiladores* para abrir el panel del árbol Recopiladores.
2. Haga clic con el botón derecho del ratón en un recopilador y haga clic en *Nuevo archivo de búsqueda.*
3. En el recuadro Nuevo archivo de búsqueda, escriba un nombre nuevo para el archivo de búsqueda y pulse Intro.
4. En la columna Coincidencia, haga doble clic en *Nuevo*… e introduzca la cadena que desea buscar y pulse Intro. Puede añadir, insertar y suprimir oraciones de coincidencia.
   - Para añadir: en la columna Coincidencia, haga clic con el botón derecho en la oración de coincidencia y haga clic en *Añadir oración de coincidencia.*
   - Para insertar: en la columna Coincidencia, haga clic con el botón derecho en la oración de coincidencia y haga clic en *Insertar oración de coincidencia.*
   - Para suprimir: en la columna Coincidencia, haga clic con el botón derecho en la oración de coincidencia y haga clic en *Suprimir oración de coincidencia.*



5. (Opcional) Para introducir comandos de análisis, haga clic con el botón derecho en la columna Análisis para abrir el editor visual. Para obtener información sobre cómo usar el editor visual, consulte Introducir comandos de análisis con el editor visual
6. Seleccione los comandos de análisis y complételos en la ventana Editor de comandos. Los comandos se muestran en la columna Análisis.
7. Una vez definidos todos los valores, éstos deben compilarse para crear un guión. Vaya a la sección Generación de guiones

Guiones

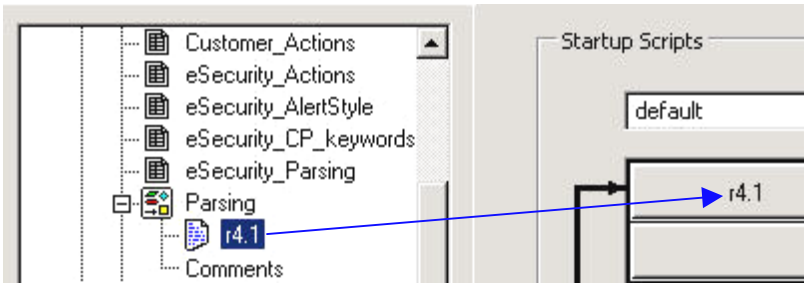
Los guiones se generan a partir de plantillas. A partir de una plantilla, es posible generar múltiples guiones. El Gestor de recopiladores permite realizar las operaciones siguientes:

- Generación de guiones
- Depuración de guiones
- Asignación de una secuencia de inicio

Generación de un guión

Generación de un guión

1. Haga clic en la pestaña *Recopiladores* para abrir el panel del árbol Recopiladores.
2. En el panel de la izquierda, seleccione la plantilla a partir de la que va a generar los guiones.
3. Seleccione *Archivo* > *Crear guiones*.
4. En la pestaña Editor de plantillas, arrastre un guión desde la plantilla hasta la columna Guiones de inicio o Guiones de restitución del panel de la derecha.



Los guiones se ejecutan en el orden en el que aparecen en las columnas Guiones de inicio y Guiones de restitución. Para reorganizar el orden de los guiones, arrastre los guiones hacia arriba o hacia abajo en las columnas.

NOTA: El guión final de una secuencia de restitución debe finalizar con el estado de procesamiento Detener.

5. (Opcional) Realice una depuración mediante el depurador.
6. Haga clic en *Archivo* > *Guardar*.
7. Para que los cambios surtan efecto, detenga e inicie el puerto mediante los botones Detener e Iniciar de la barra de herramientas.

Habilitación de la autogeneración para recopiladores de versiones anteriores a la 5.0

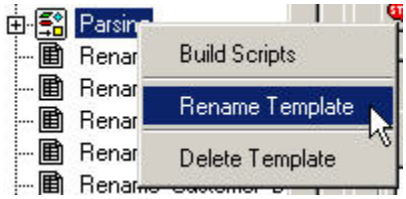
La habilitación de la función Autogenerar permite evitar el paso de generar el guión cuando configura e implanta recopiladores.

Para habilitar la autogeneración para recopiladores de versiones anteriores a la 5.0

1. Copie los archivos siguientes desde un recopilador v5.* existente y péguelos en el recopilador en el que desea habilitar la autogeneración.
   - auto.tem
   - auto.asd

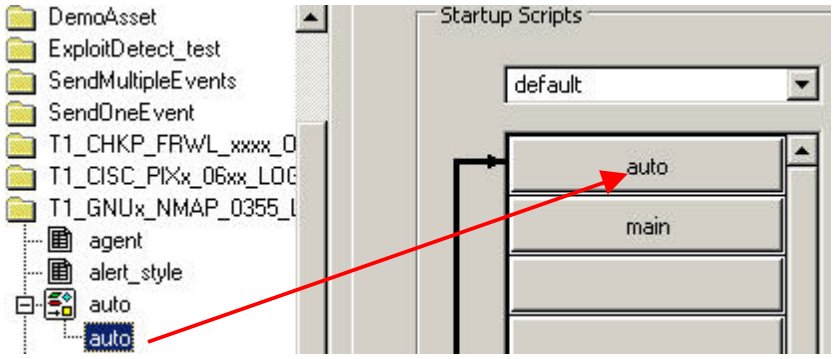
- auto.lkp
- auto.par

2. Cambie el nombre del archivo de plantilla por main.tem. Puede realizar esta operación en el Generador de recopiladores.



3. Resalte el archivo de plantilla renombrado y haga clic en la pestaña *Parámetros*. Cambie el nombre del encabezado de la columna que tiene el nombre del archivo de guión (por ejemplo, r4.1) por main y pulse la tecla Intro.

4. Haga clic en el botón *Guardar*.
5. En la cadena de inicio, haga clic con el botón derecho del ratón y arrastre el archivo auto.asd hasta una posición anterior al archivo main.



Depuración de un guión

Cuando inicia el proceso de depuración, el estado del puerto está definido como “Depurar" en el panel de información del puerto. Para depurar un guión, consulte Depuración de un puerto del asistente en el capítulo 2.

Asignación de una secuencia de inicio a un guión

Si desea que un puerto se ejecute durante el inicio, puede asignar una secuencia de inicio para que ejecute un conjunto específico de guiones al iniciar. Una secuencia de inicio es un archivo que contiene los nombres de los guiones que se ejecutan durante el inicio.

Asignación de una secuencia de inicio a un guión

1. Haga clic con el botón derecho del ratón en el árbol Recopiladores y seleccione Secuencia de inicio nueva. Aparecerá el recuadro de diálogo Secuencia de inicio nueva.
2. En el recuadro de diálogo Secuencia de inicio nueva, escriba el nombre de la secuencia y haga clic en *Aceptar*. El nombre de la secuencia de inicio nueva se añade al menú de la parte superior del panel de guiones de inicio. Las siguientes restricciones se aplican a los nombres de secuencias:
   - No utilice inicio y restitución como nombres de secuencias.
   - No utilice más de una vez el mismo nombre de una secuencia dentro del mismo recopilador.
3. Arrastre los nombres de los archivos de guiones desde el árbol Recopiladores hasta la columna Guiones de inicio. Los guiones se ejecutan en el orden en el que aparecen en la columna, en orden descendente.
4. Para reorganizar el orden de los guiones, arrastre los guiones desde la columna o haga clic con el botón derecho del ratón en el panel de *guiones de inicio* y seleccione *Reordenar guión de inicio.*

Creación de un puerto del asistente

Para un recopilador, es posible crear más de un puerto. Para algunos tipos de sensores, puede que necesite crear más de una instancia del mismo recopilador y asignar cada instancia a un puerto diferente.

Los tipos de conexión del puerto determinan cómo se leerán los datos de seguridad, la información que se leerá y cuándo se establecerá una conexión. Los tipos de conexión son:

- Tipo de conexión en serie
- Tipo de conexión por zócalo
- Tipo de conexión Nuevos en archivo
- Tipo de conexión Todos en archivo
- Tipo de conexión Proceso permanente
- Tipo de conexión Proceso transitorio
- Tipo de conexión Mensaje de alerta SNMP
- Tipo de conexión Ninguna

Tipo de conexión en serie

El tipo de conexión en serie se utiliza si los datos se leerán desde un puerto en serie RS-232C (a través de un cable de serie o de una conexión por módem). Debe especificar el puerto en serie adecuado (por ejemplo, COM1 o COM2) en el recuadro Valor Rx/Tx. El host que ejecuta el producto que se va a monitorizar también debe tener una conexión en serie al host del recopilador, ya sea a través de un cable en serie directamente o a través de modems en cada extremo de la conexión.

Cuando se usa este tipo de conexión, es posible que se deban introducir otras modificaciones o entradas.

Tipo de conexión por zócalo

El tipo de conexión por zócalo se utiliza si los datos se leerán desde una conexión por zócalo TCP. Debe especificar la dirección IP y el número de puerto TCP del host remoto en el recuadro Valor Rx/Tx. La dirección IP y el número de puerto TCP deben separarse con una coma. Por ejemplo, para especificar el puerto SMTP, introduzca lo siguiente en el recuadro Valor Rx/Tx:

<Dirección IP>:<puerto>

Es posible que también sea necesario situar un proceso del servidor por zócalo TCP en el host remoto y configurarlo para proporcionar datos al puerto TCP.

Para obtener más información sobre cómo configurar recopiladores con este tipo de conexión, consulte la documentación sobre recopiladores (p. ej., Collectors Snort, Cisco PIX y Solaris Syslog) que se encuentra en:

```
%workbench_home%\elements\<Nombre del recopilador>\docs
```

Tipo de conexión Nuevos en archivo

El tipo de conexión Nuevo en archivo se utiliza para leer sólo los datos de eventos seguridad que se añaden a un archivo después de que se haya iniciado el guión. Nuevos en archivo abre este archivo y lo lee desde el final del archivo. Debe especificar la vía del archivo de registro en el recuadro Valor Rx/Tx.

Para obtener más información sobre cómo configurar un recopilador con este tipo de conexión, consulte la documentación sobre recopiladores (p. ej., Collector Solaris Syslog) que se encuentra en:

```
%workbench_home%\elements\<Nombre del recopilador>\docs
```

Tipo de conexión Todos en archivo

El tipo de conexión Todos en archivo se utiliza para leer todos los datos de eventos de seguridad en un archivo.

Si selecciona Nuevos en archivo o Todos en archivo, puede introducir inputfile o outputfile para el Valor Rx/Tx. El formato es el siguiente:

inputfile, outputfile

o

inputfile

o

outputfile

Si selecciona Nuevos en archivo o Todos en archivo y el archivo disminuye de tamaño, el archivo se lee desde el principio.

Para obtener más información sobre cómo configurar recopiladores con este tipo de conexión, consulte la documentación sobre recopiladores (p. ej., Collectors Solaris Syslog y Windows 2000 Event Log) que se encuentra en:

```
%workbench_home%\elements\<Nombre del recopilador>\docs
```

Tipo de conexión Proceso permanente

El tipo de conexión Proceso permanente se utiliza para lanzar un proceso permanente cuando el puerto está iniciado. El proceso establece comunicación entre el recopilador asignado a ese puerto y una aplicación externa a través de estados de Recepción y Transmisión.

El Proceso permanente comienza al principio de cada estado de lectura/escritura y continúa ejecutándose mientras el puerto esté activo. El puerto finaliza el proceso como parte del proceso de apagado del puerto. Cuando el puerto se detiene, se envía un evento de nivel 5. Cuando el puerto se inicia, se envía un evento de nivel 1.

Para obtener más información, vaya al apartado Procesos permanente y transitorio Para obtener más información sobre cómo configurar el Valor Rx/Tx, vaya a la sección Configuración del Valor Rx/Tx para conexiones permanente y transitoria (tipo Rx/Tx). Para obtener más información sobre cómo configurar recopiladores con un tipo de conexión permanente, consulte la documentación sobre recopiladores (p. ej., Collector Check Point Firewall & VPN) que se encuentra en:

```
%workbench_home%\elements\<Nombre del recopilador>\docs
```

Tipo de conexión Proceso transitorio

El tipo de conexión Proceso transitorio se utiliza para lanzar un proceso transitorio cuando el puerto está iniciado. El proceso establece comunicación entre el recopilador asignado a ese puerto y una aplicación externa a través de estados de Recepción y Transmisión.

Un Proceso transitorio se puede iniciar varias veces. El puerto finaliza el proceso como parte del proceso de apagado del puerto.

NOTA: Si selecciona el Proceso permanente o el Proceso transitorio, el Valor Rx/Tx debe incluir la vía y el nombre de archivo del proceso que se ejecutará. Puede utilizar la vía completa y el nombre del archivo o una vía relativa (%WORKBENCH_HOME%) y el nombre del archivo. Por ejemplo:

Vía completa:

```
C:\Archivos de programa\Cisco\Csids_client – start
```

Vía relativa:

```
.\elements\Cisco\Csids_client – start
```

Para procesos permanentes, el proceso asumirá la relativa a no ser que se introduzca un Valor Rx/Rt como una vía completa.

Terminación del Proceso transitorio: si el Proceso transitorio se detiene antes de finalizar el analizador, se reinicia en el estado de lectura o escritura siguiente sin que se envíe ningún evento.

Para obtener más información, vaya al apartado Procesos permanente y transitorio Para obtener más información sobre cómo configurar el Valor Rx/Tx, vaya a la sección Configuración del Valor Rx/Tx para conexiones permanente y transitoria (tipo Rx/Tx).

Tipo de conexión Mensaje de alerta SNMP

El tipo de conexión Mensaje de alerta SNMP se utiliza para recibir mensajes de alerta SNMP v1, v2 y v3. Los sensores envían estos mensajes de alerta a la dirección IP del servidor del asistente. El Gestor de recopiladores habilita el análisis a través del recopilador adecuado según la dirección IP y el identificador de objeto (OID) del dispositivo que realiza el envío. El estado Rx (análisis) transmite datos de mensajes de alerta SNMP entrantes al recopilador.

La información que utiliza para recopilar y analizar mensajes de alerta SNMP v1, v2 y v3 se puede configurar:

- Los mensajes de alerta SNMP v1 se identifican mediante la dirección IP y el identificador de objeto (OID), mediante el código de mensaje de alerta.
- Los mensajes de alerta SNMP v2 y v3 se identifican mediante la dirección IP, el nombre de seguridad, el ID del motor, las claves de autenticación y cifrado (si están habilitadas en el mensaje de alerta) y el identificador de objeto (OID) del mensaje de alerta.

El formato original del mensaje de alerta, en cuanto a los valores de los mensajes de alerta se refiere, se mantiene lo más parecido posible. El formato se suele definir en la MIB (base de información de gestión) del sensor que ha originado el mensaje de alerta.

Para obtener más información, consulte Configuración de mensajes de alerta SNMP.

Tipo de conexión Ninguna

El tipo de conexión Ninguna se utiliza sin un puerto de comunicación. Es más eficiente porque no intenta establecer una conexión. Este tipo de conexión debe utilizarse si un recopilador no utiliza el estado de Recepción y sólo procesa comandos.

Para obtener información más detallada sobre cómo configurar recopiladores con este tipo de conexión, consulte la documentación sobre recopiladores (p. ej., Collectors ISS RealSecure y ISS SiteProtector) que se encuentra en:

```
%workbench_home%\elements\<Nombre del recopilador>\docs
```

Creación, asignación, inicio y detención de un puerto del asistente

Creación de un puerto del asistente

1. Diríjase a la documentación de recopiladores que se encuentra en %workbench_home%\elements\<Nombre del recopilador >\docs para obtener información sobre la configuración del recopilador:
2. Haga clic en la pestaña *Recopiladores* y seleccione un recopilador.
3. En el Generador de recopiladores, haga clic en la pestaña Hosts del asistente y seleccione un host.
4. En el panel de información del puerto de la derecha, haga doble clic en *nuevo*, escriba el nombre del puerto y pulse Intro.
5. Seleccione un *tipo Rx/Tx*.

6. Especifique las opciones de configuración de acuerdo con el tipo de conexión seleccionado.
   - Para conexiones en serie y por zócalo: en el recuadro Nombre del puerto, haga clic con el botón derecho en el nombre del puerto y seleccione *Editar Valor Rx/Tx*. Especifique uno de los siguientes grupos de opciones:
     - Para conexiones en serie: seleccione la velocidad en baudios, el tamaño de palabra, la paridad y los bits de parada. Haga clic en Aceptar.
     - Para conexiones por zócalo: introduzca una dirección IP y un nombre de puerto para la máquina host, separados por una coma. Si no se va a utilizar el estado de Recepción, seleccione el tipo de conexión Ninguna y haga clic en *Aceptar*.
   - Para el resto de tipos de conexión: haga doble clic en la celda *Valor Rx/Tx,* introduzca la información pertinente y pulse Intro.
   - Para el tipo de conexión mensaje de alerta SNMP, consulte Configuración de mensajes de alerta SNMP
7. Haga doble clic en la celda Recopilador y seleccione el nombre de un recopilador.
8. Haga clic con el botón derecho del ratón en el *nombre del puerto* y haga clic en *Otras opciones del puerto.* Aparecerá el recuadro de diálogo Otras opciones del puerto.
9. En el recuadro de diálogo *Otras opciones del puerto*, seleccione o deseleccione la casilla de verificación *Ejecutar puerto durante el inicio*, seleccione una *secuencia de inici*o y haga clic en *Aceptar*.
10. Si va a crear un puerto para el host local: haga clic en *Archivo* > *Guardar* y seleccione Información del *puerto*.

    Si va a crear un puerto para un host remoto: haga clic en *Archivo* > *Cargar/Descargar*.

    El puerto se añade al panel de información del puerto. No es necesario reiniciar el sistema para implementar el nuevo puerto. Haga clic en *Iniciar* para cambiar el estado del nuevo puerto de inactivo a activo.

Procesos permanente y transitorio

Mediante los procesos permanente y transitorio, el asistente puede interactuar con otra aplicación a través de guiones que reciben y transmiten datos y analizan respuestas. Cada uno de estos guiones se ejecuta en un puerto independiente y cada puerto está conectado a una aplicación específica.

NOTA: Otra aplicación se especifica en el recuadro Valor Rx/Tx.

Los nombres de los procesos pueden incluir los elementos siguientes:

- Espacios
- Barras inclinadas e invertidas (para incluir distintos sistemas operativos)
- Argumentos de comando
- Vías absolutas y relativas (la variable de entorno WORKBENCH_HOME se considera la relativa HOME)

Cuando se produce un estado de Recepción/Transmisión (Rx/Tx), se inicia el proceso especificado en el recuadro Valor Rx/Tx. Cuando el analizador finaliza, el proceso termina.

Cuando un Proceso permanente finaliza, se envía un evento de nivel 5. Cuando se inicia un Proceso permanente, se envía un evento de nivel 1.

La salida estándar (stdout) del Proceso permanente/transitorio se conecta al estado de lectura de recepción del analizador. La salida estándar (stdin) del Proceso permanente/transitorio se conecta al estado de escritura de transmisión del analizador.

Configuración del Valor Rx/Tx para conexiones permanente y transitoria (tipo Rx/Tx)

Existen tres procesos de conector para configurar las conexiones permanente y transitoria. Son los siguientes:

- DBConnector (un conector de proceso JDBC)
- Cliente Lea
- RDEP (Remote Data Exchange Protocol, protocolo de intercambio de datos remotos)

No utilice las comillas en el recuadro Valor Rx/Tx para los procesos permanente y transitorio. Si el proceso tiene una vía absoluta con un nombre de archivo ejecutable largo con espacios, introdúzcalo sin comillas. Por ejemplo:

```
%WORKBENCH_HOME%\e-security\elements\checkpoint\lea_clien
   t checkpoint\lea_client.conf –new
```

No utilice espacios en argumentos al ejecutable en el recuadro Valor Rx/Tx. Estos argumentos están limitados por el espacio, por lo tanto, si contienen espacios, el software detectará dos argumentos en lugar de uno. Si los argumentos proporcionan la ubicación de un archivo de configuración, como para un punto de verificación, utilice una vía completa desde %WORKBENCH_HOME%. Por ejemplo:

checkpoint/\lea_client checkpoint/\lea_client.conf -new

DBConnector

DBConnector (un conector de proceso JDBC) ejecuta un cliente que se conecta al servidor de la base de datos, ejecuta una consulta SQL en la base de datos y devuelve los resultados a la salida estándar en formato de par nombre/valor La consulta SQL que se va a ejecutar se lee desde la entrada estándar o desde un archivo. El nombre en el resultado del par nombre/valor se obtiene del nombre de la columna del conjunto de resultados. Por ello, el nombre deseado para la columna debe indicarse específicamente en el SQL. La sintaxis varía según el servidor de la base de datos.

Esta aplicación se instala con el Gestor de recopiladores en $WORKBENCH_HOME/dbconnector.

Para obtener más información sobre la utilización de DBConnector, consulte el archivo README (LÉAME) que viene con la aplicación, la documentación de recopiladores de Sentinel para Entercept Host IDS 4.0 (a través de JDBC), o visite el portal del cliente e-Security en http://www.esecurityinc.com.

Cliente Lea

El cliente_lea de Sentinel utiliza la API de exportación de registros de OPSEC para obtener datos desde Check Point Firewall-1 y los devuelve en el formato de par nombre/valor. El cliente_lea se utiliza normalmente para transferir datos al recopilador Check Point Firewall-1 de Sentinel, donde los datos se normalizan y, dependiendo de la acción del evento (p. ej., abandonar, rechazar o aceptar), se envía una alerta al servidor de Sentinel.

Esta aplicación se instala con el Gestor de recopiladores en $WORKBENCH_HOME/checkpoint.

Para obtener más información sobre la utilización del cliente_lea Check Point, consulte el archivo README (LÉAME) que viene con la aplicación, la documentación de recopiladores de Sentinel para Check Point Firewall & VPN Collector (a través de OPSEC), o visite el portal del cliente eSecurity en http://www.esecurityinc.com.

RDEP (Remote Data Exchange Protocol, protocolo de intercambio de datos remotos)

El cliente_rdep, una aplicación Java, obtiene los datos desde los sensores remotos Cisco IDS v4.0 que ejecutan RDEP. El cliente_rdep se conecta al sensor remoto IDS a través de una conexión HTTP o HTTPS. Una vez que el cliente se ha conectado, se abre una suscripción o se usa otra abierta previamente. La suscripción describe el tipo de datos que el servidor IDS enviará al cliente. El tipo de datos que una nueva suscripción recuperará se puede modificar si se edita el archivo de configuración cliente_rdep. Mediante la suscripción, el cliente inicia una petición de datos del evento desde el sensor IDS. El sensor IDS devuelve los datos del evento en formato XML, convertidos en pares nombre/valor por el cliente RDEP de Sentinel y, entonces, el recopilador los analiza y normaliza. El recopilador envía el evento normalizado a Sentinel.

Esta aplicación se instala con el Gestor de recopiladores en $WORKBENCH_HOME/cisco/rdep_client.

Para obtener más información sobre RDEP, consulte el archivo README (LÉAME) que viene con la aplicación, la documentación de recopiladores para el recopilador Cisco IDS 4.0 (a través de RDEP), o visite el portal del cliente eSecurity en http://www.esecurityinc.com.

Configuración del mensaje de alerta SNMP

Sentinel puede recibir mensajes de alerta SNMP que representan eventos que se han producido desde un sensor en una red. Estos eventos se envían a Sentinel en una red a través del protocolo SNMP. Se admiten los mensajes de alerta SNMP v1, v2 y v3. Es necesario crear un asistente de recopilador que use el tipo de conexión de mensajes de alerta SNMP (Rx/Tx) para habilitar a Sentinel para recibir mensajes de alerta SNMP.

Puede configurar los valores de los mensajes de alerta SNMP para especificar los parámetros que permitirán a los recopiladores SNMP del asistente proporcionar mensajes de alerta a Sentinel como eventos binarios.

La ventana de configuración de mensajes de alerta SNMP se utiliza para configurar los valores de los recopiladores SNMP del asistente, incluido el puerto utilizado para los mensajes de alerta SNMP, los códigos de mensajes de alerta, la autenticación y la información de cifrado.

Cómo acceder a la ventana Mensajes de alerta SNMP

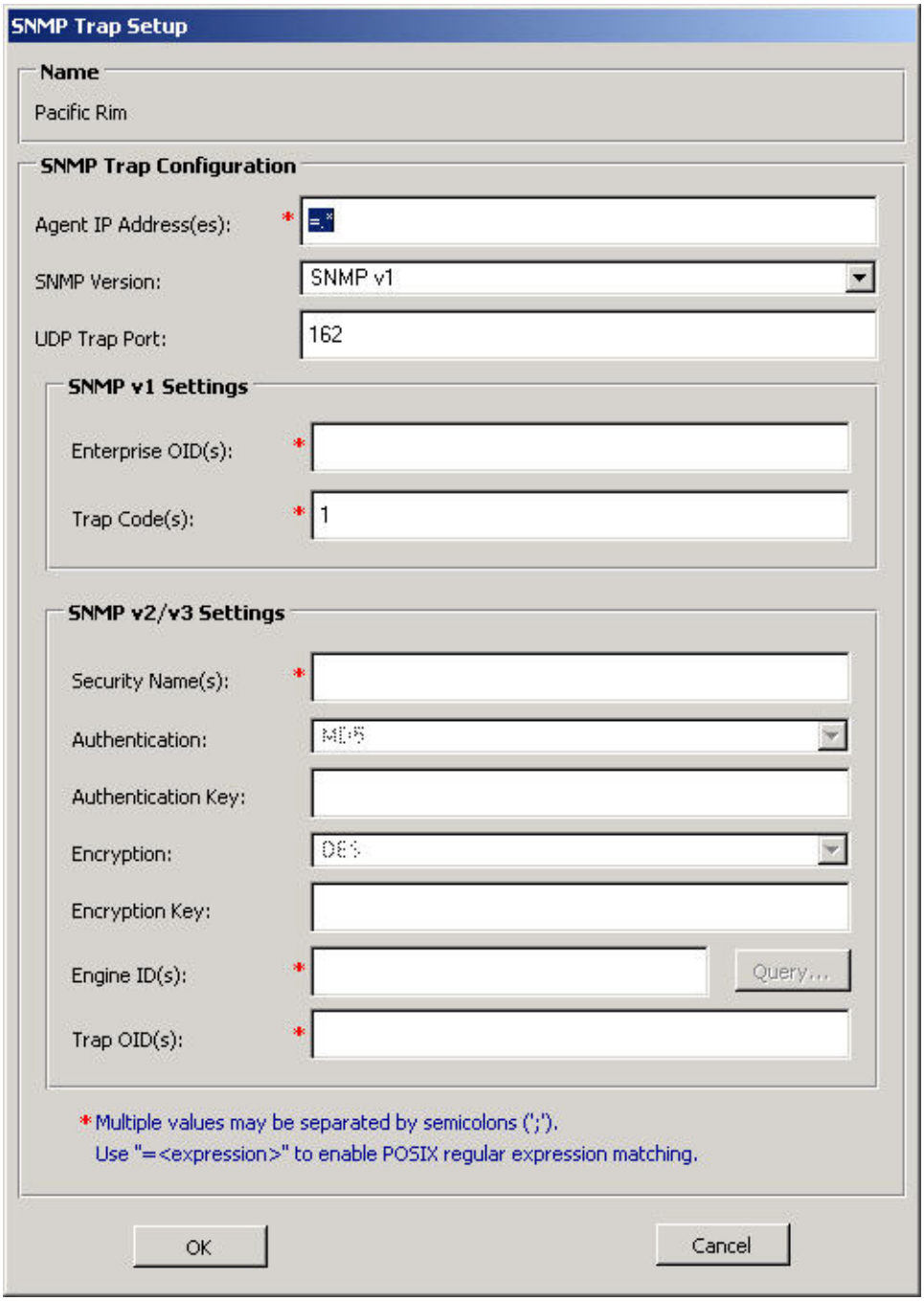
1. En el Generador de recopiladores, asigne un nombre de puerto a su recopilador SNMP.
2. Para el tipo Rx/Tx, seleccione el mensaje de alerta SNMP.
3. Haga clic con el botón derecho en el nombre del puerto, seleccione *Editar Valor Rx/Tx.*
4. Introduzca la información de SNMP.

NOTA: El puerto de mensajes de alerta UDP por defecto es 162. Asegúrese de que este puerto está disponible. Si no es así, puede elegir otro número de puerto.

NOTA: A diferencia de otros puertos de recopilador, el campo Valor Rx/Tx se rellenará en función de los valores establecidos en la ventana de configuración de mensajes de alerta SNMP. Para un recopilador SNMP, no es posible editar manualmente el campo Valor Rx/Tx.

5. El recopilador SNMP queda guardado y cargado.
6. Para activar el recopilador, detenga y reinicie el Gestor de recopiladores.

NOTA: Para activar este recopilador, debe detener y reiniciar el Gestor de recopiladores como se describe en el paso 6.



La configuración SNMP consta de:

- Direcciones IP del recopilador
- Versión de SNMP
- Puerto del mensaje de alerta UDP
- Configuración de SNMP v1
  - OID empresariales
  - Códigos de mensaje de alerta

- Configuración de SNMP v2/v3
  - Nombres de seguridad
  - Autenticación
  - Clave de autenticación
  - Cifrado
  - Clave de cifrado
  - ID de motor con botón de consulta
  - OID de mensajes de alerta

Puede configurar el asistente en el recuadro de diálogo de configuración de mensajes de alerta SNMP (que se abre si se hace clic con el botón derecho del ratón en un nombre de puerto en el panel de información del puerto del Generador de recopiladores y, a continuación, hace clic en Editar Valor Rx/Tx). Puede configurar para el asistente para que realice las operaciones siguientes:

- Recibir mensajes de alerta en puertos diferentes del puerto UDP 162 (el puerto por defecto).
- Crear un guión de análisis del asistente simple para procesar los mensajes de alerta desde múltiples direcciones IP, con información como múltiples códigos de mensajes de alerta y múltiples identificadores de objetos de mensajes de alerta (OID).
- Permitir que la expresión regular POSIX concuerde con la dirección IP, el identificador de objeto empresarial (OID), con el código de mensaje de alerta y con los campos de OID de los mensajes de alerta:
- Una vez decodificado el mensaje de alerta, el asistente define los valores para las variables incluidas en el guión.

Direcciones IP del recopilador

Las direcciones IP del recopilador son direcciones IP que se requieren para recibir mensajes de alerta. Separe varios valores con puntos y coma (;). Puede utilizar el formato =<expresión> para encontrar expresiones regulares compatibles con POSIX. El asterisco (*) es un modificador del carácter o la expresión precedente y el punto (.) puede usarse como carácter comodín y puede aparecer en cualquier lugar dentro de la cadena si se utilizan expresiones regulares.

Las expresiones regulares más comunes que probablemente usará son:

=	Busca cualquier secuencia de caracteres de cualquier longitud.
= 192\.168.*	Busca cualquier secuencia de caracteres que contenga 192.168. Para que comience por un comportamiento determinado, use: ^192.168... Con ^ como valor de anclaje de principio de línea. Para que termine con un comportamiento determinado, use 0.47$...: Con $ como valor de anclaje de fin de línea.
= [abc]	Busca a, b o c.
= [a-zA-Z0-9]	Busca cualquier carácter simple del abecedario (en mayúsculas o minúsculas) o cualquier dígito del 0 al 9.

Básicamente, las reglas de los ejemplos citados más arriba de expresiones regulares comunes son:

`.` Busca cualquier carácter.

`*` Busca cero o más apariciones del patrón precedente.

`[]` Busca cualquier carácter simple a partir del patrón definido entre paréntesis.

NOTA: Estas reglas se pueden combinar.

Versión de SNMP

Sólo se puede configurar una versión de SNMP. Las opciones de los paneles de configuración de SNMP v1 y v2/v3 se habilitan según la versión que seleccione.

Puerto de mensaje de alerta UDP

El puerto de destino UDP por defecto es el 162.

Configuración de SNMP v1

Esta configuración se habilita sólo si selecciona SNMP v1 de la lista de versiones de SNMP.

- OID empresariales: los ID de objeto se utilizan para identificar el tipo de recopilador que envía el mensaje de alerta. Separe varios valores con puntos y coma (;).
- Códigos de mensaje de alerta: son los códigos de mensaje de alerta para sensores que envían los mensajes de alerta SNMP. Estos códigos de mensaje de alerta representan los tipos de mensaje de alerta enviados por el recopilador SNMP en cuestión. Separe varios valores con puntos y coma (;).

Configuración de SNMP v2/v3

- Nombres de seguridad: son los nombres de usuario que se usan para acceder al recopilador. Los nombres de seguridad distinguen entre mayúsculas y minúsculas. Separe varios valores con puntos y coma (;).
- Autenticación: método de autenticación. Los valores son:
  - Ninguno: en los mensajes de alerta SNMP v3 no se efectúa autenticación.
  - MD5: el nombre de seguridad se configura para usar el algoritmo MD5 para crear una firma digital para la autenticación.
- Clave de autenticación: es la contraseña usada para autenticar al usuario en el recopilador. Se habilita sólo si la autenticación es MD5. Debe contener al menos ocho caracteres. Las claves de autenticación distinguen entre mayúsculas y minúsculas. Se debe configurar la misma clave en el recopilador SNMP de envío.
- Cifrado: es el método de cifrado. Los valores son:
  - Ninguno: en los mensajes de alerta SNMP v3 no se efectúa cifrado.
  - DES: espera recibir los mensajes de alerta cifrados con el método de cifrado DES (Estándar de cifrado de datos).

- Clave de cifrado: es la clave utilizada para descifrar los mensajes de alerta enviados a los recopiladores del asistente. Debe contener al menos ocho caracteres. La clave de cifrado distingue entre mayúsculas y minúsculas. Sólo se habilita si se selecciona DES de la lista de cifrado.
- ID de motor: es el único identificador para los recopiladores SNMP v3. Existe un botón de consulta de ID de motor que encuentra la dirección IP que desea consultar. Una consulta satisfactoria devuelve la información y añade el ID del motor. Si tiene un ID del motor en el recuadro, se añade uno nuevo.
- Mensajes de alerta OID: son los ID de objeto de los mensajes de alerta que identifican el tipo específico de mensaje de alerta recibido.

NOTA: Si especifica varios nombres de seguridad y varios ID de motor, se utiliza el mismo esquema de autenticación y cifrado para todos.

NOTA: Si se requieren diferentes claves de autenticación y cifrado para diferentes recopiladores SNMP, se deben configurar puertos separados para cada uno de ellos.

Variables de mensajes de alerta SNMP

Algunas variables de mensajes de alerta son válidas para todos los mensajes de alerta (SNMP v1 y v3) y algunas son válidas sólo para una versión. Las tablas siguientes muestran una lista de todas las variables de mensajes de alerta SNMP, que están agrupadas según la versión SNMP con la que funcionan:

- Variables de mensajes de alerta SNMP para SNMP v1 y v3
- Variables de mensajes de alerta SNMP para SNMP v1
- Variables de mensajes de alerta SNMP para SNMP v3

Variables de mensajes de alerta SNMP para SNMP v1 y v3

Variable	Descripción
`s_Trap_IP`	Dirección IP del sensor/recopilador que ha enviado el mensaje de alerta.
`s_Trap_Time`	Valor del tiempo de funcionamiento notificado por el recopilador/sensor que ha enviado el mensaje de alerta. Normalmente es el período de tiempo durante el cual el recopilador ha estado ejecutándose. Formato: D:HH:MM:SS.ss (días, horas, minutos, segundos, centésimas de segundo).
`i_Trap_Version`	Valor para una versión específica de SNMP: 1 = SNMP v1 3 = SNMP v3
`i_Trap_Vars`	Número de enlaces de variables en el mensaje de alerta.
`s_Trap_OID[]`	Una matriz (de tamaño "i_Trap_Vars") de los nombres de las variables MIB vinculadas al mensaje del mensaje de alerta. Cada elemento de la matriz s_Trap_OID es un OID como, por ejemplo, "1.3.6.1.4.1.4286....".
`s_Trap_Value[]`	Una matriz (de tamaño "i_Trap_vars") de los valores de las variables MIB vinculadas al mensaje del mensaje de alerta. Los índices de esta matriz y de la matriz s_Trap_OID coinciden, de manera que s_Trap_OID[0] es el nombre y que s_Trap_Value[0] es el valor.

Variables de mensajes de alerta SNMP para SNMP v1

Variable	Descripción
s_Trap_Ent	Identificador de objeto empresarial (OID) del recopilador/sensor que ha enviado el mensaje de alerta.
s_Trap_Code_Generic	Código genérico del mensaje de alerta. Los valores son: 1-5 = estándar, tipos de mensaje de alerta definidos mediante IETF (Internet Engineering Task Force, grupo de trabajo en ingeniería de Internet). 6 = mensaje de alerta específico para empresas (el código está definido en s_Trap_Code_Specific)
s_Trap_Code_Specific	Código específico de mensaje de alerta. Sólo es relevante si s_Trap_Code_Specific = 6.

Variables de mensajes de alerta SNMP para SNMP v3

Variable	Descripción
s_Trap_Engine_ID	ID de motor del recopilador SNMP v3 que ha enviado el mensaje de alerta.
s_Trap_OID	Identificador de objeto (OID) que identifica el tipo de mensaje de alerta SNMP v3 recibido. Para identificar el mensaje de alerta, el OID del mensaje de alerta SNMP v3 ocupa el lugar del OID empresarial SNMP v1 y los códigos de mensaje de alerta específico o genérico.
s_Trap_Security_Name	Nombre de seguridad con el que se conoce al recopilador SNMP que ha enviado el mensaje de alerta.

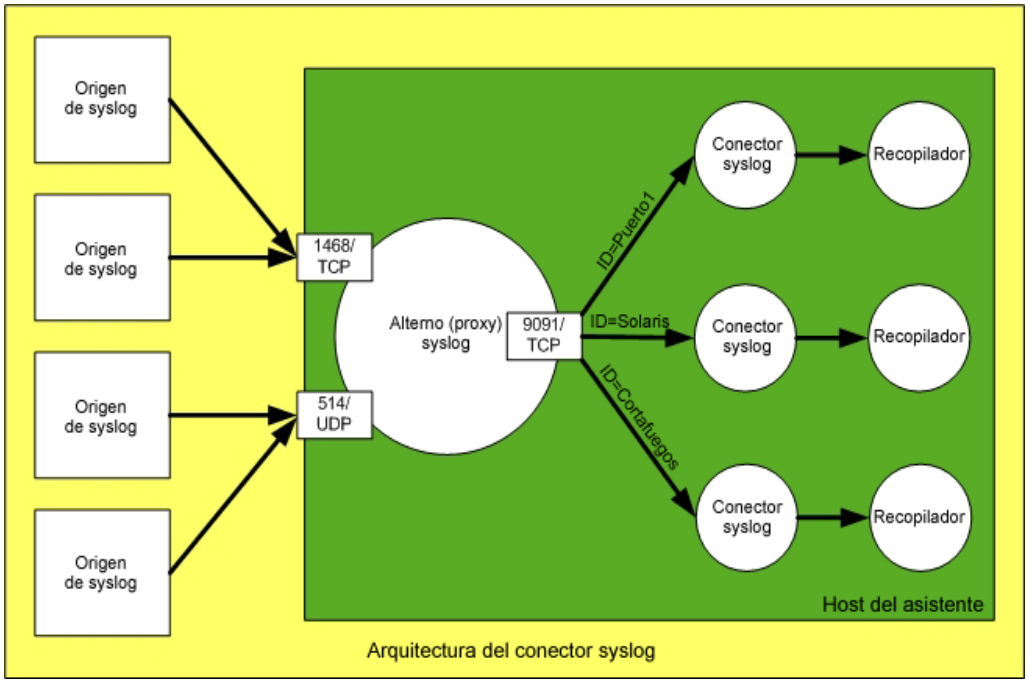
A Recopilador syslog v1.0.2

NOTA: El término Agente puede intercambiarse con Recopilador. En adelante, los agentes se denominarán recopiladores.

Novell ha lanzado el recopilador syslog para facilitar la integración de los recopiladores de Sentinel con otros productos que también generen mensajes syslog. En este documento se describe la arquitectura, la instalación, el uso y las opciones del conector syslog.

Arquitectura

El conector del syslog se compone de dos partes Una parte es el alterno (proxy) syslog y otro es el cliente del conector syslog. El alterno (proxy) syslog escucha los puertos UDP y TCP seleccionados. El puerto UDP, por defecto, es el 514, mientras que el del TCP es el 1468, que es el puerto que suele utilizar Cisco PIX al enviar mensajes vía el protocolo TCP.



Arquitectura del conector syslog

Las funciones de cada componente del conector syslog se describen a continuación:

- Alterno (proxy) syslog
  - Escucha al puerto TCP o al UDP, o a ambos, para los mensajes de syslog.
  - Analiza los mensajes de entrada en busca de los componentes estándar del mensaje (prioridad, fecha, nombre del host y mensaje).
  - Si origen del mensaje envía un mensaje en el que falta la prioridad, la fecha o el nombre del host, cumple el "protocolo Syslog BSD" RFC 3164 e inserta la fecha complementaria.
  - Una vez se ha determinado la aplicación y el nivel de la prioridad, así como el nombre del host, el alterno (proxy) publica el mensaje en las sesiones del conector syslog interesadas en el mensaje.
  - Si la sesión del cliente del conector syslog termina, el alterno (proxy) syslog pone en cola los mensajes de entrada de ese cliente durante diez minutos. De esta forma se asegura que el recopilador no pierde mensajes mientras se está reiniciando o cuando está temporalmente parado.
  - El alterno (proxy) syslog escucha en el puerto TCP, normalmente 9091, para dar servicio a las sesiones del cliente del conector syslog.
- Cliente del conector syslog
  - El conector se inicia como un proceso permanente con todas las opciones del tiempo de ejecución introducidas en el valor RX/TX.
  - Un tiempo de ejecución es el ID. El ID configurado para un conector syslog concreto debe ser exclusivo entre todos los conectores syslog que estén conectados al mismo alterno (proxy) syslog.
  - Un filtro de contenido se puede especificar durante el tiempo de ejecución para limitar el ámbito de los mensajes enviados al recopilador para que los analice.
  - El conector syslog establece una conexión con el servicio cliente del conector del alterno (proxy).
  - El conector syslog registra el ID y el filtro de contenido en el alterno (proxy) syslog.
  - Los mensajes que el alterno (proxy) syslog asocia al ID los lee el conector syslog y se dirigen a la salida estándar.
  - Actualmente, la estructura y el contenido de los mensajes se transmiten al recopilador tal cual. En el futuro, el conector syslog permitirá formatear los mensajes para cumplir con los requerimientos del análisis del recopilador.

Tradicionalmente, y también en el presente, el protocolo de syslog se ha sido definido como un protocolo basado en UDP. A falta de una gama variada de aplicaciones y dispositivos con capacidad para enviar mensajes mediante TCP o un estándar reconocido para syslog vía TCP, se ha adoptado el método de Cisco PIX para terminar mensajes de syslog (retorno de carro + salto de línea). La terminación de los mensajes es necesaria para syslog vía TCP, ya que no hay ningún estándar definido ni límites naturales entre los mensajes Syslog vía UDP tiene un mensaje de terminación natural, porque un paquete UDP transporta un solo mensaje y el UDP está desconectado.

Instalación y desinstalación

El conector syslog ha sido diseñado para funcionar en cualquier plataforma de asistente. Debido a tal requisito de portabilidad, ambos componentes se escriben en Java. A continuación, se muestran listas de los requisitos de software y de hardware:

Requisitos del sistema

Software

- Java 1.4.1 o superior.
- Asistente 4.2 o superior.
- Windows (2000/XP/2003), Solaris (8/9), RedHat Enterprise Linux (v3 ES/AS).

Hardware

- 14 MB de memoria RAM adicionales (45 MB de memoria virtual) para cada instancia del conector y del alterno (proxy) syslog

Instalación

Tanto el alterno (proxy) como los archivos del cliente del conector syslog se instalan automáticamente cuando se instala el Servicio de recopilador. Los archivos de syslog se encuentran en el directorio siguiente:

Para UNIX:

```
$ESEC_HOME/wizard/syslog
```

Para Windows:

```
%ESEC_HOME%\wizard\syslog
```

El asistente no iniciará el syslog alterno (proxy) de manera automática. Por tanto, si desea tenerlo activado automáticamente, debe instalarlo como un servicio. Siga las instrucciones de instalación del alterno (proxy) syslog como un servicio que se indican a continuación.

Instalación como servicio de Windows (Windows)

NOTA: El alterno (proxy) syslog se puede instalar como un servicio de Windows para que se ejecute de manera automática. Para instalar el alterno (proxy) syslog como un servicio, ejecute los comandos siguientes en el indicador de comandos:

1. cd /d "%ESEC_HOME%\wizard\syslog"
2. syslog-server.bat install

   Esta operación creará un servicio de Windows denominado "eSecurity Syslog Service".

Instalación como servicio (UNIX)

NOTA: El alterno (proxy) syslog se puede instalar como un servicio en UNIX de modo que se ejecute de manera automática cuando se inicie el equipo. Para instalar el alterno (proxy) syslog como un servicio, ejecute los comandos siguientes:

1. Entre a la sesión como Root.
2. cd $ESEC_HOME/wizard/syslog
3. syslog-server.bat install

   Con esto conseguirá que el alterno (proxy) syslog se inicie automáticamente cuando el equipo arranque. Por defecto, el alterno (proxy) syslog se ejecutará como el usuario Root. Esto es necesario porque, por defecto, el alterno (proxy) syslog se asociará al puerto 514, que requiere privilegios de Root. Para ejecutar el alterno (proxy) syslog como un usuario distinto de Root, modifique el guión /etc/init.d/esyslogserver. Compruebe que dicho usuario tiene privilegios para asociarse al puerto en que va a escuchar los mensajes. A continuación se muestran algunos ejemplos de cómo realizar esta operación:

   - Utilice el comando "sudo" para iniciar el alterno (proxy) syslog y el usuario obtendrá los privilegios de "sudo" de usuario para asociarse al puerto requerido.
   - Modifique la configuración del syslog (syslog.conf) y asocie el alterno (proxy) syslog a un puerto que no requiera privilegios Root (p. ej., >1024). En este caso, probablemente deberá redirigir los mensajes enviados al puerto 514 al nuevo puerto que ha seleccionado utilizar.

Desinstalación

Para desinstalar el Servicio de Windows, ejecute los comandos siguientes en el indicador de comando:

Desinstalación como servicio de Windows (Windows)

1. cd /d "%ESEC_HOME%\wizard\syslog"
2. syslog-server.bat remove

Desinstalación como servicio (UNIX)

Para desinstalar el alterno (proxy) syslog como un servicio, ejecute los comandos siguientes:

1. Entre a la sesión como Root.
2. cd $ESEC_HOME/wizard/syslog
3. ./syslog-server.sh remove

Uso

Servidor de Syslog alterno (proxy)

El asistente no iniciará el servidor alterno (proxy) syslog de manera automática. Si desea que se inicie automáticamente, debe instalarlo como un servicio. Siga las instrucciones que aparecen en la sección Instalación para instalar el alterno (proxy) syslog como un servicio.

La configuración del alterno (proxy) syslog se almacena en el archivo siguiente:

Para UNIX:

```
$ESEC_HOME/wizard/syslog/config/syslog.conf
```

Para Windows:

```
%ESEC_HOME%\wizard\syslog\config\syslog.conf
```

El alterno (proxy) syslog se configura para que utilice la configuración siguiente por defecto:

- Dispositivo de escucha en el puerto UDP 514 para los mensajes syslog.
- Dispositivo de escucha en el puerto TCP 1468 para los mensajes de syslog.
- Dispositivo de escucha en el puerto TCP 9091 para las conexiones de los conectores.

El alterno (proxy) syslog se puede configurar para escuchar en otros puertos tanto si la finalidad es recibir mensajes de syslog como si es aceptar conexiones de clientes. Estos conmutadores respectivamente son:

-udp <puerto>	Puerto para escuchar los mensajes UDP de los dispositivos, por defecto, 514.
-tcp <puerto>	puerto para escuchar las conexiones TCP de los dispositivos, por defecto 1468
-connector <puerto>	Puerto para escuchar las conexiones TCP de los conectores, por defecto, 9091.

Para editar estos valores, modifique la siguiente sección del archivo syslog.conf:

```
wrapper.app.parameter.3=-tcp
wrapper.app.parameter.4=1468
wrapper.app.parameter.5=-udp
wrapper.app.parameter.6=514
wrapper.app.parameter.7=-connector
wrapper.app.parameter.8=9091
```

Por ejemplo, si desea modificar los valores del puerto por los siguientes:

- Dispositivo de escucha del puerto UDP 4514 para los mensajes de syslog.
- Dispositivo de escucha del puerto TCP 4168 para los mensajes de syslog.
- Dispositivos de escucha del puerto TCP 4991 para las conexiones de los conectores.

La sección del archivo syslog.conf anterior debe modificarse del modo siguiente:

```
wrapper.app.parameter.3=-tcp
wrapper.app.parameter.4=4168
wrapper.app.parameter.5=-udp
wrapper.app.parameter.6=4514
wrapper.app.parameter.7=-connector
wrapper.app.parameter.8=4991
```

Por defecto, la configuración del alterno (proxy) syslog está ajustada para aceptar las conexiones de cliente desde cualquier host. Para aumentar la seguridad, el alterno (proxy) syslog se puede configurar para que tan solo acepte las conexiones de cliente que residan en el mismo host. Es una precaución de seguridad, ya que no hay confidencialidad, control de acceso ni autentificación entre el cliente del conector y el alterno Los conmutadores siguientes realizan estas operaciones:

-private	Escuchan las conexiones de los conectores en retrobucle.
-shared	Por defecto, escuchan las conexiones de los conectores en retrobucle.

El conmutador –shared indicará al alterno (proxy) que debe asociar el dispositivo de escucha de la conexión del cliente a un zócalo que pueda acceder a hosts remotos.

Para editar estos valores, modifique la sección siguiente del archivo syslog.conf:

```
wrapper.app.parameter.2=-shared
```

Por ejemplo, para permitir únicamente las conexiones del cliente desde el mismo host, debe modificar los valores del modo siguiente:

```
wrapper.app.parameter.2=-shared
```

El alterno (proxy) syslog se puede configurar para que registre todos los mensajes recibidos en un archivo de registro. El formato de los mensajes aparecerá en la forma que lo usaría el alterno (proxy) syslog si fuera a transmitir los mensajes a otro servidor syslog. Como resultado, el <PRI> o la prioridad utilizados por el servidor syslog receptor para evaluar el nivel y la aplicación de los mensajes aparecerá al principio de cada mensaje. El conmutador siguiente permite este tipo de registro.

`-log <nombre del archivo>`	Nombre del archivo de registro al que se añadirá.

Para permitir este tipo de registro, añada las dos líneas que aparecen a continuación al archivo syslog.conf después del ultimo parámetro “wrapper.app.parameter”:

```
wrapper.app.parameter.11=-log
wrapper.app.parameter.12=<nombre_del_archivo>
```

Por ejemplo, para permitir este tipo de registro en el archivo $ESEC_HOME/wizard/syslog/messages.log, es necesario modificar los datos siguientes:

```
wrapper.app.parameter.7=-connector
wrapper.app.parameter.8=9091
wrapper.app.parameter.9=-messageSize
wrapper.app.parameter.10=5000
wrapper.app.parameter.11=-log
wrapper.app.parameter.12=messages.log
```

Si no se ha especificado una vía absoluta para el nombre del archivo, ésta será relativa al directorio $ESEC_HOME/wizard/syslog.

NOTA: El archivo de registro puede llegar a ser bastante grande, por lo que asegúrese de que la ubicación en la que se va a escribir el archivo tiene espacio suficiente (p. ej., un directorio distinto en $ESEC_HOME).

Se recomienda que el alterno (proxy) syslog se ejecute con un mínimo de 64 MB y un máximo de 256 MB de memoria de la pila de JVM. Con esta configuración se obtendrá el funcionamiento siguiente:

Límites del servidor alterno (proxy):

▪ Número máximo de eventos:	500 eps (total para todos los puertos clientes)
▪ Tamaño máx. del conector Q	5.000 mensajes (valor por defecto si no se especifica ninguno)
▪ Nº máx. de conectores:	5

Para modificar la configuración de la memoria, edite la sección siguiente del archivo syslog.conf:

```
# Initial Java Heap Size (en MB)
wrapper.java.initmemory=64

# Maximum Java Heap Size (en MB)
wrapper.java.maxmemory=256
```

Cliente del conector syslog

El cliente del conector syslog se conecta con el alterno (proxy) syslog recopilando los mensajes para el que esté suscrito. Los mensajes que el cliente recopila se envían a la salida estándar. La sesión del cliente con el servidor no termina hasta que el proceso del cliente o el alterno (proxy) syslog no termina. El funcionamiento y los resultados hacen que sea adecuado para que los motores de recopiladores lo utilicen como un conector de procesos permanentes.

En la ventana de configuración del puerto del Generador de recopiladores, configure un puerto con un tipo Rx/Tx de proceso permanente y un valor Rx/Tx similar a la sintaxis genérica siguiente.

Para UNIX:

```
syslog/SyslogConnectorAgent.sh <argumentos>
```

Para Windows:

```
syslog\SyslogConnectorAgent.bat <argumentos>
```

Una vez que haya completado el valor Rx/Tx, seleccione el recopilador apropiado de la biblioteca y cargue la configuración del puerto y, posiblemente, el recopilador también al asistente remoto.

El cliente del conector syslog se ha diseñado para que utilice un número de argumentos por defecto con el fin de simplificar el uso general. La línea de comando más simple para el cliente del conector syslog es:

Para UNIX:

```
syslog/SyslogConnectorAgent.sh –id "Mi_ID_exclusivo"
```

Para Windows:

```
syslog\SyslogConnectorAgent.bat –id "Mi_ID_exclusivo"
```

La interpretación de esta línea de comando es la siguiente:

- Conectar con el alterno (proxy) syslog que escucha esta conexión en 127.0.0.1:9091.
- Suscribirse a todos los mensajes enviados con todas las aplicaciones posibles de syslog.
- Suscribirse a todos los mensajes enviados con todos los niveles posibles de syslog.
- Suscribirse a todos los mensajes sin tener en cuenta el origen de la dirección IP incluida en el encabezado IP.
- Suscribirse a todos los mensajes sin tener en cuenta la designación del host dentro del mensaje.
- Asignar a esos parámetros de suscripción de sesión la ID de “Mi_ID_exclusivo”.

La sesión del cliente del conector syslog se registrará con el alterno (proxy) syslog mediante el filtro de suscripción anterior con el ID de “Mi_ID_exclusivo”. El ID es necesario. La elección del ID es arbitraria, pero debe ser único entre todas las sesiones del cliente del conector syslog con el mismo alterno (proxy) syslog. Si se configura un cliente del conector syslog con el mismo ID, una de las dos conexiones con el mismo ID se abandonará Tan solo permanecerá la última sesión que se haya conectado con el mismo ID.

El filtro genérico en el filtro anterior puede desperdiciar el esfuerzo del procesamiento del recopilador si los mensajes que cumplen los requisitos del filtro; que son todos los mensajes recibidos, no son importantes para esta operación del recopilador en particular. Partiendo del ejemplo anterior, puede parecer que la expresión del filtro es muy versátil. En el ejemplo siguiente, para UNIX, se establece una descripción más restrictiva, aunque precisa, de lo que son los mensajes importantes para el recopilador.

```
syslog/SyslogConnectorAgent.sh -facilities “user,kernel” -
   levels “warning,error” -sender
   “192.16.0.12,192.16.0.0/16” -host
   “17.16.8.0/24,10.1.1.13” -id “Mi_otro_ID_exclusivo”
```

La interpretación de esta línea de comando es la siguiente:

- Conectar con el alterno (proxy) syslog que escucha esta conexión en 127.0.0.1:9091.
- (-facilities) Suscribirse a todos los mensajes enviados con las aplicaciones de usuario o núcleo.
- (-levels) Suscribirse a todos los mensajes enviados con los niveles de advertencia o error.
- (-sender) Suscribirse a los mensajes identificados por la dirección IP de origen de los mensajes de entrantes en el alterno (proxy) syslog. El argumento parece el alterno (proxy) syslog en la información del encabezado con el fin de evaluar este criterio. Esto permite que el filtro pueda alojar los servidores de transmisión syslog, los cuales no se identifican a sí mismos en los mensajes que transmiten. A pesar de que este argumento se hubiera diseñado para alojar los mensajes transmitidos, éste se puede usar para filtrar los mensajes enviados directamente desde el origen del syslog. En concreto, los servidores de transmisión u origen del syslog de interés son 192.16.0.12 y 192.16.0.0/16. El segundo de ellos, en realidad, representa un rango de direcciones IP; siempre y cuando la dirección IP de origen se encuentre entre 192.16.0.0 y 192.16.255.255 estos mensajes pasarán los criterios de filtro. Los nombres del host no son válidos para ninguna resolución de nombres del host que se lleve a cabo para determinar los nombres del host del las direcciones IP de origen.

- (-host) Suscribirse a los mensajes que contienen designadores de host 17.16.8.0/24 ó 10.1.1.13 dentro del mensaje del syslog. El primer elementos es un rango de direcciones IP. Si el mensaje contiene un designador de host en forma dirección IP y está dentro del rango de 17.16.8.0 a 17.16.8.255, el mensaje pasa esta condición dentro del filtro. El argumento -host admite los nombres del host. El nombre del host se puede designar de forma literal o por medio de una expresión regular. Tenga en cuenta que no se lleva a cabo ninguna resolución del nombre del host para este argumento. Se puede suponer que el hecho de configurar un nombre del host o una dirección IP va a dar como resultado que el filtro aloje el esquema de denominación opuesto. Por ejemplo, al configurar -host 172.16.0.90 no da como resultado un filtro que concuerde con un mensaje que contenga el nombre del host de "testbox1" aunque los servicios de resolución de nombres hayan asignado 172.19.0.90 a "testbox1". Por tanto, la designación del host de la IP sólo concordará con direcciones IP y la designación del host del nombre del host solamente concordará con nombres del host.

El filtro del ejemplo anterior se puede describir con la expresión booleana siguiente:

(Facility="user" or Facility="kernel") and (Level="warning" or Level="error") and (Sender="192.16.0.12" or Sender=192.16.0.0/16") and (Host="17.16.8.0/24" or Host="10.1.1.13")

El número de combinaciones posibles de esos argumentos es el producto cartesiano de los tipos de argumento, donde cada tipo de argumento es un conjunto. De acuerdo con PRINCIPIA CYBERNETICA WEB (http://pespmc1.vub.ac.be/ASC/CARTES_PRODU.html) el producto cartesiano es:

> "El conjunto de todas las n-tuplas ordenadas que se puedan formar para que contengan un elemento del primer conjunto, uno del segundo,... y un elemento del enésimo conjunto. Este conjunto puede verse como un componente de un espacio enésimo dimensional en el que cada n-tupla designa una celda. El producto cartesiano más simple de dos conjuntos es una tabla bidimensional o una tabulación cruzada en la que las celdas se pueden utilizar para introducir frecuencias, designar posibilidades (ver relación) o imposibilidades (ver restricción) o crear un gráfico de las transiciones que componen el comportamiento del sistema. (Krippendorff)"

NOTA: A fecha de publicación de este documento, el sitio Web mencionado más arriba es correcto.

Esto implica que, en teoría, algunos mensajes distintos pueden pasar este filtro. Sólo las condiciones de funcionamiento prácticas serán las que realmente impondrán los mensajes distintos.

Además, para filtrar los argumentos de la línea de comando, también existen los siguientes argumentos de líneas de comando opcionales:

`-proxy <dirección_del_servidor>:<n°_puerto#>`	Dirección del host del alterno (proxy) syslog y número de puerto al que se conectará.
`-log <nombre_archivo>`	Permite registrarse en el archivo especificado.

El argumento -proxy se utiliza para configurar el cliente del conector para que se conecte al puerto TCP que no es el valor por defecto o a otro distinto del host local. El alterno (proxy) syslog espera que la conexión de un cliente del conector se encuentre en 9091 por defecto. En el caso de que 9091 no sea adecuado para el host en el cual el alterno (proxy) syslog se está ejecutando, el puerto se puede ajustar durante el inicio del alterno syslog y, mediante el argumento -proxy, es posible indicar a los clientes que se conecten a ese puerto alternativo. Además, el host de destino del cliente del conector se puede especificar para que sea un host distinto del sistema local. En el caso de que un alterno (proxy) syslog acepte sesiones de cliente del conector remoto, un cliente del conector syslog se puede configurar para establecer una sesión con ese alterno (proxy) syslog remoto. La dirección IP y el puerto del cliente del conector syslog alterno (proxy) se configurarán con el argumento -proxy.

El argumento -log permite la función de registro del cliente del conector. El cliente del conector tomará nota de los mensajes a medida que los reciba del alterno (proxy) syslog. A diferencia del archivo de registro del alterno (proxy) syslog, el contenido del mensaje se filtrará según la información de suscripción registrada y, además, todos los mensajes registrados no contendrá el campo <PRI> ni de prioridad. El contenido será coherente con lo que reciba el recopilador del mismo cliente del conector syslog.

NOTA: El archivo de registro puede llegar a ser bastante grande, por lo que asegúrese de que la ubicación donde se escribirá el archivo tiene espacio suficiente (p. ej., un directorio distinto en $ESEC_HOME).

Un ejemplo, para UNIX, del uso de los argumentos -proxy y -log es:

```
syslog/SyslogConnectorAgent.sh –proxy localhost:9091 –log
   connector_messages.log –id "Mi_ID_exclusivo"
```

Configuración del registro del servidor alterno (proxy) syslog

El servidor alterno (proxy) syslog imprime los mensajes de registro en el archivo:

```
$ESEC_HOME/wizard/syslog/syslog_trace*.*.log
```

Los niveles de registro se pueden modificar mediante la edición del archivo de propiedades de registro:

```
$ESEC_HOME/wizard/syslog/syslog_log.prop
```

Éste es el archivo de propiedades de registro como se especifica en la siguiente línea en el archivo syslog.conf:

```
wrapper.java.additional.1=-
   Djava.util.logging.config.file=syslog_log.prop
```

Para ajustar los niveles de registro, realice las modificaciones en la sección siguiente:

```
###### Configure the logging levels
# Logging level rules are read from the top down. Start
   with the most general, then get more specific.
…
######
```

Argumentos de la línea de comando de ejemplo

Es posible ejecutar el servidor alterno (proxy) syslog y el cliente del conector sin utilizar los guiones que se proporcionan en la instalación. Para ello, deberá utilizar los argumentos de la línea de comando que se encuentran en esta sección.

Alterno (proxy) syslog:

```
java –server –Xms64m –Xmx256m –
   Djava.util.logging.config.file=syslog-logger.prop -jar
   syslog.jar [-udp <puerto>] [-tcp <puerto>] [-connector
   <puerto>] [-private|-shared] [-log <ruta archivo>] [-
   messageSize <número>]
```

Argumentos válidos:

`–server`	Se debe usar siempre. Usado por el JVM
`–Xms64m`	Especifica el tamaño de memoria inicial del alterno (proxy) syslog. Se recomiendan 64 megabytes.
`–Xmx256m`	Especifica el tamaño máximo de memoria del alterno (proxy) syslog. Se recomienda, por defecto, 256 megabytes. Permite al servidor alterno manejar volúmenes de datos, múltiples conectores del cliente y manejar buffers si los conectores consiguen la reconexión. Este valor puede significar cambios en un número más elevado si hay memoria disponible y volúmenes de datos, y el número conectores del cliente que se conecta. No debería exceder 1.2 Gigabytes por servidor syslog alterno (proxy), ej.: Xmx1200m
`–Djava.util. logging.config. file`	Esta propiedad especifica el nombre del archivo/vía de configuración del registro de depuración. Por tanto, debe apuntar hacia donde se encuentra el archivo. Si no se especifica ninguna vía, examinará el directorio actual desde donde se ha ejecutado el JVM. Por ejemplo: %workbench_home%\syslog-logger.prop
`-udp <puerto>`	Puerto que escucha los mensajes UDP desde dispositivos, por defecto, 514.
`-tcp <puerto>`	Puerto que escucha las conexiones TCP desde dispositivos, por defecto, 1468.
`-connector <puerto>`	Puerto que escucha las conexiones TCP desde conectores; por defecto, 9091.
`-private`	Escucha las conexiones del conector en retrobucle, es el valor por defecto.
`-shared`	Escucha las conexiones del conector en el host local. Si este valor no está definido, se generará un error de comunicación.
`-log`	Nombre de un archivo de registro que se añadirá al final.
`-help`	Proporciona este mensaje de ayuda.

-version	Ofrece la versión del alterno (proxy) (0.91-poc).
-messageSize	Número de mensajes almacenados para reenviar debido a la pérdida temporal de conexión. El tamaño máximo es de 5.000 sin comas. Si el valor opcional no se usa o si es superior a 5.000, el comando por defecto será 5000.

Cliente del conector syslog.

```
java -jar syslogconnector.jar -id <UniqueId> [-proxy
   <número del Puerto del host>] [-facilities
   <aplicación1,aplicación2,…>] [-levels <nivel1,
   nivel2,…>] [-sender <Origen IP1[/integer subnet mask],
   Source IP2[/integer subnet mask],…>] [-host <
   IP1[/integer subnet mask]|Hostname1 | Hostname Regex1,
   IP2[/integer subnet mask]|Hostname2 | Hostname Regex2,
   …>] [-log <ruta del archive a registro del archivo>]
```

Argumentos válidos:

-proxy <número del puerto del host:número del puerto>	El alterno (proxy) syslog para conectar al puerto del host, por defecto es 127.0.0.1:9091.
-facilities <aplicación1,aplicación2,…>	Lista separada por comas de las aplicaciones deseadas, por defecto, son todas las aplicaciones.
-levels <nivel1, nivel2,…>	Lista separada por comas de la gravedad deseada, por defecto, son todos los niveles.
-sender <Origen IP1[/integer subnet mask], Source IP2[/integer subnet mask],…>	Lista separada por comas de los remitentes deseados, por defecto, son todos los remitentes.
-host < IP1[/integer subnet mask]|Hostname1 | Hostname Regex1, IP2[/integer subnet mask	Lista separada por comas de los hosts deseados, por defecto, son todos los hosts.
-log <vía del archivo al archivo de registro>	Nombre de un archivo de registro al que se añadirá al final.
-id <Id exclusivo>	Especifica la identidad del conector (REQUERIDO).
-help	Proporciona este mensaje de ayuda.
-version	Ofrece la versión del conector (proxy) (0.91-poc).

Tabla de aplicaciones compatibles

Los nombres de las aplicaciones no distinguen entre minúsculas y mayúsculas cuando se especifican dentro de la línea de comando del cliente del conector syslog.

KERNEL	UUCP	LOCAL0
USER	CRON	LOCAL1
MAIL	SECURITY	LOCAL2
DAEMON	DAEMON de FTP	LOCAL3
AUTH	NTP	LOCAL4
SYSLOG	LOG AUDIT	LOCAL5
LPR	LOG ALERT	LOCAL6
NEWS	CLOCK DAEMON	LOCAL7

Tabla de niveles compatibles

Los nombres de los niveles no distinguen entre minúsculas y mayúsculas cuando se especifican dentro de la línea de comando del cliente del conector syslog.

EMERGENCY	WARNING
ALERT	NOTICE
CRITICAL	INFORMATIONAL
ERROR	DEBUG

Notas de distribución

Mensajes de transmisión para el alterno (proxy) syslog

La mayoría de los servidores syslog permiten redirigir los mensajes de syslog que reciben a un servidor syslog alternativo además de procesar los mensajes entrantes. En un escenario de distribución, puede ser interesante modificar un host del registro existente para proporcionar la transmisión de mensajes al alterno (proxy) syslog. Desafortunadamente, hay comportamientos entre algunos servidores syslog que pueden hacer de esta una mala elección.

Se ha observado que las bibliotecas del servidor syslog para Solaris 7, 9 y Linux 8, que puede ser representativo de otras versiones distribuidas, no colocan el nombre del host ni la dirección IP del host en los mensajes que envían al host. El servidor syslog que recibe los mensajes asocia la dirección IP de origen o el nombre del host (mediante la resolución de nombres) a los mensajes recibidos en los archivos de registro que genera. En el caso de Solaris 9 actuando de transmisor para un alterno (proxy), éste no rellena los mensajes que remite al alterno con la dirección IP o el nombre del host del origen del mensaje original. Este fenómeno es extraño, teniendo en cuenta que el archivo de registro del sistema Solaris 9 muestra una dirección IP o un nombre de host. Sin tener el nombre de host complementario en el mensaje, el alterno (proxy) syslog se ve forzado a deducir el mensaje originado en el servidor de transmisión y no en el host original. El alterno (proxy) syslog complementará el mensaje con la dirección IP del host de transmisión en todos los mensajes que reciba de un transmisor Solaris 9. Las consecuencias son serias. El origen de un evento de seguridad no es visible para el recopilador y tampoco para la solución Sentinel.

Es muy recomendable que el alterno (proxy) no sea un destinatario de mensajes transmitidos si dichos mensajes no contienen la dirección IP o el nombre de host del origen auténtico. Esta recomendación puede tener consecuencias logísticas significativas si el alterno (proxy) se utiliza en un entorno de producción.

Por ejemplo:

Un evento su tiene lugar en ultrabookIIi (172.16.0.70) ejecutando Solaris 7, que está remitiendo los mensajes de syslog a talkabout (172.16.0.72) ejecutando Solaris 9, que, a su vez, está transmitiendo al alterno (proxy) syslog. Los siguientes son mensajes generados por el conector de Sentinel.

Proxy:

```
<37>Apr 02 06:54:11 [172.16.0.72.151.234] su: 'su root'
   succeeded for oespadm on /dev/pts/0
```

Cliente del conector:

```
Apr 02 06:54:11 [172.16.0.72.151.234] su: 'su root'
   succeeded for oespadm on /dev/pts/0
```

A continuación se muestra el seguimiento del paquete del mismo mensaje que primero llega a talkabout y, a continuación, se transmite al alterno (proxy) syslog en pes020.esecurity.net.

```
# snoop -x0 udp port 514
Using device /dev/dmfe0 (promiscuous mode)
ultrabookIIi -> talkabout SYSLOG C port=42830 <37>Apr 1
   18:54:11

0: 0000 83cd 1395 0040 2082 202b 0800 4500   .......@ .
   +..E.
16: 0061 fa09 4000 ff11 28d3 ac10 0046 ac10
   .aú.@...(....F..
32: 0048 a74e 0202 004d 5d7e 3c33 373e 4170
   .H.N...M]~<37>Ap
48: 7220 2031 2031 383a 3534 3a31 3120 7375    r  1
   18:54:11 su
64: 3a20 2773 7520 726f 6f74 2720 7375 6363    : 'su root'
   succ
80: 6565 6465 6420 666f 7220 6f65 7370 6164    eeded for
   oespad
96: 6d20 6f6e 202f 6465 762f 7074 732f 30      m on
   /dev/pts/0

talkabout -> pes020.esecurity.net SYSLOG C port=38890
   <37>Apr  1 18:54:11
```

```
0: 000a 5e02 a335 0000 83cd 1395 0800 4500
   ..^..5........E.
16: 0061 304b 4000 ff11 f031 ac10 0048 ac10
   .a0K@....1...H..
32: 02a6 97ea 0202 004d 6a82 3c33 373e 4170
   .......Mj.<37>Ap
48: 7220 2031 2031 383a 3534 3a31 3120 7375    r  1
   18:54:11 su
64: 3a20 2773 7520 726f 6f74 2720 7375 6363    : 'su root'
   succ
80: 6565 6465 6420 666f 7220 6f65 7370 6164    eeded for
   oespad
96: 6d20 6f6e 202f 6465 762f 7074 732f 30      m on
   /dev/pts/0
```

El mensaje siguiente se ha registrado en talkabout:

```
Apr  1 18:54:11 ultrabookIIi su: 'su root' succeeded for
   oespadm on /dev/pts/0
```

B Configuración de un servidor de zócalo en un host UNIX

NOTA: El término Agente puede intercambiarse con Recopilador. En adelante, los agentes se denominarán recopiladores.

Un servidor de zócalo provee un punto final para las conexiones por zócalo desde el Gestor de recopiladores del asistente de UNIX. Por ejemplo, si desea monitorizar un archivo de registro o un equipo UNIX desde un asistente remoto y debe atravesar un cortafuegos para acceder al puerto del equipo UNIX.

A continuación se indican las instrucciones para configurar un servidor de zócalo en un host UNIX y podrá monitorizar un archivo de registro ASCII en el host UNIX.

Para configurar un proceso de servidor de zócalo en un host UNIX

1. Cree el guión que ofrecerá los datos a la conexión por zócalo TCP. Para ello, cree un nuevo archivo de texto y copie las líneas siguientes en éste, sustituyendo <archivo de registro> por el nombre de la vía completa del archivo que desee monitorizar.

   ```
   #!/bin/sh
   /bin/tail -f <archivo de registro>
   ```

   Guarde el archivo, la vía y el nombre del archivo es arbitrario pero el archivo se debe localizar en algún lugar donde no se vaya a eliminar, además éste debe tener un nombre que especifique su función como por ejemplo:

   ```
   /usr/local/bin/logfileserver
   ```

2. Seleccione un puerto TCP sin privilegios en el host UNIX para que lo use el proceso del servidor. El número del puerto sin privilegios es un número arbitrario entre 1.025 y 65.535. Para comprobar si el número de puerto ya está en uso, utilice el comando siguiente (sustituyendo el <número de puerto> por el puerto deseado):

   ```
   netstat -an | grep LISTEN | grep <número de puerto>
   ```

   Si se obtiene una línea, como la siguiente, el puerto ya está en uso, por lo que tendrá que elegir uno diferente.

   ```
   *.5555*.*0000 LISTEN
   ```

3. Como usuario Root, edite el archivo /etc/services y añada una entrada para el nuevo servicio de zócalo al final del archivo. El siguiente ejemplo añade una línea para el servicio denominado “syslog_monitor” configurado para escuchar en el puerto TCP 5555:

   ```
   syslog_monitor5555/tcp
   ```

4. Edite el archivo /etc/inetd.conf y añada una entrada nueva al nuevo servicio de zócalo al final del archivo. El ejemplo siguiente añade una línea a un servicio denominado “syslog_monitor” configurado para ejecutar el guión /usr/local/bin/in.syslog_monitor.

   Los datos siguientes se deben introducir como campos separados por tabulaciones de una única línea, sin tener en cuenta la paginación que aparezca.

   ```
   syslog_monitor stream tcp nowait nobody
      /usr/local/bin/in.syslog_monitor in.syslog_monitor
   ```

5. Ejecute el comando siguiente para habilitar el proceso del servidor de zócalo:

   ```
   kill -HUP `/bin/ps -ef | grep inetd | grep -v grep |
      awk '{print $2}'`
   ```

6. Realice una prueba en el servidor de zócalo Para ello, ejecute Telnet en el puerto que elija y obtendrá el contenido del archivo de registro:

   ```
   % telnet localhost 5555
   ```

   Si desea salir de la sesión de Telnet, utilice ^] (Control++]) y escriba “quit” en el indicador de Telnet.

Índice