

Novell® Sentinel™

www.novell.com

5.1.3

Volumen II: GUÍA DEL USUARIO DE SENTINEL

7 de julio de 2006

N

Novell®

Aviso legal

Novell, Inc. no otorga ninguna garantía respecto al contenido y el uso de esta documentación, y específicamente renuncia a cualquier garantía explícita o implícita de comercialización o adecuación para un fin determinado. Asimismo, Novell, Inc. se reserva el derecho a revisar esta publicación y a realizar cambios en su contenido en cualquier momento, sin obligación de notificar tales cambios a ninguna persona o entidad.

Además, Novell, Inc. no ofrece ninguna garantía con respecto a ningún software, y rechaza específicamente cualquier garantía explícita o implícita de comercialización o adecuación para un fin determinado. Por otra parte, Novell, Inc. se reserva el derecho a realizar cambios en cualquiera de las partes o en la totalidad del software de Novell en cualquier momento, sin obligación de notificar tales cambios a ninguna persona ni entidad.

Cualquier producto o información técnica suministrado al amparo de este acuerdo puede estar sujeto a controles de exportación de EE.UU., así como a las leyes comerciales de otros países. Usted manifiesta estar de acuerdo en cumplir todas las normativas de control de exportación y obtener cualquier licencia o clasificación necesaria para exportar, reexportar o importar artículos. Asimismo, manifiesta su acuerdo en no exportar ni reexportar a entidades que se encuentran en las listas actuales de exclusión de exportación de los EE.UU. o que radiquen en países bajo embargo o terroristas, tal como se especifica en las leyes de exportación de los EE.UU. Asimismo, manifiesta estar de acuerdo en no utilizar artículos cuyo uso final esté destinado a armamento nuclear, de misiles o químico biológico prohibido. Consulte www.novell.com/info/exports/ para obtener más información acerca de cómo exportar software de Novell. Novell no asume ninguna responsabilidad si no consigue obtener las aprobaciones necesarias para la exportación.

Copyright © del 1999 al 2006, Novell, Inc. Reservados todos los derechos. Ninguna parte de esta publicación puede ser reproducida, fotocopiada, almacenada en un sistema de recuperación o transmitida sin la expresa autorización por escrito del editor.

Novell, Inc. posee derechos de propiedad intelectual sobre la tecnología incorporada en el producto descrito en este documento. En concreto, y sin limitaciones, dichos derechos de propiedad intelectual pueden incluir una o varias patentes de los EE.UU. listadas en <http://www.novell.com/company/legal/patents/> y una o varias patentes adicionales o aplicaciones pendientes de patente en los EE.UU. y en otros países.

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 pertenecen a sus respectivos propietarios.

Avisos legales de otros fabricantes

Sentinel 5 contiene las siguientes 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 renunciaciones de responsabilidad, visite <http://www.apache.org/licenses/>.
- ANTLR. Para obtener más información y consultar las restricciones y renunciaciones de responsabilidad, 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 renunciaciones de responsabilidad, 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 renunciaciones de responsabilidad, 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 de Lesser GNU Public License. Para obtener más información y consultar las restricciones y renunciaciones de responsabilidad, visite <http://www.enterprisedt.com/products/edftpj/purchase.html>.
- Enhydra Shark, con licencia de 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 © del 1996 al 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 renunciaciones de responsabilidad, 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 correspondientes, 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 de responsabilidad, 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 de responsabilidad, 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 © del 1993 al 2005. Para obtener más información y consultar las restricciones y renuncias de responsabilidad, 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 de Lesser General Public License. Para obtener más información y consultar las restricciones y renuncias de responsabilidad, 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 de responsabilidad, visite <http://www.java.sun.com/products/javawebstart/download-jnlp.html> y haga clic en download > license.
- Java Service Wrapper. Partes con copyright 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 de responsabilidad, visite <http://wrapper.tanukisoftware.org/doc/english/license.html>.
- JIDE. Copyright © del 2002 al 2005, JIDE Software, Inc.
- jTDS con licencia de Lesser GNU Public License. Para obtener más información y consultar las restricciones y renuncias de responsabilidad, 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 de responsabilidad, 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, del 1998 al 2000, Junta de regentes de la Universidad de California; Copyright © del 2001 al 2003 Networks Associates Technology, Inc.; Copyright © del 2001 al 2003, Cambridge Broadband, Ltd.; Copyright © 2003 Sun Microsystems, Inc. y Copyright © del 2003 al 2004, Sparta, Inc. Para obtener más información y consultar las restricciones y renuncias de responsabilidad, 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 de responsabilidad, 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 la licencia de Apache Software License. Para obtener más información y consultar las restricciones y renunciaciones de responsabilidad, 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 renunciaciones de responsabilidad, visite <http://grinninglizard.com/tinyxmldocs/index.html>.
- SecurityNexus. Copyright © del 2003 al 2006. SecurityNexus, LLC. Reservados todos los derechos.
- Xalan y Xerces, ambos se otorgan con licencia de Apache Software Foundation Copyright © del 1999 al 2004. Para obtener más información y consultar las restricciones y renunciaciones de responsabilidad, visite <http://xml.apache.org/dist/LICENSE.txt>.
- yWorks. Copyright © del 2003 al 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 dañado 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.

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 Novell.

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 la instalación de:

- 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
- Supervisión de eventos
- Filtrado de eventos
- Correlación de eventos
- Gestor de datos de Sentinel
- Configuración de eventos para relevancia empresarial
- Asignación de servicios
- Informes históricos
- Gestión del host del asistente
- Incidencias
- Casos
- Gestión del usuario
- 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 para guiones del asistente
- Comandos de análisis del asistente
- Funciones de administrador del asistente
- Metaetiquetas de Sentinel y el asistente
- Motor de correlación de Sentinel
- Permisos del usuario
- Opciones de línea de comandos de correlaciones
- Esquema de la base de datos de Sentinel

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

- Remedy
- Operaciones de HP OpenView
- HP Service Desk

Contenido

1 Introducción a Sentinel	1-1
Arquitectura funcional.....	1-3
Funciones de Sentinel.....	1-3
Descripción general de la arquitectura.....	1-4
Plataforma iSCALE.....	1-4
Evento de Sentinel.....	1-6
Tiempo.....	1-11
Eventos internos o del sistema.....	1-12
Procesos.....	1-13
Arquitectura lógica.....	1-16
Nivel de recopilación y enriquecimiento.....	1-17
Nivel de lógica empresarial.....	1-20
Nivel de presentación.....	1-25
Módulos del producto.....	1-25
Centro de control de Sentinel.....	1-25
Asistente de Sentinel.....	1-25
Asesor de Sentinel.....	1-25
Contenido.....	1-26
Convenciones usadas.....	1-26
Notas y precauciones.....	1-26
Comandos.....	1-26
Otros materiales de consulta de Novell.....	1-26
Cómo ponerse en contacto con Novell.....	1-27
2 Navegación por el Centro de control de Sentinel	2-1
Inicio del Centro de control de Sentinel.....	2-2
Inicio del Centro de control de Sentinel en Windows.....	2-2
Inicio del Centro de control de Sentinel en UNIX.....	2-2
Barra de menús.....	2-2
Menú Archivo.....	2-2
Menú Opciones.....	2-2
Menú Ventanas.....	2-3
Vistas Active Views™.....	2-3
Incidencias.....	2-3
iTRAC™.....	2-3
Análisis.....	2-3
Asesor.....	2-3
Recopiladores.....	2-3
Admin.....	2-3
Ayuda.....	2-3
Barra de herramientas.....	2-4
Barra de herramientas del sistema.....	2-4
Pestaña Vistas Active Views™.....	2-4
Pestaña Incidencias.....	2-5
iTRAC.....	2-5
Pestañas Análisis y Asesor.....	2-6
Pestaña Recopiladores.....	2-6
Pestaña Admin.....	2-6
Pestañas.....	2-7

Cambio de apariencia del Centro de control de Sentinel	2-7
Ajuste de la posición de la pestaña	2-7
Cómo mostrar u ocultar la ventana del navegador	2-7
Cómo anclar o hacer flotar la ventana del navegador	2-7
Disposición de las ventanas en cascada	2-7
Disposición de las ventanas en mosaico	2-8
Minimización y restauración de todas las ventanas.....	2-8
Para restaurar todas las ventanas al tamaño original.....	2-8
Para restaurar una ventana individual	2-8
Cierre de todas las ventanas abiertas a la vez.....	2-8
Almacenamiento de las preferencias del usuario	2-8
Cambio de la contraseña del Centro de control de Sentinel	2-9

3 Pestaña Vistas Active Views™ 3-1

Pestaña Vistas Active Views: Descripción	3-2
Reconfiguración del valor en caché y del número máximo de eventos en la vista Active Views	3-3
Para ver eventos en tiempo real.....	3-4
Para reajustar los parámetros, el tipo de diagrama o la tabla de eventos de una vista Active Views	3-7
Rotación de un diagrama de barras o de cintas 3D.....	3-8
Cómo mostrar u ocultar la información de los eventos.....	3-9
Envío de mensajes acerca de eventos e incidencias por correo electrónico	3-10
Creación de una incidencia	3-12
Visualización de eventos que han activado un evento correlacionado.....	3-13
Investigación de un evento o eventos	3-13
Investigar: Asignador de gráficos	3-15
Investigar: Consulta de eventos	3-16
Análisis: Visualización de los datos del asesor	3-16
Análisis: Visualización de datos del activo	3-17
Análisis: Visualización de vulnerabilidades	3-18
Integración con otros fabricantes	3-23
Uso de las opciones de menú personalizadas con eventos	3-23
Gestión de las columnas en una ventana de la instantánea o del navegador visual.....	3-24
Toma de una instantánea de una ventana del navegador visual	3-25
Orden de columnas en una instantánea.....	3-25
Cierre de una instantánea o del navegador visual	3-25
Supresión de una instantánea o del navegador visual	3-26
Adición de eventos a una incidencia	3-26

4 Pestaña Incidencias 4-1

Pestaña Incidencias: Descripción.....	4-1
Relación entre eventos e incidencias	4-2
Visualización de una incidencia.....	4-2
Adición de una vista de incidencias.....	4-4
Información y campos de incidencias	4-5
Creación de una incidencia	4-6
Visualización y almacenamiento de adjuntos	4-6
Envío de una incidencia por correo electrónico.....	4-8
Modificación de una incidencia.....	4-8
Supresión de una incidencia.....	4-9

5 Pestaña iTRAC™	5-1
Plantillas (Definición del proceso)	5-1
Gestor de plantillas	5-2
Plantillas por defecto	5-2
Ejecución del proceso	5-6
Creación de una instancia de un proceso.....	5-6
Ejecución de una actividad automática	5-6
Ejecución de una actividad manual	5-6
Listas de trabajo	5-7
Elementos de trabajo.....	5-8
Aceptación de un elemento de trabajo	5-8
Actualización de variables del elemento de trabajo.....	5-9
Finalización del elemento de trabajo	5-10
Gestión de procesos	5-10
Monitor de procesos	5-10
Inicio o terminación de un proceso	5-12
Creación de una actividad mediante la estructura de actividades.....	5-12
Modificación de una actividad.....	5-14
Importación o exportación de una actividad	5-14
6 Pestaña Análisis	6-1
Descripción.....	6-1
Los diez informes más habituales	6-1
Ejecución de un informe desde Crystal Reports.....	6-2
Ejecución de un informe de consulta de eventos	6-2
Ejecución de un informe de eventos correlacionados	6-3
7 Pestaña Asesor	7-1
Ejecución de informes de asesor	7-1
Instalación independiente: Actualización manual del asesor	7-1
Descarga directa de Internet: Actualización manual del asesor	7-3
Cambio de la configuración del correo electrónico y la contraseña del servidor del asesor.....	7-3
Cambio de la contraseña del servidor del asesor (independiente).....	7-3
Cambio de la contraseña del servidor del asesor (descarga directa)	7-3
Cambio de la configuración del correo electrónico del servidor del asesor	7-4
Cambio de la hora de los datos.....	7-4
8 Pestaña Recopiladores	8-1
Disposición.....	8-1
Monitorización de un recopilador.....	8-2
Monitorización de un host del asistente.....	8-3
Creación de una vista de recopilador	8-3
Modificación de una vista de recopilador.....	8-4
Detención, inicio e información de recopiladores	8-4
9 Pestaña Admin	9-1
Pestaña Admin: Descripción	9-1
Opciones de configuración de informes para los informes de análisis y asesor.....	9-1
Reglas de correlación de Sentinel.....	9-3
Carpetas de reglas y reglas.....	9-3
Tipos de reglas de correlación.....	9-4
Distribución de reglas del motor de correlación.....	9-5

Importación y exportación de reglas de correlación	9-6
Función de la base de datos en el almacenamiento de reglas de correlación.....	9-6
Condiciones lógicas para las reglas de correlación.....	9-6
Apertura de la ventana Reglas de correlación.....	9-7
Copia y creación de una carpeta de reglas o una regla	9-8
Supresión de una carpeta de reglas o de reglas de correlación.....	9-8
Importación o exportación de una carpeta de reglas de correlación	9-9
Edición en la ventana de correlación.....	9-9
Activación o desactivación de un motor de correlación	9-9
Distribución de reglas de correlación.....	9-10
Vistas del servidor.....	9-11
Monitorización de un proceso.....	9-12
Creación de una vista del servidor	9-12
Inicio, detención y reinicio de procesos	9-13
Filtros	9-14
Filtros públicos.....	9-14
Filtros privados	9-14
Filtros globales	9-15
Configuración de filtros públicos y privados.....	9-16
Ajustes del menú de configuración.....	9-20
Adición de una opción al menú Configuración del menú	9-21
Clonación de una opción del menú Configuración del menú.....	9-22
Modificación de una opción del menú Configuración del menú.....	9-23
Visualización de los parámetros de opción de Configuración del menú.....	9-23
Activación o desactivación de una opción del menú Configuración del menú.....	9-23
Reorganización de las opciones del menú Evento	9-23
Supresión de una opción del menú Configuración del menú.....	9-23
Edición de los parámetros del navegador para la opción Configuración del menú	9-24
Estadísticas DAS.....	9-25
Información sobre el archivo de eventos.....	9-27
Configuraciones del usuario.....	9-27
Apertura de la ventana Gestor de usuarios	9-28
Creación de una cuenta de usuario.....	9-28
Modificación de una cuenta de usuario	9-30
Visualización de la información de una cuenta de usuario	9-30
Clonación de una cuenta de usuario	9-30
Supresión de una cuenta de usuario	9-31
Anulación de una sesión activa	9-31
Adición de una función iTRAC.....	9-31
Supresión de una función de iTRAC	9-31
Visualización de la información de una función	9-31

10 Gestor de datos de Sentinel

10-1

Instalación del SDM	10-1
Inicio de la GUI de SDM.....	10-2
Conexión a la base de datos	10-2
Particiones.....	10-4
Espacio de tabla	10-7
Pestaña Asignación.....	10-7
Pestaña Eventos	10-17
Pestaña Datos de informes	10-23
Línea de comando del SDM.....	10-28
Cómo guardar las propiedades de conexión para el Gestor de datos de Sentinel	10-28
Gestión de particiones.....	10-30
Gestión de los archivos de reserva	10-34
Gestión de la importación.....	10-37
Gestión de los espacios de tabla.....	10-40

Actualización de asignaciones (línea de comando).....	10-41
Uso del guión de gestión automática Novell suministrado (sólo para Windows).....	10-42
Configuración del archivo Manage_data.bat para el archivado de datos y la adición de particiones	10-42
Programación del archivo Manage_data.bat para el archivado de datos y la adición de particiones	10-44
11 Utilidades	11-1
Inicio y detención del servidor de Sentinel y del Gestor de recopiladores en UNIX.....	11-1
Inicio del servidor de Sentinel para UNIX	11-1
Detención del servidor de Sentinel para UNIX	11-1
Inicio del Gestor de recopiladores para UNIX.....	11-1
Detención del Gestor de recopiladores para UNIX.....	11-1
Inicio y detención del servidor de Sentinel y del Gestor de recopiladores en Windows	11-2
Inicio del Gestor de recopiladores para Windows.....	11-2
Detención del Gestor de recopiladores para Windows	11-2
Inicio del servidor de Sentinel para Windows	11-2
Detención del servidor de Sentinel para Windows	11-2
Inicio del servidor de comunicaciones de Sentinel para Windows.....	11-3
Detención del servidor de comunicaciones de Sentinel para Windows	11-3
Archivos de guión de Sentinel.....	11-3
Eliminación de los archivos de bloqueo del servidor de comunicaciones.....	11-4
Inicio del servidor de comunicaciones en modo de consola	11-4
Detención del servidor de comunicaciones en modo de consola	11-5
Reinicio de los contenedores de Sentinel.....	11-6
Información sobre la versión	11-7
Información sobre la versión del servidor de Sentinel	11-7
Información sobre la versión de los archivos .dll y .exe de Sentinel.....	11-7
Información sobre la versión del archivo .jar de Sentinel	11-8
Configuración del correo electrónico de Sentinel	11-8
Actualización de la clave de licencia	11-11
12 Inicio rápido	12-1
Analistas de seguridad	12-1
Pestaña Vistas Active Views	12-1
Detección de explotaciones.....	12-2
Datos del activo	12-3
Consulta de eventos	12-3
Analista de informes.....	12-5
Pestaña Análisis	12-5
Consulta de eventos	12-6
<i>Administradores</i>	12-6
Correlación básica.....	12-6
A Eventos del sistema para Sentinel 5	A-1
Eventos de autenticación	A-1
Error en la autenticación.....	A-1
Evento de usuario de tipo incorrecto	A-1
Objetos Usuario duplicados.....	A-1
Cuenta bloqueada	A-2
Sesiones de usuario.....	A-2
Salida del usuario	A-2
Entrada del usuario	A-2
Usuario descubierto.....	A-2
Evento	A-3

Error al mover el archivo finalizado	A-3
Error al insertar eventos	A-3
Error al abrir el archivo de reserva	A-3
Error al escribir el archivo de reserva	A-4
Escritura en la partición desbordada (P_MAX).....	A-4
La inserción de eventos está bloqueada	A-4
La inserción de eventos se reanuda.....	A-5
El espacio de la base de datos ha alcanzado el umbral de tiempo especificado	A-5
El espacio de la base de datos ha alcanzado el umbral de porcentaje especificado	A-5
Poco espacio en la base de datos.....	A-6
Adición	A-6
Error al insertar datos de resumen en la base de datos	A-6
Servicio de asignación	A-6
Error al inicializar una asignación con ID.....	A-6
Actualización de la asignación desde el caché.....	A-7
Actualización de la asignación desde el servidor	A-7
Tiempo límite de actualización de asignación	A-7
Error al actualizar la asignación.....	A-8
Asignación grande cargada.....	A-8
La carga de la asignación tarda mucho tiempo	A-8
TimeoutWaitingForCallback.....	A-9
Router de eventos.....	A-10
El router de eventos está en ejecución.....	A-10
El router de eventos se está inicializando.....	A-10
El router de eventos se está deteniendo	A-10
El router de eventos está terminando.....	A-11
Motor de correlación.....	A-11
El motor de correlación está en ejecución.....	A-11
El motor de correlación se ha detenido	A-11
La distribución de reglas se ha iniciado	A-11
La distribución de reglas se ha detenido	A-12
La distribución de reglas se ha modificado.....	A-12
Vigilante	A-12
El proceso controlado se ha iniciado	A-12
El proceso controlado se ha detenido	A-13
El proceso de vigilancia se ha iniciado	A-13
El proceso de vigilancia se ha detenido	A-13
Gestor y motor del recopilador	A-13
Inicio del puerto	A-13
Detención del puerto	A-14
El proceso permanente se ha cancelado	A-14
El proceso permanente se ha reiniciado	A-14
Servicio de eventos	A-15
Dependencia cíclica	A-15
Vista Active Views	A-15
Vista Active Views creada	A-15
Vista Active Views unida.....	A-15
Vista Active Views inactiva eliminada	A-16
Vista Active Views permanente inactiva eliminada.....	A-16
Vista Active Views ahora permanente	A-16
La vista Active Views ya no es permanente	A-17
Resumen.....	A-18

1

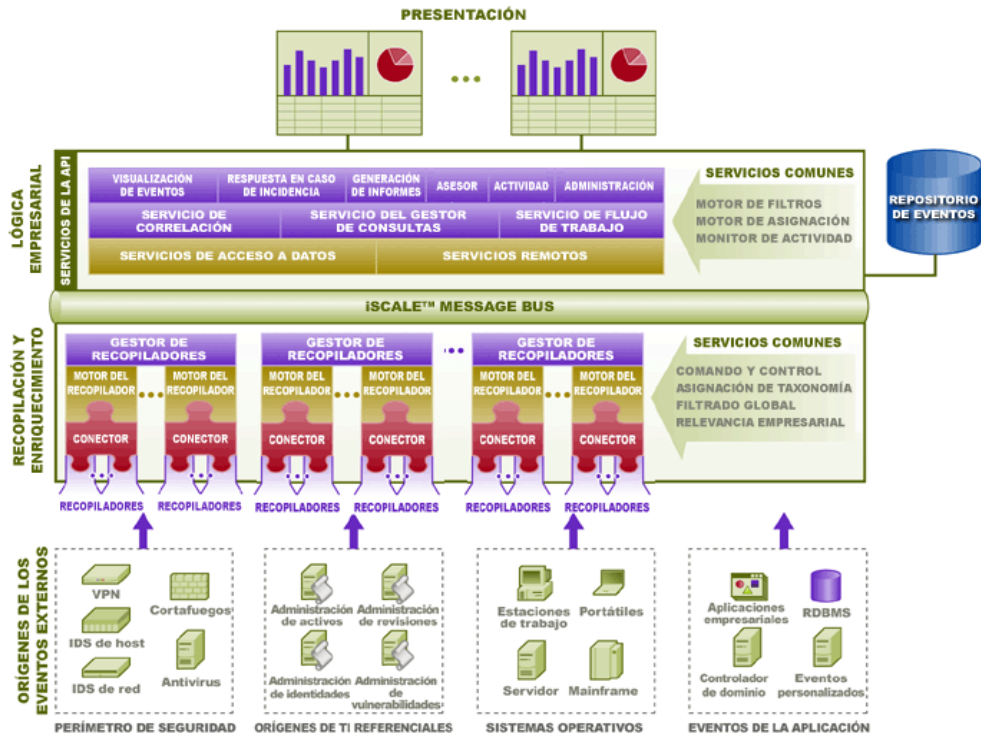
Introducción a Sentinel

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

Sentinel™ 5 es la solución de monitorización de conformidad y de gestión de información de seguridad líder que recibe información recopilada de varias fuentes mediante una empresa, la normaliza, establece un orden de prioridades y realiza una correlación en tiempo real. Sentinel recopila datos de varios productos de seguridad del mercado y proporciona la flexibilidad para recopilar datos de nuevas tecnologías y productos a medida que las instalaciones y los requisitos empresariales evolucionan.

La mayoría de las capacidades de Sentinel 5 son el resultado de un rediseño arquitectónico de Sentinel 4.0 basado en las necesidades de los clientes de Novell. A medida que las amenazas de seguridad y la presión legislativa aumentan, las organizaciones buscan una solución que les permita:

- Obtener la visibilidad y la perspicacia necesarias para gestionar un entorno de seguridad de forma más rentable.
- Monitorizar continuamente la conformidad con directivas internas y regulaciones gubernamentales (p. ej., Sarbanes-Oxley, HIPAA, GLBA, FISMA, NISPOM, DCID 6/3 y DITSCAP).
- Identificar y resolver incidencias con mayor rapidez y de una forma más rentable a través de una resolución y recopilación automatizada y centralizada de datos de amenazas o directivas.
- Proporcionar informes operativos y ejecutivos para evaluar continuamente la seguridad y el nivel de cumplimiento y dirigirse tanto a objetivos tácticos como estratégicos.
- Reducir los costes operativos asociados a la monitorización de conformidad y la seguridad, la identificación de incidencias y las soluciones.



Un evento es una acción o un acontecimiento notificado a Sentinel. Un evento recibido desde un dispositivo de seguridad se denomina un evento externo y un evento generado por Sentinel se denomina un evento interno. Los eventos pueden estar relacionados con la seguridad, con el rendimiento o con la información. Por ejemplo, un evento externo puede ser un ataque detectado por un sistema de detección de intrusos (IDS), una entrada a la sesión correcta notificada por un sistema operativo o una situación definida por el usuario como, por ejemplo, un usuario que accede a un archivo. Sentinel genera eventos internos para indicar un cambio significativo en el estado del sistema como, por ejemplo, la detención de un recopilador o la inhabilitación de una regla de correlación.

La correlación es el proceso de análisis de eventos de seguridad para identificar patrones dentro de un evento o de un flujo de eventos. Por ejemplo, puede crearse una regla de correlación para detectar si se producen eventos ICMP o externos en el período de tiempo de un minuto. El tráfico de gran volumen (desbordamiento) de ICMP puede provocar un ataque de denegación de servicio. La correlación puede detectar patrones en un flujo de eventos desde un único dispositivo, desde un conjunto de dispositivos similares o desde una recopilación arbitraria de dispositivos. Esto permite que el usuario pueda determinar mejor el riesgo de la gravedad de la incidencia.

Sentinel también incorpora información adicional en los datos, como información acerca de los equipos de la red y los servicios y las vulnerabilidades conocidos. Esta información está disponible en tiempo real y ofrece una información más detallada sobre la importancia de los eventos que se supervisan.

El Centro de control de Sentinel utiliza [procesos](#) en segundo plano para mostrar eventos en tiempo real y resúmenes de eventos (Active Views™), incidencias, informes históricos (análisis) e informes del asesor.

Los eventos considerados de una importancia significativa pueden agruparse conjuntamente en un objeto denominado *Incidencia*. El usuario puede crear una incidencia manual o automáticamente mediante el motor de correlación. La incidencia puede contener información adicional como, por ejemplo, información acerca de activos que están siendo atacados, las vulnerabilidades de estos activos, información acerca del ataque recuperado del componente del Asesor de Sentinel. Además, puede añadirse otra información como adjuntos.

Esta guía asume que está familiarizado con los conceptos básicos de la seguridad de red, la administración de la base de datos y con los entornos de sistemas operativos Windows y UNIX.

En este capítulo se describe la arquitectura lógica y funcional de Sentinel 5 y los módulos de los productos principales.

Arquitectura funcional

Sentinel 5 se compone de tres subsistemas de componentes que forman el núcleo de la arquitectura funcional:

- Plataforma iSCALE: estructura adaptable basada en eventos
- Integración de orígenes de datos: estructura de recopiladores extensible
- Integración de aplicaciones: estructura de aplicaciones extensible

Sentinel considera los “servicios” y las “aplicaciones” como puntos finales de servicios abstractos que pueden responder fácilmente a eventos asíncronos. Los servicios son “objetos” que no necesitan entender protocolos ni el procedimiento de envío de los mensajes en servicios de pares.

Funciones de Sentinel

Sentinel es una aplicación para el usuario final con una gran cantidad de características que permite la monitorización y gestión de una variedad de funciones. Algunas de las funciones principales son las siguientes:

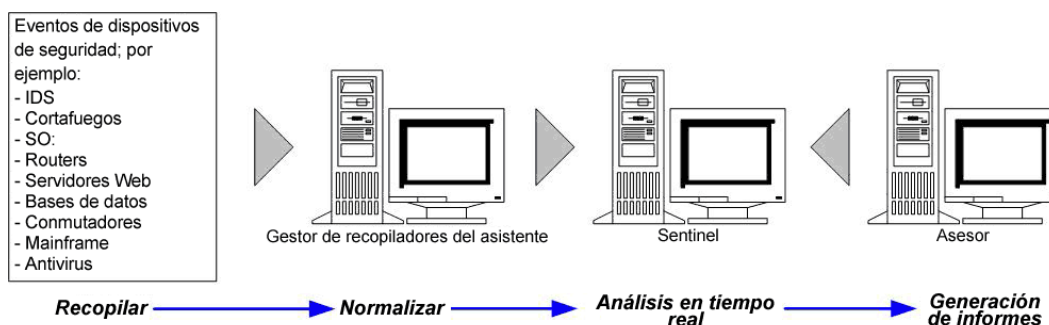
- Proporciona vistas en tiempo real de grandes flujos de eventos
- Ofrece habilidades de generación de informes basados en eventos de historial y en tiempo real
- Regula los usuarios y lo que pueden ver y hacer mediante asignación de permisos
- Permite restringir los eventos a los que los usuarios no tienen acceso
- Permite organizar eventos en incidencias para obtener un seguimiento y una gestión eficientes de las respuestas
- Permite detectar patrones en eventos y en flujos de eventos

Descripción general de la arquitectura

El sistema Sentinel es el responsable de recibir eventos desde el Gestor de recopiladores del asistente. A continuación, se muestran los eventos en tiempo real y se introducen en una base de datos para el análisis histórico.

A un alto nivel, el sistema Sentinel utiliza una base de datos relacional y se compone de procesos de Sentinel y un motor de generación de informes. El sistema acepta eventos desde el Gestor de recopiladores como su entrada. El Gestor de recopiladores interactúa con productos de otros fabricantes y normaliza los datos de dichos productos. Los datos normalizados se envían a la base de datos y a los procesos de Sentinel.

El informe y el análisis de historial pueden realizarse utilizando el motor de informes integrado de Sentinel. El motor de informes extrae los datos de la base de datos e integra las visualizaciones del informe en el Centro de control de Sentinel utilizando documentos HTML mediante una conexión HTTP.



Las funciones de Sentinel son:

- Procesamiento en tiempo real de los eventos que se reciben desde el Gestor de recopiladores del asistente
- Lenguaje intuitivo y flexible basado en reglas para la correlación
- Reglas compiladas para un mayor rendimiento
- Arquitectura adaptable, con múltiples hilos, distribuible y extensible

Los procesos de Sentinel se comunican entre ellos mediante un middleware orientado a mensajes (MOM).

Plataforma iSCALE

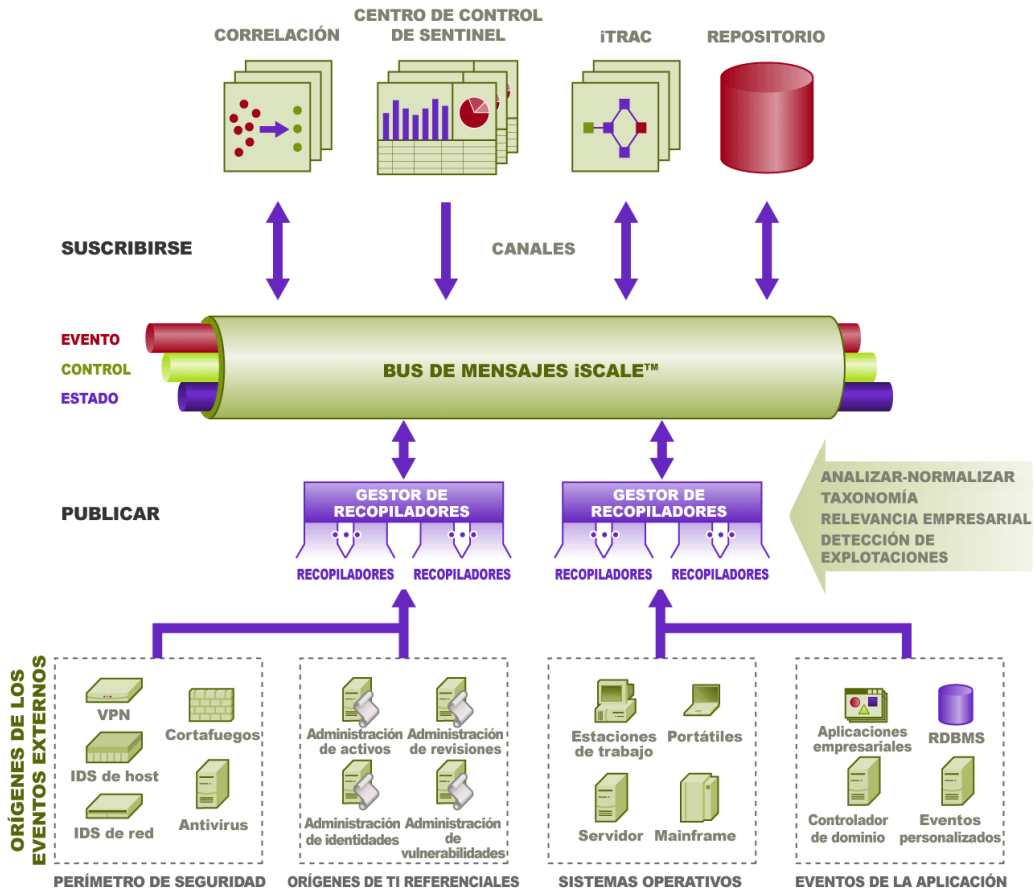
La arquitectura iSCALE™ de Sentinel se genera utilizando una arquitectura orientada a servicios (SOA) basada en estándares que combina las ventajas de la informática distribuida y el procesamiento en memoria. En el centro de iSCALE existe un bus de mensajes especializado capaz de gestionar grandes volúmenes de datos. Generada desde cero utilizando un óptimo enfoque basado en estándares, iSCALE puede adaptarse de forma rentable.

Bus de mensajes

El bus de mensajes de iSCALE permite la ampliación independiente de componentes individuales, además de una integración basada en estándares con aplicaciones externas. El factor clave para la capacidad de ampliación es que, a diferencia de otro software distribuido, no se comunican dos componentes de pares entre ellos directamente. Todos los componentes se comunican mediante el bus de mensajes, que es capaz de desplazar miles de paquetes de mensajes por segundo.

Mediante el potenciamiento de las funciones únicas del bus de mensajes, el canal de comunicación de alto rendimiento puede maximizar y sostener una alta velocidad de rendimiento de datos mediante los componentes independientes del sistema. Los eventos se comprimen y se cifran en el cable para garantizar una entrega segura y eficiente desde la periferia de la red o de los puntos de recolección hasta el nodo central del sistema, donde se realizan los análisis en tiempo real.

El bus de mensajes iSCALE utiliza una gran variedad de servicios en cola que mejoran la fiabilidad de la comunicación por encima de los aspectos de seguridad y rendimiento de la plataforma. Mediante el uso de una gran variedad de colas transitorias y duraderas, el sistema ofrece una excelente fiabilidad y tolerancia a fallos. Por ejemplo, los mensajes importantes en tránsito se guardan (en colas) en caso de que se produzca un fallo en la vía de comunicación. El mensaje en cola se entrega al destino después de que el sistema se recupere del estado de fallo.



Canales

La plataforma iSCALE utiliza un modelo basado en datos o eventos que permite la ampliación independiente de componentes en todo el sistema en función de la cantidad de trabajo. Esto ofrece un modelo de distribución flexible, ya que cada entorno del cliente varía: es posible que un sitio tenga un gran número de dispositivos con pocos volúmenes de eventos y, en cambio, es posible que otro sitio tenga menos dispositivos con grandes volúmenes de eventos. Las densidades de eventos (p. ej. el patrón de adición de eventos y de multiplexado de eventos en el cable desde los puntos de recolección) son diferentes en estos casos y el bus de mensajes permite una ampliación coherente de cantidades de trabajo dispares.

iSCALE se aprovecha de un entorno independiente y con múltiples canales, que elimina virtualmente la disputa y fomenta el procesamiento paralelo de eventos. Estos canales y subcanales no sólo funcionan para el transporte de datos de eventos sino que también ofrecen un control del proceso de granulado fino para poder realizar una ampliación y un balance de la carga del sistema bajo condiciones de carga variable. Mediante el uso de canales de servicio independiente, como canales de control y canales de estado, además del canal de eventos principales, se permite una ampliación sofisticada y rentable de la arquitectura basada en eventos.

Evento de Sentinel

Sentinel recibe información desde dispositivos, la normaliza en una estructura denominada *Evento de Sentinel* o *Evento* y envía el evento para su procesamiento. Los eventos son procesados por la visualización en tiempo real, el motor de correlación y el servidor secundario.

Un evento consta de más de 200 etiquetas. Las etiquetas son de diferentes tipos y sirven para diferentes fines. Existen algunas etiquetas predefinidas como gravedad, importancia, IP de destino y puerto de destino. Existen dos conjuntos de etiquetas configurables: Las Etiquetas reservadas son para uso interno en Novell con el fin de permitir la futura expansión y las Etiquetas de cliente son para extensiones de clientes.

Las etiquetas pueden determinarse de nuevo renombrándolas. El origen de una etiqueta puede ser *externo*, lo que significa que es definido explícitamente por el dispositivo o el recopilador correspondiente, o *referencial*. El valor de una etiqueta referencial se calcula como una función de una o más etiquetas utilizando el servicio de asignación. Por ejemplo, puede definirse una etiqueta para que sea el código de generación para la asignación que contiene el activo mencionado como la IP de destino de un evento. Por ejemplo, el servicio de asignación puede calcular una etiqueta utilizando una asignación definida por el cliente mediante una IP de destino desde el evento.

Servicio de asignación

El servicio de asignación permite que un mecanismo sofisticado transmita datos de relevancia empresarial a través del sistema. Este servicio facilita la capacidad de ampliación y ofrece una ventaja de extensión mediante la activación de la transferencia de datos inteligentes entre diferentes nodos del sistema distribuido.

El servicio de asignación es un servicio de propagación de datos que proporciona la capacidad de realizar referencias cruzadas de datos de escáners de vulnerabilidad con firmas del sistema de detección de intrusiones (p. ej. datos del activo, datos de relevancia empresarial). Esto permite obtener una notificación inmediata cuando un ataque intenta explotar un sistema vulnerable. Existen tres componentes independientes que proporcionan esta funcionalidad:

- recopilación de eventos en tiempo real desde una fuente de detección de intrusos;
- comparación de las firmas con las exploraciones de vulnerabilidad más recientes; y
- remisión de datos de ataque mediante el asesor de Sentinel (módulo del producto opcional que ofrece referencias cruzadas entre las firmas de ataques IDS en tiempo real y los datos del escáner de vulnerabilidad del usuario).

El servicio de asignación transmite información dinámicamente a través del sistema sin que la carga del sistema se vea afectada. Cuando se actualizan conjuntos de datos importantes (p. ej. “asignaciones” como la información de activos o la información de actualización de revisiones) en el sistema, el Servicio de asignación transmite las actualizaciones a través del sistema, el cual puede tener a menudo centenares de megabytes de tamaño.

Los algoritmos del servicio de asignación de iSCALE gestionan una gran cantidad de conjuntos de datos referenciales a través de un sistema de producción que procesa grandes volúmenes de datos en tiempo real. Estos algoritmos “reconocen actualizaciones” y sólo empujan selectivamente los cambios o los “conjuntos de datos Delta” desde el repositorio hasta la periferia o el perímetro del sistema.

Asignaciones de emisión continua

El Servicio de asignaciones utiliza un modelo de actualización dinámico y emite las asignaciones de un punto hacia otro, evitando la generación de grandes asignaciones estáticas en una memoria dinámica. El valor de esta función de emisión es particularmente importante en un sistema en tiempo real esencial como Sentinel donde debe haber un movimiento seguro, predictivo y ágil de independencia de datos de alguna carga transitoria en el sistema.

Detección de explotaciones (Servicio de asignación)

Sentinel ofrece la función de realizar referencias cruzadas en firmas de datos de eventos con datos del escáner de vulnerabilidad. Los usuarios son notificados automática e inmediatamente cuando un ataque intenta explotar un sistema vulnerable. Esto se realiza mediante:

- Datos del asesor
- Detección de intrusiones
- Exploración de vulnerabilidades
- Cortafuegos

El asesor proporciona una referencia cruzada entre firmas de datos de eventos y datos del escáner de vulnerabilidad. Los datos del asesor disponen de datos de alerta y de ataque. Los de alerta contienen información acerca de vulnerabilidades y amenazas. Los datos de ataque son una normalización de firmas de eventos y plug-ins de vulnerabilidades. Para obtener información sobre la instalación del asesor, consulte la *Guía de instalación de Sentinel*.

Los sistemas compatibles son:

Sistemas de detección de intrusos

- Cisco Secure IDS
- Enterasys Dragon Host Sensor
- Enterasys Dragon Network Sensor
- Intrusion.com (SecureNet_Provider)
- ISS BlackICE
- ISS RealSecure Desktop
- ISS RealSecure Network
- ISS RealSecure Server
- ISS RealSecure Guard
- Snort
- Symantec Network Security 4.0 (ManHunt)
- Symantec Intruder Alert
- McAfee IntruShield

Exploradores de vulnerabilidades

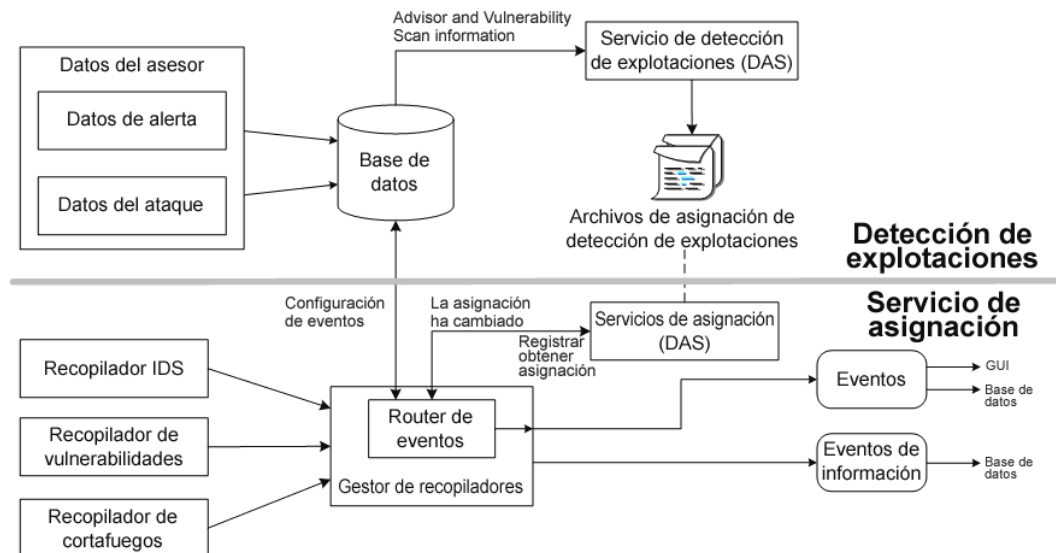
- eEYE Retina
- Foundstone Foundscan
- ISS Database Scanner
- ISS Internet Scanner
- ISS System Scanner
- ISS Wireless Scanner
- Nessus
- nCircle IP360
- Qualys QualysGuard

Cortafuegos

- Cisco IOS Firewall

Se requiere como mínimo un explorador de vulnerabilidades y un sistema IDS o cortafuegos de cada categoría anterior. El nombre del dispositivo (DeviceName) del cortafuegos y del sistema IDS (rv31) debe aparecer en el evento resaltado en gris como se muestra más arriba. Además, el sistema IDS y el cortafuegos deben rellenar correctamente el campo DeviceAttackName (rt1) (el acceso a WEB-PHP Mambo uploadimage.php).

Los datos del asesor se envían a la base de datos y, a continuación, al servicio de detección de explotaciones. El servicio de detección de explotaciones generará uno o dos archivos según el tipo de datos que se hayan actualizado.



El Servicio de asignación utiliza los archivos de asignación de detección de explotaciones para asignar ataques en explotaciones de vulnerabilidades.

Los exploradores de vulnerabilidades exploran áreas vulnerables al sistema (activos). IDS detecta ataques (si los hay) contra estas áreas vulnerables. Los cortafuegos detectan si existe tráfico contra cualquier área vulnerable. Si se asocia un ataque a cualquier vulnerabilidad, se explota el activo.

El servicio de detección de explotaciones genera dos archivos ubicados en:

`SESEC_HOME/sentinel/bin/map_data`

Los dos archivos son `attackNormalization.csv` y `exploitDetection.csv`.

El archivo `attackNormalization.csv` se genera posteriormente



- Datos del asesor
- Inicio de DAS (si se activa en `das_query.xml`, inhabilitado por defecto)

El archivo `exploitDetection.csv` se genera después de una de las acciones siguientes:

- Datos del asesor
- Exploración de vulnerabilidades
- Inicio del servidor de Sentinel (si se activa en `das_query.xml`, inhabilitado por defecto)

Por defecto, hay dos columnas de eventos configurados utilizadas para la detección de explotación y se hacen referencia desde una asignación (todas las etiquetas asignadas tendrán el icono de desplazamiento).

- Vulnerabilidad
- ID del ataque

Severity	Vulnerability	AttackId
	0	
	0	

Si el campo Vulnerabilidad (*vul*) es igual a 1, no se explota el activo ni el dispositivo de destino. Si el campo Vulnerabilidad es igual a 0, no se explota el activo ni el dispositivo de destino.

Sentinel se preconfigura con los siguientes nombres de asignación asociados a los archivos `attackNormalization.csv` y `exploitDetection.csv`.

Nombre de asignación	Nombre de archivo csv
▪ AttackSignatureNormalization	▪ attackNormalization.csv
▪ IsExploitWatchlist	▪ exploitDetection.csv

Existen dos tipos de orígenes de datos:

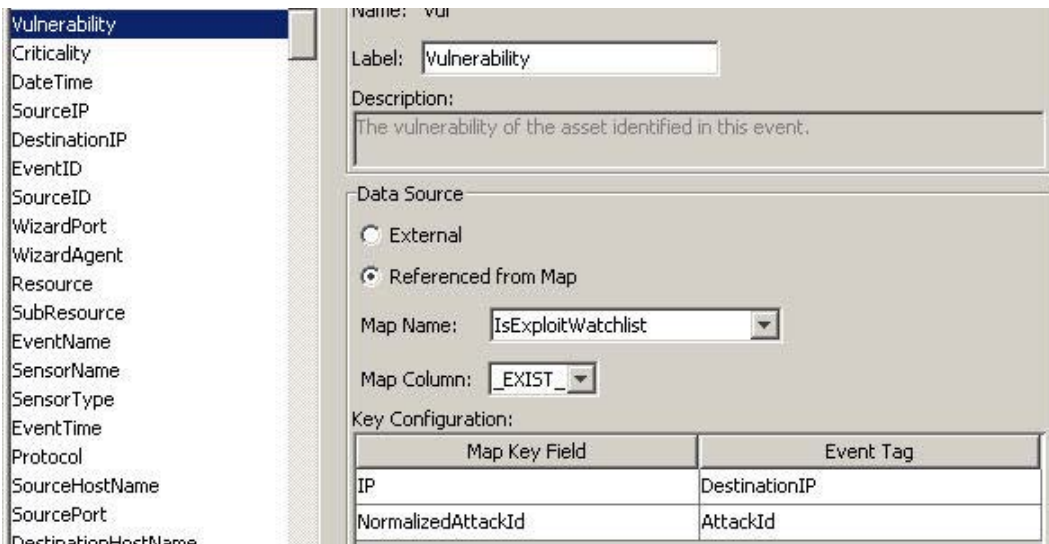
- Externo: recupera información del recopilador.
- Con referencia desde la asignación: recupera información desde un archivo de asignación para rellenar la etiqueta.

La etiqueta `AttackId` tiene las columnas `Device` (el tipo de dispositivo de seguridad, p. ej. Snort) y `AttackSignature` definidas como Claves y utiliza la columna `NormalizedAttackID` en el archivo `attackNormalization.csv`. En una fila en la que la etiqueta de eventos `DeviceName` (un dispositivo IDS como Snort, información introducida por la información de vulnerabilidades y del asesor desde la base de datos de Sentinel) es la misma que `Device` y en la que la etiqueta de eventos `DeviceAttackName` (información de ataque introducida por la información del asesor en la base de datos de Sentinel mediante el servicio de detección de explotaciones) es la misma que `AttackSignature`, el valor de `AttackId` se encuentra en la intersección de la fila con la columna `NormalizedAttackID`.



Device	AttackSignature	NormalizedAttackId	AttackId entry
Secure	BackDoorProbe (TCP 1234)	3	Trojan: Backdoor.SubSeven
Secure	BackDoorProbe (TCP 1999)	3	Trojan: Backdoor.SubSeven
Dragon	RWALLD:SYLOG-FORMAT	4	Sun Microsystems Solaris rwall Elevated F
Snort	RPC TCP rwallid request	4	Sun Microsystems Solaris rwall Elevated F
Snort	RPC UDP rwallid request	4	Sun Microsystems Solaris rwall Elevated F
Snort	WEB-IIS foxweb.dll access	12	Microsoft Exchange Server Arbitrary Code
RealSecure	SMTP_Exchange_Verb_DoS	12	Microsoft Exchange Server Arbitrary Code

La etiqueta Vulnerability está compuesta por una entrada de columna “_EXIST_”, que significa que el valor del resultado de asignación será 1 si la clave está en IsExploitWatchlist (archivo exploitDetection.csv) ó 0 si no lo está. Las columnas clave para la etiqueta vulnerability son IP y NormalizedAttackId. Cuando un evento entrante con una etiqueta de evento DestinationIP coincide con la entrada de la columna IP y una etiqueta de evento AttackId coincide con la entrada de la columna NormalizedAttackId en la misma fila, el resultado es uno (1). Si no coinciden en una misma fila, el resultado es cero (0).



Integración de orígenes de datos

El uso de tecnología adaptable y flexible es fundamental para la estrategia de integración de orígenes de datos de Sentinel, que se consigue mediante recopiladores interpretativos (también denominados recopiladores) que analizan y normalizan los eventos en el flujo de datos.

Estos recopiladores pueden modificarse según sea necesario y no están vinculados a un entorno específico. La creación, modificación, distribución y el mantenimiento de los recopiladores son simples y pueden realizarlos directamente los usuarios. Un entorno de desarrollo integrado permite la creación interactiva de recopiladores utilizando un paradigma “arrastrar y soltar” desde una interfaz de usuario gráfica. Incluso los usuarios que no son programadores pueden crear recopiladores, siempre y cuando se aseguren de que se cumplen los requisitos actuales y futuros en un entorno IT en evolución permanente. La operación de ejecución y control de los recopiladores (p. ej., iniciar, detener) se realiza centralmente desde el Centro de control de Sentinel.

Integración de aplicaciones

La integración de aplicaciones externas a través de las API estándar es fundamental para Sentinel. Por ejemplo, una API bidireccional para sistemas de mensajes de problemas incluido Remedy® y el servicio de atención al cliente de HP OpenView® permite la integración sencilla con sistemas externos.

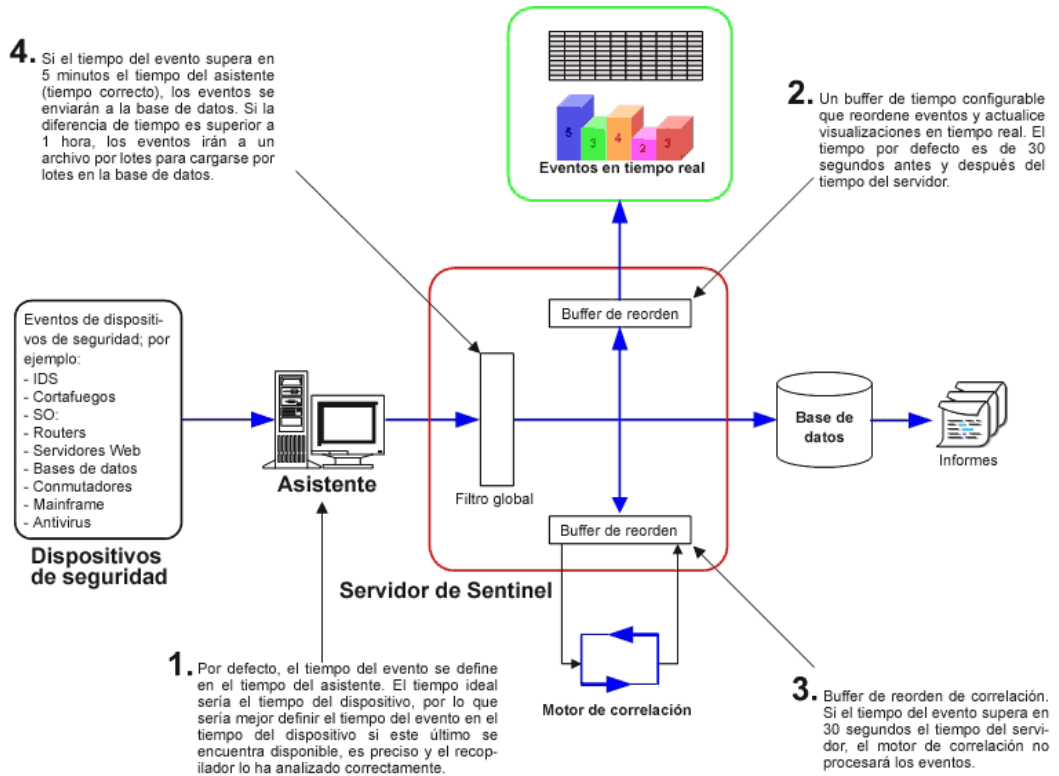
La API está basada en servicios Web y, por lo tanto, permite que sistemas externos que reconocen el protocolo SOAP se aprovechen de la integración dominante con el sistema Sentinel.

Tiempo

El tiempo de un evento es crucial para su procesamiento. Es importante para fines de generación de informes y auditivos, así como para el procesamiento en tiempo real. El motor de correlación procesa flujos de eventos ordenados por tiempo y detecta patrones dentro de eventos, además de patrones temporales en el flujo. Sin embargo, es posible que el dispositivo que genera el evento no conozca el tiempo real de generación del evento. Para adaptarlo, Sentinel permite dos opciones en alertas de procesamiento desde dispositivos de seguridad: confíe en el tiempo que el dispositivo notifica y utilícelo como el tiempo del evento o bien, en lugar de esperar el tiempo del dispositivo, marque el evento en el momento que es procesado por primera vez por Sentinel (por el recopilador).

Sentinel es un sistema distribuido y comprende varios procesos que pueden encontrarse en diferentes partes de la red. Además, puede haber algún retraso introducido por el dispositivo. Para adaptarlo, los procesos de Sentinel reordenan los eventos en un flujo ordenado por tiempo antes de procesarlo.

En la siguiente ilustración se explica el concepto del tiempo de Sentinel.



1. Por defecto, el tiempo del evento se establece en el tiempo del asistente. El tiempo ideal sería el tiempo del dispositivo. Por lo que sería mejor definir el tiempo del evento en el tiempo del dispositivo si este último se encuentra disponible, es preciso y el recopilador lo ha analizado correctamente.
2. Un buffer de tiempo configurable que reordene eventos y actualice visualizaciones en tiempo real. El tiempo por defecto es de 30 segundos antes y después del tiempo del servidor.
3. Buffer de reorden de correlación. Si el tiempo del evento supera en 30 segundos el tiempo del servidor, el motor de correlación no procesará los eventos.
4. Si el tiempo del evento supera en 5 minutos el tiempo del asistente (tiempo correcto), los eventos se enviarán a la base de datos.

Eventos internos o del sistema

Los eventos internos o del sistema son un medio para generar informes del estado y del cambio de estado del sistema. Existen dos tipos de eventos generados por el sistema interno:

- Eventos internos
- Eventos de rendimiento

Los eventos internos son informativos y describen un único estado o cambio de estado en el sistema. Generan un informe de cuándo un usuario inicia sesión o no puede autenticar, cuando se inicia un proceso o se activa una regla de correlación. Los eventos de rendimiento se generan periódicamente y describen los recursos medios utilizados por diferentes partes del sistema.

Todos los eventos del sistema rellenan los atributos siguientes:

- Campo ST (tipo de sensor): en eventos internos se ajusta en 'I' y en eventos de rendimiento se ajusta en 'P'
- ID de evento: un único UUID para el evento
- Tiempo del evento: el tiempo en el que se generó el evento
- Origen: el UUID del proceso que ha generado el evento
- Nombre de sensor: el nombre del proceso que ha generado el evento (por ejemplo, DAS_Binary)
- RV32 (categoría del evento): ajustado en 'ESEC'
- Recopilador: "Rendimiento" para eventos de rendimiento e "Interno" para eventos internos

Además de los atributos comunes, cada evento del sistema también ajusta el recurso, el subrecurso, la gravedad, el nombre del evento y las etiquetas del mensaje. En los eventos internos, el nombre del evento es lo suficientemente específico para identificar el significado exacto del evento (por ejemplo, UserAuthenticationFailed). Las etiquetas de mensajes añaden información específica; en el ejemplo anterior la etiqueta del mensaje contiene el nombre del usuario, el nombre del SO, si está disponible, y el nombre del equipo. En los eventos de rendimiento, el nombre del evento es genérico al describir el tipo de datos estadísticos y los propios datos se encuentran en la etiqueta del mensaje.

Los eventos de rendimiento se envían directamente a la base de datos. Para visualizarlos, realice una consulta rápida.

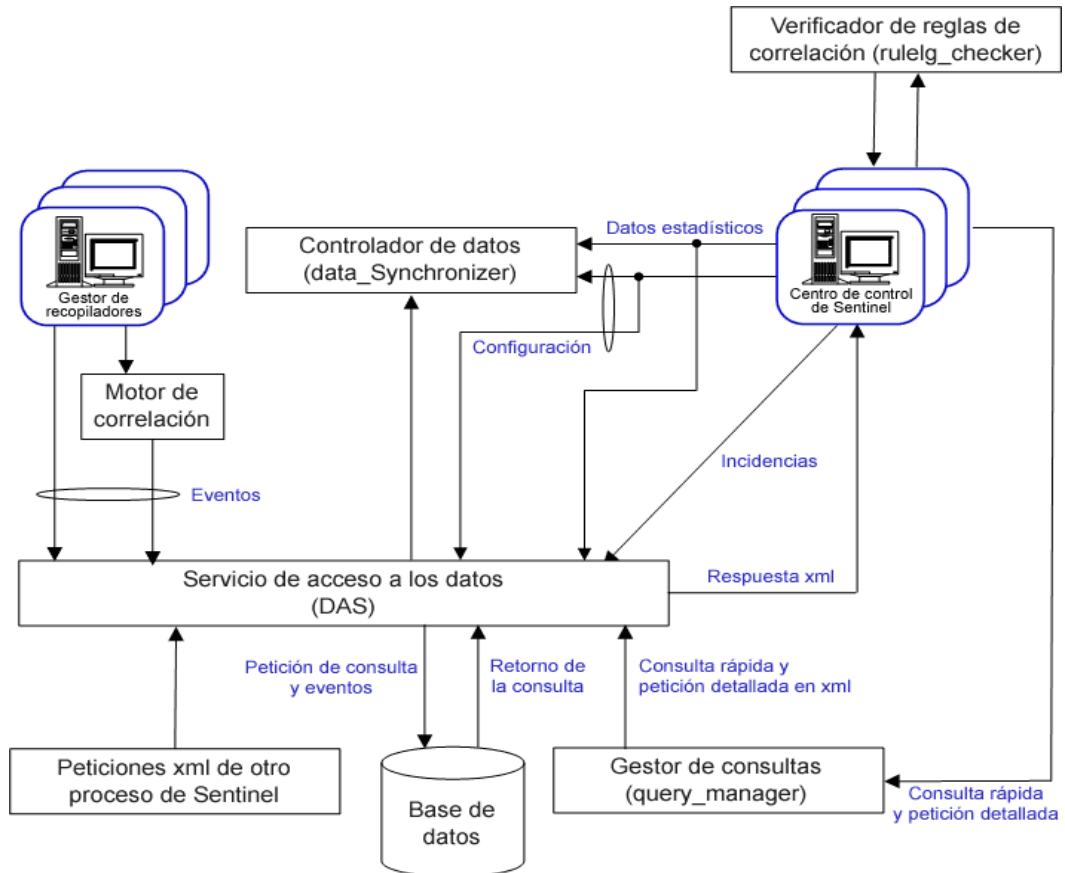
Consulte el Apéndice A – Eventos del sistema.

Procesos

Los procesos siguientes y el servicio de Windows se comunican entre ellos a través de iSCALE: el middleware orientado a mensajes (MOM).

- [Vigilancia](#)
- [Estadísticas de eventos](#)
- [Sincronizador de datos](#) (Controlador de datos)
- [Motor de correlación](#)
- [Verificador RuleLg](#) (Verificador de reglas de correlación)
- [Servicio de acceso a los datos \(DAS\)](#): binario, de consulta y vistas Active Views™
- [Gestor de consultas](#)
- Servicio Sentinel (sólo MSSQL): consulte [Vigilancia](#)

A continuación se describe la arquitectura para el servidor de Sentinel.



Proceso de vigilancia

El proceso de vigilancia es un proceso de Sentinel que gestiona otros procesos de Sentinel. Si se detiene un proceso diferente del proceso de vigilancia, éste generará un informe acerca de lo sucedido y, a continuación, reiniciará el proceso.

En Windows, la vigilancia es un servicio y se denomina Sentinel. Si se detiene este servicio, se detendrán todos los procesos de Sentinel de ese equipo.

Estadísticas de eventos

El motor Estadísticas de eventos es un componente del proceso `das_binary`. Gestiona los datos utilizados por los diagramas de vistas Active Views y las tablas de eventos en el Centro de control de Sentinel.

El motor mantiene un conjunto de eventos y datos estadísticos para cada filtro y combinación de atributos de eventos especificados en el asistente de vistas Active Views. La primera vez que un usuario crea una vista Active View con un filtro determinado y un atributo de evento, se crea un nuevo conjunto de datos. Este conjunto de datos contiene los totales del atributo a través de intervalos fijos, además de los eventos más recientes de cada uno de los intervalos. Cada conjunto de datos está configurado para retener las 24 horas de datos más recientes.

Los intervalos se envían al Centro de control de Sentinel tras un breve retraso, para estabilizar los datos que pueden haber llegado tarde debido a retrasos de red y desviación de tiempo.

Las vistas Active Views son compartidas automáticamente por múltiples usuarios si el filtro y el atributo del evento deseado son los mismos. Cuando una vista Active Views no sigue en uso por ningún usuario, será descartada tras un periodo de una hora. Sin embargo, si una vista Active View se guarda en las preferencias del usuario, continuará recolectando datos durante 100 horas.

Proceso sincronizador de datos (Controlador de datos)

El proceso de sincronizador de datos (`data_synchronizer`) gestiona la modificación de los datos de configuración por múltiples usuarios. Cuando un usuario solicita modificar los datos a través del Centro de control de Sentinel, `data_synchronizer` bloquea el registro de datos. Los detalles acerca de quién ha bloqueado los datos se publican en los otros centros de control de Sentinel activos y ningún usuario puede modificarlos. Si un centro de control de Sentinel está cerrado antes de desbloquear los datos que ha bloqueado, los bloqueos excederán el tiempo límite.

Proceso del motor de correlación (correlation_engine)

El proceso del motor de correlación (`correlation_engine`) recibe eventos del Gestor de recopiladores del asistente y publica los eventos correlacionados en función de las reglas de correlación definidas por el usuario.

Proceso del verificador RuleLg (rulelg_checker)

El proceso del verificador RuleLg (`rulelg_checker`) valida la sintaxis de las expresiones de filtros y las reglas de correlación. El Centro de control de Sentinel utiliza estos resultados para determinar si se puede guardar un filtro o una regla de correlación.

Proceso de servicio de acceso a los datos (DAS)

El proceso del Servicio de acceso a los datos (DAS) es un servicio permanente del servidor de Sentinel y proporciona una interfaz en la base de datos. Ofrece acceso basado en datos al módulo secundario de la base de datos.

DAS es un contenedor, formado por cinco procesos diferentes. Cada proceso es responsable de diferentes tipos de operaciones de la base de datos. Estos procesos son controlados por los siguientes archivos de configuración:

- `das_binary.xml`: se utiliza para las operaciones de inserción de eventos y de eventos correlacionados.
- `das_query.xml`: se utiliza para todas las demás operaciones de la base de datos.
- `activity_container.xml`: se utiliza para la ejecución y configuración de servicio de actividades.
- `workflow_container.xml`: se utiliza para la configuración del servicio de flujo de trabajo (iTRAC).
- `das_rt.xml`: se utiliza para la configuración de la función Active Views en la consola de control de Sentinel.

DAS recibe peticiones desde los diferentes procesos de Sentinel, las convierte en una solicitud contra la base de datos, procesa el resultado desde la base de datos y lo vuelve a convertir en una respuesta. Admite peticiones para recuperar eventos para una consulta rápida y para el detalle de eventos, para recuperar información de vulnerabilidades e información del asesor y para modificar la información de configuración. DAS también gestiona la entrada de todos los eventos que se reciben desde el Gestor de recopiladores del asistente y peticiones para recuperar y almacenar la información de configuración.

Proceso del gestor de consultas (query_manager)

El proceso del gestor de consultas (query_manager) recibe peticiones de consulta rápida y de detalle desde el Centro de control de Sentinel y las remite a la base de datos mediante DAS. Las peticiones del Centro de control de Sentinel definen los eventos necesarios de un filtro. Si se utiliza un filtro, el gestor de consultas recupera la definición del filtro y convierte el filtro en un criterio xml. A continuación, el gestor de consultas envía la petición a DAS. No todos los filtros pueden convertirse completamente en consultas que puedan ser procesadas por la base de datos. Si el filtro se convierte completamente, el gestor de consultas ordena a DAS que envíe la respuesta directamente al Centro de control de Sentinel. Si el filtro contiene expresiones regulares que no pueden convertirse a SQL, el gestor de consultas convierte todo lo posible y genera un criterio conservador que devuelve un superconjunto de los eventos requeridos. En ese caso, el gestor de consultas ordena a DAS que devuelva el resultado al gestor de consultas. Cuando la respuesta vuelve al gestor de consultas, éste la filtra en la memoria y envía los eventos que pasan el filtro al Centro de control de Sentinel.

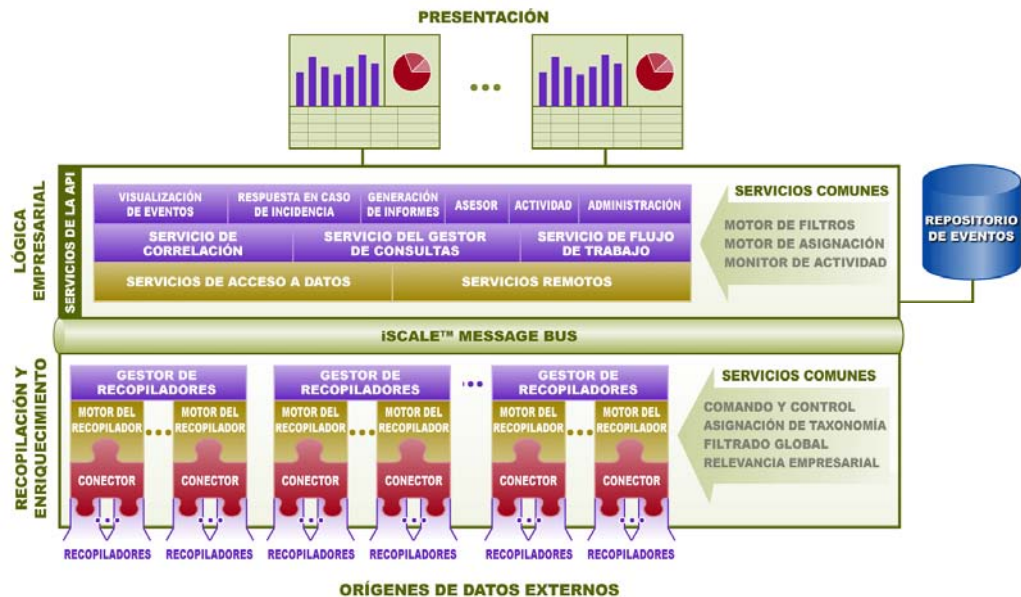
Arquitectura lógica

Sentinel 5 está formado por tres niveles lógicos:

- nivel de recopilación y enriquecimiento
- nivel de lógica empresarial
- nivel de presentación.

El nivel de recopilación y enriquecimiento añade los eventos de orígenes de datos externos, transforma los formatos específicos para dispositivos en formato Sentinel, enriquece el origen de los eventos nativos con datos de relevancia empresarial y expide los paquetes de eventos al bus de mensajes. El componente clave que dirige esta función es el recopilador, ayudado por una asignación de taxonomía y un servicio de filtro global.

El nivel de lógica empresarial contiene un conjunto de componentes distribuibles. El componente básico es un servicio remoto que añade capacidades de mensajes a los objetos de datos y a los servicios para permitir el acceso a datos transparentes en toda la red y un Servicio de acceso a los datos que es un servicio de gestión de objetos para permitir que los usuarios definan objetos utilizando metadatos. Los servicios adicionales incluyen correlación, gestor de consultas, flujo de trabajo, visualización de eventos, respuesta en caso de incidencia, actividad, asesor, generación de informes y administración.



El nivel de presentación procesa la interfaz de aplicación al usuario final. Una consola extensa denominada Centro de control de Sentinel ofrece un banco de trabajo de usuario integrado que consiste en una matriz de siete aplicaciones diferentes accesible mediante una única estructura común. Esta estructura entre plataformas se genera en estándares Java™ 1.4 y ofrece una vista unificada en componentes independientes de lógica empresarial y gráficos interactivos en tiempo real, respuesta en caso de incidencia accionable, flujo de trabajo aplicable automatizado, generación de informes, solución de incidencias contra explotaciones conocidas además de otras funciones.

Cada uno de los niveles está ilustrado en la imagen anterior y discutido posteriormente en detalle en las siguientes secciones.

Nivel de recopilación y enriquecimiento

Los eventos se añaden utilizando un conjunto de recopiladores flexibles y configurables, que recopilan datos desde un gran número de sensores y otros dispositivos y orígenes. El usuario puede utilizar recopiladores previamente generados, modificar recopiladores existentes o generar sus propios recopiladores para garantizar que el sistema cumpla todos los requisitos.

Los datos añadidos por los recopiladores en forma de eventos se normalizan posteriormente y se transforman en formato XML, enriquecidos con una serie de metadatos (p. ej., datos sobre datos) mediante un conjunto de servicios de relevancia empresarial y propagados al servidor para un análisis informático exhaustivo utilizando la plataforma del bus de mensajes. El nivel de recopilación y enriquecimiento está formado por los componentes siguientes:

- Conectores y recopilador
- Gestor y motor del recopilador
- Generador de recopiladores

Conectores y recopiladores

Un conector es un concentrador o adaptador multiplexado que conecta el motor del recopilador a los dispositivos reales monitorizados.

Los recopiladores son las agregaciones a nivel de componentes de datos de eventos desde un origen específico. Sentinel 5 admite principalmente conexiones remotas “sin recopilador” a orígenes; sin embargo, los recopiladores pueden ser distribuidos en dispositivos específicos en los que un acceso remoto es menos eficiente.

Los recopiladores están controlados desde el Centro de control de Sentinel, que dirige la comunicación entre los recopiladores y la plataforma de Sentinel para el análisis en tiempo real, el cálculo de correlación y la respuesta en caso de incidencia.

Gestor y motor del recopilador

El Gestor de recopiladores gestiona los recopiladores, monitoriza los mensajes de estado del sistema y realiza un filtrado de eventos según sea necesario. Entre las principales funciones del gestor de recopiladores se incluyen la transformación de eventos, la adición de relevancia empresarial en eventos mediante taxonomía, la realización de un filtrado global en eventos, el encaminamiento de los eventos y envío de mensajes de la actividad al servidor de Sentinel.

Un motor de recopilador es el componente intérprete que analiza el código del recopilador.

Generador de recopiladores

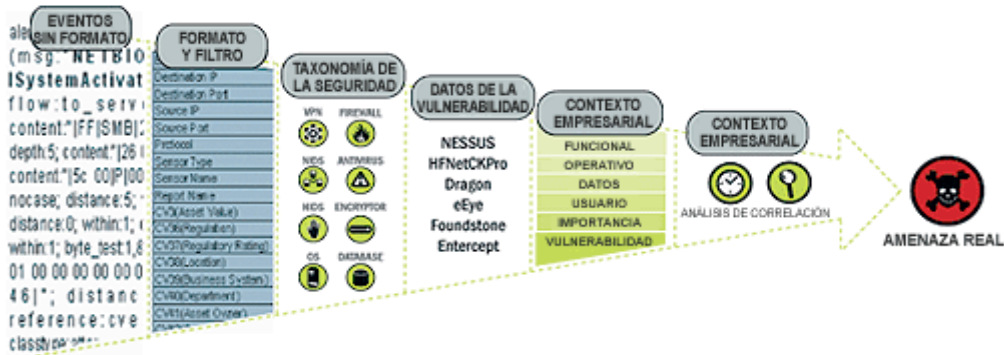
El Generador de recopiladores es una aplicación independiente que se utiliza para generar, configurar y depurar recopiladores. Esta aplicación sirve de entorno de desarrollo integrado (o IDE) que permite que el usuario pueda crear nuevos recopiladores para analizar datos desde dispositivos de origen mediante un idioma informativo para un propósito especial diseñado para gestionar la naturaleza de la red y los eventos de seguridad.

Servicios comunes

Todos los componentes descritos anteriormente en este nivel de recopilación y enriquecimiento son dirigidos por un conjunto de servicios comunes. Estos servicios de utilidades forman el tejido de la recopilación y el enriquecimiento de datos y facilitan el filtrado del ruido de la información (mediante filtros globales), aplicando etiquetas definidas por el usuario para enriquecer la información de los eventos (mediante los servicios de relevancia empresarial y de asignación de taxonomía) y dirigiendo las funciones de los recopiladores de datos (mediante servicios de ejecución y control).

Taxonomía: casi todos los productos de seguridad producen eventos en diferentes formatos y con contenido variable. Por ejemplo, Windows y Solaris generan un informe diferente de un error en el inicio de sesión.

La taxonomía de Sentinel convierte automáticamente los datos de productos heterogéneos en términos significativos, lo que permite una vista homogénea en tiempo real de la seguridad de red completa. La taxonomía de Sentinel formatea y filtra los eventos de seguridad sin formato antes de agregar un contexto de evento al flujo de datos. Este proceso formatea todos los datos de seguridad en la estructura óptima para el procesamiento mediante el motor de correlación de Sentinel, como se puede observar en el siguiente diagrama.



Relevancia empresarial: Sentinel 5 aplica datos contextuales de relevancia empresarial directamente en el flujo de eventos. Incluye hasta 135 campos personalizables en los que los usuarios pueden agregar información específica de activos, como la unidad empresarial, el propietario, el valor de activo, la geografía. Una vez se ha agregado esta información al sistema, todos los demás componentes pueden aprovecharse del contexto adicional.

SERVER	REGULATION	LOCATION	DEPARTMENT	OPERATING ENVIRONMENT				
IP Address	Asset Value	Regulation	Regulatory Rating	Location	Business System	Department	Asset Owner	Operation Env
172.16.2.45	3500000	HIP AA	Medium	San Francisco HQ	Claim Mgt	Claims Processing	MP Claims	Production
192.168.0.5	3500	None	Not Applicable	San Diego Bldg	Personal Productivity	Claims Adjustments	MP Claims	Production
10.15.69.32	350000	None	Not Applicable	Los Angeles Center	RISKE	Application Development	MP Risk Apps Dev	Development
10.85.145.98	3500000	Sarbanes Oxley	High	San Diego Bldg	Financial Management	Finance	CFO	Production

Labels below the table: ASSET VALUE, REGULATORY RATING, BUSINESS SYSTEM, OWNER

Detección de explotaciones: permite la notificación inmediata y accionable de ataques en sistemas vulnerables. Ofrece un enlace en tiempo real entre las firmas IDS y los resultados de la exploración de vulnerabilidad, notificando a los usuarios automática e inmediatamente cuando un atacante intenta explotar un sistema vulnerable. De este modo, se mejora drásticamente la eficiencia y la efectividad de respuesta en caso de incidencia.

La detección de explotaciones ofrece a los usuarios actualizaciones de asignaciones entre firmas de escáners de vulnerabilidad y las del sistema IDS. Las asignaciones incluyen una lista extensa de escáners de vulnerabilidad e IDS. Los usuarios simplemente cargan los resultados de la exploración de vulnerabilidad en Sentinel. La detección de explotaciones los analiza automáticamente y actualiza los recopiladores de IDS adecuados. Utiliza el conocimiento incrustado de estado de vulnerabilidad para establecer prioridades eficientemente y con efectividad en las respuestas a amenazas de seguridad en tiempo real.

Cuando se lanza un ataque contra un activo vulnerable, la detección de explotaciones alerta a los usuarios con el nivel de gravedad correspondiente de la vulnerabilidad explotada. Los usuarios pueden realizar una acción inmediata en eventos de alta prioridad. Esta acción elimina las conjeturas de la supervisión de alertas y aumenta la eficiencia en la respuesta en caso de incidencia centrando la reacción en ataques conocidos en contra de los activos vulnerables.

La detección de explotaciones también permite a los usuarios asignar firmas y vulnerabilidades o “quitar la asignación” para poner a punto negativos y positivos falsos y para aprovechar firmas personalizadas o exploraciones de vulnerabilidad.

Nivel de lógica empresarial

El núcleo de la plataforma de Sentinel 5 está formado por un conjunto de servicios conectados que pueden ejecutarse en una configuración independiente o en una topología distribuida. Esta arquitectura orientada a servicios (SOA) se denomina iSCALE. Específicamente, la SOA de Sentinel comprende un conjunto de motores, servicios y API que trabajan conjuntamente para la ampliación lineal de la solución contra el aumento de la carga de datos y/o el procesamiento de la cantidad de trabajo.

Los servicios de Sentinel se ejecutan en contenedores especializados y permiten un procesamiento y una ampliación excelentes, ya que están optimizados para el transporte de mensajes y el cálculo. Los servicios principales que forman el servidor de Sentinel incluyen:

- Servicio remoto
- Servicio de acceso a los datos
- Servicio del gestor de consultas
- Servicio de correlación
- Servicio de flujo de trabajo
- Visualización de eventos
- Respuesta en caso de incidencia
- Generación de informes
- Asesor
- Actividad
- Administración

Servicio remoto

El servicio remoto de Sentinel 5 ofrece el mecanismo mediante el cual el servidor y los programas cliente se comunican. Este mecanismo se denomina normalmente aplicación de objeto distribuido.

Específicamente, el servicio remoto ofrece:

- Localizar objetos remotos: Esto se consigue mediante metadatos que describen el nombre del objeto o el testigo de registro, aunque no se requiere la ubicación actual, ya que el bus de mensajes iSCALE permite la transparencia de ubicaciones.
- Comunicarse con objetos remotos: La información acerca de la comunicación entre los objetos remotos es gestionada por el bus de mensajes de iSCALE.
- Segmentación y emisión de objetos: Cuando se deben pasar grandes cantidades de datos una y otra vez del cliente al servidor, estos objetos se optimizan para cargar los datos a pedido.
- Devoluciones de llamadas: Otro patrón y nivel de abstracción generado en el servicio remoto que permite la comunicación de objetos remotos PTP.
- Supervisión del servicio y estadísticas: Proporciona rendimiento y carga estadísticas para el uso de estos servicios remotos.

Servicio de acceso a los datos

El servicio de acceso a los datos (DAS) es un servicio de gestión de objetos que permite que los usuarios definan objetos utilizando metadatos. DAS gestiona el objeto y su acceso y automatiza la transmisión y la permanencia. DAS también sirve de fachada para acceder a los datos desde cualquier almacén de datos permanente como bases de datos, servicios de directorio o archivos. Las funciones de DAS incluyen acceso uniforme a los datos mediante JDBC y estrategias de inserción de eventos de alto rendimiento opcionales utilizando conectores nativos (p. ej. OCI para Oracle 9i y ADO para Microsoft SQL Server).

Servicio del gestor de consultas

El servicio del gestor de consultas dirige las solicitudes de detalle y del historial de eventos desde el Centro de control de Sentinel. Este servicio es un componente incorporado para implementar el algoritmo de paginación utilizado en la función de examinación del Historial de eventos. Convierte filtros definidos por el usuario en criterios válidos y les añade criterios de seguridad al final antes de recuperar los eventos. Este servicio también garantiza que los criterios no cambien durante una transacción del historial de eventos paginado.

Servicio de correlación

El algoritmo de correlación de Sentinel 5 calcula eventos correlacionados analizando el flujo de datos en tiempo real. Publica los eventos correlacionados basados en reglas definidas por el usuario antes de que los eventos alcancen la base de datos. Las reglas del motor de correlación pueden detectar un patrón en un único evento de una ventana de eventos en ejecución. Una vez que se ha detectado una concordancia, el motor de correlación genera un evento correlacionado describiendo el patrón encontrado y puede crear una incidencia o activar un flujo de trabajo de soluciones mediante iTRAC. El motor de correlación funciona con un componente de verificador de reglas que calcula las expresiones de reglas de correlación y valida la sintaxis de los filtros. Además de proporcionar un conjunto extenso de reglas de correlación, el motor de correlación de Sentinel ofrece ventajas específicas acerca de los motores de correlación centrados en bases de datos.

- Al confiar en el procesamiento de la memoria antes que en las inserciones y lecturas de la base de datos, el motor de correlación realiza, durante grandes volúmenes en estado seguro y durante eventos en estado de ataque, el tiempo en el que el rendimiento es más crítico.
- El volumen de correlación no disminuye la velocidad de otros componentes del sistema, de modo que la interfaz de usuario permanece receptiva, especialmente con grandes volúmenes de eventos.
- Correlación distribuida: las organizaciones pueden distribuir múltiples motores de correlación, cada uno en su propio servidor, sin necesidad de duplicar configuraciones ni añadir bases de datos. La ampliación independiente de componentes ofrece un rendimiento y una capacidad de ampliación rentables.
- El motor de correlación puede añadir eventos en incidencias después de haberse determinado una incidencia.

Se anima a los usuarios a calcular una métrica denominada Reglas de eventos por segundo (ERPS). ERPS es el cálculo del número de eventos que pueden examinarse mediante una regla de correlación por segundo. Esta medida es un buen indicador de rendimiento, ya que estima el impacto en el rendimiento cuando dos factores se cruzan: los eventos por segundo y el número de reglas en uso.

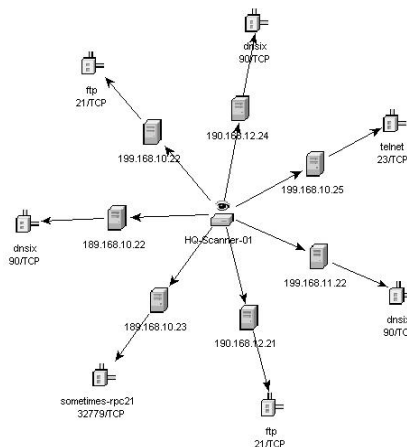
Servicio de flujo de trabajo (iTRAC)

El servicio de flujo de trabajo recibe activadores en la creación de incidencias e inicia procesos de flujo de trabajo basados en plantillas de flujo de trabajo predefinidas. Gestiona el ciclo de vida de estos procesos generando elementos de trabajo o ejecutando actividades. Este servicio también mantiene un historial de procesos completados que puede utilizarse para las respuestas en caso de incidencias auditivas.

Visualización de eventos

Active Views™, la interfaz de usuario gráfica interactiva para la visualización de eventos, proporciona una consola de gestión de seguridad integrada con un extenso conjunto de herramientas de visualización y análisis en tiempo real para facilitar el análisis y la detección de amenazas. Los usuarios pueden supervisar los eventos en tiempo real y realizar detalles instantáneos desde segundos a horas en el pasado. Una amplia matriz de ayudas y diagramas de visualización permite supervisar la información mediante una representación en diagramas de barras 3D, diagramas 2D apilados y diagramas de cintas y de líneas, entre otros. La información útil adicional puede visualizarse desde la consola de vistas Active Views, incluida la notificación de explotaciones de activos (detección de explotaciones), visualizando la información de activos y las asociaciones de diagramas entre las IP de origen pertinentes y las IP de destino.

Dado que Active Views utiliza la arquitectura iSCALE, los analistas pueden realizar rápidamente un análisis más detallado, ya que Active Views proporciona acceso directo a los datos de eventos residentes en la memoria en tiempo real, lo que permite gestionar fácilmente miles de eventos por segundo sin ninguna degradación en el rendimiento. Los datos se guardan en la memoria y se escriben en la base de datos según sea necesario (las vistas Active Views pueden almacenar hasta 8 horas de datos en la memoria con cargas de eventos habituales). Esta vista en tiempo real sin interrupción orientada al rendimiento es esencial tanto en estado de ataque como en estado seguro.



La estructura de automatización de iTRAC funciona utilizando dos componentes clave: el contenedor de actividades y el contenedor de flujos de trabajo. El primero automatiza la ejecución de actividades para el conjunto de pasos especificado basándose en reglas de entrada y, el segundo, automatiza la ejecución de flujos de trabajo basándose en actividades mediante una lista de trabajo. Las reglas de entrada se basan en el estándar XPDL (lenguaje de definición de procesos XML) y ofrecen un modelo formal para expresar procesos ejecutables en una empresa. Este enfoque basado en estándares hacia la implementación de reglas específicas empresariales y conjuntos de reglas asegura una futura comprobación del procesamiento de definiciones para clientes.

Servicio de generación de informes

El servicio de generación de informes permite la generación de informes, incluidos los informes de vulnerabilidades y del historial. Sentinel 5 incluye informes listos para usar y permite a los usuarios configurar sus propios informes utilizando Crystal Reports. Algunos ejemplos de los informes incluidos en Sentinel 5 son:

- Análisis de tendencias
- Estado de seguridad de líneas de negocios o activos críticos
- Tipos de ataques
- Activos de destino
- Tiempo de respuesta y resolución
- Infracciones de conformidad con directivas

Asesor

El asesor de Sentinel, un módulo opcional, ofrece referencias cruzadas entre datos de alerta en tiempo real con información sobre vulnerabilidades y soluciones. De ese modo, se disminuye la brecha entre la detección de un ataque y la respuesta a éste. Con el asesor, las organizaciones pueden determinar si los eventos explotan vulnerabilidades específicas y cómo impactan estos ataques a sus activos. El asesor también contiene información específica acerca de las vulnerabilidades que los ataques intentan explotar, los efectos potenciales de los ataques, si son correctos, y los pasos necesarios para su solución. Los pasos recomendados para la solución son seguidos utilizando los procesos de respuesta en caso de incidencia de iTRAC.

Actividad

El servicio Actividad permite a los usuarios obtener una extensa vista de la plataforma distribuida de Sentinel 5. Añade información de actividades desde varios procesos que son distribuidos normalmente en varios servidores. La información de actividades se muestra periódicamente en el Centro de control de Sentinel destinada al usuario final.

Administración

La función Administración permite las funciones de gestión de usuarios y ajuste de configuraciones normalmente necesarias para los administradores de la aplicación de Sentinel 5.

Servicios comunes

Todos los componentes descritos anteriormente en este nivel de lógica empresarial de la arquitectura son dirigidos por un conjunto de servicios comunes. Estos servicios de utilidades facilitan a los usuarios el filtrado de granulado fino de eventos (mediante el motor de filtros), la continua monitorización de estadísticas de actividades del sistema (mediante el monitor de actividades) y las actualizaciones dinámicas de todos los datos del sistema (mediante el servicio de asignación). Conjuntamente, estos servicios de utilidades forman la fábrica de los servicios conectados que permiten una ampliación y un procesamiento excelentes del transporte basado en bus de mensajes para el cálculo y el análisis en tiempo real.

Nivel de presentación

El nivel de presentación procesa la interfaz de aplicación al usuario final. El Centro de control de Sentinel es una extensa consola que presenta la información al usuario.

Módulos del producto

Centro de control de Sentinel

El Centro de control de Sentinel ofrece una consola de gestión de seguridad potente e integrada. Las visualizaciones intuitivas permiten a los analistas identificar rápidamente las nuevas tendencias o los ataques, modificar e interactuar con información gráfica en tiempo real y responder a incidencias. Las funciones clave incluyen:

- Vistas Active Views: análisis y visualización en tiempo real
- Incidencias: creación y gestión de incidencias
- Análisis: definición y gestión de definiciones de reglas de correlación
- iTRAC: gestión de procesos de documentación, aplicación y seguimiento de procesos de resolución de incidencias.
- Generación de informes: informes y medidas de historial

Asistente de Sentinel

El Asistente de Sentinel recopila datos de dispositivos de origen y ofrece un flujo de eventos más intenso aplicando taxonomía, detección de explotaciones y relevancia empresarial en el flujo de datos antes de que los eventos se correlacionen, analicen y envíen a la base de datos. Un flujo de datos más intenso significa que los datos se correlacionan con el contexto empresarial necesario para identificar y dar solución a las amenazas internas o externas y a las infracciones de directivas. En cualquier configuración, es posible que se hayan implantado uno o varios asistentes que ofrecen al cliente la capacidad de implantar componentes de productos en su infraestructura según la topología de red.

Asesor de Sentinel

El asesor de Sentinel, un módulo opcional, ofrece referencias cruzadas entre datos de alerta en tiempo real con información sobre vulnerabilidades y soluciones.

Contenido

Esta guía incluye los siguientes capítulos:

- Capítulo 1 – Introducción a Sentinel
- Capítulo 2 – Navegación en el Centro de control de Sentinel
- Capítulo 3 – Pestaña Vistas Active Views™
- Capítulo 4 – Pestaña Incidencias
- Capítulo 5 – Pestaña iTRAC™
- Capítulo 6 – Pestaña Análisis
- Capítulo 7 – Pestaña Asesor
- Capítulo 8 – Pestaña Recopiladores
- Capítulo 9 – Pestaña Admin
- Capítulo 10 – Gestor de datos de Sentinel
- Capítulo 11 – Utilidades
- Capítulo 12 – Inicio rápido
- Apéndice A – Eventos del sistema

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
```

Otros materiales de consulta de Novell

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

- Guía de instalación de Sentinel™ 5
- Guía del usuario de Sentinel™
- Guía del usuario del asistente de Sentinel™ 5
- Guía de referencia del usuario de Sentinel™ 5
- Guía de integración de productos de otros fabricantes en Sentinel™ 5
- Notas de revisión

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

Navegación por el Centro de control de Sentinel

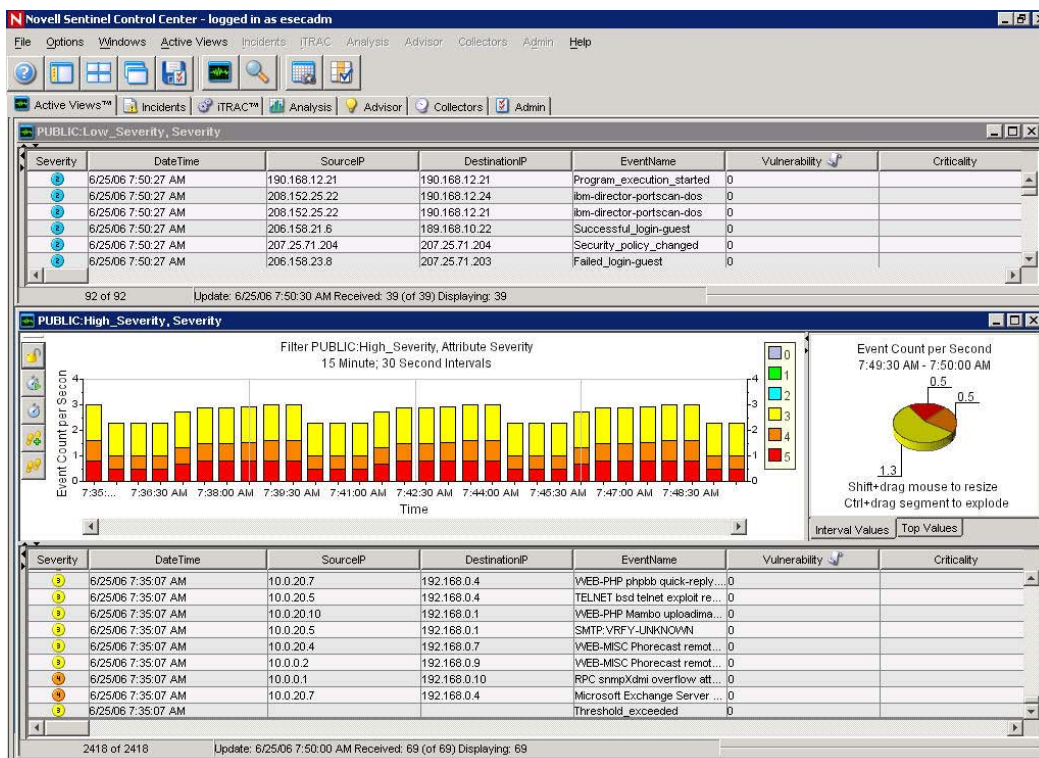
NOTA: El término agente puede intercambiarse con recopilador. En adelante, los agentes se denominarán recopiladores.

El Centro de control de Sentinel está formado por:

- [Barra de menús](#)
- [Barra de herramientas](#)
- [Pestañas](#)

Además, se tratarán los temas siguientes:

- [Inicio del Centro de control de Sentinel](#)
- [Cambio de apariencia del Centro de control de Sentinel](#)
- [Almacenamiento de las preferencias del usuario](#)
- [Cambio de la contraseña de Sentinel](#)



Inicio del Centro de control de Sentinel

Inicio del Centro de control de Sentinel en Windows

Inicio del Centro de control de Sentinel en Windows

1. Haga clic en *Inicio > Sentinel > Centro de control de Sentinel* o haga clic en *Centro de control de Sentinel* en el escritorio.
2. Introduzca el nombre de usuario, la contraseña y haga clic en *Aceptar*.

Inicio del Centro de control de Sentinel en UNIX

Inicio del Centro de control de Sentinel en UNIX

1. Como usuario esecadm, cambie al directorio siguiente:

```
$ESEC_HOME/sentinel/console
```
2. Ejecute el comando siguiente:

```
./run.sh
```
3. Introduzca el nombre de usuario, la contraseña y haga clic en *Aceptar*.

Barra de menús

Debajo de la barra de título hay diez menús. Desde la izquierda, por toda la parte superior de la ventana se encuentran Archivo, Opciones, Ventanas, Vistas Active Views, Incidencias, iTRAC, Asesor, Recopiladores, Admin y Ayuda.

Las opciones Archivo, Opciones, Ventanas y Ayuda siempre están disponibles. Existen otras opciones disponibles, en función de la pestaña que está activa y de los permisos de que disponga.

Menú Archivo

- Guardar preferencias
- Salir

Menú Opciones

- Cambiar la contraseña
- Colocación de pestañas
 - Arriba
 - Abajo
- Anclar navegador
- Mostrar el navegador

Menú Ventanas

- Disponer todo en cascada
- Disponer todo en mosaico
 - Mejor puesta en mosaico
 - Poner en mosaico horizontal
 - Poner en mosaico vertical
- Minimizar todo
- Restaurar todo
- Cerrar todo

Vistas Active Views™

- Propiedades
- Crear una vista Active Views
- Consulta de eventos
- Tiempo real del evento
 - Instantánea
 - Gestionar las columnas

Incidencias

- Visualizar el gestor de vistas de incidencias
- Crear incidencia
- Configuración del visor de adjuntos

iTRAC™

- Visualizar el gestor de procesos

Análisis

- Crear un informe

Asesor

- Crear un informe

Recopiladores

- Visualizar el gestor de vistas del recopilador

Admin

- Configuración de informes
- Reglas de correlación
- Gestor de motores de correlación
- Configuración del filtro global
- Configuración del menú
- Configuración del filtro
- Configuración del usuario

Ayuda






- Ayuda
- Acerca de Sentinel

Barra de herramientas

Siempre se muestran cinco botones de la barra de herramientas en todo el sistema. Los otros botones se muestran en función de la pestaña o de la ventana que esté activa y de los permisos del usuario.

Barra de herramientas del sistema

Los cinco botones de la barra de herramientas del sistema son:

-  Ver la ayuda de Sentinel
-  Mostrar u ocultar la ventana de navegación
-  Disponer en mosaico todas las ventanas de visualización
-  Disponer en cascada todas las ventanas de visualización
-  Guardar las preferencias del usuario

Pestaña Vistas Active Views™

Cuando la pestaña Vistas ActiveViews™ está activa, están disponibles las siguientes opciones.

-  Vistas Active Views
-  Lanzar la consulta de eventos

Ventana de eventos a lo largo del tiempo

Cuando la ventana de eventos a lo largo del tiempo está activa, se muestran las opciones siguientes.

















-  Instantánea de una tabla de eventos a lo largo del tiempo
-  Gestionar las columnas de una tabla de eventos a lo largo del tiempo

Diagrama de eventos a lo largo del tiempo

Cuando el diagrama de eventos a lo largo del tiempo está activo, están disponibles las siguientes opciones en el diagrama de eventos.


-  Bloquear o desbloquear el diagrama
-  Aumentar el intervalo de visualización
-  Disminuir el intervalo de visualización
-  Aumentar el tiempo de visualización
-  Disminuir el tiempo de visualización

Al hacer clic en el botón Bloquear, los botones disponibles son:

-  ▪ Bloquear o desbloquear el diagrama
-  ▪ Aumentar el intervalo de visualización
-  ▪ Disminuir el intervalo de visualización
-  ▪ Aumentar el tiempo de visualización
-  ▪ Disminuir el tiempo de visualización
-  ▪ Acercar
-  ▪ Alejar
-  ▪ Detallar hasta los eventos
-  ▪ Guardar como archivo html




Ventana Instantánea

Cuando la ventana Instantánea está activa, está disponible la opción siguiente.

-  Gestionar las columnas


Pestaña Incidencias

Cuando la pestaña Incidencias está activa, están disponibles las siguientes opciones.

-  Visualizar el gestor de vistas de incidencias
-  Crear una incidencia nueva
-  Configurar visores de adjuntos


Incidencia

Cuando una incidencia está abierta, está disponible la siguiente opción.

-  Gestionar columnas de eventos asociados


iTRAC

Cuando la pestaña iTRAC está activa, está disponible la siguiente opción.

-  Visualizar el gestor de vistas del proceso



Pestañas Análisis y Asesor

Cuando la pestaña Análisis o Asesor está activa, está disponible la opción siguiente.

-  Crear un informe









Pestaña Recopiladores

Cuando la pestaña Recopiladores está activa, están disponibles las siguientes opciones.

-  Muestra el gestor de vistas del Gestor de recopiladores
-  Muestra el gestor de vistas del recopilador



Pestaña Admin

Cuando la pestaña Admin está activa, están disponibles las siguientes opciones.

- | | |
|--|---|
| ▪  Visualizar la configuración de la información | ▪  Visualizar las reglas de correlación |
| ▪  Visualizar el gestor de motores de correlación | ▪  Visualizar la configuración del filtro global |
| ▪  Visualizar la configuración del menú | ▪  Visualizar el gestor de filtros |
| ▪  Visualizar el gestor de usuarios | ▪  Gestor de vistas del servidor |





Ventana Gestor de filtros

Cuando la ventana Gestor de filtros está activa, están disponibles las siguientes opciones.

-  Crear un filtro nuevo
-  Suprimir el filtro seleccionado (está activa cuando se selecciona un filtro)

Menú Configuración del menú

Cuando la ventana Configuración del menú está activa y en modo modificar, están disponibles las opciones siguientes.

- | | |
|---|---|
| ▪  Crear un nuevo elemento de menú | ▪  Suprimir elemento de menú |
| ▪  Activar elemento de menú | ▪  Desactivar elemento de menú |

Pestañas

Según sus permisos de usuario, el Centro de control de Sentinel mostrará las siguientes pestañas. Debe tener el permiso específico para ver cada pestaña.

- Vistas Active Views™
- Incidencias
- iTRAC™
- Análisis
- Asesor
- Recopiladores
- Admin

Para obtener más información acerca de las Pestañas, consulte los capítulos individuales de cada pestaña.

Cambio de apariencia del Centro de control de Sentinel

Puede cambiar la apariencia del Centro de control de Sentinel realizando una de las acciones siguientes:

- [Ajustar la posición de la pestaña](#)
- [Mostrar u ocultar la ventana del navegador](#)
- [Anclar o hacer flotar la ventana del navegador](#)
- [Disponer las ventanas en cascada](#)
- [Disponer las ventanas en mosaico](#)
- [Minimizar y restaurar todas las ventanas](#)
- [Cerrar todas las ventanas abiertas](#)

Ajuste de la posición de la pestaña

Para ajustar la posición de la pestaña

1. Haga clic en *Opciones > Colocación de pestañas*.
2. Seleccione Arriba o Abajo.

Cómo mostrar u ocultar la ventana del navegador

Para mostrar u ocultar la ventana del navegador

1. Haga clic en *Opciones > active o desactive Mostrar el navegador*.

Cómo anclar o hacer flotar la ventana del navegador

Para anclar o flotar la ventana del navegador

1. Haga clic en *Opciones > active o desactive Anclar el navegador*.

Disposición de las ventanas en cascada

Para disponer las ventanas en cascada

1. Haga clic en *Ventanas > Disponer todo en cascada*. Todas las ventanas abiertas del panel derecho se dispondrán en cascada.

Disposición de las ventanas en mosaico

Para disponer las ventanas en mosaico

1. Haga clic en *Ventanas > Disponer todo en mosaico*.
2. Señale una de estas opciones:
 - Mejor puesta en mosaico
 - Poner en mosaico vertical
 - Poner en mosaico horizontal

Minimización y restauración de todas las ventanas

Para minimizar todas las ventanas

1. Haga clic en *Ventanas > Minimizar todo*. Todas las ventanas abiertas del panel derecho se minimizarán.

Para restaurar todas las ventanas al tamaño original

Para restaurar todas las ventanas al tamaño original

1. Haga clic en *Ventanas > Restaurar todo*. Todas las ventanas del panel derecho se restaurarán al tamaño original.

Para restaurar una ventana individual

Para restaurar una ventana individual

1. Haga clic en la ventana minimizada. La ventana se restaurará al tamaño original.

Cierre de todas las ventanas abiertas a la vez

Para cerrar todas las ventanas

1. Haga clic en *Ventanas > Cerrar todo*.

Almacenamiento de las preferencias del usuario

Debe tener el permiso de usuario Guardar área de trabajo.

Las preferencias que se pueden guardar son:

- Ventanas permanentes, aquellas que pueden volver a crearse porque no dependen de los datos disponibles en el momento que fueron creadas originalmente. Por ejemplo, pueden guardarse las visualizaciones de resúmenes y las vistas Active Views. Sin embargo, las ventanas temporales, como las instantáneas y las consultas rápidas, no pueden guardarse. Se guardan todas las ventanas de la lista del navegador Admin pero, en cambio, no se guarda ninguna de las ventanas secundarias que se ha abierto haciendo doble clic en una de ellas.
- Posiciones de ventanas

- Tamaños de ventanas, incluida la ventana de aplicación
- Posiciones de pestañas
- Navegador anclado o flotando y mostrado u oculto

Para guardar las preferencias

1. Haga clic en *Archivo > Guardar preferencias* o haga clic en *Guardar preferencias*.



Cambio de la contraseña del Centro de control de Sentinel

NOTA: Para satisfacer las estrictas configuraciones de seguridad que requiere la certificación de criterios comunes, es muy recomendable que se utilice una contraseña segura con las características siguientes:

1. Elija contraseñas con una longitud mínima de 8 caracteres y que incluya al menos un carácter en MAYÚSCULA, uno en minúscula, un símbolo especial (!@#\$%^&*()_+) y un signo numérico (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).
-

Para cambiar su contraseña del Centro de control de Sentinel

1. Haga clic en *Opciones > Cambiar la contraseña*.
2. Escriba la contraseña antigua.
3. Escriba la contraseña nueva y vuelva a escribirla para verificarla.

NOTA: Novell recomienda encarecidamente que, como práctica recomendada, para la contraseña se utilice una longitud mínima de 8 caracteres alfanuméricos.

4. Haga clic en *Aceptar*.

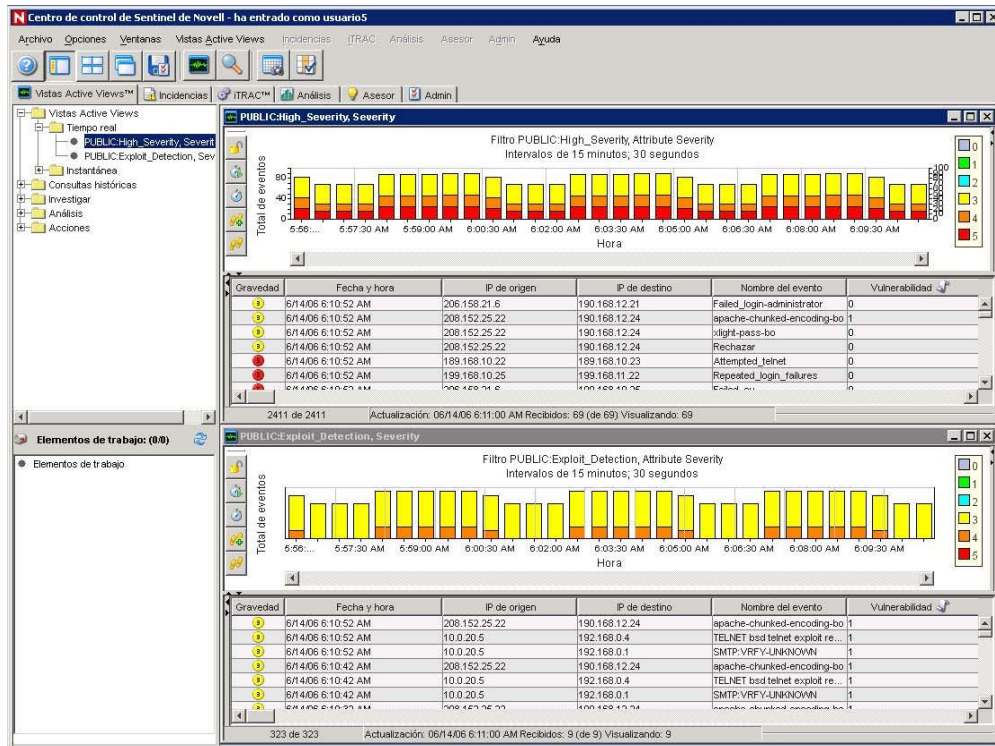
3

Pestaña Vistas Active Views™

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

Para utilizar la pestaña Vistas Active Views™ debe tener los permisos adecuados. Si no se asigna este permiso, no estará disponible ninguno de los permisos relacionados con las acciones de esta pestaña.

En la pestaña Vistas Active Views, puede monitorizar eventos, casi en tiempo real, en el momento en el que están sucediendo y realizar consultas sobre estos eventos. Puede monitorizarlos en forma de tabla o a través de una representación en diagramas de barras 3D, diagramas 2D apilados y diagramas de cintas y de líneas.



Pestaña Vistas Active Views: Descripción

El formato de las vistas de eventos es de tablas. La configuración de la vista Active Views se determina mediante el archivo `das_rt.xml`. Los dos tipos de vistas Active Views son una tabla de eventos casi en tiempo real con representación gráfica e instantánea.

- Tabla de eventos casi en tiempo real
 - Retiene hasta 750 eventos en un plazo de 30 segundos.
 - Por defecto, el cliente mantiene un plazo de 24 horas de eventos en caché. Esta opción puede configurarse en [Propiedades de la vista Active Views](#).
 - Por defecto, la tabla de eventos mostrará un máximo de 30.000 eventos. Esta opción puede configurarse en [Propiedades de la vista Active Views](#).
 - Por defecto, la tabla de eventos se actualiza cada 30 segundos (retraso de tiempo de envío) y se representa mediante una línea gris en la tabla de eventos.

3	2005.06.21 / 06:34:38 EDT			Threshold_ex
2	2005.06.21 / 06:34:38 EDT	206.158.21.6	192.168.10.1	Password_ex
2	2005.06.21 / 06:34:28 EDT	190.168.12.21	190.168.12.21	Program_exe

Cuando hay más de 750 eventos en un plazo de 30 segundos, aparecerá una línea de separación roja que indica que hay más eventos de los que aparecen.

3	2005.06.21 / 07:07:00 EDT	172.16.112.50	172.16.0.65	unsuccessfu
3	2005.06.21 / 07:07:00 EDT	172.16.112.50	172.16.0.65	suspicious-fil
3	2005.06.21 / 07:06:58 EDT	172.16.112.50	172.16.0.65	successful-a

- Al guardar las preferencias del usuario, continuará recopilando datos durante 4 días. Por ejemplo, si guarda sus preferencias, cierra la sesión y vuelve a entrar a la sesión el día siguiente, la vista Active Views mostrará cualquier dato como si no se hubiera desconectado.
- Si se crea una vista Active Views y no se guarda, continuará recopilando datos durante una hora. En este plazo de tiempo de una hora, si se crea una vista Active Views idéntica, la vista Active Views mostrará los datos de la última hora.
- Instantánea: vistas en marca horaria de una tabla de vistas de eventos en tiempo real.

Los elementos siguientes hacen que una vista Active Views sea única.

- El filtro asignado a una vista Active Views
- El atributo del eje z
- El filtro de seguridad asignado a un usuario

La pestaña Vistas Active Views permite:

- [Volver a configurar la vista Active Views](#)
- [Añadir eventos a una incidencia](#)
- [Cerrar una ventana de la instantánea o del navegador visual](#)
- [Crear una incidencia](#)
- [Opciones de menú personalizadas con eventos](#)
- [Suprimir una ventana de la instantánea o del navegador visual](#)
- [Consulta de eventos](#)
- [Asignador de gráficos](#)
- [Visualizar datos del asesor](#)
- [Gestionar las columnas](#)
- [Enviar mensajes acerca de eventos e incidencias por correo electrónico](#)
- [Mostrar u ocultar información de los eventos](#)
- [Instantánea de una ventana del navegador visual](#)
- [Ver eventos que han activado un evento correlacionado](#)
- [Ver la visualización de vulnerabilidades](#)
- [Ver datos del activo](#)
- [Realizar una operación de HP: operaciones de OpenView y Service Desk](#)
- [Realizar operaciones de Remedy](#)

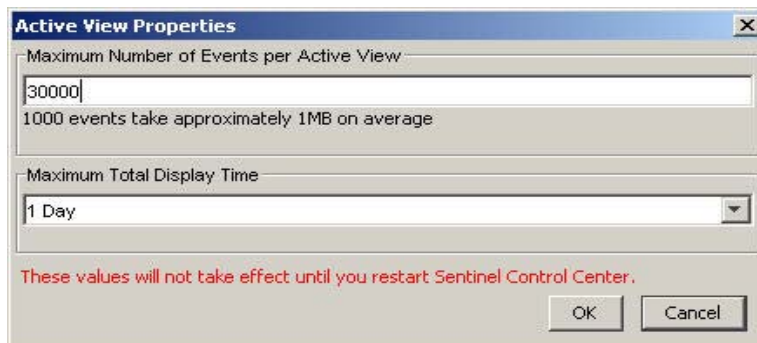
Como usuario, puede cambiar valores (nombres de columnas) para mostrar nombres lógicos e introducirlos en todo el sistema. Puede aplicar atributos al flujo de eventos que sean importantes para su empresa. Para obtener más información, consulte el *capítulo 10, Gestor de datos de Sentinel*, la *Guía del usuario del asistente de Sentinel* y la *Guía de referencia del usuario de Sentinel*.

Reconfiguración del valor en caché y del número máximo de eventos en la vista Active Views

Las propiedades de la vista Active Views permiten configurar el número máximo de eventos que pueden mostrarse en la vista Active Views y el tiempo en caché de cada cliente. El número máximo de eventos totales por defecto en una vista Active Views es de 30.000 eventos. El valor del tiempo en caché por defecto en una vista Active Views es de 24 horas.

Para volver a configurar el valor en caché y el número máximo de eventos en la vista Active Views

1. Haga clic en la pestaña *Vistas Active Views*.
2. Haga clic en *Vistas Active Views > Propiedades*.
3. Realice los cambios.



Los valores nuevos no surtirán efecto hasta que no reinicie el Centro de control de Sentinel.

Para ver eventos en tiempo real

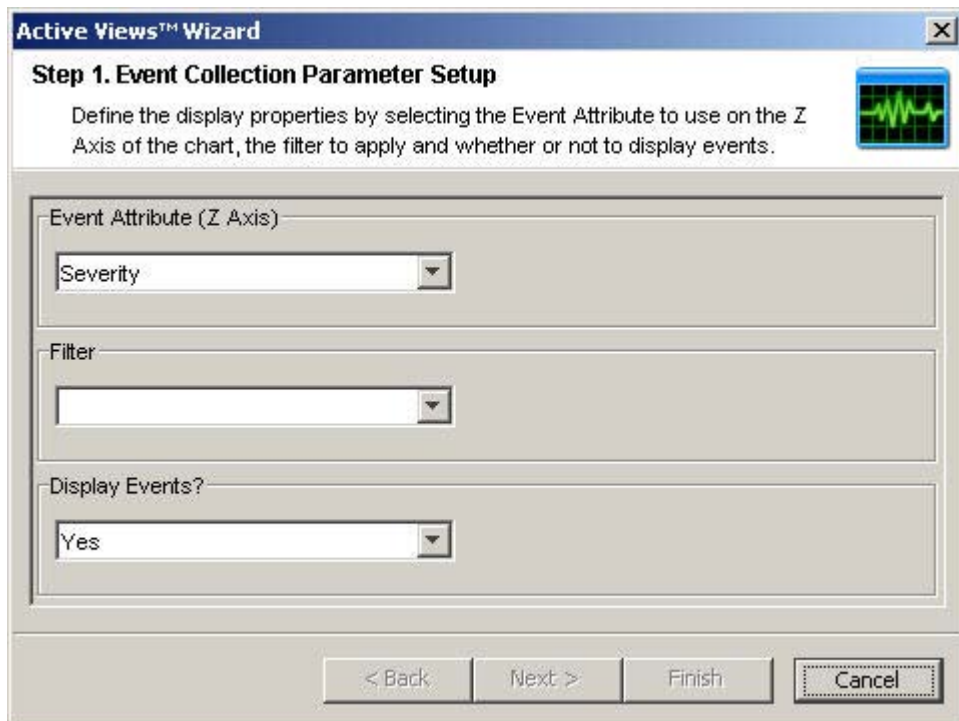
Para ver eventos en tiempo real

1. Haga clic en la pestaña *Vistas Active Views*.
2. Haga clic en *Vistas Active Views > Crear una vista Active Views* o haga clic en *Crear una vista Active Views*.



3. En la ventana del asistente de visualización de eventos, haga clic en las flechas hacia abajo para seleccionar el eje Z, filtrar y visualizar eventos (Sí o No).

NOTA: En la ventana de selección del filtro puede crear su propio filtro o seleccionar uno de los ya creados. Al seleccionar el filtro *Todos* aparecerán todos los eventos en la ventana. Al crear una vista Active Views, si el filtro asignado a la vista Active Views se cambia o se suprime tras la creación de la vista Active Views, ésta no se ve alterada.



Tras realizar su selección, puede hacer clic en *Siguiente* o *Finalizar*. Si selecciona *Finalizar*, se seleccionarán los siguientes valores por defecto:

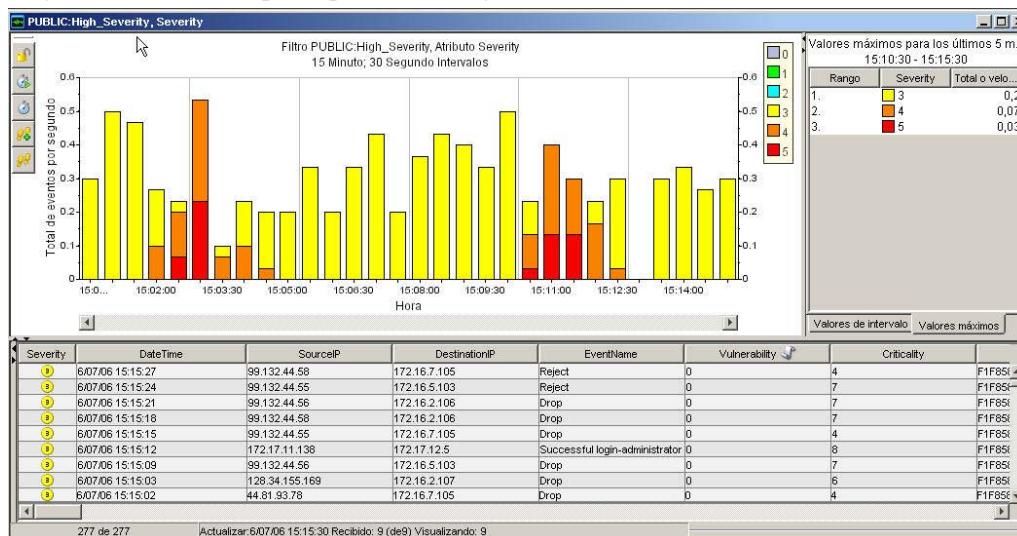
- Velocidad de actualización y visualización de 30 segundos
- Tiempo de visualización de 15 minutos
- Eje Y como total de eventos
- Tipo de diagrama: 2D de barras apiladas

4. Si hace clic en *Siguiente*, haga clic en las flechas hacia abajo para seleccionar:
 - Velocidad de actualización y visualización: número de segundos para que la frecuencia de eventos se actualice
 - Tiempo de visualización: cantidad de tiempo para visualizar el diagrama
 - Eje Y: total de eventos o total de eventos por segundo
 Haga clic en *Siguiente*.
5. Seleccione el tipo de diagrama. Haga clic en *Siguiente*.
 - Tipo de diagrama: diagrama de barras 3D, diagrama 2D apilado, diagramas de cintas o de líneas
6. Además de la selección del filtro, puede ajustar la tabla de eventos. Tiene las condiciones opcionales siguientes:
 - Ninguno
 - es exactamente
 - no es
 - es < (es inferior a)
 - es <= (es inferior o igual a)
 - es > (es superior a)
 - es >= (es superior o igual a)
 - contiene
 - no contiene
 - está vacío
 - no está vacío

Tras haber creado los criterios, haga clic en *Añadir a la lista*. Haga clic en *Finalizar*.

NOTA: Tras haber creado la vista, puede editar o eliminar este ajuste de la tabla de eventos, para ello, haga clic con el botón derecho en el área del diagrama y seleccione las propiedades. Para obtener más información, consulte [Para reajustar los parámetros, el tipo de diagrama o la tabla de eventos de una vista Active Views](#).

El gráfico tendrá un aspecto parecido al siguiente:



NOTA:Propiedades de la vista Active Views: ajustar la tabla de eventos no afectará la representación gráfica.

Los cinco botones de la izquierda del diagrama realizan las funciones siguientes:



- Bloquear o desbloquear el diagrama: se utiliza cuando se detalla, se acerca, se aleja, se acerca a la selección y se guarda un diagrama como archivo html.



- Aumentar el intervalo de visualización: aumenta el intervalo del tiempo de visualización durante eventos entrantes.



- Disminuir el intervalo de visualización: disminuye el intervalo del tiempo de visualización durante eventos entrantes



- Aumentar el tiempo de visualización: aumenta el intervalo de tiempo en el eje X.



- Disminuir el tiempo de visualización: disminuye el intervalo de tiempo en el eje X.

Al hacer clic en el botón *Bloquear*, los botones adicionales disponibles son:



- Bloquear o desbloquear el diagrama: se utiliza cuando se detalla, se acerca, se aleja, se acerca a la selección y se guarda un diagrama como archivo html.



- Acercar: se acerca sin cambiar la configuración del tiempo del diagrama.



- Alejar: se aleja sin cambiar la configuración del tiempo del diagrama.



- Acercar a la selección: se acerca a una selección de intervalos de tiempo de eventos.



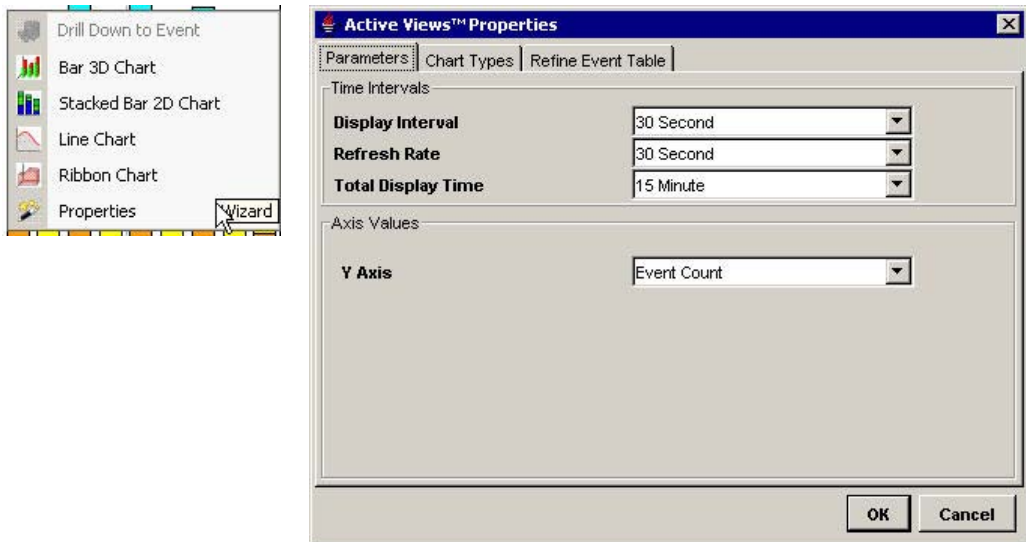
- Permite guardar la información del navegador como un archivo html con diagrama como imágenes y eventos en un formato tabular.

Para reajustar los parámetros, el tipo de diagrama o la tabla de eventos de una vista Active Views

Al visualizar una vista Active Views, puede reajustar los parámetros del diagrama, cambiar el tipo de diagrama y si hay eventos de interés, puede filtrar otros eventos en lugar de crear una vista Active Views nueva y un filtro.

Para reajustar los parámetros, el tipo de diagrama o la tabla de eventos de una vista Active Views

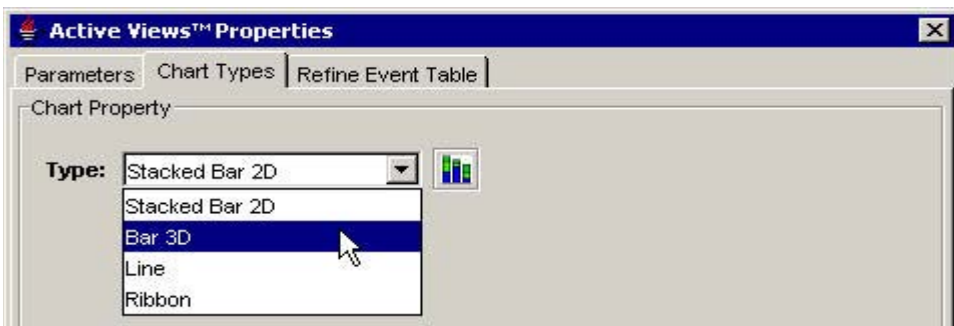
1. En una vista Active Views que muestre un diagrama, haga clic con el botón derecho y seleccione *Propiedades*.



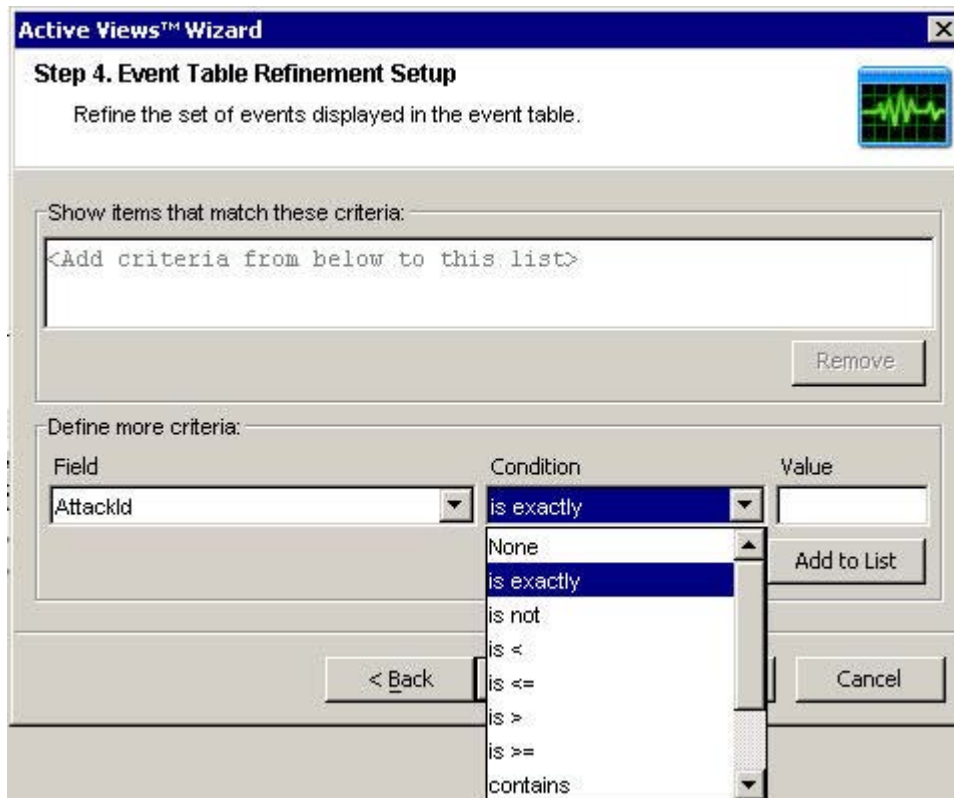
En la pestaña Parámetros, puede definir:

- Intervalo de visualización: tiempo entre cada intervalo.
- Velocidad de actualización: número de segundos para que la frecuencia de eventos se actualice.
- Tiempo total de visualización: cantidad de tiempo para visualizar el diagrama.
- Eje Y: total de eventos o total de eventos por segundo.

En la pestaña Tipos de diagramas, puede definir el diagrama como diagrama de barras 3D, diagrama 2D apilado, diagramas de cintas o de líneas.



En la pestaña Ajustar la tabla de eventos puede filtrar el campo de eventos en la vista Active Views.



Por ejemplo, puede filtrar eventos con una entrada específica en el campo, como DeviceAttackName es exactamente Back_Door_Probe (TCP 3128). Esto provocará una tabla de eventos con eventos que sólo contienen DeviceAttackName equivalente a Back_Door_Probe (TCP 3128).

206.158.21.6	192.168.10.25	TCP_back_door_probe
206.158.21.6	192.168.10.25	TCP_back_door_probe
f 564)		(DeviceAttackName is exactly Back_Door_Probe (TCP 3128))

Al ajustar una tabla de eventos, verá los criterios de filtro en la parte inferior derecha de la tabla de eventos.

Rotación de un diagrama de barras o de cintas 3D

Para rotar un diagrama de barras 3D o de cintas

1. Haga clic en cualquier parte del diagrama y mantenga pulsado el botón del ratón.
2. Cambie la posición del diagrama según sea necesario desplazando el ratón al mismo tiempo que mantiene el botón pulsado.

Cómo mostrar u ocultar la información de los eventos

Para mostrar la información de los eventos

1. En una tabla en tiempo real de eventos del navegador visual o de la instantánea, haga doble clic o haga clic con el botón derecho en un evento y, a continuación, en *Mostrar información*. La información de los eventos aparecerá en el panel izquierdo de la tabla en tiempo real de eventos.

The screenshot shows the Active Views interface. On the left, a context menu is open over a table of events, with 'Show Details' selected. The main area is divided into two panels. The left panel shows the properties of the selected event, and the right panel shows a list of events with their severity, date, and source IP.

Propiedad	Valor	Severity	DateTime	SourceIP
Base		3	6/07/06 18:45:29	
Severity	5	3	6/07/06 18:45:29	
DateTime	6/07/06 18:45:29	3	6/07/06 18:45:29	
DestinationIP	172.30.2.211	3	6/07/06 18:45:29	
EventName	EventInsertionFailed	3	6/07/06 18:45:29	
EventID	F65D67D9-EF2B-1028-927E-001372129DF8	3	6/07/06 18:45:29	
SourceID	05504CB6-EE77-1028-9449-001372129DF8	3	6/07/06 18:45:29	
WizardAgent	Internal	4	6/07/06 18:45:29	128.34.155.169
Resource	EventSubsystem	3	6/07/06 18:45:28	
SubResource	EventBulkLoader	3	6/07/06 18:45:28	
SensorName	DAS_Binary	3	6/07/06 18:45:28	
SensorType	I	3	6/07/06 18:45:28	
DestinationHostName	es2k3sp1	3	6/07/06 18:45:28	
ReporterName	es2k3sp1	3	6/07/06 18:45:28	
Message	Failed to insert 9 events to DB--Events were stored for later insertion. Check the log files and the database for more information. The error: java.lang.RuntimeException: Error saving events, cause java.sql.BatchUpdateException: Violation of PRIMARY KEY constraint	3	6/07/06 18:45:28	
		3	6/07/06 18:45:28	
		3	6/07/06 18:45:27	
		3	6/07/06 18:45:27	
		3	6/07/06 18:45:27	
		3	6/07/06 18:45:27	
		3	6/07/06 18:45:27	
		3	6/07/06 18:45:27	
		3	6/07/06 18:45:27	
		3	6/07/06 18:45:27	
		3	6/07/06 18:45:27	

2929 de 4123 Actualizar: 6/07/06 18:45:30 Recibido: 156 (de 156) Visualizando: 156

2. Si desea que la información aparezca la próxima vez que abra el Centro de control de Sentinel, haga clic en *Archivo > Guardar preferencias* o haga clic en *Guardar las preferencias del usuario*.



Para ocultar información de un evento

1. En una tabla en tiempo real de eventos del navegador visual o de la instantánea, con información de eventos en el panel izquierdo, haga clic con el botón derecho en un evento y, a continuación, en *Mostrar información*. La ventana de la información de los eventos se cerrará.
2. Si no desea que la información aparezca la próxima vez que abra el Centro de control de Sentinel, haga clic en *Archivo > Guardar preferencias* o haga clic en *Guardar las preferencias del usuario*.



Envío de mensajes acerca de eventos e incidencias por correo electrónico

La posibilidad de enviar mensajes de correo electrónico se define en el archivo `execution.properties` durante la instalación. Este archivo se puede editar después de la instalación y se encuentra en la ubicación siguiente:

En Windows:

```
%ESEC_HOME%\sentinel\config
```

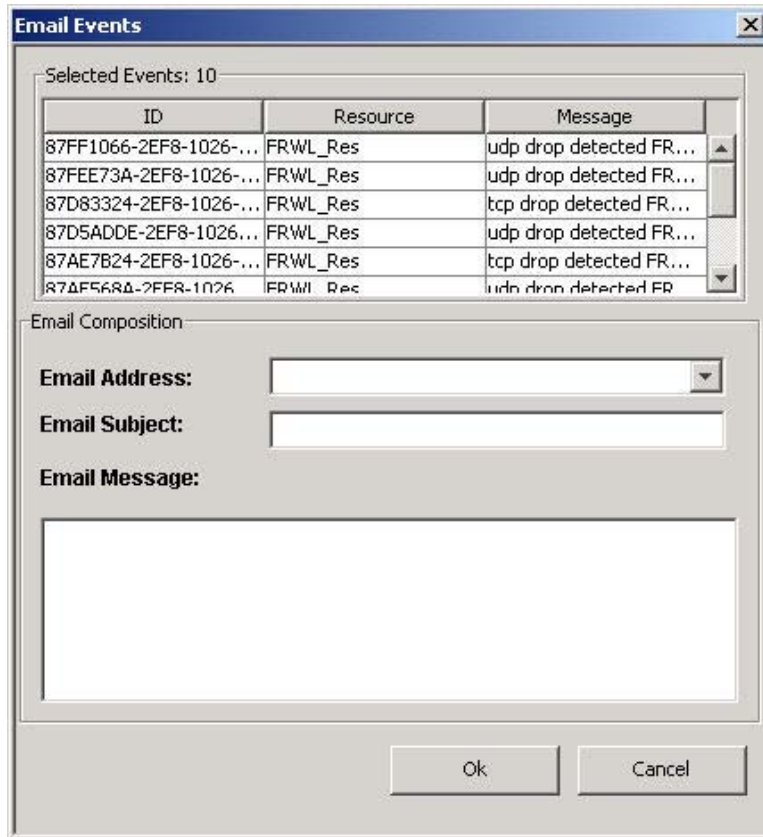
En UNIX:

```
$(ESEC_HOME)/sentinel/config
```

Para obtener más información, vaya al capítulo 11, *Utilidades, Configuración del correo electrónico de Sentinel*.


Para enviar un mensaje de evento por correo electrónico

1. En una tabla en tiempo real de eventos del navegador visual o de la instantánea, seleccione un evento o un grupo de eventos, haga clic con el botón derecho y seleccione *Correo electrónico*.



2. Complete la información siguiente:
 - Dirección de correo electrónico
 - Tema del correo electrónico
 - Mensaje de correo electrónico
3. Haga clic en *Aceptar*.

Para enviar un mensaje de incidencia por correo electrónico

1. Tras guardar la incidencia, haga clic en la pestaña Incidencias, *Incidencias > Visualizar el gestor de vistas de incidencias*.
2. Haga doble clic en *Todas las incidencias*.
3. Haga doble clic en una incidencia.
4. Haga clic en *Incidencia del correo electrónico* .
5. Introduzca:
 - Dirección de correo electrónico
 - Tema del correo electrónico
 - Mensaje de correo electrónico
6. Haga clic en *Aceptar*. El mensaje de correo electrónico tendrá adjuntos html que tratan la información de incidencias, eventos, activos, vulnerabilidades, la información del asesor y el historial de incidencias.

Creación de una incidencia

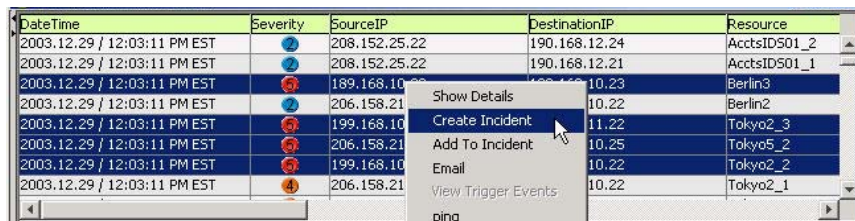
Para llevar a cabo esta función debe tener el permiso de usuario para crear incidencias.

Ésta resulta útil para agrupar una serie de eventos que en conjunto representen algo de interés (grupo de eventos similares o conjunto de eventos diferentes que indiquen un patrón de interés como un ataque).

NOTA: Si los eventos no se visualizan inicialmente en una incidencia recién creada, es muy probable que se deba a una demora en el tiempo entre la visualización en la ventana Eventos en tiempo real y la inserción en la base de datos. Si esto sucede, es posible que los eventos originales tarden unos minutos en insertarse finalmente en la base de datos y en visualizarse en la incidencia.

Para crear una incidencia

1. En una tabla en tiempo real de eventos del navegador visual o de eventos de la instantánea, seleccione un evento o un grupo de eventos, haga clic con el botón derecho y seleccione *Crear incidencia*.



DateTime	Severity	SourceIP	DestinationIP	Resource
2003.12.29 / 12:03:11 PM EST	2	208.152.25.22	190.168.12.24	AcctsID501_2
2003.12.29 / 12:03:11 PM EST	2	208.152.25.22	190.168.12.21	AcctsID501_1
2003.12.29 / 12:03:11 PM EST	2	189.168.10.22	10.22	Berlin3
2003.12.29 / 12:03:11 PM EST	2	206.158.21	10.22	Berlin2
2003.12.29 / 12:03:11 PM EST	2	199.168.10	11.22	Tokyo2_3
2003.12.29 / 12:03:11 PM EST	2	206.158.21	10.25	Tokyo5_2
2003.12.29 / 12:03:11 PM EST	2	199.168.10	10.22	Tokyo2_2
2003.12.29 / 12:03:11 PM EST	2	206.158.21	10.22	Tokyo2_1

En la ventana Nueva incidencia, dispone de las siguientes pestañas:

- Eventos: muestra los eventos que forman la incidencia.
- Activos: muestra los activos afectados.
- Vulnerabilidad: muestra las vulnerabilidades relacionadas con los activos.
- Asesor: ataque de activos e información de alertas.
- Flujo de trabajo: en esta pestaña, puede asignar un flujo de trabajo (iTrac).
- Historial: historial de incidencias.
- Adjuntos: puede adjuntar cualquier documento o archivo de texto con información relacionada con esta incidencia.

En el recuadro de diálogo Crear incidencia, introduzca:

- Título
 - Estado
 - Gravedad
 - Prioridad
 - Categoría
 - Responsable: la cuenta de usuario asignada al caso.
 - Descripción
 - Resolución
2. Haga clic en *Guardar*. La incidencia se añade a la pestaña Incidencias del Centro de control de Sentinel.

Visualización de eventos que han activado un evento correlacionado

Debe hacer clic con el botón derecho en un evento correlacionado para ver los eventos que han activado el evento correlacionado. En la tabla de eventos en la que está seleccionando el evento, busque en la parte derecha del panel de visualización de resumen un evento que tenga una propiedad de tipo de sensor con un valor C (C: evento correlacionado) o W (W: lista de vigilancia).

Para ver eventos que han activado un evento correlacionado

1. En una tabla en tiempo real de eventos del navegador visual o de la instantánea, o en una tabla de consulta de eventos, haga clic con el botón derecho en un evento correlacionado y seleccione Ver los eventos activadores. Se abre una ventana que muestra los eventos que han activado la regla y el nombre de la regla de correlación.



Investigación de un evento o eventos

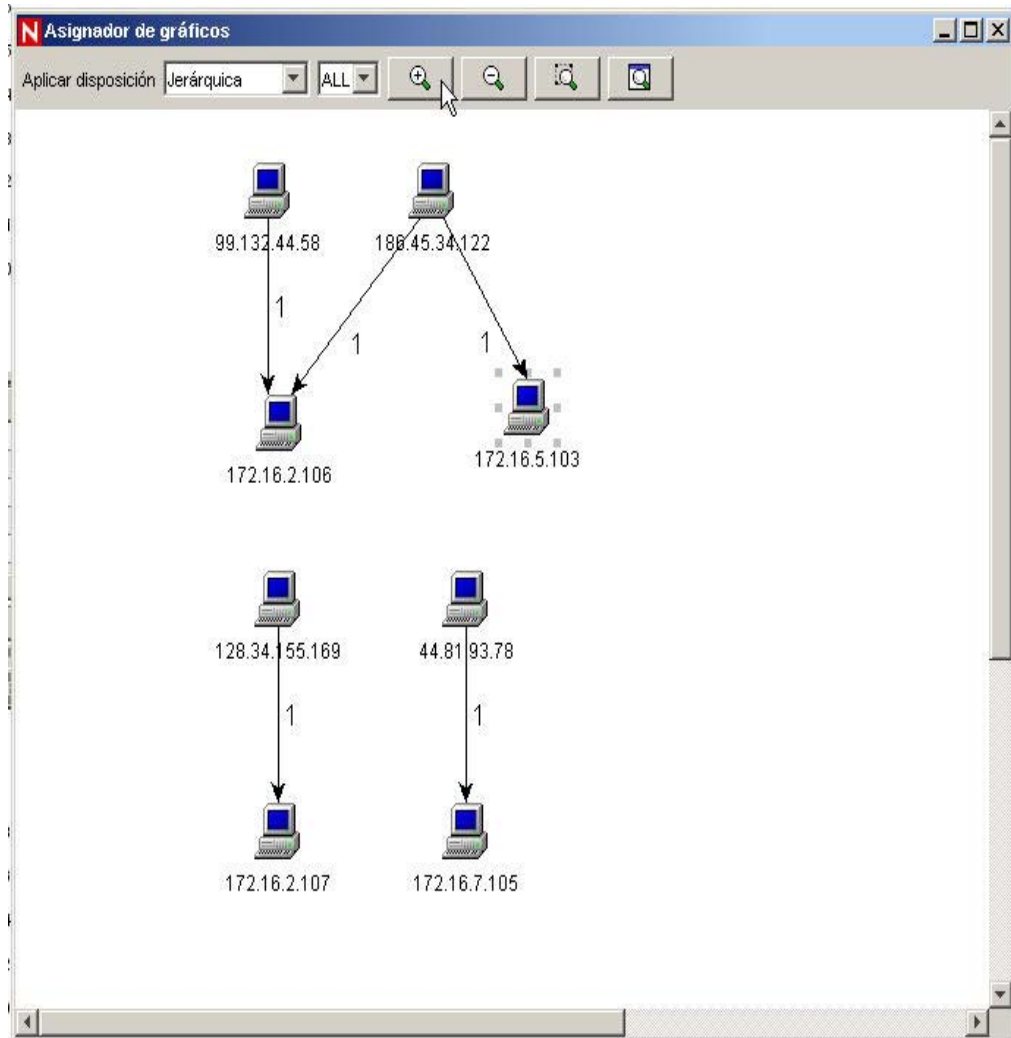
Esta función permite:

- Visualizar gráficamente los campos de origen (IP, puerto, evento, tipo de sensor, nombre del recopilador, etc.) asignados a los campos de destino (IP, puerto, evento, tipo de sensor, nombre del recopilador, etc.) de los eventos seleccionados.
- Realizar una consulta de eventos de la última hora en un único evento para obtener la información siguiente:

NOTA: No es posible realizar una consulta en un campo nulo (vacío).

- Direcciones IP de destino
- Direcciones IP de origen
- Nombre del evento

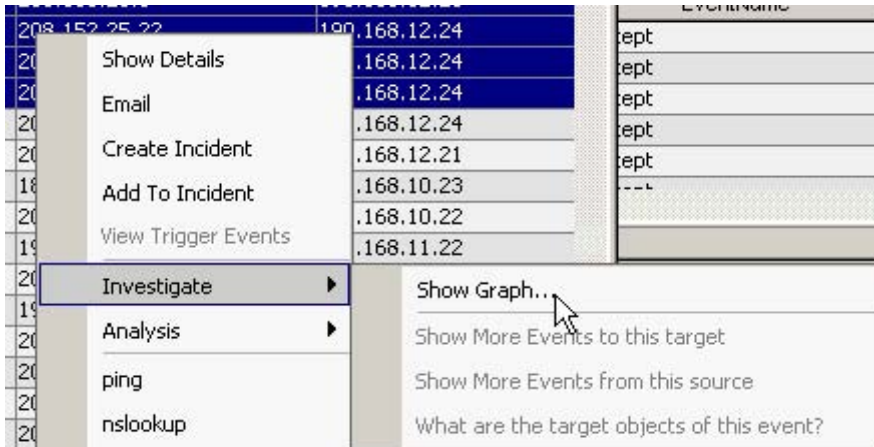
A continuación, se muestra una ilustración de direcciones IP de origen a direcciones IP de destino.



Investigar: Asignador de gráficos

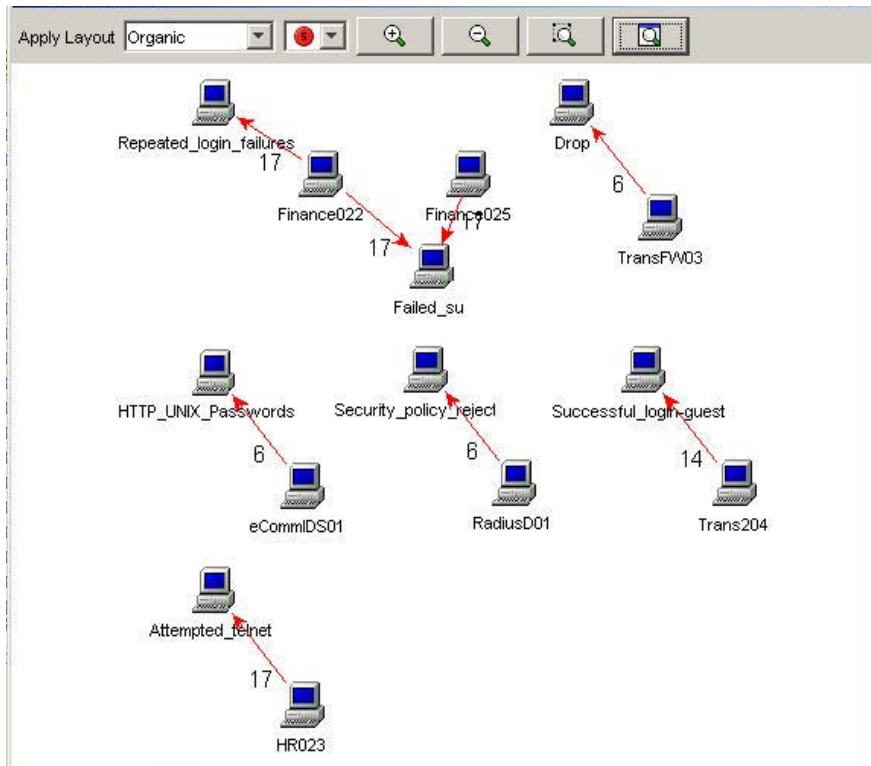
Para crear un asignador de gráficos

1. En una tabla en tiempo real de eventos de la ventana del navegador visual o de la instantánea, haga clic con el botón derecho en un *evento o eventos* > *Investigar* > *Visual* > *Mostrar el gráfico*.



A continuación, se muestra una descripción gráfica del nombre del sensor al nombre del evento de gravedad 5 en un formato orgánico. Puede visualizar una asignación gráfica en los siguientes formatos:

- Circular
- Jerárquica
- Orgánica
- Ortogonal



Investigar: Consulta de eventos

Esta función permite consultar los eventos de la última hora.

Para realizar una consulta de eventos utilizando la función Investigar

1. En la ventana del navegador visual o de la instantánea, *haga clic con el botón derecho en un evento > Investigar > <seleccione una de las tres opciones siguientes>*

Opción	Función
Mostrar más eventos en este destino	Dirección IP de destino
Mostrar más eventos en este origen	Dirección IP de origen
¿Cuáles son los objetos de destino de este evento?	Nombre del evento

Análisis: Visualización de los datos del asesor

El asesor ofrece referencias cruzadas entre las firmas IDS en tiempo real de los atacantes y la base de datos de vulnerabilidades con la que cuenta. Los datos del asesor disponen de datos de alerta y de ataque. Los datos de alerta contienen información acerca de vulnerabilidades y virus. Los datos de ataque enumeran las explotaciones asociadas a vulnerabilidades.

Los sistemas de detección de intrusos admitidos son:

- Cisco Secure IDS
- Enterasys Dragon Host Sensor
- Enterasys Dragon Network Sensor
- ISS BlackICE PC Protection
- ISS RealSecure Desktop
- ISS RealSecure Network
- ISS RealSecure Server Sensor
- ISS RealSecure Guard
- Snort/Sourcefire
- Symantec ManHunt
- Symantec Intruder Alert
- McAfee IntruShield

El recopilador IDS rellena el campo DeviceAttackName (rt1) de un evento. El asesor utiliza esta información para generar información de ataques y vulnerabilidades. A continuación, se muestran algunos ejemplos de vulnerabilidades:

- FINGER:Cfinger Search Probe
- SMTP:SmartServer3 MAIL FROM Buffer Overflow
- HTTP:Dragon Fire IDS Web Interface Remote Execution
- FTP:MKDIR-DOS
- hp-printer-flood
- wh00t-backdoor
- nt-telnet
- FINGER / execution attempt
- tellurian-tftpdnt-filename-bo
- FTP MKD Stack Overflow

Para visualizar los datos del asesor

1. En una tabla en tiempo real de eventos del navegador visual o de la instantánea, *haga clic con el botón derecho en un evento o en una serie de eventos seleccionados > Análisis > Datos del asesor*. Si el campo DeviceAttackName está relleno adecuadamente, aparecerá un informe similar al que se muestra a continuación. Este ejemplo es para WEB-MISC amazon 1-click cookie theft.

Advisor Summary

Attack	Attack ID	Alert IDs
WEB-MISC amazon 1-click cookie theft	9991272	1087, 1194, 8835, 9010
WEB-MISC amazon 1-click cookie theft	9992801	1194, 8835, 9010

Advisor Report

Microsoft Excel XLM Arbitrary Macro Execution (id 9991272) [top](#)

3 **4**
Urgency Severity

Microsoft Excel contains a flaw that may allow a malicious user to run a macro without warning the user. The issue is triggered when a malicious user creates an Excel macro command, and embeds commands in a spreadsheet that launch the macro without asking the user for permission. If a malicious user can persuade the user to launch the file containing embedded macros, it may result in a loss of integrity and/or availability of data.

Scenario:

Impact:
Loss of Integrity

Safeguards:

Análisis: Visualización de datos del activo

Esta función permite visualizar y guardar la vista como un archivo HTML del informe de activos. Debe ejecutar el recopilador de gestión de activos para ver los datos. Los datos disponibles para su visualización son:

Hardware

- Dirección MAC
- Nombre
- Tipo
- Proveedor
- Producto
- Versión
- Valor
- Importancia
- Sensibilidad
- Entorno
- Ubicación

Red

- Dirección IP
- Nombre del host

Software

- Nombre
- Tipo
- Proveedor
- Producto
- Versión

Contactos

- Orden
- Nombre
- Función
- Correo electrónico
- Número de teléfono

Ubicación

- Sala
- Bastidor
- Dirección

Para ver los datos del activo

1. En una tabla en tiempo real de eventos de la ventana del navegador visual o de la instantánea, haga clic con el botón derecho en un evento o eventos > *Análisis* > *Datos del activo*. Aparecerá una ventana similar a la que aparece a continuación.

Asset Report

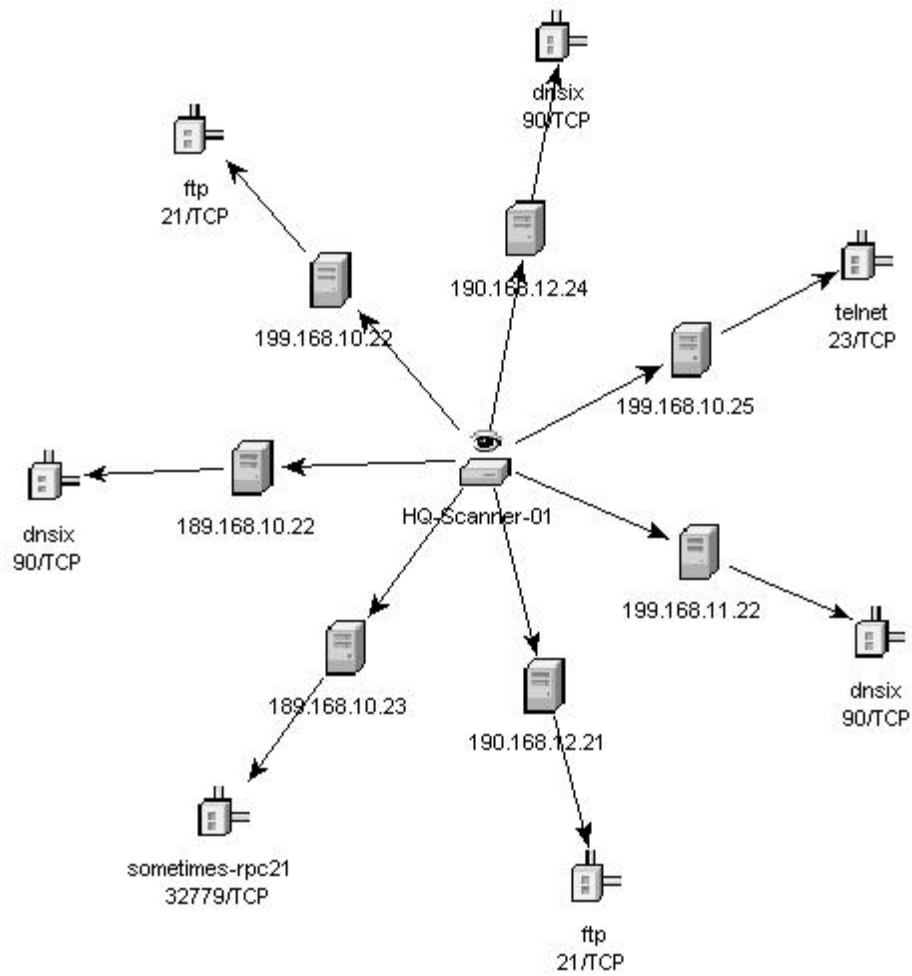
desk.acmeinc.net					
Hardware	MAC Address	A0:12:56:78:90:00			
	Name	Build Machine	Value	500	
	Type	Server	Criticality	High	
	Vendor	Dell	Sensitivity	Low	
	Product	Precision	Environment	Production	
	Version	360	Location	Internal	
	Network	IP	Hostname		
199.16.2.23		desk.acmeinc.net			
Software	Name	Type	Vendor	Product	Version
	ClearCase	APPLICATION	IBM	ClearCase	5.0
	C++	APPLICATION	Microsoft	Visual C++	6.0
Contacts	Order	Name	Role	Email	Phone Number
	1	Erickson, Stein	USER	serickson@acmedomain.net	(703) 555-8865
	2	IT	Administrator	LAN_FOLKS@acmedomain.net	(703) 555-9876
Location	Room	server room			
	Rack	#17			
	Address	HQ			
		Agent 86 Security Circle Suite 86 Washington DC 12345 USA			

Análisis: Visualización de vulnerabilidades

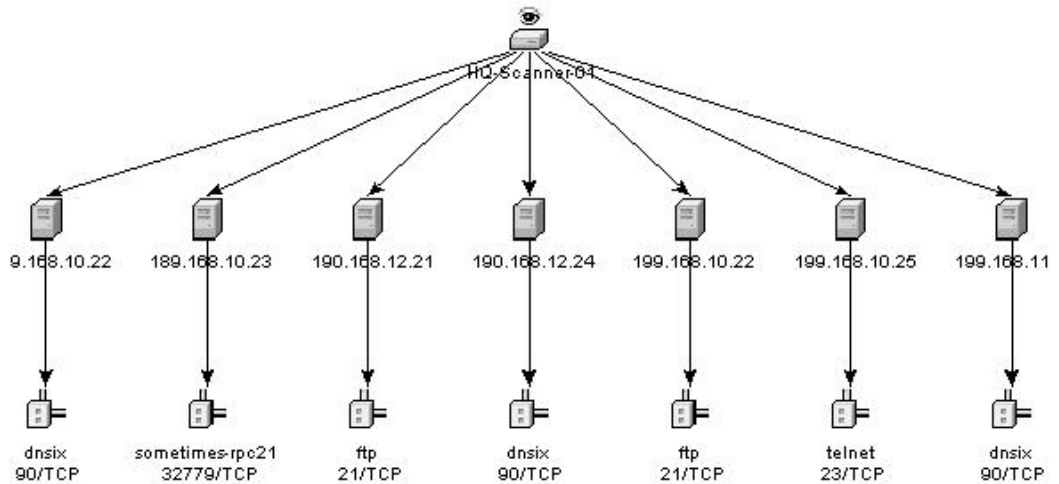
Novell tiene recopiladores disponibles que procesan las exploraciones de vulnerabilidades desde exploraciones Nessus, ISS, Foundstone, eEye y Qualys. La visualización de vulnerabilidades ofrece una representación gráfica de datos de eventos en tiempo real frente a sistemas vulnerables y está disponible en un evento para la vulnerabilidad actual y de tiempo de evento.

La función recupera y muestra datos de vulnerabilidad para las IP de destino de los eventos seleccionados. Para obtener más información, consulte la documentación del pdf del recopilador que se encuentra en %ESEC_HOME%\wizard\elements\

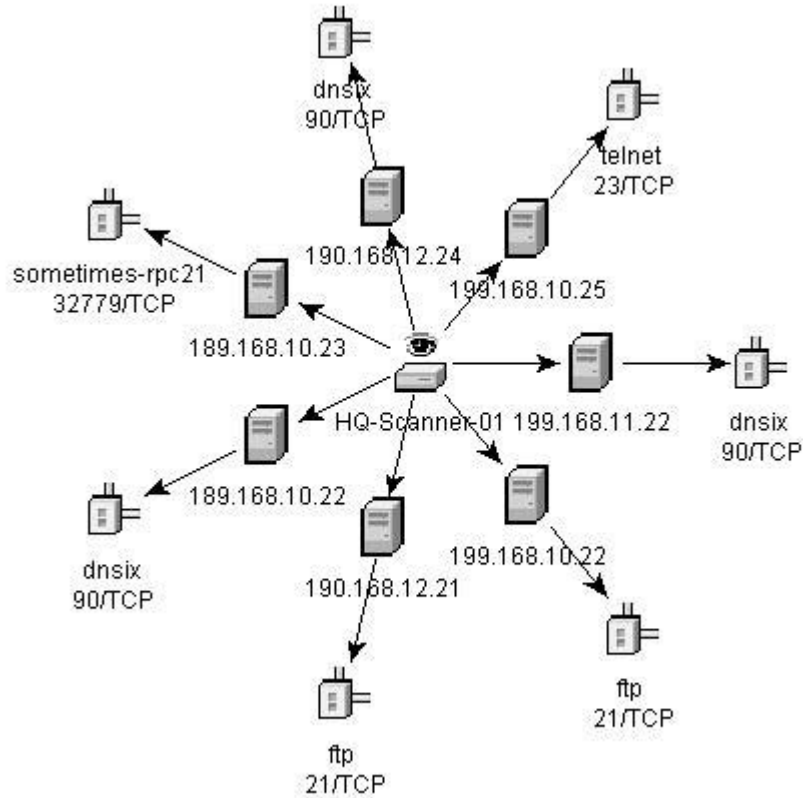
NOTA: El recopilador de vulnerabilidades es un recopilador de información, no un recopilador de eventos.



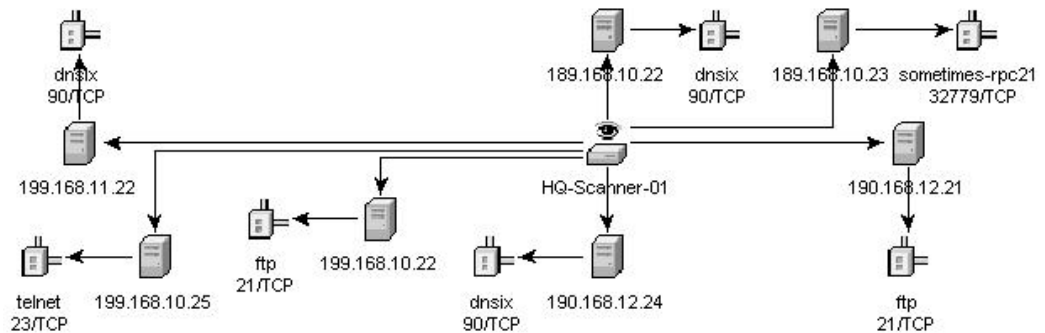
Orgánica



Jerárquica



Circular



Ortogonal

En la visualización gráfica hay cuatro paneles. Son los siguientes:

- panel gráfico
- panel de árbol
- panel de control
- panel de información/eventos

La visualización del panel gráfico asocia vulnerabilidades a una combinación de puertos/protocolos de un recurso (dirección IP). Por ejemplo, si un recurso tiene cinco combinaciones únicas de puertos/protocolos que son vulnerables, habrá cinco nodos adjuntos a ese recurso. Los recursos se agrupan conjuntamente en el explorador que ha explorado los recursos y ha generado informes de las vulnerabilidades. Si se han utilizado dos exploradores diferentes (ISS y Nessus), habrá dos nodos de explorador independientes que tendrán vulnerabilidades asociadas.

NOTA: La asignación de eventos sólo se produce entre los eventos seleccionados y los datos de vulnerabilidad devueltos.

El panel de árbol organiza los datos en la misma jerarquía que el gráfico. Además, permite a los usuarios ocultar o mostrar nodos en cualquier nivel de la jerarquía.

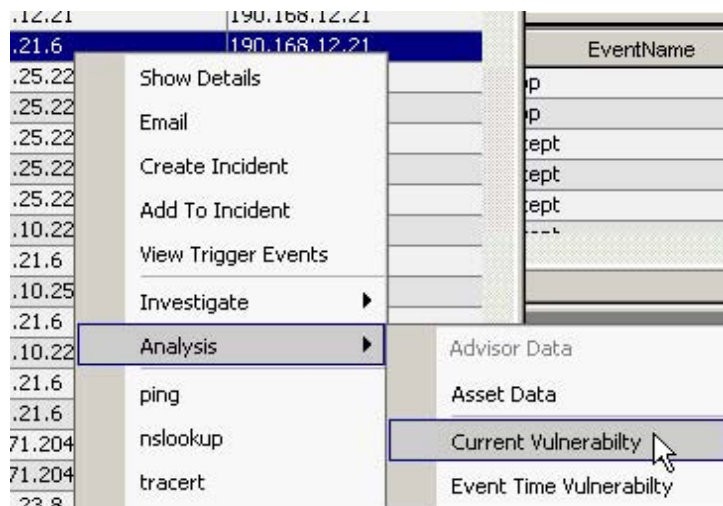
El panel de control expone todas las funciones disponibles en la visualización, entre las que se incluyen:

- cuatro algoritmos diferentes para visualizar
- capacidad para mostrar todos los nodos o los seleccionados que tengan eventos asignados
- acercarse y alejarse de las áreas seleccionadas del gráfico

En el panel Información/Eventos, hay dos pestañas. En la pestaña Información, si se hace clic en un nodo se visualizará la información del nodo. En la pestaña Eventos, si se hace clic en un evento asociado a un nodo, el nodo se visualizará en un formato tabular como en la ventana Tiempo real o Consulta de eventos.

Para ejecutar una visualización de vulnerabilidades

1. En una tabla en tiempo real de eventos del navegador visual o de la instantánea, haga clic con el botón derecho en un evento o en una serie de eventos seleccionados y haga clic en:
 - Análisis
 - Vulnerabilidad actual: consulta a la base de datos las vulnerabilidades que están activas (vigentes) en la fecha y hora actuales.
 - Vulnerabilidad de hora del evento: consulta a la base de datos las vulnerabilidades que estaban activas (efectivas) en la fecha y hora del evento seleccionado.



2. En la parte inferior de la ventana de resultados de vulnerabilidad, haga clic en una de las opciones siguientes:
 - Evento en gráfico de vulnerabilidad
 - Informe de vulnerabilidades
3. (En Evento en gráfico de vulnerabilidad) En la visualización, puede:
 - Desplazar nodos y sus etiquetas.
 - Utilizar uno de los cuatro algoritmos de disposición diferentes para visualizar el gráfico.
 - Mostrar todos los nodos o sólo los que tienen eventos asignados.
 - Filtrar árboles en línea en caso de que un gran número de recursos sean vulnerables.
 - Acercarse y alejarse de las áreas seleccionadas.

Integración con otros fabricantes

La integración con otros fabricantes permite enviar eventos desde cualquier pantalla de visualización incluidos incidencias y objetos asociados a:

- HP Service Desk
- Remedy

Para enviar un evento o varios eventos para software de otros fabricantes

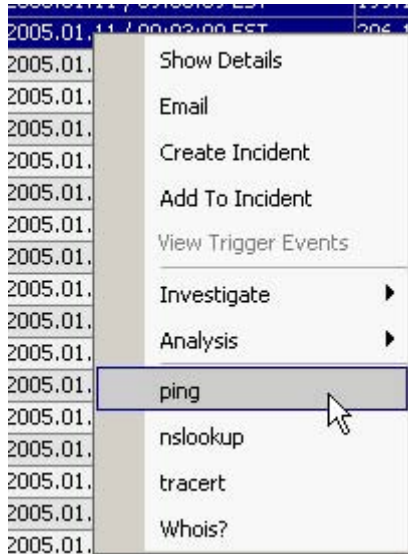
1. En una tabla en tiempo real de eventos de la ventana del navegador visual o de la instantánea, en función del software de otros fabricantes que se haya instalado, haga clic con el botón derecho en un evento y haga clic en Enviar evento a:
 - HP Service Desk
 - Remedy

Uso de las opciones de menú personalizadas con eventos

Para utilizar una opción de menú personalizada con un evento

1. En una tabla en tiempo real de eventos existente del navegador visual o de la instantánea, seleccione un evento o un grupo de eventos, haga clic con el botón derecho y haga clic en una opción. Se abrirá un recuadro de diálogo con la información con la que la opción de menú se ha configurado o le permitirá completar la información necesaria para realizar una acción. Las opciones de menú personalizadas por defecto son las siguientes:
 - ping
 - nslookup
 - traceroute
 - Whois?

Puede asignar un permiso de usuario para visualizar la vulnerabilidad y realizar operaciones de HP. Puede añadir opciones mediante la ventana Configuración del menú que está disponible en la pestaña Admin.



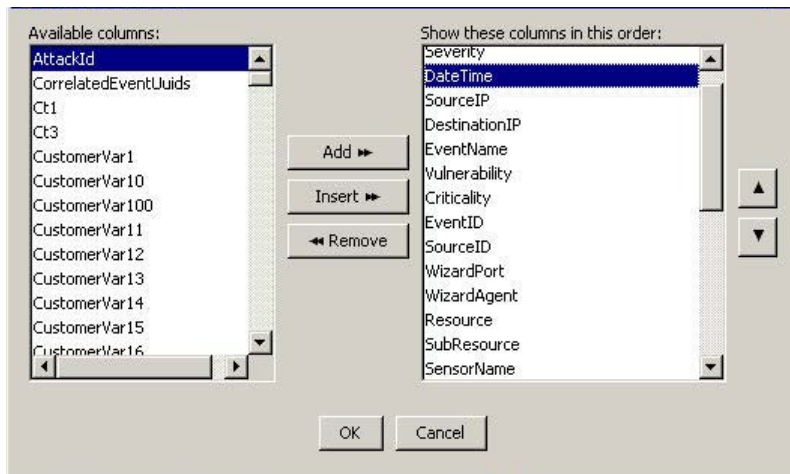
Gestión de las columnas en una ventana de la instantánea o del navegador visual

Para seleccionar y organizar columnas en una instantánea o en un navegador visual

1. Con una ventana de la instantánea o del navegador visual abierta, haga clic en *Vistas Active Views > Tiempo real del evento > Gestionar las columnas de la tabla en tiempo real de eventos.*



2. Utilice los botones *Añadir* y *Eliminar* para desplazar los títulos de la columna entre la lista *Columnas disponibles* y la lista *Mostrar columnas* en este orden. El botón *Insertar* puede utilizarse para colocar un elemento de la columna disponible en una ubicación específica. Por ejemplo, en la ilustración siguiente al hacer clic en *Insertar* se colocará un *AttackId* antes de *DateTime*.



Utilice los botones de flecha hacia arriba y hacia abajo para organizar el orden de las columnas como desee que se visualicen en la tabla en tiempo real de eventos. El orden descendente de los títulos de la columna del recuadro de diálogo Gestionar las columnas determina el orden de izquierda a derecha de las columnas de la tabla en tiempo real de eventos.

3. En el recuadro de diálogo Gestionar las columnas, haga clic en *Aceptar*.
4. Si desea visualizar las columnas la próxima vez que abra el Centro de control de Sentinel, haga clic en *Archivo > Guardar preferencias* o haga clic en el botón *Guardar las preferencias del usuario*.



Toma de una instantánea de una ventana del navegador visual

Para llevar a cabo esta función debe tener el permiso de usuario de instantánea.

Ésta resulta de gran utilidad para estudiar eventos de interés, ya que el navegador visual se actualiza automáticamente y la alerta o las alertas de interés pueden desplazarse fuera de la pantalla. Además, con una instantánea, puede ordenar por columna.

Para tomar una instantánea de una tabla en tiempo real de eventos

1. Con una ventana del navegador visual abierta, haga clic en *Vistas Active Views > Tiempo real del evento > Instantánea* o haga clic en *Tabla en tiempo real de eventos de la instantánea* de la barra de menús.



Se abrirá una ventana de la instantánea y se añadirá a la lista de carpetas Instantánea bajo las vistas de eventos del navegador. La visualización gráfica no formará parte de la instantánea.

Orden de columnas en una instantánea

Para ordenar columnas en una instantánea

1. Haga clic en cualquier encabezado de columna para ordenar de forma ascendente y doble clic para ordenar de forma descendente.

Cierre de una instantánea o del navegador visual

Para cerrar una instantánea o una tabla en tiempo real de eventos

1. Con una ventana de la instantánea o del navegador visual abierta, si desea que la tabla esté disponible la próxima vez que inicie el Centro de control de Sentinel, haga clic en *Archivo > Guardar preferencias*.
2. Cierre la tabla utilizando el botón Cerrar (esquina superior derecha en Windows o esquina superior izquierda en UNIX).

Supresión de una instantánea o del navegador visual

Para suprimir una ventana de la instantánea o del navegador visual

1. Si tiene una ventana de la instantánea o del navegador visual abierta, ciérrela mediante el botón Cerrar (esquina superior derecha en Windows o esquina superior izquierda en UNIX).
2. Haga clic en *Archivo > Guardar preferencias* o haga clic en *Guardar las preferencias del usuario*.



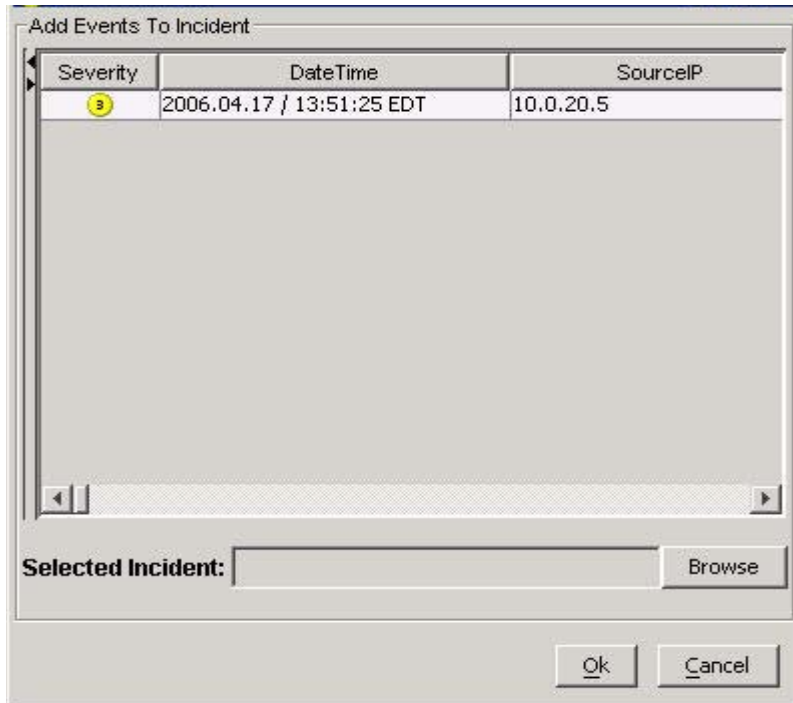
La vista o instantánea no volverá a visualizarse cuando cierre y vuelva a abrir el Centro de control de Sentinel.

Adición de eventos a una incidencia

Para realizar esta función debe tener permisos de usuario para modificar incidencias y asignar incidencias.

Para añadir eventos a una incidencia

1. En una tabla en tiempo real de eventos o en una instantánea, seleccione un evento o un grupo de eventos, haga clic con el botón derecho para visualizarla y haga clic en *Añadir a la incidencia*.
2. En el recuadro de diálogo *Añadir a la incidencia*, haga clic en Examinar.



- Haga clic en *Examinar* para enumerar las incidencias disponibles.

NOTA: Puede definir los criterios para buscar mejor una incidencia particular o incidencias.

- Haga clic en *Buscar* para visualizar una lista de las incidencias.

Severity	DateCreated	Priority	Criticality Ra...	Severity Rat...
Medium	04/17/2006 ...	None	0.0	0.0
Medium	04/17/2006 ...	None	0.0	0.0

Search Add Cancel

Show items that match these criteria:

<Add criteria from below to this list>

Remove

Define more criteria:

Relations: None

Field	Condition	Value
None	None	

Add to List

- Resalte una incidencia y haga clic en *Añadir*.
- Haga clic en *Aceptar*. Los eventos seleccionados se añadirán a la incidencia en el navegador de incidencias.

NOTA: Si los eventos no se visualizan inicialmente en una incidencia recién creada, es muy probable que se deba a una demora en el tiempo entre la visualización en la ventana Eventos en tiempo real y la inserción en la base de datos. Si esto sucede, es posible que los eventos originales tarden unos minutos en insertarse finalmente en la base de datos y visualizarse en la incidencia.

4

Pestaña Incidencias

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

Para utilizar la pestaña Incidencias debe tener los permisos adecuados. Si no se asigna este permiso, no estará disponible ninguno de los demás permisos relacionados con las acciones de esta pestaña.

En este capítulo se tratan las incidencias. Las incidencias son grupos de uno o más eventos de interés.

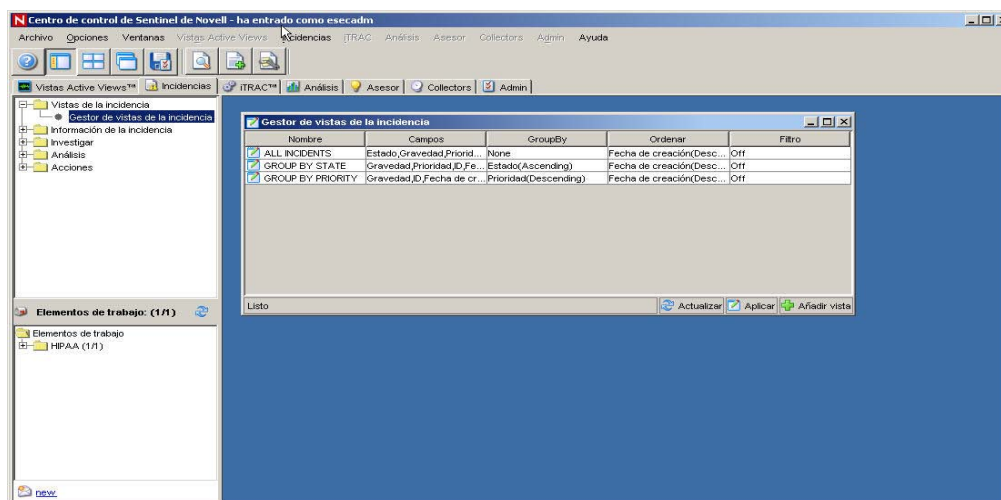
Las incidencias pueden crearse en:

- Ventana Tiempo real, los eventos pueden seleccionarse individualmente para crear una nueva incidencia o añadirse a una incidencia existente.
- Las incidencias también pueden crearse automáticamente mediante reglas de correlación activadas.

Pestaña Incidencias: Descripción

Las incidencias permiten:

- [Enviar una incidencia por correo electrónico](#)
- [Modificar una incidencia](#)
- [Visualizar una incidencia](#)
- [Suprimir una incidencia](#)
- [Añadir una vista de incidencias](#)



Relación entre eventos e incidencias

Un evento es una acción o un acontecimiento detectado por un dispositivo de seguridad o programa. Los eventos se consideran “sin estado”.

Una incidencia es el grupo de uno o más eventos que son considerados importantes (un posible ataque). Las incidencias tienen “estados” en los que se requiere una respuesta y un cierre.

Visualización de una incidencia

Debe disponer del permiso de usuario para ver incidencias.

Para visualizar una incidencia

1. Haga clic en la pestaña *Incidencias*.
2. Haga clic en *Incidencias > Visualizar el gestor de vistas de incidencias* o haga clic



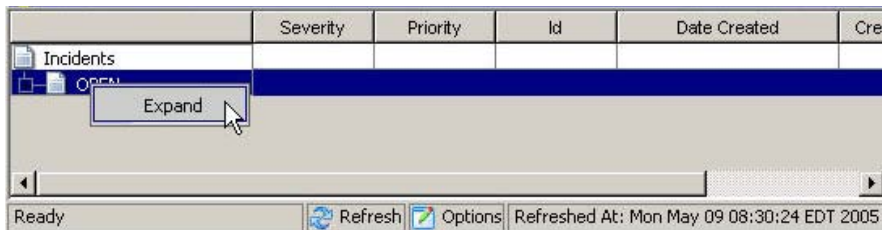
en el *Gestor de vistas de la incidencia*.

3. En la ventana Gestor de vistas de la incidencia, puede seleccionar las vistas siguientes:

- Todas las incidencias
- Agrupar por estado
- Agrupar por prioridad

Haga doble clic en el nombre de una vista.

4. Haga clic con el botón derecho > *Expandir para ver las incidencias*.



Para definir una opción de vista de incidencia

1. Haga clic en la pestaña *Incidencias*.
2. Haga clic en *Incidencias > Visualizar el gestor de vistas de incidencias* o haga clic en



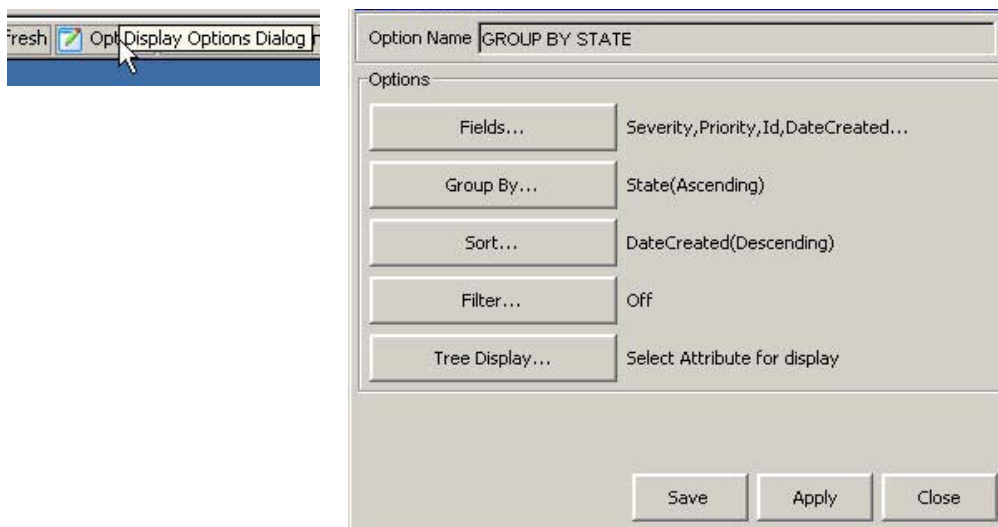
Visualizar el gestor de vistas de incidencia.

3. En la ventana Gestor de vistas de la incidencia, haga doble clic en el nombre de una vista.

Name	Fields	GroupBy	Sort	Filter
ALL INCIDENTS	State,Severity,Priority,Id	None	DateCreated(Descending)	Off
GROUP BY STATE	Severity,Priority,Id,DateCr...	State(Ascending)	DateCreated(Descending)	Off
GROUP BY PRIORITY	Severity,Id,DateCreated,C...	State(Ascending),Priority(D...	DateCreated(Descending)	Off

Refresh Apply Add View

4. Haga clic en *Opciones*.



En esta ventana también puede definir las opciones siguientes:

- Campos...
- Agrupar por...
- Ordenar...
- Filtro...
- Visualización del árbol

Haga clic en *Aplicar* y en *Guardar*.

5. En la ventana Gestor de vistas de la incidencia, haga doble clic en el nombre de una vista.

A continuación, se muestra una vista por defecto de la ventana de vista de todas las incidencias.

	State	Severity	Priority	Id	Responsible
Incidents					
sev4	OPEN	High (4)	None (0)	103	esecadm
mixed severity	OPEN	Medium (3)	None (0)	102	esecadm
sev2	OPEN	Low (2)	None (0)	101	esecadm
sev3	OPEN	Medium (3)	Medium (2)	100	

Ready Refresh Options Refreshed At: Mon May 09 08:44:52 EDT 2005

La siguiente imagen es una vista ordenada por gravedad, con campos (gestión de columnas) para las primeras cuatro columnas definidos en Gravedad, Fecha de creación, Prioridad, Evaluación de la importancia.

	Severity	Date Created	Priority	Criticality Rating	Severity Rating	Modified By	
Incidents							
sev4	High (4)	05/09/2005 ...	None (0)	0.0	0.0	esecadm	OPEI
mixed severity	Medium (3)	05/09/2005 ...	None (0)	0.0	0.0	esecadm	OPEI
sev2	Low (2)	05/09/2005 ...	None (0)	0.0	0.0	esecadm	OPEI
sev3	Medium (3)	05/09/2005 ...	Medium (2)	0.0	0.0	esecadm	OPEI

Ready Refresh Options Refreshed At: Mon May 09 08:44:52 EDT 2005

La siguiente es una vista agrupada por título.

	Severity	Date Created	Priority	Criticality Rating	Severity Rating	Modified By
Incidents						
mixed severity						
mixed severity	Medium (3)	05/09/2005 ...	None (0)	0.0	0.0	esecadm OPEI
sev2						
sev3						
sev4						

El siguiente es un árbol de vistas por fecha de creación (Fecha de creación).

	Severity	Date Created	Priority	Criticality Rating	Severity Rating	Modified
Incidents						
mixed severity						
05/09/2005 08:44:25 EDT	Medium (3)	05/09/2005 ...	None (0)	0.0	0.0	esecadm
sev2						
05/09/2005 08:44:07 EDT	Low (2)	05/09/2005 ...	None (0)	0.0	0.0	esecadm
sev3						

Adición de una vista de incidencias

Al añadir una vista de incidencias, tiene las opciones siguientes:

- Campos...
- Agrupar por...
- Ordenar...
- Filtro...
- Visualización del árbol

Para añadir una vista de incidencias

1. En el Gestor de vistas de la incidencia, haga clic en *Añadir vista*.

Option Name

Options

Fields...	None
Group By...	None
Sort...	None
Filter...	Off
Tree Display...	Select Attribute for display

2. Introduzca un nombre de opción y seleccione las opciones que desee, haga clic en *Guardar*.

Información y campos de incidencias

Campos de incidencias

- Título: nombre de la incidencia
- Estado
 - Abierto
 - Reconocido
 - Asignado
 - Investigando
 - Positivo falso
 - Verificado
 - Aprobado
 - Cerrado
- Gravedad
 - Ninguna (0)
 - Leve (1)
 - Baja (2)
 - Media (3)
 - Alta (4)
 - Grave (5)
- Prioridad
 - Baja (1)
 - Media (2)
 - Alta (3)
 - Urgente (4)
 - Máxima (5)
- Categoría: (opcional), entrada de texto que puede utilizarse para una mejor identificación de la incidencia.
- Responsable: la cuenta de usuario asignada al caso.
- Descripción: entrada de texto.
- Resolución: entrada de texto.

Información de incidencias

- Eventos: eventos asociados a la incidencia.
- Activos: lista de todos los activos asociados a la incidencia.
- Vulnerabilidad: muestra las vulnerabilidades asociadas a la incidencia.
- Asesor: muestra la información de ataque asociada a la incidencia.
- Flujo de trabajo: muestra flujo de trabajo asociado a la incidencia. En esta pestaña, puede asignar:
 - Ninguno
 - Proceso de conformidad con HIPAA
 - Proceso de respuesta en caso de incidencia de SANS
 - Proceso de conformidad de FTP con Sarbanes Oxley
 - Respuesta automática
- Historial: historial de incidencias (enumera todas las acciones que se realizaron en la incidencia, esto incluye la fecha/hora de la acción del usuario y una breve descripción).
- Adjuntos: puede adjuntar cualquier información (archivos de texto o documentos) relacionada con esta incidencia.
- Datos externos

NOTA: Cuando se añaden eventos a una incidencia, la pestaña de activos/vulnerabilidades y la pestaña Asesor se rellenan con una lista de todos los datos del activo/vulnerabilidad/asesor correspondientes a los nombres del host DIP/destino de los eventos asociados.

NOTA: Los botones *Añadir* y *Eliminar* de la pestaña Activos/Vulnerabilidad/Asesor permiten a los usuarios añadir o eliminar manualmente datos de activos, de vulnerabilidades o del asesor.

Creación de una incidencia

Creación de una incidencia

1. Haga clic en la pestaña *Incidencias*.
2. Haga clic en *Incidencias > Crear incidencia* o haga clic en *Crear una incidencia nueva*.



Vulnerability	Severity	DateTime
---------------	----------	----------

En el recuadro de diálogo Crear incidencia, introduzca la información en los campos vacíos.

3. Haga clic en *Guardar*.

Visualización y almacenamiento de adjuntos

Para ver un adjunto

1. Haga clic con el botón derecho del ratón en un adjunto > *Ver* o *Guardar* el adjunto.

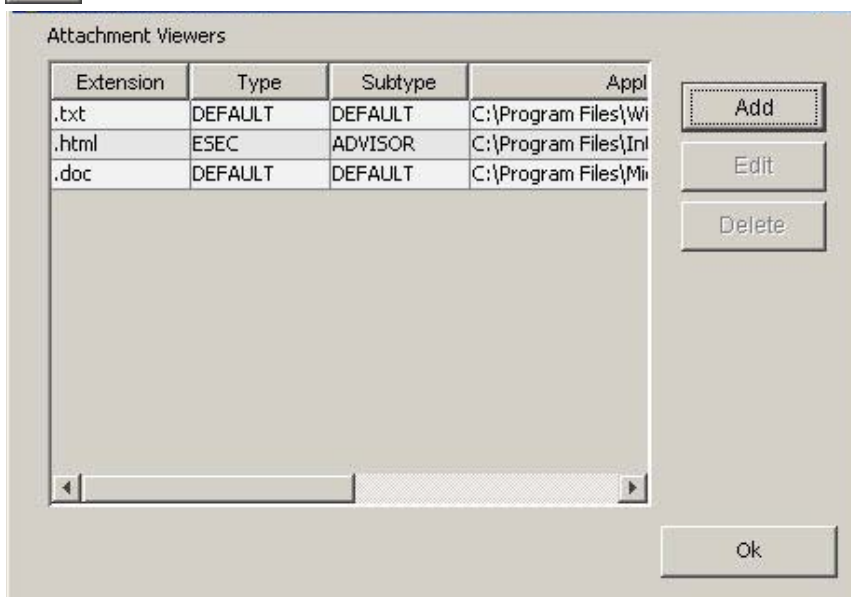
NOTA: Un visor de adjuntos debe configurarse para visualizar un adjunto.

Si un adjunto no está configurado para abrir un archivo, aparecerá un indicador en el que se solicitará con qué programa desea abrir el archivo. Los archivos adjuntos se guardan en la base de datos de Sentinel.

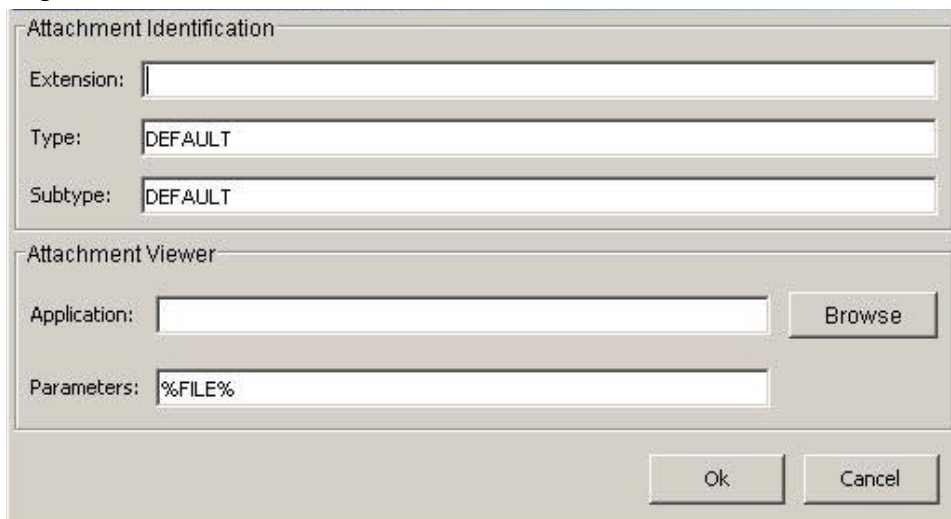
Configuración del visor de adjuntos

Configuración del visor de adjuntos

1. Haga clic en la pestaña *Incidencias*.
2. Haga clic en *Incidencias > Configuración del visor de adjuntos* o haga clic en *Configurar visores de adjuntos*.



3. Haga clic en *Añadir*.



Introduzca el tipo de extensión (como .doc, .xls, .txt, .html, etc.) y haga clic en *Examinar* o escriba el programa de la aplicación que lanzará el tipo de archivo (como notepad.exe para Notepad).

4. Haga clic en *Aceptar*.

Envío de una incidencia por correo electrónico


La posibilidad de enviar mensajes de correo electrónico se define en el archivo `execution.properties` durante la instalación. Para configurar este archivo, consulte el capítulo 11, *Utilidades*.

Envío de una incidencia por correo electrónico

1. Haga clic en la pestaña *Incidencias*.
2. Si es posible, en el navegador, expanda la carpeta *Incidencias* o haga clic en *Incidencias >* en la lista *Ver incidencias* o haga clic en la lista *Ver incidencias*.



3. Haga doble clic en el nombre de una *vista de incidencias*.
4. Haga doble clic en una incidencia.

5. Haga clic en *Enviar incidencia por correo electrónico* .

6. Introduzca:

- Dirección de correo electrónico
- Tema del correo electrónico
- Mensaje de correo electrónico

7. Haga clic en *Aceptar*. El mensaje de correo electrónico tendrá adjuntos html que tratan la información de incidencias, eventos, activos, vulnerabilidades, la información del asesor y el historial de incidencias.

Modificación de una incidencia

Para modificar una incidencia

1. Haga clic en la pestaña *Incidencias*.
2. Haga clic en *Incidencias > Visualizar el gestor de vistas de incidencias* o haga clic en

Visualizar el gestor de vistas de incidencia .

3. Haga doble clic en una vista de incidencias.
4. Haga doble clic en una incidencia.
5. Se abrirá la ventana de información de la incidencia.
6. De manera opcional, en una incidencia, puede editar los campos siguientes:
 - Título
 - Estado
 - Gravedad
 - Prioridad
 - Categoría
 - Responsable
 - Descripción
 - Resolución
7. En la pestaña *Adjuntos*, puede añadir o eliminar adjuntos.
8. Haga clic en *Guardar*.

Supresión de una incidencia

NOTA: Para suprimir una incidencia adjunta a un flujo de trabajo (iTRAC), deberá finalizar el proceso iTRAC.

Para eliminar una incidencia

1. Haga clic en la pestaña *Incidencias*.
2. Haga clic en *Incidencias > Visualizar el gestor de vistas de incidencias* o haga clic en



Visualizar el gestor de vistas de incidencias.

3. Haga doble clic en una vista de incidencias.
4. En la ventana Vista de incidencias, haga clic con el botón derecho en una incidencia > *Suprimir*.

NOTA: Para suprimir una incidencia adjunta a un flujo de trabajo (iTRAC), deberá finalizar el proceso iTRAC. Un proceso iTRAC puede finalizarse mediante el Gestor de vistas de procesos de la pestaña iTRAC. Para obtener más información, consulte el *capítulo 5, Pestaña iTRAC*.

5. En la ventana de confirmación, haga clic en *Sí*.

5

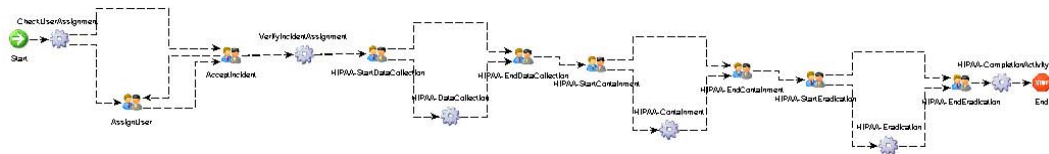
Pestaña iTRAC™

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

El flujo de trabajo de iTRAC (flujo de trabajo) implica la automatización de los procedimientos y la capacidad para responder a las incidencias. Sentinel ofrece un sistema de gestión iTRAC que brinda la automatización de los procedimientos. La estructura de actividades de Sentinel está vinculada a iTRAC. La estructura de actividades proporciona las actividades que pueden realizarse automáticamente en cada paso del proceso iTRAC.

Las plantillas (definición del proceso) y la ejecución del proceso constituyen el sistema de gestión del flujo de trabajo.

Plantillas (Definición del proceso)



La plantilla es el diseño que controla el flujo de ejecuciones en iTRAC. La plantilla está formada por una red de actividades y sus relaciones, criterios para la transición entre actividades e información acerca de actividades individuales. Las plantillas tienen atributos que el usuario puede modificar.

iTRAC permite a los usuarios ajustar atributos de tiempo límite en una plantilla de iTRAC.

Una actividad es una unidad lógica e independiente de trabajo dentro del proceso iTRAC. Una actividad representa el trabajo, que será procesado por usuarios o por funciones (actividad manual) o bien por aplicaciones informatizadas (actividades automáticas).

Las actividades también disponen de tiempos límite y los usuarios pueden habilitar o inhabilitar estos tiempos límite de todas las actividades manuales o automáticas.

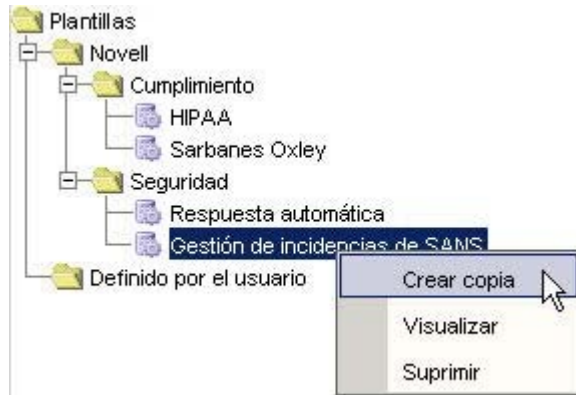
Las actividades manuales, además de los atributos de tiempo límite, permiten que los usuarios configuren el atributo del recurso que determina el usuario o la función que realiza esta actividad.

Las actividades automáticas, además de los atributos de tiempo límite, permiten que los usuarios configuren la actividad automática desde la estructura de actividades de Sentinel que se ejecutará.

Gestor de plantillas

iTRAC permite que los usuarios creen plantillas nuevas, modifiquen los atributos del proceso y las actividades en una plantilla existente y supriman plantillas mediante la ventana del gestor de plantillas de la pestaña iTRAC.

Para acceder al gestor de plantillas, haga clic en el nodo del gestor de plantillas del árbol de navegación de la pestaña iTRAC.



Plantillas por defecto

iTRAC se suministra con cuatro plantillas por defecto que cuentan con actividades automáticas y manuales. Los atributos del proceso y las actividades de estas plantillas se han ajustado en algunos valores predefinidos, los usuarios pueden modificarlos para satisfacer sus necesidades. Las plantillas por defecto son:

- HIPAA
- Sarbanes Oxley
- Gestión de incidencias de SANS
- Respuesta automática

Creación de plantillas nuevas

1. Haga clic en la pestaña *iTRAC*.
2. En el navegador, haga clic en *Administración de iTRAC > Gestor de plantillas*.
3. Resalte un proceso existente (HIPAA, Sarbanes-Oxley, SANS o un proceso definido por el usuario), haga clic con el botón derecho en *> Crear copia*.
4. Introduzca un nombre.
5. Si selecciona un tiempo límite, debe introducir una dirección de correo electrónico y un período de tiempo. Éste es en números enteros. Puede seleccionar minutos, segundos, horas o días.
6. Escriba una descripción. Consulte la sección *Modificación de plantillas existentes* para cambiar los atributos del proceso y actividades. Haga clic en *Aceptar*.
7. En el Personalizador de plantillas, haga clic en *Guardar*.

Modificación de plantillas existentes

Al modificar un proceso, puede modificar los atributos del proceso o los atributos de las actividades del proceso:

Pueden modificarse los siguientes atributos del proceso:

- nombre
- período de tiempo límite o inhabilitar el período de tiempo límite
- descripción

Modificación de los atributos del proceso

1. Haga clic en la pestaña *iTRAC*.
2. En el navegador, haga clic en *Administración de iTRAC > Gestor de plantillas*.
3. Resalte una plantilla existente, haga clic con el botón derecho en *> Visualizar*.

En la ventana de la plantilla, haga clic en el botón Información del proceso.



4. En el recuadro de diálogo Personalizador de procesos, puede editar los parámetros siguientes:

- Nombre
- Duración (minutos, segundos, horas o días)
- Tiempo límite (si está habilitado deberá introducir una dirección de correo electrónico y el período de tiempo)
- Descripción

La imagen muestra una ventana de diálogo titulada "Personalizador de procesos". En la parte superior izquierda hay un icono de engranajes. El campo "Nombre:" contiene el texto "SANS Incident Handling". El campo "Duración:" es un menú desplegable con "minutos" seleccionado. El campo "Correo electrónico:" está vacío. Hay un botón de opción desactivado etiquetado "Tiempo límite". El campo "Límite:" está vacío. En la parte inferior, hay un campo de texto etiquetado "Descripción" que contiene "SANS Incident Handling". En la parte inferior derecha hay dos botones: "Aceptar" y "Cancelar".

Modificación de actividades manuales

Puede editar el recurso (usuario y función), el tiempo límite y la descripción de las actividades manuales.

1. Haga clic en la pestaña *iTRAC*.
2. En el navegador, haga clic en *Administración de iTRAC > Gestor de plantillas*.
3. Resalte una plantilla existente, haga clic con el botón derecho en *> Visualizar*.
4. La plantilla aparece en una ventana independiente.
5. Para editarla, haga doble clic en cualquiera de los iconos de actividad manual de la plantilla y realice los cambios.

NOTA: Las siguientes actividades manuales de las plantillas existentes pueden modificarse utilizando este método.



- AssignUser
- AcceptIncident
- ConfirmStartDataCollection
- ConfirmEndDataCollection
- ConfirmStartContainment
- ConfirmEndContainment
- ConfirmStartEradication
- ConfirmEndEradication

Personalizador de actividades

Nombre: AcceptIncident

Tipo: Manual

Recurso: Analyst

Tiempo límite

Límite: minutos

Descripción

Accept this Incident

Aceptar Cancelar

Modificación de actividades automáticas

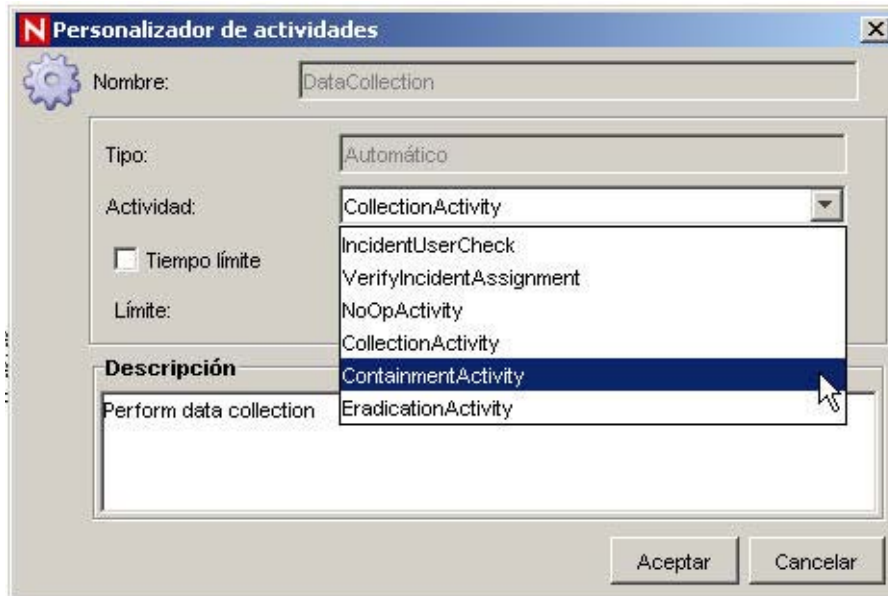
Puede editar la actividad, el Tiempo límite y la Descripción de una actividad automática.

1. Para ello, haga doble clic en cualquiera de los iconos de actividad automática de la plantilla y realice los cambios.
2. La lista desplegable de los recuadros de diálogo del personalizador de actividades muestra la lista de actividades que pueden utilizarse como actividades automáticas. Las actividades de la lista se crean mediante la estructura de actividades.

NOTA: Pueden modificarse de este modo las actividades automáticas siguientes de la plantilla existente.



- DataCollection
- Containment
- Eradication



Supresión de plantillas

1. Haga clic en la pestaña *iTRAC*.
2. En el navegador, haga clic en *Administración de iTRAC > Gestor de plantillas*.
3. Resalte una plantilla existente, haga clic con el botón derecho en *> Suprimir*.
4. Haga clic en *Sí* en la ventana emergente para suprimir plantillas.

Ejecución del proceso

La ejecución del proceso es el plazo de tiempo durante el cual el proceso es operativo, con instancias de procesos que se están creando y gestionando.

Cuando se ejecuta o se instancia un proceso iTRAC en el servidor iTRAC, el servidor iTRAC crea, gestiona y, finalmente, termina una instancia del proceso en función de la definición del proceso. Mientras el proceso avanza para finalizar o terminar, éste ejecuta varias actividades definidas en la plantilla de flujo de trabajo en función de los criterios de las transiciones entre éstas. El servidor de flujo de trabajo de iTRAC procesa actividades manuales y automáticas de otra manera.

Un proceso iTRAC depende de una incidencia de Sentinel, una instancia de un proceso no puede existir si no existe ninguna incidencia relacionada con éste. Por otro lado, puede existir una incidencia sin estar relacionada con el servidor de flujo de trabajo. Sólo puede asociarse 1 incidencia a una instancia del proceso iTRAC.

Creación de una instancia de un proceso

Puede crearse una instancia de un proceso iTRAC en el servidor de iTRAC asociando una incidencia a un proceso iTRAC mediante uno de los 3 métodos siguientes:

- Asociar un proceso iTRAC a la incidencia en el momento de la creación de la incidencia
- Asociar un proceso iTRAC a la incidencia después haber creado una incidencia
- Asociar un proceso iTRAC a una incidencia a través de una correlación

Consulte el capítulo sobre la pestaña Incidencias para obtener más información acerca de la asociación de un proceso a una incidencia.

Ejecución de una actividad automática

Cuando la instancia del proceso ejecuta una actividad automática, ésta ejecuta la actividad asociada definida en la plantilla. La actividad asociada es una actividad creada mediante la estructura de actividades. El servidor de iTRAC ejecuta la actividad, almacena el resultado en variables del proceso y realiza una transición a la actividad siguiente de la plantilla de iTRAC.

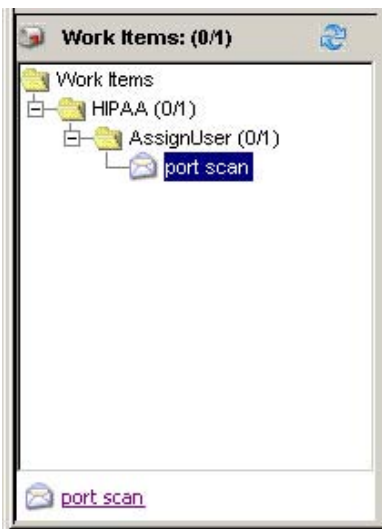
Por ejemplo, la actividad de la estructura de actividades puede definirse para que realice un ping en un servidor y adjuntar los resultados a la incidencia asociada.

Ejecución de una actividad manual

Al detectar una actividad manual, el servidor de iTRAC envía notificaciones en formato de elementos de trabajo al recurso asignado. Si el recurso asignado es un usuario, el elemento de trabajo sólo se enviará a ese usuario. Si la actividad se ha asignado a una función, se enviará un elemento de trabajo a todos los usuarios de la función. El servidor de iTRAC espera a que el usuario finalice el elemento de trabajo antes de continuar con la actividad siguiente.

Listas de trabajo

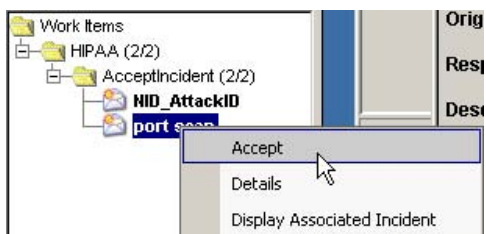
Los elementos de trabajo se presentan al usuario a través de la lista de trabajo, que conserva la información de todos los elementos de trabajo asignados al usuario. Es la lista de tareas del usuario.



La lista de trabajo se puede visualizar desde cualquier pestaña de la IU de Sentinel. Los elementos de trabajo se agrupan por proceso y actividad a los que pertenecen. Los elementos de trabajo en negrita indican los que el usuario todavía no ha aceptado.

La lista de trabajo permite que los usuarios interactúen con los elementos de trabajo individuales.

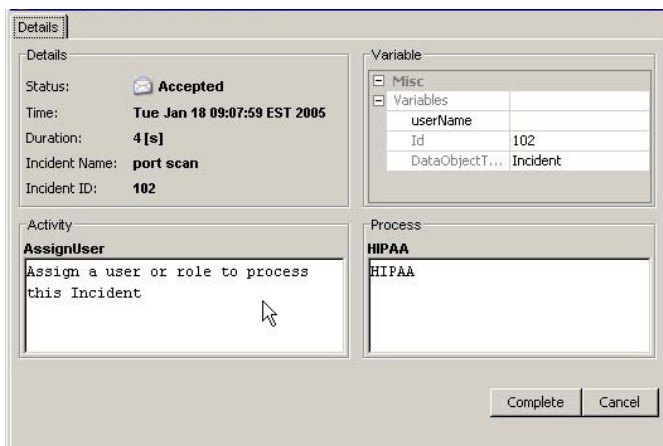
- Los usuarios pueden hacer doble clic o hacer clic con el botón derecho en > *Información* para ver la información del elemento de trabajo.
- Los usuarios pueden hacer clic con el botón derecho del ratón en > *Aceptar* los elementos de trabajo no aceptados.
- Los usuarios pueden hacer clic con el botón derecho del ratón en > *Ver* la información de las incidencias asociadas.



Elementos de trabajo

Un elemento de trabajo constituye la tarea que debe llevar a cabo el usuario para la actividad manual que se está ejecutando actualmente en un proceso iTRAC. El control y la progresión del elemento de trabajo continúa siendo responsabilidad del usuario.

El servidor de iTRAC espera a que el usuario finalice la tarea antes de continuar con la actividad siguiente en la instancia del proceso.



El recuadro de diálogo Información del elemento de trabajo que aparece más arriba incluye la información siguiente:

- Información del elemento de trabajo
- Variables del elemento de trabajo
- Descripción de la actividad
- Descripción del proceso

Existen tres pasos implicados en la interacción con un elemento de trabajo:

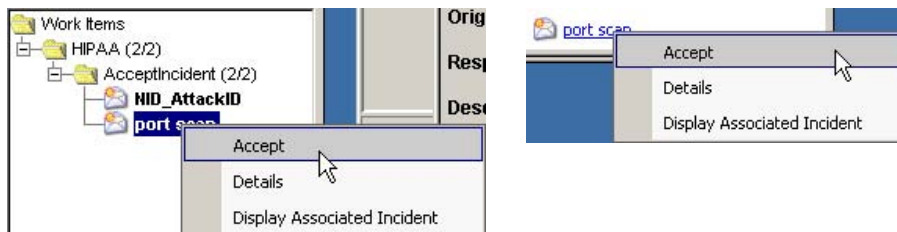
- Aceptación de un elemento de trabajo
- Actualización de variables del elemento de trabajo
- Finalización del elemento de trabajo

Aceptación de un elemento de trabajo

Un elemento de trabajo puede asignarse a todos los usuarios de una función o sólo a un usuario. Un elemento de trabajo debe ser aceptado por el usuario antes de realizar otra acción en el elemento de trabajo. Al aceptarse el elemento de trabajo, el usuario se convierte en el propietario del elemento de trabajo y éste se elimina de la lista de trabajo del resto usuarios asignados.

Aceptación de elementos de trabajo

1. En la lista de trabajo, puede hacer clic con el botón derecho del ratón en un elemento de trabajo y realizar las operaciones siguientes:



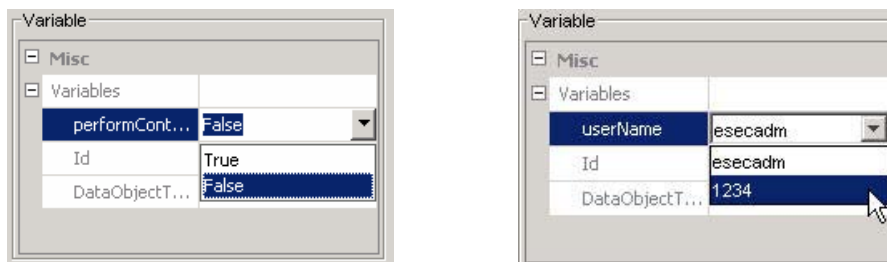
- Aceptar (cuando el proceso se encuentra en el paso Aceptar)
- Como alternativa, puede activar la ventana de información y hacer clic en el botón Aceptar.

Actualización de variables del elemento de trabajo

El servidor de iTRAC utiliza elementos de trabajo para obtener información sobre usuarios en formato de variables de elementos de trabajo y así determinar la actividad siguiente con un proceso. El usuario puede acceder a las variables sólo después de aceptar el elemento de trabajo.

iTRAC admite variables de sólo lectura y variables actualizables; las variables de sólo lectura se utilizan para informar al usuario; por ejemplo, del estado de una actividad, de la identificación de una incidencia, etc.

Las variables actualizables se utilizan para aceptar las entradas de los usuarios. Actualmente, en iTRAC existen dos tipos de variables actualizables, la lista de usuarios y la lista booleana.



Actualización de variables

1. Haga clic o doble clic en el elemento de trabajo para ver el recuadro de diálogo Información.
2. Sólo se encuentran en modo de edición las variables actualizables, las variables de sólo lectura no pueden editarse.
3. Haga clic en la casilla de opciones y seleccione el valor adecuado.

- Haga doble clic en una de las vistas por defecto o cree una vista nueva. Las vistas por defecto son:
 - Todos los procesos
 - Procesos por incidencia
 - Procesos por estado
- En el Gestor de procesos activos, resalte un proceso y haga doble clic en éste.

State	IncidentOwner	IncidentId	LastUpdateTime
running		102	2005.01.18 / 09:08:53 EST
running		100	2005.01.18 / 09:05:00 EST

Event Time	Id	InstanceID	EventType	Old State	New State
Tue Jan 18 09:07:57 EST...	HIPAA	3_ITrac_HIPAA	process_created		
Tue Jan 18 09:07:57 EST...	HIPAA	3_ITrac_HIPAA	process_context_changed	{}	{containmentOutput=, p...
Tue Jan 18 09:07:58 EST...	HIPAA	3_ITrac_HIPAA	process_context_changed	{Id=}	{Id=102}
Tue Jan 18 09:07:59 EST...	HIPAA	3_ITrac_HIPAA	process_context_changed	{userName=null}	{userName=null}
Tue Jan 18 09:07:59 EST...	HIPAA	3_ITrac_HIPAA	process_state_changed	not_started	running

Para definir una opción del Gestor de procesos

- Haga clic en la pestaña *iTRAC*.
- Haga doble clic en cualquiera de los procesos.
- Haga clic en el botón Opciones. En esta ventana también podrá definir las opciones siguientes:
 - Campos...
 - Agrupar por...
 - Ordenar...
 - Filtro...
 - Visualización del árbol
- Haga clic en *Aplicar* y en *Guardar*.

La siguiente vista es una Visualización del árbol definida en Estado (en ejecución y sin iniciar).

State	IncidentId	LastUpdateTime	Description
running	104	2005.01.19 / 09:38:58 EST	SANS Incident H...
not_started	101	2005.01.18 / 08:52:59 EST	SANS Incident H...

Inicio o terminación de un proceso

Inicio o terminación de un proceso

1. Haga clic en la pestaña *iTRAC*.
2. Haga clic en el botón *Mostrar el gestor de opciones*.



3. Haga doble clic en una de las vistas por defecto o cree una vista nueva. Las vistas por defecto son:
 - Todos los procesos
 - Procesos por incidencia
 - Procesos por estado
4. En el Gestor de procesos activos, resalte un proceso, haga clic con el botón derecho y seleccione *Iniciar proceso* o *Terminar proceso*.

Creación de una actividad mediante la estructura de actividades

Creación de una actividad

1. Haga clic en la pestaña *iTRAC*.
2. En el navegador, haga clic en *Administración de iTRAC > Gestor de actividades*.
3. Haga clic con el botón derecho del ratón en *> Nueva actividad*.
4. Seleccione una de las opciones siguientes:



- Actividad del comando de incidencia: inicia un comando específico con o sin argumentos.

La Salida de la incidencia ofrece los argumentos siguientes:

- DIP
- DIP:Port
- incident
- RT1 (DeviceAttackName)
- SIP
- SIP:Port
- Text

La opción Personalizar permite introducir sus propios argumentos personalizados.

En esta actividad también puede establecer que envíe por correo electrónico la salida o que adjunte la salida a la incidencia.

- Actividad interna de la incidencia: permite enviar por correo electrónico o adjuntar información acerca de:
 - Vulnerabilidad para (SIP o DIP)
 - Activo
 - Datos del asesor

- Actividad compuesta por varias incidencias: permite crear una actividad combinando una o más actividades existentes.

SrNo	ActivityName
1	ContainmentActivity
2	CollectionActivity
3	EradicationActivity

Navigation buttons '< Back', 'Finish', and 'Cancel' are at the bottom.

Modificación de una actividad

Modificación de una actividad

1. Haga clic en la pestaña *iTRAC*.
2. En el navegador, haga clic en *Administración de iTRAC > Gestor de actividades > Actividades de iTRAC*.
3. Haga doble clic en una actividad de iTRAC. Edítela y haga clic en *Aceptar*.

Importación o exportación de una actividad

Las actividades se exportan como archivos xml. Estos archivos pueden importarse de un sistema a otro.

Exportación de una actividad

1. Haga clic en la pestaña *iTRAC*.
2. En el navegador, haga clic en *Administración de iTRAC > Gestor de actividades*.
3. Haga clic con el botón derecho en *Actividades de iTRAC > Actividad de importación y exportación*.
4. Seleccione *Exportar actividad* y haga clic en *Explorar*.
5. Busque la ubicación en la que desee guardar el archivo exportado.
6. Asigne un nombre al archivo y haga clic en *Exportar*.
7. Haga clic en *Siguiente*.
8. Seleccione una o más actividades para exportar.
9. Haga clic en *Siguiente* y en *Finalizar*.

Importación de una actividad

1. Haga clic en la pestaña *iTRAC*.
2. En el navegador, haga clic en *Administración de iTRAC > Gestor de actividades*.
3. Haga clic con el botón derecho en *Actividades de iTRAC > Actividad de importación y exportación*.
4. Seleccione *Importar actividad* y haga clic en el botón *Explorar*.
5. Busque el archivo de importación. Haga clic en *Importar*.
6. Haga clic en *Siguiente*.
7. Haga clic en *Siguiente* y en *Finalizar*.

6

Pestaña Análisis

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

Para utilizar la pestaña Análisis debe tener los permisos adecuados. Si no se asigna este permiso, no estará disponible ninguno de los demás permisos relacionados con las acciones de esta pestaña.

Descripción

La pestaña Análisis permite generar informes históricos. Los informes históricos y de vulnerabilidades se publican en un servidor Web, éstos se ejecutan directamente contra la base de datos de Sentinel y aparecen en las pestañas Análisis y Asesor de la barra del navegador.

NOTA: Sentinel está integrado con Crystal Reports® para generar y visualizar informes. El administrador debe configurar la ubicación del servidor Crystal Enterprise que publica informes en la ventana de opciones generales de la pestaña Admin. En la ventana del navegador se ofrece una lista de informes disponibles.

Para ejecutar las plantillas de informes, debe tener instalado Crystal Reports Enterprise Edition y el Centro de control de Sentinel debe estar configurado para poder acceder a dicho servidor. Para obtener más información, consulte la *Guía de instalación de Sentinel™ 5*.

También se proporcionan informes de ejemplo en formato pdf.

Los diez informes más habituales

Para ejecutar uno de los 10 informes más habituales, la función de adición debe estar habilitada y [EventFileRedirectService](#) en DAS_Binary.xml debe estar activado. Para obtener información acerca de cómo activar la función de adición, consulte la *Guía del usuario de Sentinel, capítulo 10, Gestor de datos de Sentinel*, la sección sobre la pestaña *Datos de informes*.

Habilitación de EventFileRedirectService para los 10 informes más habituales de Sentinel

Habilitación de EventFileRedirectService

1. En la máquina de DAS, mediante un editor de texto, abra:

En UNIX:

```
$ESEC_HOME/sentinel/config/das_binary.xml
```

En Windows:

```
%ESEC_HOME%\sentinel\config\das_binary.xml
```


2. En EventFileRedirectService, cambie el estado a Activo (ON).
`<property name="status">on</property>`
3. En Windows, reinicie el servicio de Sentinel. En UNIX, reinicie la máquina de DAS.

Ejecución de un informe desde Crystal Reports

Para crear un informe desde una plantilla de Crystal Reports

1. Haga clic en la pestaña *Análisis*.
2. En el *navegador de análisis*, haga clic en un informe de los informes disponibles.

NOTA: Para ejecutar uno de los 10 informes más habituales, la función de adición debe estar habilitada y [EventFileRedirectService](#) en DAS_Binary.xml debe estar activado. Para obtener información acerca de cómo activar la función de adición, consulte la *Guía del usuario de Sentinel, capítulo 10, Gestor de datos de Sentinel*, la sección sobre la pestaña *Datos de informes*.

3. Haga clic en *Análisis > Crear un informe* o haga clic en *Crear un informe*.



4. Complete la información de la plantilla y haga clic en *Ver informe*. Aparecerá el informe.

Ejecución de un informe de consulta de eventos

Para crear un informe de consulta de eventos

1. Haga clic en la pestaña *Análisis*.
2. En el navegador de análisis, abra la carpeta *Informes históricos*.
3. Haga clic en *Consulta de eventos*.
4. Haga clic en *Análisis > Crear un informe* o haga clic en *Crear un informe*.



Se abrirá una ventana de consulta de eventos.

5. Defina los elementos siguientes:
 - plazo de tiempo
 - filtro
 - nivel de gravedad
 - tamaño del lote (es el número de eventos que se visualizarán: los eventos se visualizan desde los más antiguos hasta los más nuevos)
6. Haga clic en *Actualizar consulta*.
7. Para visualizar el siguiente lote de eventos, haga clic en *Más*.
8. Reorganice las columnas arrastrando y soltándolas y ordénelas haciendo clic en el encabezado de columna.
9. Una vez haya finalizado la consulta, ésta se añadirá a la lista de consultas rápidas del navegador.

Ejecución de un informe de eventos correlacionados

Para crear un informe de eventos correlacionados

1. Haga clic en la pestaña *Análisis*.
2. En el navegador de análisis, abra la carpeta de informes históricos.
3. Haga clic en *Eventos correlacionados*.
4. Haga clic en *Análisis > Crear un informe* o haga clic en *Crear un informe*.



Se abrirá una ventana de un informe de eventos correlacionados.

Event Id:	Correlation rule:	Batch size:		
<input type="text"/>	<input type="text"/>	100		
DateTime	Severity	EventName	SourceIP	DestinationIP

5. En el campo ID de correlación, introduzca uno de los datos siguientes:
 - Número del ID de evento
 - CorrelatedEventUUID

NOTA: CorrelatedEventUUID sólo está disponible en una tabla de eventos en tiempo real.

6. Para visualizar el siguiente lote de eventos, haga clic en *Más*.



7

Pestaña Asesor

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

Para utilizar la pestaña Asesor debe tener los permisos adecuados. Si no se asigna este permiso, no estará disponible ninguno de los demás permisos relacionados con las acciones de esta pestaña.

El asesor es un módulo opcional. Si no dispone de una licencia del asesor, al hacer clic en la pestaña Asesor obtendrá una pantalla de notificación en la que se indicará su ausencia.

El asesor de Sentinel ha sido desarrollado por SecurityNexus. El asesor proporciona información en tiempo real de las vulnerabilidades de la empresa, consejos técnicos y los pasos a seguir para solucionar los posibles agujeros de seguridad. Asimismo, ofrece referencias cruzadas entre las firmas IDS en tiempo real de los atacantes y la base de datos de vulnerabilidades con la que cuenta. Si desea obtener más información,

Los datos del asesor contienen dos partes:

- Datos de alerta: información relativa a amenazas y vulnerabilidades de seguridad conocidas.
- Datos de ataque: normalización de firmas de detección de intrusos y módulos auxiliares (plug-in) de exploración de vulnerabilidades.

NOTA: Durante la instalación y hasta los datos iniciales de SecurityNexus, la función de hacer clic con el botón derecho en un evento (con el campo rt1 relleno) para los datos del asesor no funcionará totalmente.

Ejecución de informes de asesor

Para crear un informe de asesor

1. Haga clic en la pestaña Asesor.
2. En el navegador del asesor, haga clic en una plantilla de informes.
3. Haga clic en *Asesor > Crear un informe*.
4. Complete la información de la plantilla y haga clic en *Ver informe*.

Instalación independiente: Actualización manual del asesor

Actualización manual de los datos del asesor

1. Vaya a la URL `//advisor.esecurityinc.com/advisordata/`.
2. Introduzca el nombre de usuario y la contraseña.
3. Vaya al último mes de las carpetas `attack` y `alert` y descargue los archivos comprimidos.

4. Coloque los nuevos archivos de datos de alerta y ataque (los archivos estarán en formato comprimido) en su equipo.

NOTA: No coloque los archivos comprimidos en los directorios attack ni alert.

5. Descomprima los archivos comprimidos de datos de ataque en:

En Windows:

```
<ubicación especificada durante la instalación para  
  los archivos de datos del asesor>\attack
```

o bien

En UNIX:

```
<ubicación especificada durante la instalación para  
  los archivos de datos del asesor>/attack
```

6. Descomprima los archivos comprimidos de datos de alerta en:

En Windows:

```
<ubicación especificada durante la instalación para  
  los archivos de datos del asesor>\alert
```

o

En UNIX:

```
<ubicación especificada durante la instalación para  
  los archivos de datos del asesor>/alert
```

7. Vaya a:

En Windows:

```
%ESEC_HOME%\sentinel\bin
```

En UNIX:

```
$ESEC_HOME/sentinel/bin
```

8. Ejecute el comando siguiente:

En Windows:

```
advisor. bat
```

En UNIX:

```
. /advisor. sh
```

NOTA: advisor. sh y advisor. bat actualizarán la base de datos y suprimirán los archivos attack y alert que se han descomprimido en los directorios attack y alert.

Descarga directa de Internet: Actualización manual del asesor

Actualización manual de los datos del asesor

1. Vaya a:
En Windows:
`%ESEC_HOME%\sentinel\bin`
En UNIX:
`$ESEC_HOME/sentinel/bin`
2. Ejecute el comando siguiente:
En Windows:
`advisor. bat`
En UNIX:
`. /advisor. sh`

NOTA: `advisor. sh` y `advisor. bat` actualizarán la base de datos y suprimirán los archivos `attack` y `alert` que se han descomprimido en los directorios `attack` y `alert`.

Cambio de la configuración del correo electrónico y la contraseña del servidor del asesor

Cambio de la contraseña del servidor del asesor (independiente)

Este procedimiento no es aplicable a configuraciones independientes.

Cambio de la contraseña del servidor del asesor (descarga directa)

Para cambiar la contraseña del servidor del asesor (descarga directa)

1. Envíe un cambio de contraseña al servicio de asistencia técnica de Novell.
2. Tras haber sido informado del cambio de contraseña desde Novell, en UNIX, entre como `esecadm o`, en Windows, entre con derechos administrativos.
3. Cambie al directorio siguiente:
En UNIX:
`$ESEC_HOME/sentinel/bin`
En Windows:
`%ESEC_HOME%\sentinel\bin`

4. Escriba los comandos siguientes:

En UNIX:

```
. /adv_change_passwd. sh <contraseña_antigua>  
  <contraseña_nueva>
```

En Windows:

```
adv_change_passwd. bat <contraseña_antigua>  
  <contraseña_nueva>
```

Cambio de la configuración del correo electrónico del servidor del asesor

Para cambiar la configuración del correo electrónico del servidor del asesor

1. Para una entrada a UNIX, como esecadm o para una entrada a Windows, con derechos administrativos.
2. Cambie al directorio siguiente:

En UNIX:

```
$ESEC_HOME/sentinel/config
```

En Windows:

```
%ESEC_HOME%\sentinel\config
```

3. Mediante un editor de texto abra alertcontainer. xml y alertcontainer. xml. Realice los cambios en el área gris.

```
<property name="advisor. mail.  
  from">de_NOMBRE@dominio. com</property>  
  
<property name="advisor. mailto.  
  list">a_NOMBRE@dominio. com</property>
```

NOTA: Para especificar más de una dirección de correo electrónico de destino, introduzca las direcciones de correo electrónico separadas por comas sin espacios.

Cambio de la hora de los datos

Por defecto, las horas de los datos son:

- Seis horas: 01: 00, 07: 00, 13: 00 y 19: 00
- Doce horas: 02: 00 y 14: 00

Para cambiar las horas de los datos

1. Entre a la máquina del asesor (para una entrada a UNIX como esecadm).
2. Para editar las horas de los datos:

En UNIX: utilice el comando 'crontab'.

En Windows: utilice el comando 'at'.

8

Pestaña Recopiladores

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

Para utilizar la pestaña Recopiladores debe tener los permisos adecuados. La pestaña Recopiladores permite una serie limitada de funciones del asistente. Para obtener la funcionalidad completa del asistente, utilice el Generador de recopiladores. La pestaña Recopiladores permite:

- [Monitorizar un host del asistente](#)
- [Monitorizar un recopilador](#)
- [Iniciar y detener recopiladores](#) (Gestor de recopiladores) para un host seleccionado



Disposición

El panel izquierdo de la pestaña Recopiladores contiene un árbol de vistas. Por defecto, la vía del árbol tiene dos elementos hijos: Vistas del Gestor de recopiladores y Vista de recopilador. El panel derecho muestra las vistas en tablas. Cada vista del panel derecho tiene una entrada en el árbol de la izquierda.

En el panel derecho se muestran cuatro vistas:

- Vista del recopilador
 - Gestor de vistas del recopilador
- Vista del Gestor de recopiladores
 - Gestor de vistas del Gestor de recopiladores

La vista del recopilador muestra información acerca de los recopiladores y la vista del Gestor de recopiladores muestra información acerca de los Gestores de recopiladores. Cada vista aparece como una tabla del árbol: el objeto se agrupa por uno o más de sus atributos. La configuración de la vista puede ajustarse. Las opciones de una vista pueden cambiarse y pueden añadirse nuevos tipos de vista. La configuración de la vista se muestra en un Gestor de vistas (Gestor de vistas del recopilador o Gestor de vistas del Gestor de recopiladores).

Cuando aparece la pestaña por primera vez, el árbol del panel izquierdo se muestra con los dos gestores de vistas y el Gestor de vistas del recopilador aparece en el panel derecho.

El Gestor de vistas del recopilador tiene tres opciones de vista preconfiguradas por defecto; las nuevas pueden crearse. Estas tres opciones son: Todos los recopiladores, Recopiladores por gestor y Recopiladores por estado.

La vista Todos los recopiladores muestra todos los recopiladores agrupados por el gestor en el que se están ejecutando.

El Gestor de vistas del Gestor de recopiladores agrupa todos los recopiladores por su gestor y, a continuación, los agrupa por su estado (activo o inactivo) dentro de cada gestor.

La vista Recopiladores por estado agrupa todos los recopiladores por estado (activo o inactivo) y, a continuación, dentro de cada estado los agrupa por gestor.

Sólo existe una vista por defecto para visualizar los Gestores de recopiladores, es la vista Todos los gestores. Muestra todos los Gestores de recopiladores del sistema sin agrupar.

Monitorización de un recopilador

En la ventana Hosts del asistente, por defecto puede [monitorizar](#) las siguientes funciones:

Gestor de vistas del Gestor de recopiladores

- Hora de inicio Hora a la que el Gestor de recopiladores se ha iniciado, en mm/dd/aa hh: mm: ss y zona horaria
- Funcionamiento El tiempo que el Gestor de recopiladores ha estado ejecutándose, en días, horas, minutos y segundos.
- Total de eventos recibidos Número de eventos recibidos desde todos los recopiladores por el Gestor de recopiladores desde que se ha iniciado.
- Velocidad de eventos recibidos Velocidad media de eventos por segundo que el Gestor de recopiladores ha recibido en el último minuto.

Gestor de vistas del recopilador

- Estado activo o inactivo
- Velocidad de eventos recibidos Velocidad media de eventos por segundo que el puerto del recopilador ha recibido en el último minuto.
- Total de eventos recibidos Número de eventos recibidos por el puerto del recopilador desde que se ha iniciado.
- Funcionamiento El tiempo que el puerto del recopilador ha estado ejecutándose, en días, horas, minutos y segundos.

Puede [crear sus propias vistas](#) con más o menos campos adicionales.

Monitorización de un host del asistente

Monitorización de un host del asistente

1. Haga clic en la pestaña Recopiladores.
2. Haga clic en *Gestor de vistas del Gestor de recopiladores*.



3. Seleccione una opción de vista haciendo doble clic en una vista o cree una nueva. Aparecerá la ventana Hosts del asistente.



Creación de una vista de recopilador

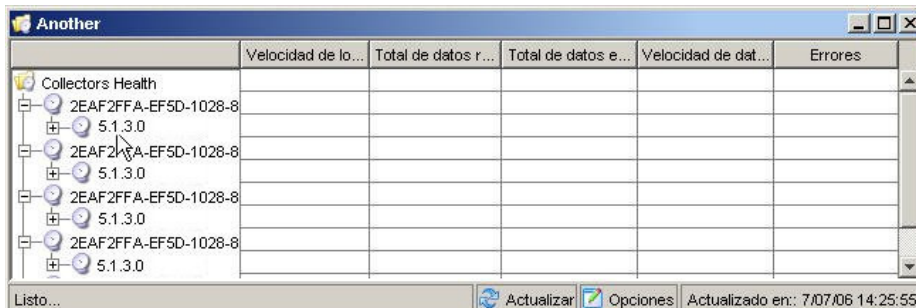
Creación de una vista de recopilador

1. Haga clic en la pestaña *Recopiladores*.
2. Haga clic en *Gestor de vistas del Gestor de recopiladores*.



3. Para crear una vista nueva, haga clic en *Añadir vista*.
 - Introduzca el nombre de la opción.
 - Para organizar los campos que se debe visualizar, haga clic en *Campos*.
 - Para agrupar títulos diferentes, haga clic en *Agrupar*.
 - Para ordenar por título, haga clic en *Ordenar*.
 - Para filtrar la vista, haga clic en *Filtro*.

A continuación, se muestra una vista definida con un grupo ajustado en UUID del gestor y por versión.

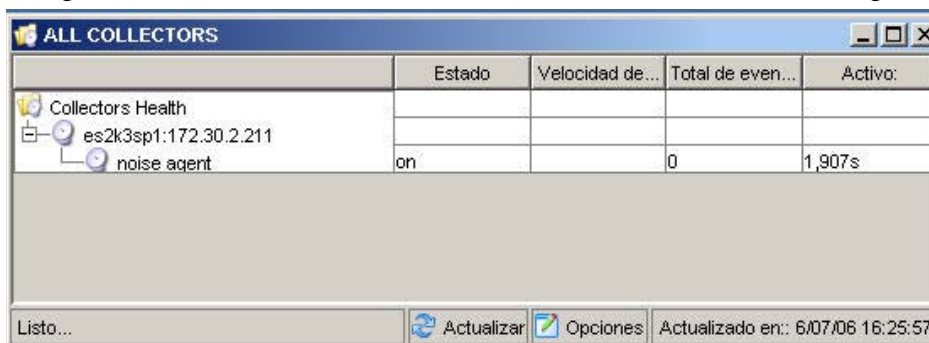


Modificación de una vista de recopilador

Modificación de una vista de recopilador

1. Abra el Gestor de vistas del recopilador.
2. Haga doble clic en cualquiera de los nombres.
3. Haga clic en *Opciones*. En esta ventana también podrá definir las siguientes opciones:
 - Campos...
 - Agrupar por...
 - Ordenar...
 - Filtro...
 - Visualización del árbol
4. Haga clic en *Aplicar* y en *Guardar*.

La siguiente vista es una visualización del árbol definida como un UUID del gestor.



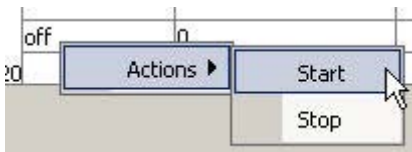
	Estado	Velocidad de...	Total de even...	Activo:
Collectors Health				
es2k3sp1:172.30.2.211				
noise agent	on		0	1,907s

Lista... Actualizar Opciones Actualizado en: 6/07/06 16:25:57

Detención, inicio e información de recopiladores

Detención e inicio de recopiladores

1. Haga clic en la pestaña *Recopiladores*.
2. Abra un Gestor de vistas del recopilador.
3. Para detener, iniciar y mostrar información acerca de un único recopilador, haga clic con el botón derecho en un *Recopilador* > *Acciones* > *Iniciar o Detener*.

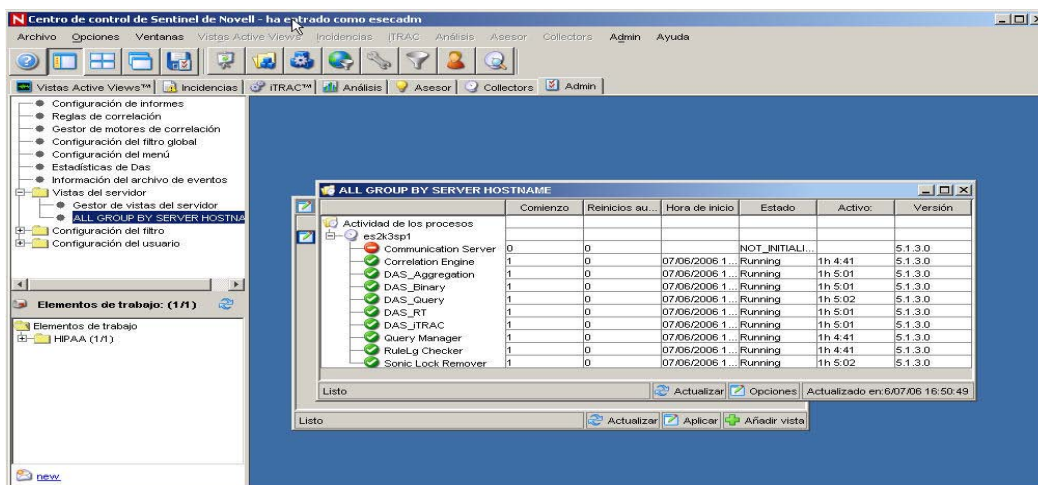


9

Pestaña Admin

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

Para utilizar esta función, se debe disponer del permiso adecuado. Si no se asigna este permiso, no estará disponible ninguno de los demás permisos relacionados con las acciones de esta pestaña.



Pestaña Admin: Descripción

La pestaña Admin permite acceder a los elementos siguientes:

- [Opciones de configuración de informes para los informes de análisis y asesor](#)
- [Gestión de filtros](#)
- [Funcionamiento con reglas de correlación de Sentinel](#)
- [Configuración de Configuración del menú](#)
- [Estadísticas DAS](#)
- [Información del archivo de eventos](#)
- [Vistas del servidor](#)
- [Configuración de cuentas de usuario](#)

Opciones de configuración de informes para los informes de análisis y asesor

Para configurar la URL de los informes de análisis y asesor

1. Haga clic en la pestaña *Admin*.
2. En el navegador *Admin*, haga clic en *Configuración de informes*.

3. En la ventana *Configuración de informes*, haga clic en *Modificar*.
 - En el recuadro URL del análisis, introduzca la URL de Crystal Enterprise Server y haga clic en *Actualizar*.

`http://<IP>/GetReports.asp?APS=<IP>&user=Guest&password=&tab=Analysis`

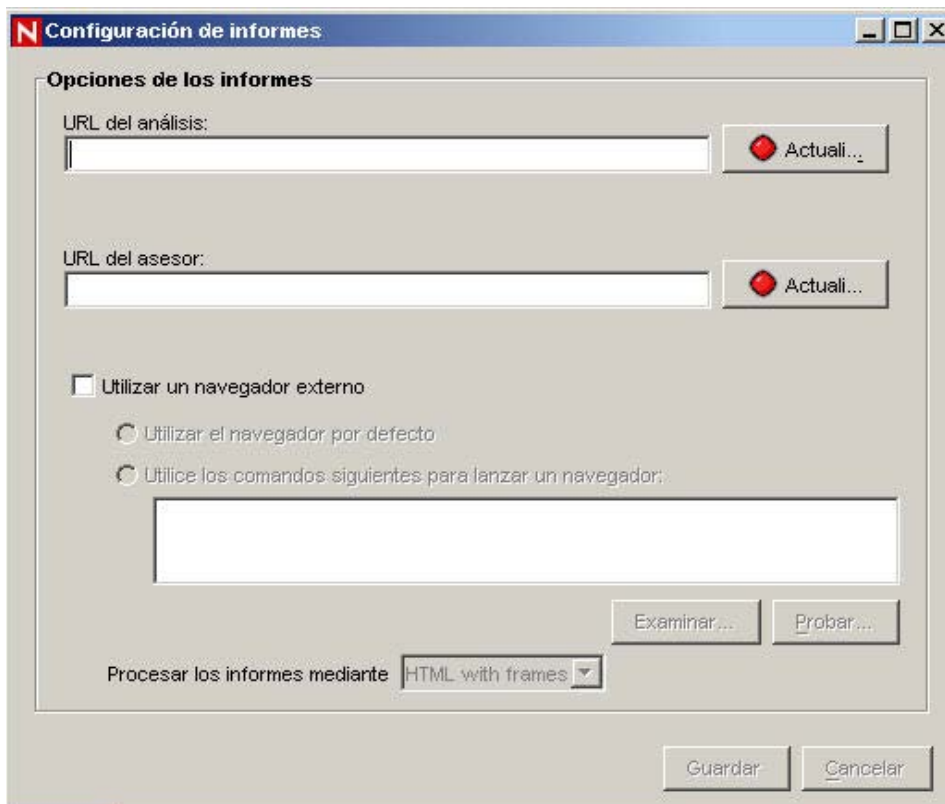
NOTA: <IP> es la dirección IP de Crystal Enterprise Server.

- En el recuadro URL del asesor, introduzca la URL de Crystal Enterprise Server y haga clic en *Actualizar*.

`http://<IP>/GetReports.asp?ASP=<IP>&user=Guest&password=&tab=Advisor`

NOTA: <IP> es la dirección IP de Crystal Enterprise Server.

Para obtener más información, consulte la *Guía de instalación*.



La opción de navegador externo permite utilizar el navegador por defecto u otro navegador. Si se utiliza un navegador distinto del navegador por defecto, la línea de comando debe ir seguida de una %URL%. Por ejemplo:

```
C:\Archivos de programa\Internet Explorer\IEXPLORE.EXE
%URL%
```

4. Espere hasta que el botón *Actualizar* cambie al color verde y haga clic en *Guardar*. Deberá salir del Centro de control de Sentinel y, a continuación, volver a entrar.

Reglas de correlación de Sentinel

La correlación añade inteligencia a la gestión de eventos de seguridad al permitir automatizar el análisis de los flujos de eventos entrantes para buscar patrones de interés. Además, la correlación permite definir reglas que identifican las amenazas importantes y los patrones complejos de ataque con el fin de asignar una prioridad a los eventos e iniciar tareas eficientes de gestión y respuesta para las incidencias.

Las carpetas de reglas son una agrupación lógica de las reglas de correlación. La agrupación de reglas de correlación en carpetas de reglas también permite obtener un conjunto de reglas que se ejecuta el día laborable o un conjunto que se ejecuta por la noche, así como otro conjunto que se ejecuta durante el fin de semana. Esencialmente, se supervisan distintas actividades en función de la hora del día.

Por ejemplo, se pueden habilitar todas las reglas de correlación diurnas a la vez a las 8.00 h de lunes a viernes y también inhabilitar las reglas de correlación nocturnas simultáneamente. Específicamente, si no es necesario agrupar reglas de correlación en carpetas de reglas, se puede crear una sola carpeta de reglas y, a continuación, crear todas las reglas de correlación en dicha carpeta.

No existe ningún límite para el número de usuarios que pueden obtener acceso a las reglas de correlación. Si más de un usuario está editando la misma regla, el último usuario a guardar su trabajo sobrescribirá todas las versiones anteriores guardadas.

En esta sección se tratan los temas siguientes:

- [Carpetas de reglas y reglas](#)
- [Tipos de reglas de correlación](#)
- [Distribución de reglas del motor de correlación](#)
- [Importación y exportación de reglas de correlación](#)
- [Función de la base de datos en el almacenamiento de reglas de correlación](#)
- [Condiciones lógicas](#)

NOTA: No es posible correlacionar en un valor nulo (vacío).

Carpetas de reglas y reglas

A continuación se define la relación entre las carpetas de reglas y las reglas. Las carpetas de reglas y las reglas se muestran en orden jerárquico en la ventana Reglas de correlación.

- Una carpeta de reglas puede contener cero o más reglas.
- El número de carpetas de reglas y reglas sólo se verá limitado por el espacio (de almacenamiento) disponible en el disco.
- Al hacer doble clic en una carpeta de reglas, aparecerá el Editor de reglas para ese tipo de regla de correlación.
- La longitud máxima para los nombres de carpetas de reglas es de 255 caracteres para la vía a la carpeta así como para los nombres de las reglas.
- Las descripciones de las carpetas de reglas y de las reglas pueden tener una longitud máxima de 1.024 caracteres.

Tipos de reglas de correlación

Al definir reglas, existen cuatro tipos de reglas de correlación que se puede elegir. Son los siguientes:

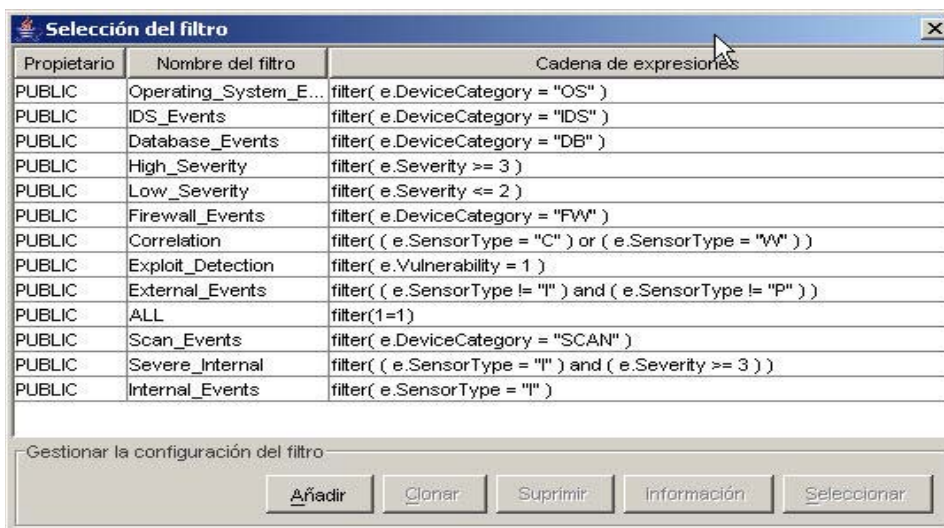
- Lista de vigilancia
- Correlación básica
- Correlación avanzada
- RuleLg sin formato

PRECAUCIÓN: Antes de utilizar este tipo de regla de correlación, deberá familiarizarse con el lenguaje de definición de reglas de correlación RuleLg. Además, si ha cambiado el nombre de una etiqueta, no utilice el nombre original al crear la regla de correlación mediante RuleLg.

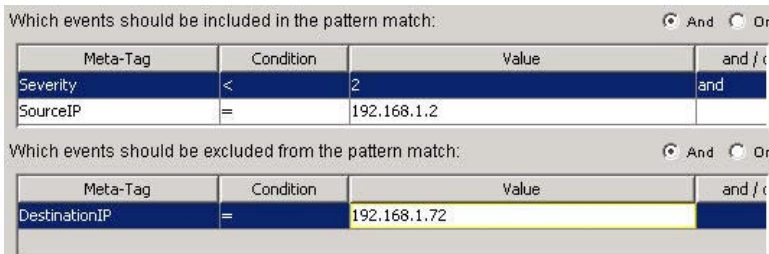
Lista de vigilancia

Se puede elegir entre cuatro tipos diferentes de filtros. Son los siguientes:

- Mostrar todo: permite que pasen todos los eventos.
- Patrón: cualquier expresión regular con una sintaxis tipo grep.
- Gestor de filtros: lista desplegable que muestra el Gestor de filtros para seleccionar o crear un filtro nuevo.



- Generador: permite crear criterios para la inclusión y exclusión de eventos basados en álgebra booleana. Hay dos paneles disponibles (incluir y excluir). Por ejemplo, introduzca los valores aquí:



Correlación básica

Se puede elegir entre cuatro tipos diferentes de filtros. Son los siguientes:

- Mostrar todo: permite que pasen todos los eventos.
- Patrón: cualquier expresión regular con una sintaxis tipo grep.
- Gestor de filtros: lista desplegable que muestra el Gestor de filtros para seleccionar o crear un filtro nuevo.
- Generador: permite crear criterios para la inclusión y exclusión de eventos basados en el álgebra booleana.

Esta regla permite contar el número de veces que se satisfacen determinadas condiciones en un plazo de tiempo específico.

Por ejemplo, una regla de correlación básica puede buscar la misma dirección IP de origen notificada cinco veces en cinco minutos, incluso si los eventos se informan desde dispositivos distintos como, por ejemplo, un sistema de detección de intrusiones (IDS) y un cortafuegos.

Correlación avanzada

Se puede elegir entre cuatro tipos diferentes de filtros. Son los siguientes:

- Mostrar todo: permite que pasen todos los eventos.
- Patrón: cualquier expresión regular con una sintaxis tipo grep.
- Gestor de filtros: lista desplegable que muestra el Gestor de filtros para seleccionar o crear un filtro nuevo.
- Generador: permite crear criterios para la inclusión y exclusión de eventos basados en álgebra booleana.

Esta regla permite realizar las operaciones siguientes:

- Contar el número de veces que se satisfacen determinadas condiciones en un plazo de tiempo específico.
- Incorporar todas las funciones de la regla de correlación básica, así como evaluar eventos en comparación con eventos anteriores.


Por ejemplo, una regla de correlación avanzada puede buscar eventos desde la misma dirección IP de origen hasta la misma dirección IP de destino con el mismo nombre de evento y que se producen tanto dentro como fuera de un cortafuegos (lo que significa que puede que un ataque ha atravesado el cortafuegos).

Correlación RuleLg de regla sin formato

El lenguaje de definición de reglas de correlación RuleLg permite un control completo de la definición de reglas de correlación. Antes de utilizar este tipo de regla de correlación, deberá familiarizarse con el lenguaje de definición de reglas de correlación RuleLg.

Distribución de reglas del motor de correlación

Para utilizar esta función, debe tener el permiso de usuario para iniciar o detener el motor de correlación. El motor de correlación tiene uno de dos estados, activado o desactivado. El estado actual se muestra en el icono.

- Activado: 
- Desactivado: 

Cuando el motor de correlación se encuentra activado, significa que está procesando carpetas de reglas de correlación activas.

Cuando el motor de correlación se encuentra desactivado, se conservan todos los datos en su memoria y no se genera ninguno evento nuevo de correlación. Este estado equivale a la desactivación de todas las carpetas de reglas. La desactivación del motor de correlación no afecta a otras secciones del sistema. Los eventos entrantes aún pasan y llenan de datos la base de datos de Sentinel.

Importación y exportación de reglas de correlación

La función de exportación permite a Sentinel crear y exportar reglas de correlación “empaquetadas” y hacer que estén disponibles para su importación en el sistema. El formato de estos documentos XML se define específicamente para el motor de correlación. Sentinel genera estas reglas preempaquetadas que están disponibles en el portal del cliente en <http://www.esecurityinc.com>.

La capacidad de exportar reglas como documentos XML proporciona ayuda cuando se necesita la asistencia de Sentinel para solucionar problemas con las reglas de correlación. La exportación también es de gran utilidad cuando existe un entorno Sentinel “de producción” y uno de “desarrollo”. Es posible desarrollar y probar reglas de correlación en el entorno de desarrollo y, a continuación, [exportarlas](#) al entorno de producción. La extensión para las reglas de correlación exportadas es.crf.

Función de la base de datos en el almacenamiento de reglas de correlación

Cuando se activa el motor de correlación (un proceso del servidor de Sentinel) en el Centro de control de Sentinel, dicho motor solicita de la base de datos la distribución de la información de las reglas. Cuando las reglas de correlación se modifican y luego se guardan, éstas se envían a la base de datos para su almacenamiento. Las modificaciones de la regla no se verán reflejadas en el motor de correlación, a menos que se satisfaga una de las condiciones siguientes:

- la regla de distribución se inhabilita y luego se habilita
- la regla es recién distribuida

Cuando se modifican reglas de distribución y luego se guardan, éstas se envían a la base de datos para su almacenamiento y al motor de correlación para su aplicación.

Condiciones lógicas para las reglas de correlación

A continuación se incluyen las condiciones lógicas que se utilizan al crear reglas de correlación. Para obtener más información sobre las metaetiquetas, consulte la *Guía de referencia del usuario de Sentinel*.

Condición	Campo de tipo	Descripción
=	numérico cadena	El contenido de la metaetiqueta seleccionada es igual al valor introducido.
!=	numérico cadena	El contenido de la metaetiqueta seleccionada no es igual al valor introducido.
<	numérico	El contenido de la propiedad seleccionada es menor que el valor introducido.

Condición	Campo de tipo	Descripción
>	numérico	El contenido de la metaetiqueta seleccionada es mayor que el valor introducido.
<=	numérico	El contenido de la metaetiqueta seleccionada es menor que o igual al valor introducido.
>=	numérico	El contenido de la metaetiqueta seleccionada es mayor que o igual al valor introducido.
=Metaetiqueta	numérico cadena	El contenido de la metaetiqueta seleccionada en la lista desplegable izquierda es igual al contenido de la metaetiqueta seleccionada a la derecha de la expresión.
!=Metaetiqueta	numérico cadena	El contenido de la metaetiqueta seleccionada en la lista desplegable izquierda no es igual al contenido de la metaetiqueta seleccionada a la derecha de la expresión.
<Metaetiqueta	numérico	El contenido de la metaetiqueta seleccionada en la lista desplegable izquierda es menor que el contenido de la metaetiqueta seleccionada a la derecha de la expresión.
>Metaetiqueta	numérico	El contenido de la metaetiqueta seleccionada en la lista desplegable izquierda es mayor que el contenido de la metaetiqueta seleccionada a la derecha de la expresión.
<=Metaetiqueta	numérico	El contenido de la metaetiqueta seleccionada en la lista desplegable izquierda es menor que o igual al contenido de la metaetiqueta seleccionada a la derecha de la expresión.
>=Metaetiqueta	numérico	El contenido de la metaetiqueta seleccionada en la lista desplegable izquierda es mayor que o igual al contenido de la metaetiqueta seleccionada a la derecha de la expresión.
=Regex	numérico cadena	Utilice un punto final (.) y un asterisco (*) en la cadena para el valor.
Subred	numérico cadena	Una operación de concordancia de subred coincidirá si la dirección IP que se está comparando se encuentra en la misma subred que la especificada en la operación de concordancia de la subred.

Apertura de la ventana Reglas de correlación

La ventana Reglas de correlación permite realizar las operaciones siguientes:

- Carpeta nueva: permite crear una carpeta de reglas nueva
- Regla nueva: permite crear una regla para una carpeta de reglas.
- Copiar carpeta de reglas: permite modificar las carpetas de reglas o reglas modificadas a la vez que se guarda la original.
- Suprimir regla o carpeta de reglas: no es posible recuperar una regla o una carpeta de reglas suprimida tras confirmar la operación.
- Renombrar: permite cambiar el nombre de una regla o carpeta de reglas.
- Importar carpeta de reglas: se abrirá una ventana de navegador.
- Exportar carpeta de reglas: se abrirá una ventana de navegador para exportar la carpeta de reglas como un archivo xml.
- Editar: permite editar y obtener una vista previa de propiedades de las reglas y carpetas.

Apertura de la ventana Reglas de correlación

1. Haga clic en la pestaña *Admin*.
2. En el navegador *Admin*, haga clic en *Reglas de correlación*.

Copia y creación de una carpeta de reglas o una regla

Creación de una carpeta de reglas

1. Abra la ventana Reglas de correlación.
2. Seleccione la carpeta principal que contendrá la nueva carpeta.
3. Haga clic con el botón derecho del ratón en *> Carpeta nueva*.
4. Escriba el nombre de la carpeta de reglas (máximo de 255 caracteres que distinguen entre mayúsculas y minúsculas y sin puntos finales).
5. (Opcional) Escriba la descripción de la regla (máximo de 1.024 caracteres).
6. Haga clic en *Aceptar*.

Creación de una regla

1. Seleccione la carpeta principal que contendrá la nueva regla.
2. Haga clic con el botón derecho del ratón en *> Regla nueva*.
3. Se iniciará el Asistente para reglas; seleccione uno de los tipos de reglas siguientes:
 - Lista de vigilancia
 - Correlación básica
 - Correlación avanzada
 - Formato libre

NOTA: Para obtener una descripción de los tipos de reglas, consulte la sección [Tipos de reglas de correlación](#)

4. Haga clic en *Finalizar*.

Supresión de una carpeta de reglas o de reglas de correlación

Supresión de reglas o de una carpeta de reglas de correlación

1. Abra la ventana Reglas de correlación.
2. Seleccione la carpeta de reglas o la regla que desee suprimir.
3. Haga clic con el botón derecho del ratón en *> Suprimir*.
4. Aparecerá un cuadro de confirmación:
 - Sí: cuando se suprime una carpeta de reglas, también se suprimirán las reglas que ésta contiene. Tras hacer clic en *Aceptar*, no será posible recuperar una regla suprimida.
 - No: permite volver a la ventana Regla de correlación.

Importación o exportación de una carpeta de reglas de correlación

Importación o exportación de una carpeta de reglas de correlación

1. Abra la ventana Reglas de correlación.
2. Seleccione una carpeta de reglas.
3. Haga clic con el botón derecho del ratón en > [*Importar la carpeta de reglas o Exportar la carpeta de reglas*].
 - Importar: se abrirá un navegador de archivos, busque la carpeta de reglas que desee importar y haga clic en *Aceptar*.
 - Exportar: se abrirá un navegador de archivos, busque el dispositivo de destino en el que desea escribir la carpeta de reglas y haga clic en *Aceptar*. La carpeta de reglas se exportará como un archivo crf.

Edición en la ventana de correlación

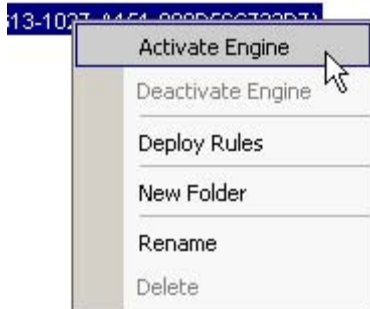
Edición en la ventana de correlación

1. Abra la ventana Reglas de correlación.
2. Haga clic con el botón derecho en > *Editar*.
3. Edite la regla y haga clic en *Finalizar*.

Activación o desactivación de un motor de correlación

Activación o desactivación de un motor de correlación

1. Abra la ventana Gestor de motores de correlación.
2. Resalte y haga clic con el botón derecho en un *motor de correlación* > *Activar el motor o Desactivar el motor*.



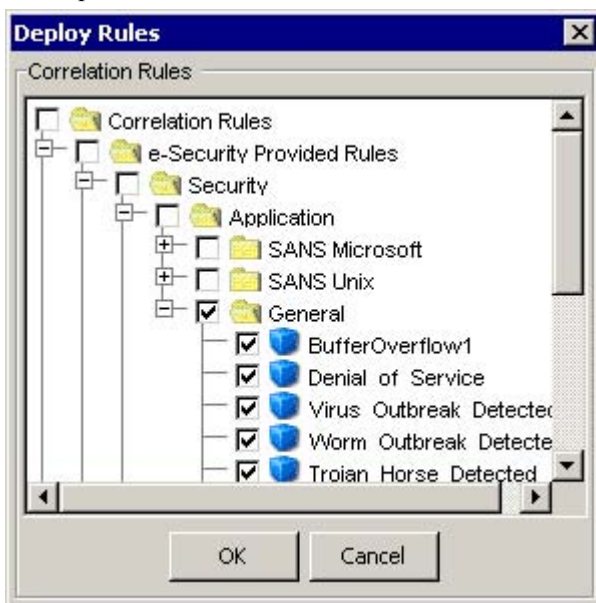
Distribución de reglas de correlación

Distribución de reglas de correlación

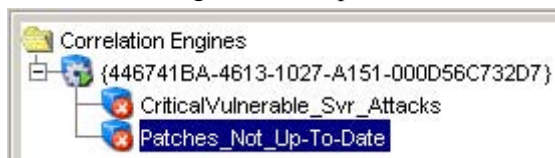
1. Abra la ventana Gestor de motores de correlación.



2. Haga clic con el botón derecho del ratón en (cualquier carpeta de la ventana o resalte el motor para distribuir la regla en dicha ubicación) > *Distribuir las reglas*.
3. Coloque una marca de verificación junto a las reglas que desea distribuir. Haga clic en *Aceptar*.

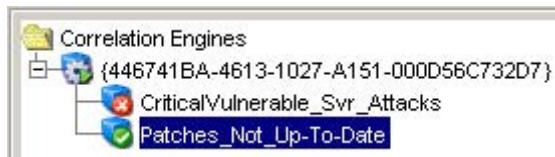


- Para iniciar la regla, debe desplazarla hacia un motor de correlación.



NOTA: Las reglas se distribuyen en estado habilitado.

- En el motor de correlación, resalte la regla y haga clic con el botón derecho del ratón en > *Habilitar regla*.



Vistas del servidor

Las vistas de servidor permiten realizar las operaciones siguientes:

- Monitorizar el estado de todos los procesos del servidor de Sentinel en todo el sistema.
 - Servidor de comunicaciones.
 - Correlation Engine
 - DAS_Binary
 - DAS_iTrac
 - DAS_Query
 - DAS_RT
 - Query Manager
 - RuleLg Checker
 - Sonic Lock Remover

NOTA: En Windows, el servidor de comunicaciones se ejecuta como un servicio de Windows, de modo que no puede monitorizarse por las vistas del servidor. Para monitorizar el servidor de comunicaciones en Windows, utilice el Gestor de servicios de Windows.

El proceso Sonic Lock Remover sólo se habilita en Windows. Si no se ha habilitado un proceso en un servidor en particular, la columna Habilitado se definirá en “0” y la columna Estado aparecerá como NOT_INITIALIZED.

Processes Health	Starts	AutoRestarts	StartTime	State	UpTime	Version
desk1						
Communication Server	0	0		NOT_INITIALIZED		5.1.2.0
Correlation Engine	1	0	04/17/2006 11:43:3...	Running	18h 45:53	5.1.2.0
DAS_Aggregation	1	0	04/17/2006 11:43:1...	Running	18h 46:14	5.1.2.0
DAS_Binary	1	0	04/17/2006 11:43:1...	Running	18h 46:14	5.1.2.0
DAS_Query	1	0	04/17/2006 11:43:1...	Running	18h 46:14	5.1.2.0
DAS_RT	1	0	04/17/2006 11:43:1...	Running	18h 46:14	5.1.2.0
DAS_iTRAC	1	0	04/17/2006 11:43:1...	Running	18h 46:14	5.1.2.0
Query Manager	1	0	04/17/2006 11:43:3...	Running	18h 45:54	5.1.2.0
RuleLg Checker	1	0	04/17/2006 11:43:3...	Running	18h 45:54	5.1.2.0
Sonic Lock Remover	1	0	04/17/2006 11:43:1...	Running	18h 46:15	5.1.2.0

- Iniciar, detener o reiniciar procesos: estas acciones pueden realizarse en un proceso haciendo clic con el botón derecho en la entrada del proceso.


NOTA: Las acciones con el botón derecho del ratón en el servidor de comunicaciones no se habilitan porque si se detiene el servidor de comunicaciones daría como resultado la pérdida de contacto de todos los procesos.

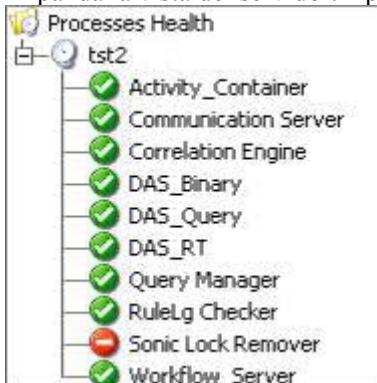
Los términos *Inicios* y *Reinicios automáticos*, en el contexto de la *vista de servidor*, se definen de la manera siguiente:

- Inicios: el número de veces que se ha iniciado el proceso, sea cual sea el motivo. Esto incluye los inicios que provoca el usuario a través de la interfaz de usuario (GUI) o que se realizan automáticamente.
- Reinicios automáticos: el número de veces que el proceso se ha reiniciado automáticamente. Puesto que esto sólo se aplica a casos de reinicio automático, no se aplica a los reinicios provocados por un usuario. Este campo es de gran utilidad a la hora de determinar si se ha cerrado el proceso (por ejemplo, debido a un error) y la vigilancia de Sentinel lo ha reiniciado automáticamente.

Monitorización de un proceso

Monitorización de un proceso

1. Haga clic en la pestaña *Admin*.
 2. Haga clic en *Vistas de servidor*.
- 
3. Haga doble clic en una vista. Aparecerá una vista.
 4. Expanda la vista del servidor. Aparecerá una lista de todos los procesos.



Creación de una vista del servidor

Creación de una vista del servidor

1. Haga clic en la pestaña *Admin*.
2. Haga clic en *Vistas de servidor*.




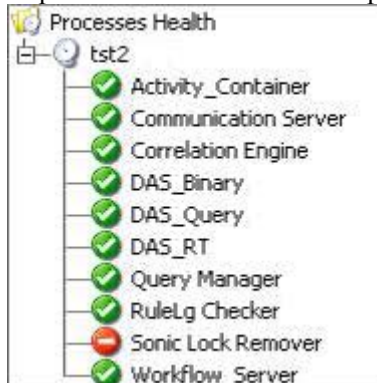
3. Para crear una vista nueva, haga clic en *Añadir vista*.
 - Introduzca el nombre de la opción.
 - Para organizar los campos que se debe visualizar, haga clic en *Campos*.
 - Para agrupar títulos diferentes, haga clic en *Agrupar*.
 - Para ordenar por título, haga clic en *Ordenar*.
 - Para filtrar la vista, haga clic en *Filtro*.
4. Haga clic en *Aceptar* y, a continuación, en *Guardar*.

Inicio, detención y reinicio de procesos

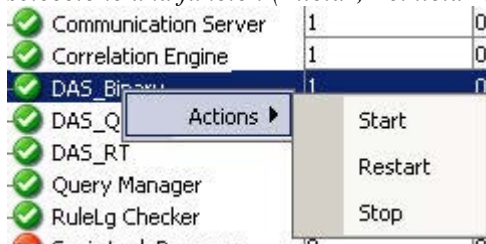
El servidor de comunicaciones no puede detenerse mediante esta función.

Inicio, detención y reinicio de procesos

1. Haga clic en la pestaña *Admin*.
 2. Haga clic en *Vistas de servidor*.
- 
3. Haga doble clic en una vista. Aparecerá una vista.
 4. Expanda la vista del servidor. Aparecerá una lista de todos los procesos.



5. Seleccione un proceso, haga clic con el botón derecho del ratón en *> Acciones > seleccione una función (Iniciar, Reiniciar o Detener)*.



Filtros

Los filtros permiten procesar datos según criterios específicos para los eventos en tiempo real y para los usuarios del sistema. Además, permite gestionar los datos que se muestran en el Centro de control de Sentinel. El motor de filtros controla las ventanas de eventos en tiempo real al mantener la estructura de datos para cada filtro de seguridad. Los filtros impiden que los usuarios visualicen eventos no autorizados y permiten abandonar eventos que los usuarios no desea visualizar. Los filtros se crean en la pestaña Admin del Centro de control de Sentinel.

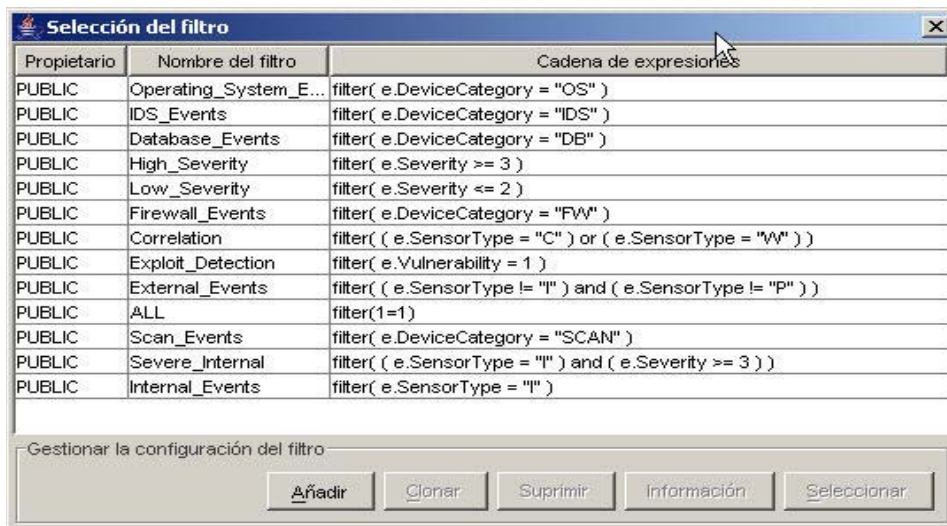
NOTA: Los caracteres siguientes no son válidos para los nombres de filtro: \$ # . * & : < > .

Existen tres tipos de filtros:

- [Filtros públicos](#)
- [Filtros privados](#)
- [Filtros globales](#)

Filtros públicos

Los filtros públicos son propiedad del sistema y se pueden utilizar como filtros de seguridad o de visualización. Los filtros de seguridad se basan en los permisos de usuario y los filtros de visualización determinan los eventos que se mostrarán en las tablas, los diagramas y los gráficos de eventos en tiempo real.



Propietario	Nombre del filtro	Cadena de expresiones
PUBLIC	Operating_System_Events	filter(e.DeviceCategory = "OS")
PUBLIC	IDS_Events	filter(e.DeviceCategory = "IDS")
PUBLIC	Database_Events	filter(e.DeviceCategory = "DB")
PUBLIC	High_Severity	filter(e.Severity >= 3)
PUBLIC	Low_Severity	filter(e.Severity <= 2)
PUBLIC	Firewall_Events	filter(e.DeviceCategory = "FW")
PUBLIC	Correlation	filter((e.SensorType = "C") or (e.SensorType = "W"))
PUBLIC	Exploit_Detection	filter(e.Vulnerability = 1)
PUBLIC	External_Events	filter((e.SensorType != "I") and (e.SensorType != "P"))
PUBLIC	ALL	filter(1=1)
PUBLIC	Scan_Events	filter(e.DeviceCategory = "SCAN")
PUBLIC	Severe_Internal	filter((e.SensorType = "I") and (e.Severity >= 3))
PUBLIC	Internal_Events	filter(e.SensorType = "I")

Gestionar la configuración del filtro

Añadir Clonar Suprimir Información Seleccionar

Filtros privados

Los filtros privados son propiedad del usuario y son filtros de visualización que se pueden compartir si el usuario tiene el permiso de visualización de filtros privados.

Filtros globales

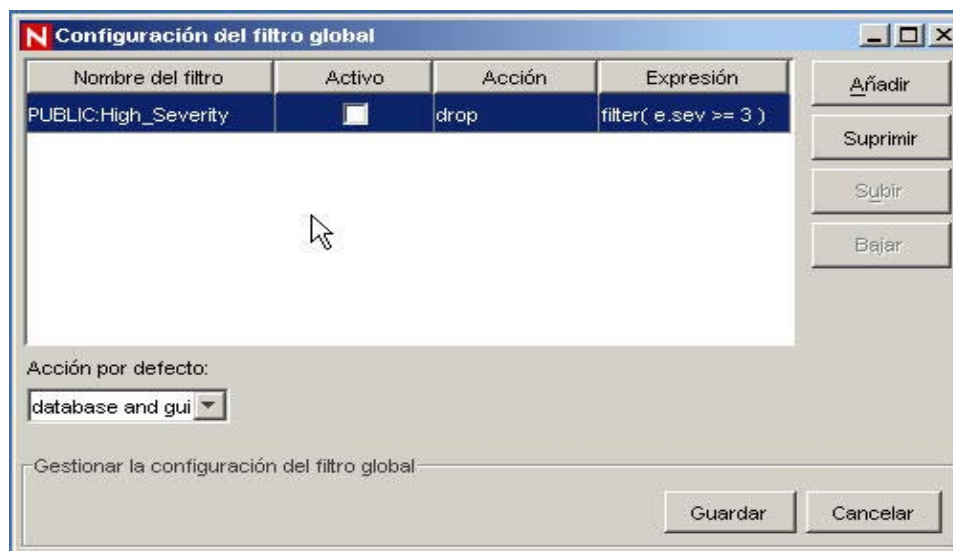
Los filtros globales se clasifican como filtros públicos y se procesan de manera secuencial en el Gestor de recopiladores para cada evento hasta que se encuentre una concordancia. La evaluación de filtro global se detendrá para dicho evento y se toma la acción de filtro global que concuerda para dicho evento. El orden de evaluación de los filtros globales es descendente, tal como se muestra en la consola. Se pueden habilitar e inhabilitar según sea necesario.

Los filtros globales realizan permiten realizar lo siguiente:

- Habilitar una acción global en los eventos como, por ejemplo, abandonar un evento, encaminar eventos a la base de datos únicamente o encaminar eventos a la base de datos y al Centro de control de Sentinel.
- Son procesados mediante el Gestor de recopiladores del asistente.
- Se configuran en la pestaña Admin, bajo la opción Configuración del filtro global, en la que se pueden habilitar e inhabilitar.
- Abandonar eventos
- Encaminar eventos solamente a la base de datos
- Encaminar eventos a la base de datos y al Centro de control de Sentinel

A través de la ventana Configuración del filtro global se puede realizar lo siguiente:

- [Crear un filtro global](#)
- [Reorganizar un filtro global](#)
- [Suprimir un filtro global](#)



Creación de un filtro global

Creación de un filtro global

1. Haga clic en la pestaña *Admin*.
2. Haga clic en *Admin > Configuración del filtro global*, o bien seleccione *Configuración del filtro global* en el árbol de navegación.
3. En la ventana Configuración del filtro global, haga clic en *Modificar* y, a continuación, en *Añadir*.

4. En la fila vacía, haga clic en la columna *Nombre del filtro*.
5. Seleccione un filtro y haga clic en *Seleccionar* o *Añadir* (si se debe crear un filtro).
6. En la columna *Activo*, haga clic en el recuadro *Activo*.
7. En la columna *Activo*, seleccione la acción que el filtro global tendrá sobre los eventos que pasarán por dicho filtro. Si un evento no satisface ninguno de los filtros globales activos, la acción por defecto determinará cómo se procesará el evento.
El cuadro *Acción por defecto* se puede definir con una de las opciones siguientes:
 - abandonar: los eventos no pasarán al Centro de control de Sentinel ni a la base de datos del servidor de Sentinel.
 - base de datos: los eventos se enviarán directamente a la base de datos, sin pasar por el Centro de control de Sentinel.
 - base de datos y GUI: los eventos se enviarán al Centro de control de Sentinel y a la base de datos del servidor de Sentinel.
8. Siga añadiendo filtros hasta que haya finalizado.
9. Haga clic en *Guardar*.

Reorganización de los filtros globales

Reorganización de los filtros globales

1. En la ventana *Configuración del filtro global*, haga clic en *Modificar*.
2. Seleccione un filtro y haga clic en *Subir* o *Bajar* para desplazarse a otra ubicación en la lista.
3. Haga clic en *Guardar*.

Supresión de un filtro global

NOTA: Al suprimir un filtro global, no aparecerá ningún mensaje de confirmación.

Para suprimir un filtro global

1. En la ventana *Configuración del filtro global*, haga clic en *Modificar*.
2. Seleccione un filtro de la lista y haga clic en *Suprimir*.
3. Haga clic en *Guardar*.

Configuración de filtros públicos y privados

La configuración de filtros públicos y privados permite realizar lo siguiente:

- [Añadir un filtro](#)
- [Ver los detalles de un filtro](#)
- [Crear un clon de un filtro](#)
- [Suprimir un filtro](#)
- [Modificar un filtro](#)

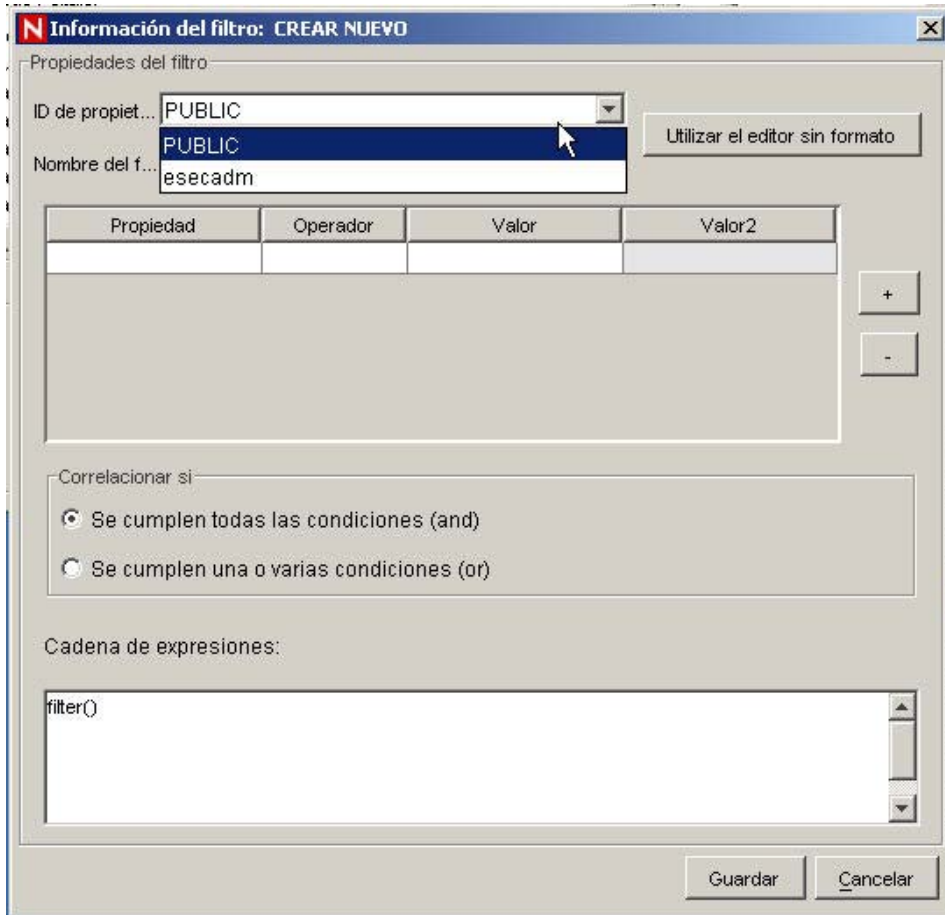
Propietario	Nombre del filtro	Cadena de expresiones
PUBLIC	Operating_System_E...	filter(e.DeviceCategory = "OS")
PUBLIC	IDS_Events	filter(e.DeviceCategory = "IDS")
PUBLIC	Database_Events	filter(e.DeviceCategory = "DB")
PUBLIC	High_Severity	filter(e.Severity >= 3)
PUBLIC	Low_Severity	filter(e.Severity <= 2)
PUBLIC	Firewall_Events	filter(e.DeviceCategory = "FW")
PUBLIC	Correlation	filter((e.SensorType = "C") or (e.SensorType = "W"))
PUBLIC	Exploit_Detection	filter(e.Vulnerability = 1)
PUBLIC	External_Events	filter((e.SensorType != "I") and (e.SensorType != "P"))
PUBLIC	ALL	filter(1=1)
PUBLIC	Scan_Events	filter(e.DeviceCategory = "SCAN")
PUBLIC	Severe_Internal	filter((e.SensorType = "I") and (e.Severity >= 3))
PUBLIC	Internal_Events	filter(e.SensorType = "I")

Gestionar la configuración del filtro

Adición de un filtro

Para añadir un filtro público y privado

1. Haga clic en la pestaña *Admin*.
2. Haga clic en *Admin > Gestor de filtros*, o bien seleccione *Gestor de filtros* en la carpeta *Configuración del filtro del navegador*.
3. Haga clic en *Añadir*.
4. Seleccione un ID de propietario (público o privado [propiedad del usuario]).



5. Introduzca un nombre para el filtro.
6. El editor de tabla es la selección por defecto para la edición del contenido.

NOTA: De manera opcional, puede hacer clic en Utilizar el editor sin formato para que aparezca un editor sin formato, que permite crear expresiones complejas que no son posibles en el editor de tabla. No obstante, una vez que se modifique la expresión con el editor sin formato, el editor de tabla no se podrá utilizar con la misma.

7. Seleccione los criterios para las columnas siguientes:
 - Propiedad
 - Operador
 - Valor

Las selecciones se muestran en el cuadro Cadena de expresiones.
8. En el cuadro Correlacionar si, haga clic en una de las opciones siguientes:
 - Se cumplen todas las condiciones (and)
 - Se cumplen una o varias condiciones (or)

9. Para crear otra expresión de filtro, haga clic en (+) *Crear una nueva expresión* para filtros para añadir otra fila a la tabla de expresiones de filtro.
10. Para eliminar una expresión de filtro, selecciónela de la tabla y haga clic en (-) *Eliminar la expresión seleccionada*.
11. Haga clic en *Guardar*.

Para crear un clon de un filtro público y privado

La clonación es una manera cómoda de duplicar un filtro para garantizar la coherencia de los criterios en un grupo de filtros o usuarios.

Para crear un clon de un filtro público y privado

1. Abra la ventana Gestor de filtros.
2. Haga clic en *Clonar*.
3. Introduzca un nuevo nombre para el filtro.
4. Cambie los criterios del filtro original según sea necesario.
5. Haga clic en *Guardar*.

Modificación de un filtro público y privado

Para modificar un filtro público y privado

1. Abra el Gestor de filtros.
2. Seleccione un filtro y haga clic en *Información*.
3. Cambie los criterios según sea necesario. No es posible cambiar el ID de propietario ni el *nombre del filtro*.
4. Haga clic en *Guardar*.

Visualización de la información de un filtro público y privado

Para visualizar un filtro público o privado

1. Abra la ventana Gestor de filtros.
2. Seleccione un filtro y haga clic en *Información*.

Supresión de un filtro público y privado

Para suprimir un filtro público y privado

1. Abra la ventana *Gestor de filtros*.
2. Seleccione un filtro y haga clic en *Suprimir*.
3. Aparecerá una ventana de confirmación.

Ajustes del menú de configuración

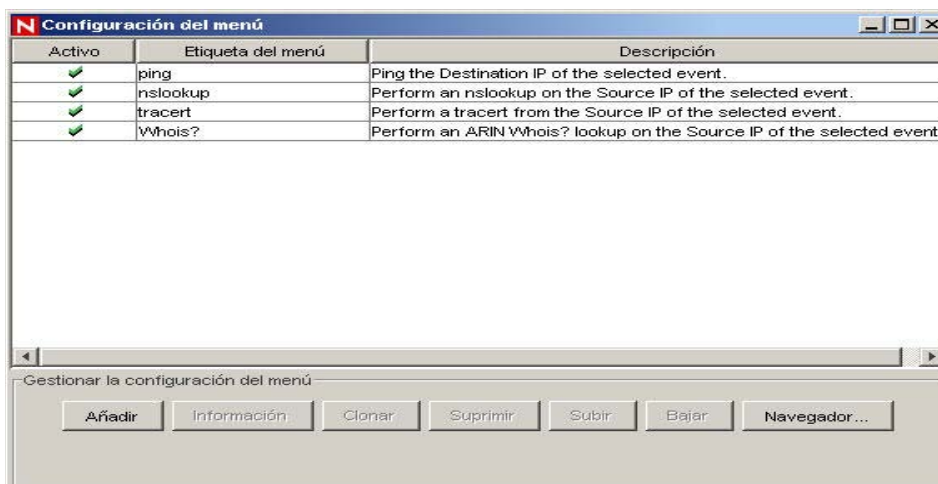
Para utilizar esta función, se debe disponer del permiso de usuario Menú de configuración.

Utilice la ventana Configuración del menú para crear los elementos de menú que aparecerán en el menú Evento, que aparece en cualquier tabla que muestre un evento (p. ej., las ventanas Tiempo real del evento, Instantánea, Eventos de incidencias, etc.) al seleccionar uno o varios eventos y hacer clic con el botón derecho del ratón. Sentinel dispone de los siguientes elementos por defecto para la configuración del menú que se pueden clonar, activar o desactivar:

- ping: para realizar un ping a la dirección IP de destino del evento seleccionado
- nslookup: para realizar una operación de nslookup en la dirección IP de origen del evento seleccionado
- traceroute (tracert en MS SQL): para realizar una operación de traceroute desde la dirección IP de origen del evento seleccionado al servidor de Sentinel
- Whois?: para realizar una búsqueda de ARIN Whois? en la dirección IP de origen del evento seleccionado.

La ventana Configuración del menú permite realizar lo siguiente:

- [Añadir una opción al menú Configuración del menú](#)
- [Crear un clon de una opción de Configuración del menú](#)
- [Modificar una opción de Configuración del menú](#)
- [Visualizar los parámetros de una opción de Configuración del menú](#)
- [Activar o desactivar una opción de Configuración del menú](#)
- [Reorganizar las opciones del menú de evento](#)
- [Suprimir una opción de Configuración del menú](#)
- [Añadir una función de navegador a la opción de Configuración del menú](#)



Adición de una opción al menú Configuración del menú

NOTA: Si ha cambiado el nombre de una etiqueta, por ejemplo, de VarCliente24 a NombreDirectiva, deberá utilizar el nombre nuevo al configurar los parámetros.

Para añadir una opción al menú Configuración del menú

1. Haga clic en la pestaña *Admin*.
2. En el navegador Admin, haga clic en *Admin > Configuración del menú*.
3. En el cuadro de diálogo Configuración del menú, introduzca los elementos siguientes:
 - Nombre
 - Descripción
 - Acción: ejecutar un comando o iniciar un navegador
 - Utilizar el navegador: si selecciona la acción “Ejecutar comando” y la configuración del navegador se ha definido para “Utilizar un navegador externo” (consulte [Edición de la configuración del navegador para la configuración del menú](#) para editar la configuración del navegador), se podrá seleccionar la opción Utilizar el navegador. Si selecciona esta opción, los resultados del comando se mostrarán mediante la configuración del navegador para la configuración del menú para el Centro de control de Sentinel.
 - Tipo de archivo: si selecciona la acción “ejecutar comando”, la configuración del navegador se ha definido para “Utilizar un navegador externo” y ha seleccionado la opción “Utilizar el navegador”, tendrá la opción de configurar el tipo de archivo para el resultado de este comando.
 - Línea de comando/URL

NOTA: En UNIX, el guión o la aplicación, o bien el enlace simbólico al guión o a la aplicación, debe encontrarse en el directorio \$ESEC_HOME\sentinel\exec. Para cualquier guión, aplicación o enlace simbólico, introduzca solamente el comando. No se tomará en cuenta ninguna vía.

NOTA: En Windows (correlación), el guión o la aplicación deben encontrarse en uno de los directorios que figuran en las variables de entorno de Windows. No se tomará en cuenta ninguna vía.

NOTA: En Windows (sin correlación), la introducción de la vía es opcional. Si se introduce un comando sin ninguna vía, el directorio por defecto será %ESEC_HOME%\sentinel\bin y el resto de vías especificadas en las variables de entorno.

-
- Parámetros: deben cerrarse mediante el símbolo de porcentaje (p. ej., %NombreEvento%)

NOTA: Para obtener una lista de las etiquetas disponibles que se pueden utilizar para especificar parámetros, haga clic en la opción Ayuda del recuadro de diálogo Configuración del menú, o bien consulte el capítulo sobre metaetiquetas en la *Guía de referencia del usuario de Sentinel*.

4. Haga clic en *Aceptar*. La nueva opción se añadirá a la lista de elementos de menú de la ventana Configuración del menú.

NOTA: Para obtener un ejemplo, resalte cualquiera de los elementos de menú por defecto y haga clic en *Información*. A continuación se muestra una configuración nslookup:

The image shows a 'Menu Item' configuration dialog box with the following fields and values:

- Name: nslookup
- Description: Perform an nslookup on the Source IP of the selected event.
- Action: Execute Command (selected from a dropdown menu)
- Use browser:
- File type: (empty)
- Command / URL: nslookup
- Parameters: %SourceIP%

Clonación de una opción del menú Configuración del menú

Para clonar una opción del menú Configuración del menú

1. Abra la ventana Configuración del menú.
2. Seleccione un elemento de menú de la tabla y haga clic en *Clonar*.
3. En el cuadro de diálogo Configuración del menú, edite los elementos siguientes:
 - Nombre
 - Descripción
 - Acción
 - Si se debe utilizar un navegador o no. Para obtener más información, consulte [Adición de una función de navegador a la opción Configuración del menú](#).
 - Línea de comando/URL
 - Parámetros
 - Seleccione una acción:
 - Ejecutar un comando
 - Iniciar navegador Web.

NOTA: Para obtener una lista de las etiquetas disponibles que se pueden utilizar para especificar parámetros, haga clic en la opción Ayuda del cuadro de diálogo Configuración del menú, o bien consulte el capítulo sobre metaetiquetas en la *Guía de referencia del usuario* de Sentinel.

4. Haga clic en *Aceptar*. La nueva opción se añadirá a la lista de elementos de menú de la ventana Configuración del menú.

Modificación de una opción del menú Configuración del menú

Para modificar una opción del menú Configuración del menú

1. Abra la ventana Configuración del menú.
2. Haga doble clic en una opción de menú.
3. Escriba los cambios deseados y haga clic en *Aceptar*.

Visualización de los parámetros de opción de Configuración del menú

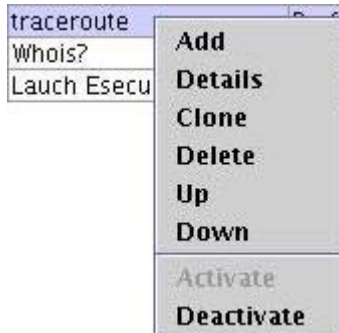
Para visualizar los parámetros de una opción del menú Configuración del menú

1. Abra la ventana Configuración del menú.
2. Resalte un elemento del menú y haga clic en *Información*.

Activación o desactivación de una opción del menú Configuración del menú

Para activar o desactivar una opción del menú Configuración del menú

1. Abra la ventana Configuración del menú.
2. Seleccione una opción de menú, haga clic con el botón derecho del ratón y seleccione *Activar* o *Desactivar*.



Reorganización de las opciones del menú Evento

Para desplazar hacia arriba o hacia abajo una opción del menú Evento

1. Abra la ventana Configuración del menú.
2. Seleccione una opción de menú y haga clic en *Subir* o bien en *Bajar*.

Supresión de una opción del menú Configuración del menú

Para suprimir una opción del menú Configuración del menú

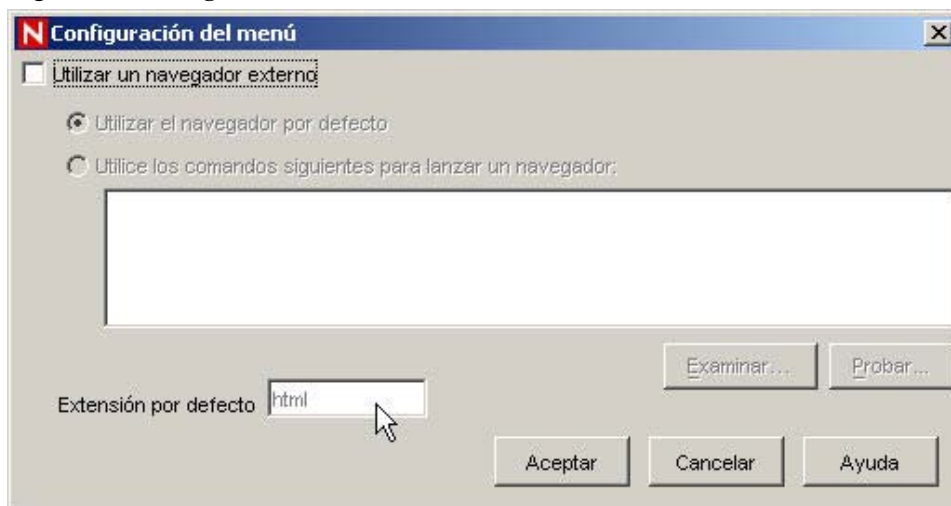
1. Abra la ventana Configuración del menú.
2. Seleccione una opción de menú y haga clic en *Suprimir*.
 - Haga clic en *Sí* para suprimir la opción de menú.
 - Haga clic en *No* para conservar la opción de menú.

Edición de los parámetros del navegador para la opción Configuración del menú

Esta opción permite enviar los resultados de la opción Configuración del menú a un navegador externo. El navegador externo puede ser cualquier aplicación; no está limitado a navegadores de Internet. Al cambiar la extensión del archivo, se puede iniciar cualquier aplicación asociada a dicha extensión. Por ejemplo, la extensión txt normalmente está asociada a la aplicación Bloc de notas. También tiene la opción de iniciar un programa específico, por ejemplo, puede abrir un archivo.txt mediante Wordpad u otro editor.

Edición de la configuración del navegador para la configuración del menú

1. Abra la ventana Configuración del menú.
2. Haga clic en *Navegador*.



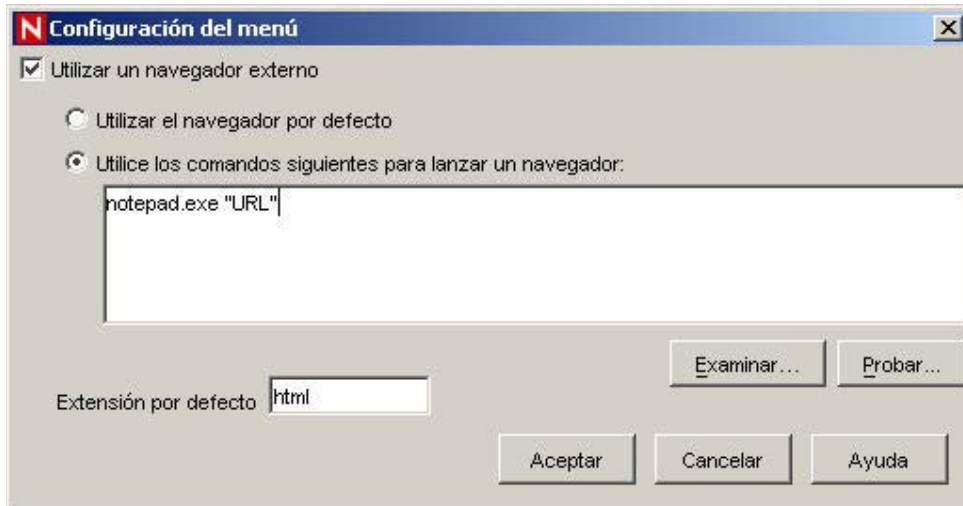
Si selecciona la casilla “Utilizar el navegador” al definir una opción Configuración del menú con la función del navegador establecida según la configuración indicada anteriormente, la opción Configuración del menú funcionará como si no se hubiera seleccionado dicha casilla.

Si activa la casilla “Utilizar un navegador externo”, tendrá la opción de realizar una de las opciones siguientes:

- “Utilizar el navegador por defecto”: permite utilizar el navegador (aplicación) por defecto asociado a la extensión del archivo definida en el campo Extensión del archivo.
- “Utilice los comandos siguientes para lanzar un navegador”: permite especificar una aplicación para iniciar. Si se utiliza un navegador distinto del navegador por defecto, la línea de comandos debe seguirse de una %URL%. Por ejemplo:

```
C:\Archivos de programa\Internet Explorer\IEXPLORE.EXE
  %URL%
```

A continuación se proporciona un ejemplo en el que el resultado de la opción de menú se iniciará en Bloc de notas.



3. Tras definir la configuración, haga clic en *Aceptar*.

Estadísticas DAS

Esta función está destinada para realizar la monitorización interna del sistema. No está diseñada para el usuario medio. La función Estadísticas DAS monitoriza los elementos siguientes:

- DAS_Binary
- DAS_Query
- DAS_rt

Las estadísticas se dividen de la manera siguiente:

- Servicio: nombre del servicio como, por ejemplo, DAS_Query
- Hora: el tiempo desde la última actualización
- Núm.: el número de solicitudes que se han procesado para esta entrada
- Tiempo de espera: el tiempo de espera medio en segundos de una solicitud antes de que se inicie su procesamiento
- Tiempo de ejecución: tiempo medio de procesamiento de una solicitud (en segundos)
- #espera: tamaño medio de la cola de espera
- #ejecución: tamaño medio de la cola de ejecución

La información se divide en tres secciones:

- Solicitudes
- Servicios
- Grupos de subprocesos

En la sección Solicitudes, mantiene todas las solicitudes por canal (por ejemplo services. CorrelationService). En la sección Servicios, hace lo mismo por servicio. A veces, proporciona un desglose al adjuntar “<categoría>” debajo del nombre; por ejemplo Services. CorrelationService o Services.RemoteObjectService.EMap.getMapPK.

En la sección Servicios, todas las llamadas de método remoto de los servicios definidos por el usuario (los servicios XML) se encuentran bajo services. RemoteObjectService.Debajo, coloca el nombre del servicio (EMap en el ejemplo anterior) y, si se le solicita, el nombre del método (getMapPK en el ejemplo anterior).

Cuando un servidor recibe una solicitud como, por ejemplo, consulta DAS, se creará y programará una tarea. A continuación, la tarea se asigna a un grupo de subprocesos para su ejecución. Puede haber más de un grupo de subprocesos y un grupo de subprocesos puede prestar servicio a varios servicios. Por ese motivo, es posible que una solicitud tenga que esperar hasta que haya un subproceso disponible, incluso si el servicio no se está utilizando de forma intensa. Si las estadísticas indican que el tiempo de espera de una solicitud es elevado y el número de solicitudes para dicho servicio es bajo, compruebe la información sobre los grupos de subprocesos.

Los números junto a una entrada representan la suma de todos sus elementos secundarios. Por lo tanto, requests 15 significa que hay 15 solicitudes para todas las llamadas de método de solicitud. Debajo, requests.configurations 1 significa que 1 de las 15 solicitudes corresponden a configuraciones, requests.esecurity.correlation.config 2 significa que 2 de las 15 corresponden a esecurity.correlation.config y así consecutivamente.

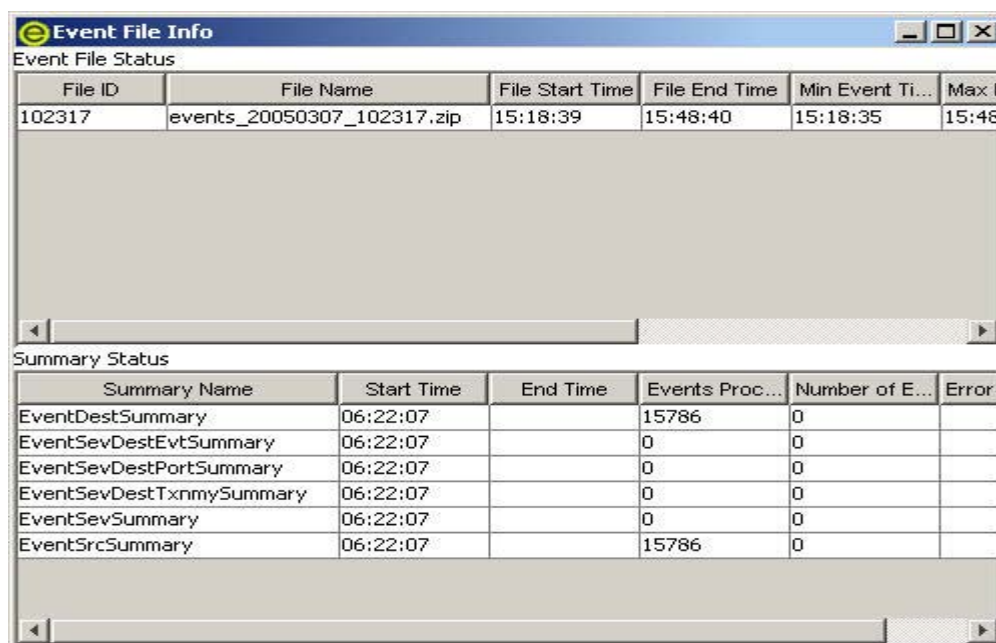
Servicio	Hora	Nombre	Núm.	Esperar (seg.)	Ejecutar (seg.)	#En espera	#En ejecución
DAS_Query-0...	14:30:00						
		ThreadPools	369	0,001	0,041	0,0	0,0
		ThreadPools....	79	0,001	0,187	0,0	0,0
		ThreadPools....	15	0,001	0,030	0,0	0,0
		ThreadPools....	9	0,002	0,118	0,0	0,0
		ThreadPools....	2	0,000	0,320	0,0	0,0
		ThreadPools....	0			0,0	0,0
		ThreadPools....	36	0,001	0,336	0,0	0,0
		ThreadPools....	1	0,000	0,563	0,0	0,0
		ThreadPools....	14	0,002	0,000	0,0	0,0
		ThreadPools....	1	0,000	0,000	0,0	0,0
		ThreadPools....	1	0,000	0,000	0,0	0,0
		ThreadPools.T...	290	0,001	0,001	0,0	0,0
		ThreadPools.T...	3	0,005	0,000	0,0	0,0
		ThreadPools.T...	15	0,000	0,018	0,0	0,0
		ThreadPools.T...	1	0,000	0,078	0,0	0,0
		ThreadPools.T...	1	0,015	0,063	0,0	0,0
		ThreadPools.T...	180	0,001	0,000	0,0	0,0
		ThreadPools.T...	90	0,001	0,000	0,0	0,0
		requests	139	0,036	0,107	0,0	0,0
		requests.LOC...	2	0,031	0,320	0,0	0,0
		requests.conf...	9	0,007	0,118	0,0	0,0
		requests.db...	0			0,0	0,0
		requests.displ...	1	0,656	0,563	0,0	0,0
		requests.es...	15	0,023	0,030	0,0	0,0
		requests.es...	36	0,033	0,336	0,0	0,0
		requests.hmo...	30	0,019	0,003	0,0	0,0
		requests.hmo...	30	0,027	0,000	0,0	0,0
		requests.syn...	0			0,0	0,0
		requests.user	14	0,032	0,000	0,0	0,0

La información puede ser de gran utilidad ya que muestra lo que está sucediendo. El número de solicitudes es de especial utilidad, ya que se puede ver a dónde se dirigen o dónde se concentran. La columna #espera es de gran utilidad, ya que muestra el nivel de actividad del servidor. Ese número debe ser bajo. Si es elevado, las solicitudes nuevas (incluso para tareas sencillas) deberán esperar hasta que finalicen las tareas lentas. Esto no es una situación deseable. El tiempo de ejecución medio es un elemento importante, ya que indica las solicitudes que están demorando en comparación con la espera de otras.

Información sobre el archivo de eventos

En el panel superior se muestra la información de estado para cada archivo de eventos. El estado representa el estado de los archivos de eventos al abrirse la ventana. El panel no mostrará el estado de ningún estado anterior del archivo de eventos. Proporciona el ID de archivo (el ID de archivado en la tabla de eventos), el nombre de archivo y estadísticas sobre el archivo (si está completo, la hora de inicio y finalización de la escritura en el archivo, el tiempo mínimo y máximo de eventos que contiene el archivo, etc.).

Cuando se resalta un archivo en el panel superior, el panel inferior mostrará el estado de resumen para dicho archivo de eventos. En el panel inferior se muestra el nombre del resumen, la hora de inicio y finalización de procesamiento, el número de eventos procesados y si existen mensajes de error.



The screenshot shows a window titled 'Event File Info' with a sub-header 'Event File Status'. It contains a table with the following data:

File ID	File Name	File Start Time	File End Time	Min Event Ti...	Max E
102317	events_20050307_102317.zip	15:18:39	15:48:40	15:18:35	15:48

Below this is a 'Summary Status' section with another table:

Summary Name	Start Time	End Time	Events Proc...	Number of E...	Error
EventDestSummary	06:22:07		15786	0	
EventSevDestEvtSummary	06:22:07		0	0	
EventSevDestPortSummary	06:22:07		0	0	
EventSevDestTxnmySummary	06:22:07		0	0	
EventSevSummary	06:22:07		0	0	
EventSrcSummary	06:22:07		15786	0	

Configuraciones del usuario

Para utilizar esta función, debe tener el permiso de usuario Configuración del usuario y poder trabajar en la ventana correspondiente.

La ventana Configuración del usuario permite realizar lo siguiente:

- [Crear una cuenta de usuario](#)
- [Modificar una cuenta de usuario](#)
- [Ver la información de una cuenta de usuario](#)
- [Clonar una cuenta de usuario](#)
- [Suprimir una cuenta de usuario](#)
- [Anular una sesión activa](#)
- [Añadir una función iTRAC](#)
- [Suprimir una función iTRAC](#)
- [Obtener la información de una función iTRAC](#)

El programa de instalación creará los usuarios por defecto siguientes en el servidor de Sentinel:

Autenticación de Oracle y MS SQL:

- esecdba: propietario del esquema (se puede configurar durante la instalación).
- esecadm: usuario Administrador de Sentinel (se puede configurar durante la instalación).

NOTA: En UNIX, el programa de instalación también crea el usuario del sistema operativo con el mismo nombre de usuario y contraseña.

- esecrpt: usuario que genera informes, contraseña como usuario admin.
- ESEC_CORR: usuarios del motor de correlación, se utilizan para crear incidencias.
- esecapp: nombre de usuario de la aplicación Sentinel para la conexión a la base de datos.

Autenticación de Windows:

- Administrador de la base de datos de Sentinel: propietario del esquema (se puede configurar durante la instalación).
- Administrador de Sentinel: usuario administrador de Sentinel (se puede configurar durante la instalación).
- Usuario de generación de informes de Sentinel: usuario de generación de informes, contraseña como el usuario admin.
- Usuario de la base de datos de aplicaciones Sentinel: nombre de usuario de la aplicación Sentinel para la conexión a la base de datos.

Apertura de la ventana Gestor de usuarios

Para abrir la ventana Gestor de usuarios

1. Haga clic en la pestaña *Admin*.
2. Haga clic en *Admin > Configuración del usuario*.

Creación de una cuenta de usuario

NOTA: Para satisfacer las estrictas configuraciones de seguridad que requiere la certificación de criterios comunes, es muy recomendable que se utilice una contraseña segura con las características siguientes:

1. Elija contraseñas con una longitud mínima de 8 caracteres y que incluya al menos un carácter en MAYÚSCULA, uno en minúscula, un símbolo especial (!@#\$%^&*()_+) y un signo numérico (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. Como contraseña, es conveniente elegir algo que a pesar de ser complejo, se vaya a recordar. Por ejemplo, Mht5!As (Mi hijo tiene cinco años) o bien HveCdh5#As (He vivido en California desde hace cinco años).
-

Para utilizar esta función, se debe disponer del permiso de usuario Crear cuenta de usuario. Los permisos de usuario suelen ser detallados, consulte la sección sobre *permisos de usuario* de la *Guía de referencia del usuario de Sentinel* para obtener más información.

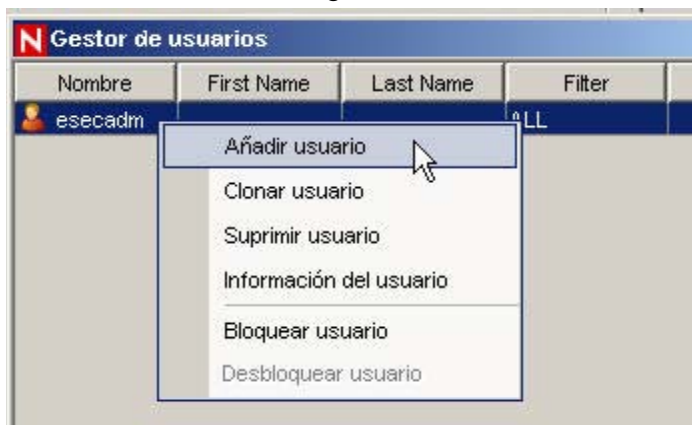
NOTA: La contraseña de usuario escrypt debe modificarse directamente en la base de datos. Para ello, se puede utilizar Enterprise Manager.

Para crear una cuenta de usuario

1. Abra la ventana Gestor de usuarios.
2. Haga clic en *Añadir un usuario nuevo*



o bien, resalte un usuario, haga clic con el botón derecho del ratón en *> Añadir usuario*.



3. En la sección Autorización, introduzca la información siguiente:
 - Nombre de usuario
 - Contraseña
 - Confirmar contraseña
 - Filtro de seguridad: para seleccionar un filtro, haga clic en la flecha hacia abajo. Aparecerá la ventana Selección del filtro. Resalte un filtro o bien haga clic en *Añadir* para crear un filtro para esta cuenta de usuario.

NOTA: Tras asignar un filtro de seguridad a un usuario, dicho filtro no se puede suprimir.

- Haga clic en *Seleccionar*.

NOTA: Se recomienda encarecidamente que, como práctica recomendada, para la contraseña se utilice una longitud mínima de 8 caracteres alfanuméricos.

(opcional) En Información, introduzca la información siguiente:

- Nombre
- Apellidos
- Departamento
- Teléfono
- Correo electrónico

4. Haga clic en la pestaña *Permisos* y asigne los permisos de usuario.
5. Haga clic en la pestaña *Funciones* y seleccione una función para el usuario.
6. Haga clic en *Aceptar*.

NOTA: Oracle no permite crear usuarios con un nombre que contenga una de las palabras reservadas de Oracle.Sentinel tampoco permite utilizar estos nombres.

Modificación de una cuenta de usuario

Para utilizar esta función, se debe disponer del permiso de usuario para modificar cuentas de usuario existentes.

NOTA: La contraseña de usuario escript debe modificarse directamente en la base de datos.Para ello, se puede utilizar Enterprise Manager.

Para modificar una cuenta de usuario

1. Abra la ventana Gestor de usuarios.
2. Haga doble clic en una cuenta de usuario o bien haga clic con el botón derecho del ratón en > *Información del usuario*.
3. Modifique la cuenta.
4. Haga clic en *Aceptar*.

Visualización de la información de una cuenta de usuario

Para utilizar esta función, se debe disponer del permiso de usuario para usar o visualizar cuentas de usuario.

Para visualizar la información de una cuenta de usuario

1. Abra la ventana Gestor de usuarios.
2. Haga doble clic en una cuenta de usuario o bien haga clic con el botón derecho del ratón en > *Información del usuario*.
3. Compruebe la información de la cuenta de usuario y cierre la ventana.

Clonación de una cuenta de usuario

Para clonar una cuenta de usuario

1. Abra la ventana Gestor de usuarios.
2. Seleccione un ID de cuenta de usuario, haga clic con el botón derecho del ratón en > *Clonar usuario*.
3. Cambie la información del usuario y los permisos del mismo.
4. Haga clic en *Guardar*.

Supresión de una cuenta de usuario

Para utilizar esta función, se debe disponer del permiso de usuario Suprimir cuenta de usuario.

NOTA: Cuando se suprime un usuario, dicho usuario no se puede volver a crear. Por ejemplo, si crea un usuario denominado José y luego suprime José, no podrá volver a crear un usuario denominado José.

Para suprimir una cuenta de usuario

1. Abra la ventana Gestor de usuarios.
2. Seleccione un ID de cuenta de usuario, haga clic con el botón derecho del ratón en > *Suprimir usuario*.

Anulación de una sesión activa

Anulación de una sesión activa

1. Abra la ventana Sesiones del usuario activo.
2. Seleccione la sesión activa que desea anular.
3. Haga clic con el botón derecho del ratón en > *Eliminar sesión*.
4. Se solicitará que envíe un mensaje de anulación. De este modo, se puede informar al usuario el motivo de la eliminación de la sesión.

Adición de una función iTRAC

Para añadir una función de iTRAC

1. Abra la ventana Gestor de funciones.
2. Haga clic en *Añadir una nueva función*



o bien, haga clic con el botón derecho del ratón en > *Añadir función nueva*.

Supresión de una función de iTRAC

Para suprimir una función de iTRAC

1. Abra la ventana Gestor de funciones.
2. Seleccione una función, haga clic con el botón derecho del ratón en > *Suprimir la función*.

Visualización de la información de una función

Par visualizar la información de una función

1. Abra la ventana Gestor de funciones.
2. Seleccione una función, haga clic con el botón derecho del ratón en > *Información de la función*.

10

Gestor de datos de Sentinel

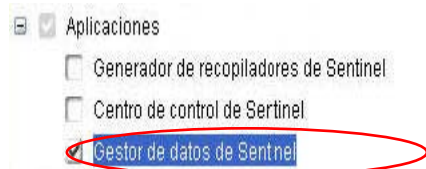
NOTA: El término agente puede intercambiarse con recopilador. En adelante, los agentes se denominarán recopiladores.

El Gestor de datos de Sentinel (SDM) es una herramienta que los usuarios pueden utilizar para gestionar la base de datos de Sentinel. El SDM permite a los usuarios realizar las operaciones siguientes:

- [Monitorizar la utilización del espacio en la base de datos](#)
- [Visualizar y gestionar las particiones de la base de datos](#)
- [Gestionar los archivos de reserva de la base de datos](#)
- [Importar datos a la base de datos](#)
- [Configurar la asignación de datos](#)
- [Configurar los nombres de etiqueta de evento](#)
- [Configurar los valores del informe resumido](#)

Instalación del SDM

El SDM se puede instalar directamente desde el asistente InstallShield de Sentinel 5. Para ello, seleccione el componente *Gestor de datos de Sentinel* en la pantalla de selección de funciones de Sentinel 5.



(Sólo para Oracle) Debe tenerse en cuenta que para que el SDM se comunique con bases de datos Oracle, se debe descargar manualmente el controlador Oracle 9.2.0.4 ó 9.2.0.5 JDBC y copiar el archivo.jar descargado en el directorio \$ESEC_HOME/lib del mismo recuadro en el que se ha instalado el SDM o bien en el directorio %ESEC_HOME%\lib si SDM se instala en Windows. El controlador JDBC se puede descargar desde la URL siguiente:

NOTA: Si se encuentra en un equipo UNIX con el componente DAS instalado, el instalador coloca el controlador JDBC automáticamente en la ubicación correcta. Por lo tanto, en este caso, no se requiere una descarga manual.

http://otn.oracle.com/software/tech/java/sqlj_jdbc/index.html

Este archivo jar suele denominarse ojdbc14.jar.

NOTA: A fecha de publicación de esta guía, el sitio Web anterior era el correcto.

NOTA: El SDM para Oracle requiere la instalación de Oracle Enterprise con particiones.

Inicio de la GUI de SDM

NOTA: Para poder utilizar la interfaz de usuario (GUI) del SDM, el archivo configuration.xml debe apuntar a un servidor de comunicaciones que tenga conectado DAS_Binary y DAS_Query. Esto suele ser el caso por defecto, siempre y cuando el servidor de comunicaciones y los procesos de DAS se estén ejecutando.

En UNIX:iniciar la GUI del SDM

1. Entre en el recuadro UNIX como miembro del grupo esec (por ejemplo:esecadm).
2. Cambie al directorio \$ESEC_HOME/sdm.
3. Introduzca la línea de comando siguiente:

```
./sdm
```

En Windows:iniciar la GUI del SDM

1. Haga clic en *Inicio > Archivos de programa > Sentinel > Gestor de datos de Sentinel*.

NOTA: Para ejecutar el SDM desde la línea de comando, consulte la sección [Línea de comando del SDM](#) de este documento.

Conexión a la base de datos

Al iniciarse el SDM, deberá establecerse una conexión a la base de datos. En el recuadro de diálogo *Conectarse a la base de datos*, introduzca los valores adecuados para cada campo.

Conexión a la base de datos

1. Inicie la GUI del SDM.
2. Seleccione el tipo de base de datos como Oracle o MSSQL.
3. Especifique el nombre de la instancia de la base de datos (por ejemplo, ESEC).
4. Especifique el host de la base de datos (utilice el nombre de host o la dirección IP).
5. Para el puerto, utilice el puerto por defecto 1521 para Oracle o el puerto por defecto 1433 para MSSQL.

6. Para el nombre de usuario y la contraseña, utilice el nombre de usuario y la contraseña de Administrador de la base de datos de Sentinel (por ejemplo, esecdba).

NOTA: En Windows y MS SQL, si ha instalado MS SQL en modo combinado, puede entrar mediante la autenticación de Windows o bien mediante la autenticación de SQL. Si ha instalado MS SQL en modo de autenticación de Windows únicamente, debe entrar mediante la autenticación de Windows. Si decide utilizar la autenticación de Windows, se autenticará en la base de datos MS SQL como el usuario con el que se ha entrado en Windows (p. ej., entrada única).

En Oracle:



The screenshot shows a dialog box titled "Connect to Database" with a key icon. It contains the following fields and options:

- Server: Oracle (dropdown menu)
- Database: ESEC
- Host: my_database
- Port: 1521
- Username: esecdba
- Password: (empty)
- Save connection settings
- Connect button

En Windows:



The screenshot shows a dialog box titled "Connect to Database" with a key icon. It contains the following fields and options:

- Server: MSSQL (dropdown menu)
- Database: ESEC
- Host: my_database
- Port: 1433
- Use Windows Authentication
- Use SQL Server Authentication
- Username: esecdba
- Password: (empty)
- Save connection settings
- Connect button

NOTA: Si opta por guardar los valores de conexión, éstos se guardarán en el archivo `sdm.connect local`. La próxima vez que se inicie la GUI, los valores de conexión se volverán a insertar desde el archivo `sdm.connect`. Este archivo se puede utilizar al ejecutar el SDM desde la línea de comando.

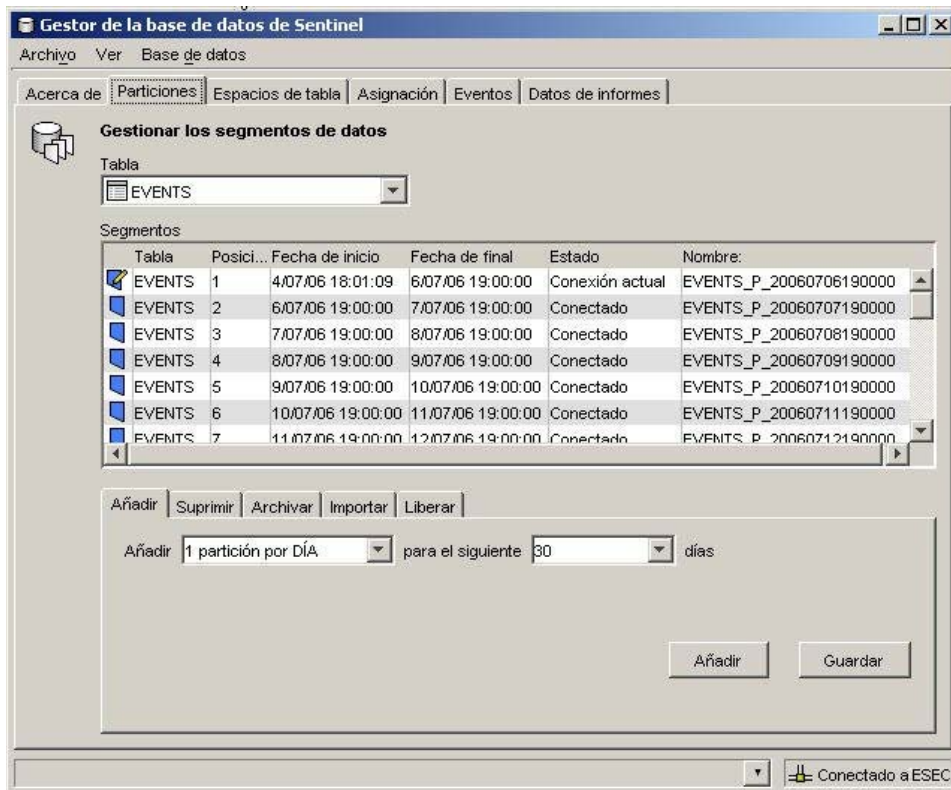
7. Haga clic en *Conectar*.

Particiones

La pestaña Particiones del SDM permite a los usuarios visualizar y gestionar las particiones de la base de datos.

Para visualizar las particiones en la GUI

1. Haga clic en la pestaña *Particiones*.
2. En la lista desplegable, seleccione la tabla que desea visualizar.



En la tabla Segmentos se muestran las particiones de la tabla de base de datos seleccionada.

En cada fila de la tabla Segmentos se muestra la tabla de base de datos relacionada, el intervalo de tiempo, el estado y el nombre de la partición.

Cada una de las particiones que se muestra en la tabla Segmentos se encontrará en uno de los estados siguientes:

Conectado	Los datos de una partición conectada están disponibles para su acceso.
Conexión actual	Partición conectada en la que se están insertando filas.
Archivado conectado	Partición cuyos datos se han archivado pero a los que aún se puede acceder debido a uno de los motivos siguientes: <ul style="list-style-type: none">▪ La partición aún no se ha abandonado.▪ La partición se ha importado.
Desconectado	Los datos de una partición desconectada no están disponibles para su acceso, ya que la partición se ha abandonado y no se ha importado.
Archivado desconectado	Partición que se ha archivado y abandonado.

Para gestionar particiones

1. Haga clic en la pestaña *Particiones*.
2. En la lista desplegable, seleccione la tabla.
3. En la parte inferior de la ventana, seleccione la pestaña relacionada con la operación que desea realizar: Añadir, Suprimir, Archivar, Importar o Liberar.

Para añadir particiones

1. Seleccione la pestaña *Añadir* particiones.
2. Especifique el número de particiones que se deben añadir y el número de días durante los cuales se deben añadir.
3. Pulse *Añadir*.

Para suprimir particiones

1. Seleccione la pestaña *Suprimir* particiones.
2. Especifique el número de días para los que se suprimirán las particiones más antiguas.
3. Pulse *Suprimir*.

Para archivar particiones

NOTA: Las tablas de adición no se archivan.

1. Seleccione la pestaña *Archivar* particiones.
2. Especifique el número de días para los que se archivarán las particiones más antiguas y el directorio en el que se almacenará el archivo de reserva.

NOTA: En UNIX, las particiones no se pueden archivar en el directorio */root*.

3. Pulse *Archivar*.

NOTA: Al archivar, asegúrese de introducir una vía válida en el servidor de base de datos con los permisos adecuados.

NOTA: La pestaña Archivar es diferente para MSSQL y Oracle. En Oracle, se permite especificar el tamaño máximo del archivo de reserva.

Pestaña Archivar particiones para Oracle:

The screenshot shows a dialog box with a tabbed interface. The 'Archive' tab is selected. At the top, there are tabs for 'Add', 'Delete', 'Archive', 'Import', and 'Release'. Below the tabs, the text reads 'Archive data partitions older than' followed by a dropdown menu showing the number '1', and 'day(s) as follows:'. Below this is a text input field labeled 'Output directory'. At the bottom left, there is a label 'Max file size' followed by a dropdown menu showing '10 MB'. At the bottom right, there are two buttons: 'Save' and 'Archive'.

Pestaña Archivar particiones para MSSQL:

The screenshot shows a dialog box with a tabbed interface. The 'Archive' tab is selected. At the top, there are tabs for 'Add', 'Delete', 'Archive', 'Import', and 'Release'. Below the tabs, the text reads 'Archive data partitions older than' followed by a dropdown menu showing the number '1', and 'day(s) as follows:'. Below this is a text input field labeled 'Output directory'. At the bottom right, there are two buttons: 'Save' and 'Archive'.

Para importar particiones

1. Seleccione la pestaña *Importar* particiones.
2. En la tabla Segmentos, seleccione la partición en la que se importarán los datos.
3. Especifique el directorio de entrada desde el que se leerán los datos.
4. Pulse *Importar*.

Para liberar particiones importadas

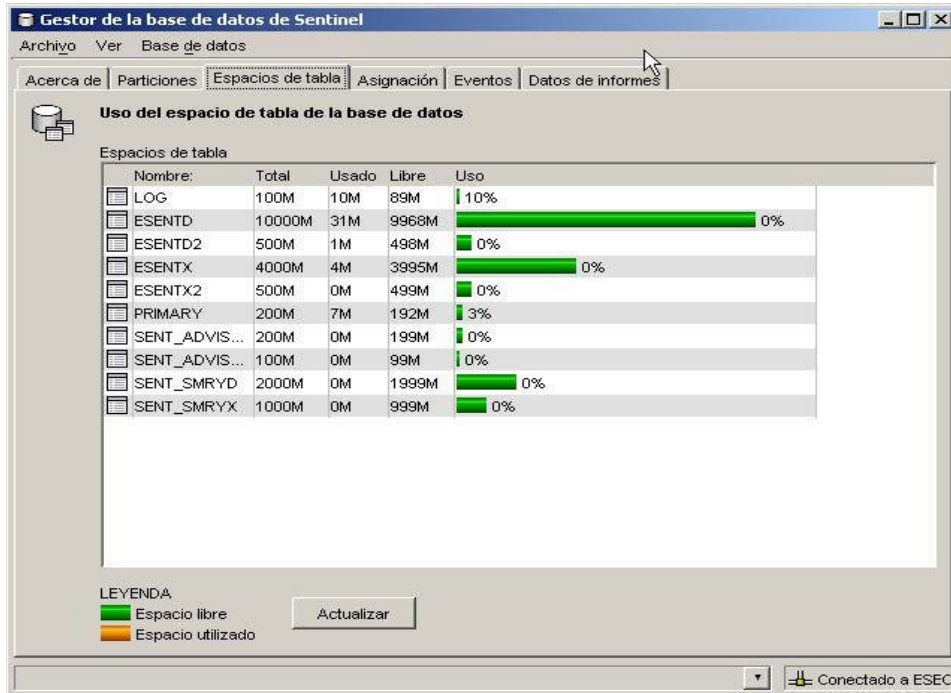
1. Seleccione la pestaña *Liberar* particiones.
2. En la tabla Segmentos, seleccione la partición que se debe liberar.
3. Pulse *Liberar*.

Espacio de tabla

La pestaña Espacios de tabla del SDM permite a los usuarios visualizar la utilización actual del espacio en la base de datos.

Para visualizar los espacios de tabla en la GUI

1. Haga clic en la pestaña *Espacios de tabla*.



En la tabla de uso del espacio de tabla se muestra el espacio total asignado a cada espacio de tabla, la cantidad de memoria que ha utilizado cada espacio de tabla y la cantidad de memoria que queda disponible (libre) para cada espacio de tabla. Los gráficos de barra de color ayudan a visualizar el espacio total asignado para cada espacio de tabla y el porcentaje de uso de cada uno.

NOTA: En MS SQL, no existen los espacios de tabla y, por lo tanto, se utilizan grupos de archivos.

Pestaña Asignación

NOTA: Para poder utilizar la pestaña Asignación, el archivo configuration.xml debe apuntar a un servidor de comunicaciones que tenga conectado DAS_Binary y DAS_Query. Esto suele ser el caso por defecto, siempre y cuando el servidor de comunicaciones y los procesos de DAS se estén ejecutando.

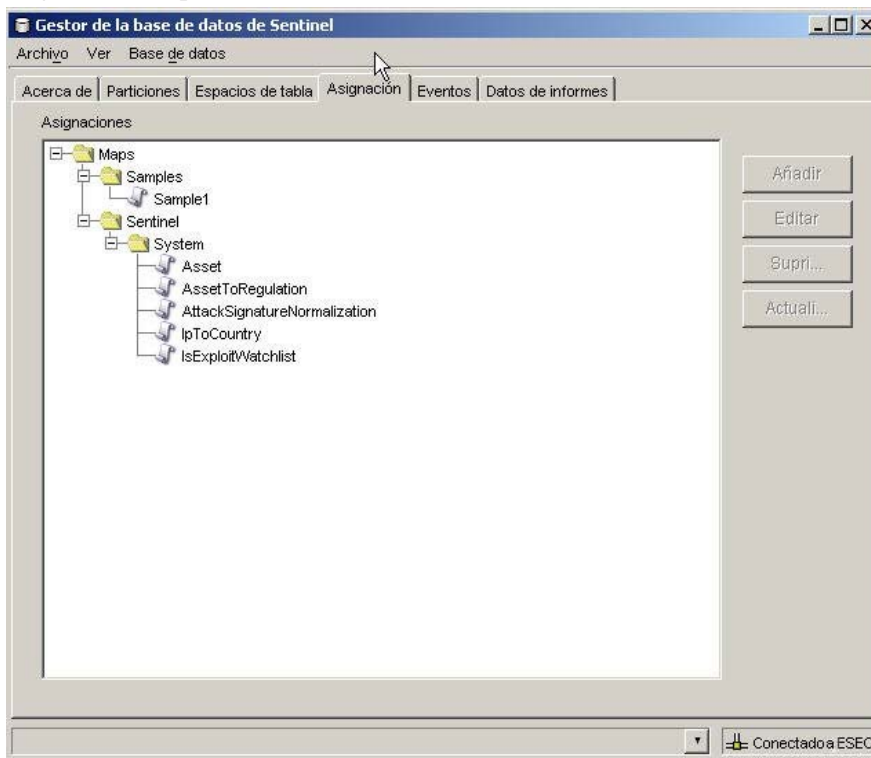
La pestaña Asignación permite realizar lo siguiente:

- Añadir nuevas definiciones de asignación
- Editar definiciones de asignación
- Suprimir definiciones de asignación
- Actualizar datos de asignación

La asignación se utiliza junto con la opción de origen de datos *Con referencia desde la asignación* de la pestaña Eventos. Puede realizar una asignación mediante una cadena o un rango de números.

Para visualizar las asignaciones en la GUI

1. Haga clic en la pestaña *Asignación*.



En la GUI principal de asignaciones se muestra un listado de todas las asignaciones que se han definido para el sistema.

NOTA: Las asignaciones de la carpeta del sistema no se pueden editar ni suprimir.

Adición de definiciones de asignación

Para añadir una definición de asignación:

1. Haga clic en la pestaña *Asignación*.
2. Haga clic en *Añadir*.
3. Si va a crear una carpeta de asignaciones nueva, haga clic en *Nuevo...* Introduzca un nombre de carpeta.

NOTA: Si se trata de la primera definición de asignación, se recomienda crear una nueva carpeta para ésta. Si se crea una definición de asignación en la carpeta del sistema, dicha definición no se podrá editar ni suprimir.

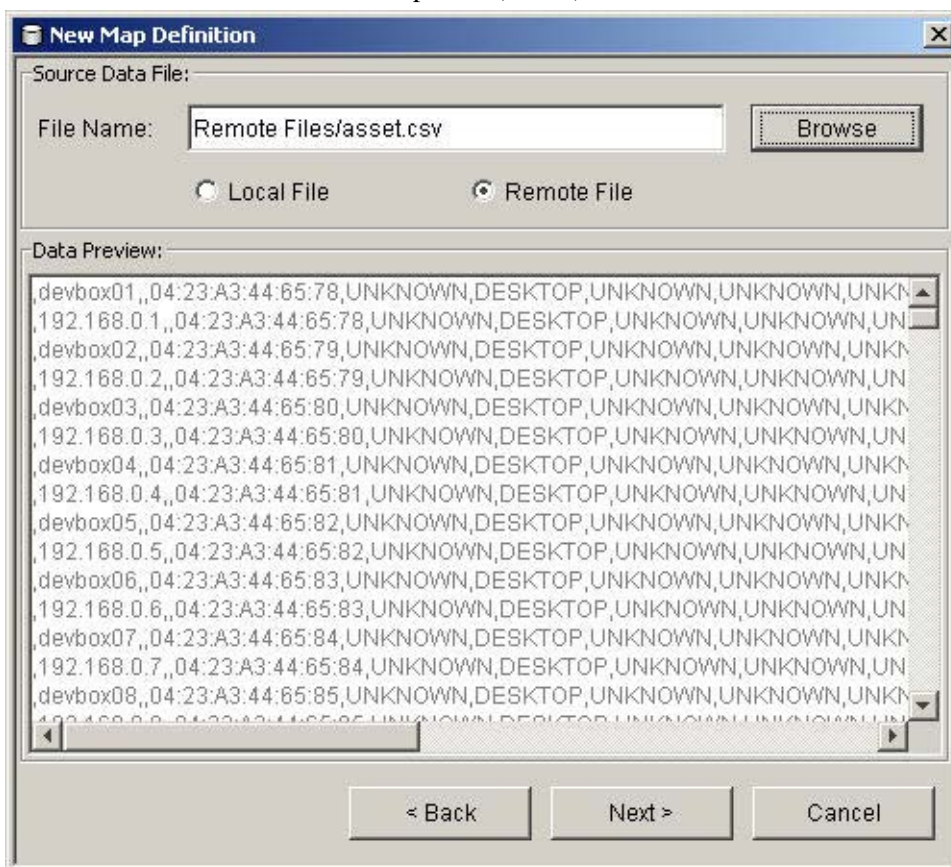
4. Asegúrese de seleccionar la carpeta en la que desea insertar la definición de asignación (p. ej., la carpeta indica que está abierta).
5. Introduzca el nombre de la asignación.

6. Haga clic en *Siguiente*.

NOTA: El recuadro de campo Tipo de asignación está inhabilitado.

7. Seleccione Archivo local o Archivo remoto.

- Archivo local: permite buscar el archivo en el sistema de archivos local (en el equipo desde el que se ha lanzado el SDM).
- Archivo remoto: permite elegir entre archivos de datos de origen de asignación en el servidor en el que se ejecuta DAS. Si se ha instalado el asesor y se han cargado los datos de vulnerabilidades, es posible que ya existan dos archivos en el servidor: `attackNormalization.csv` y `exploitDetection.csv`. Un archivo remoto apunta al directorio `%ESEC_HOME%\sentinel\bin\map_data` (Windows) o `$(ESEC_HOME)/sentinel/bin/map_data` (UNIX)



Seleccione el archivo de definición de asignación. Haga clic en *Siguiente*.

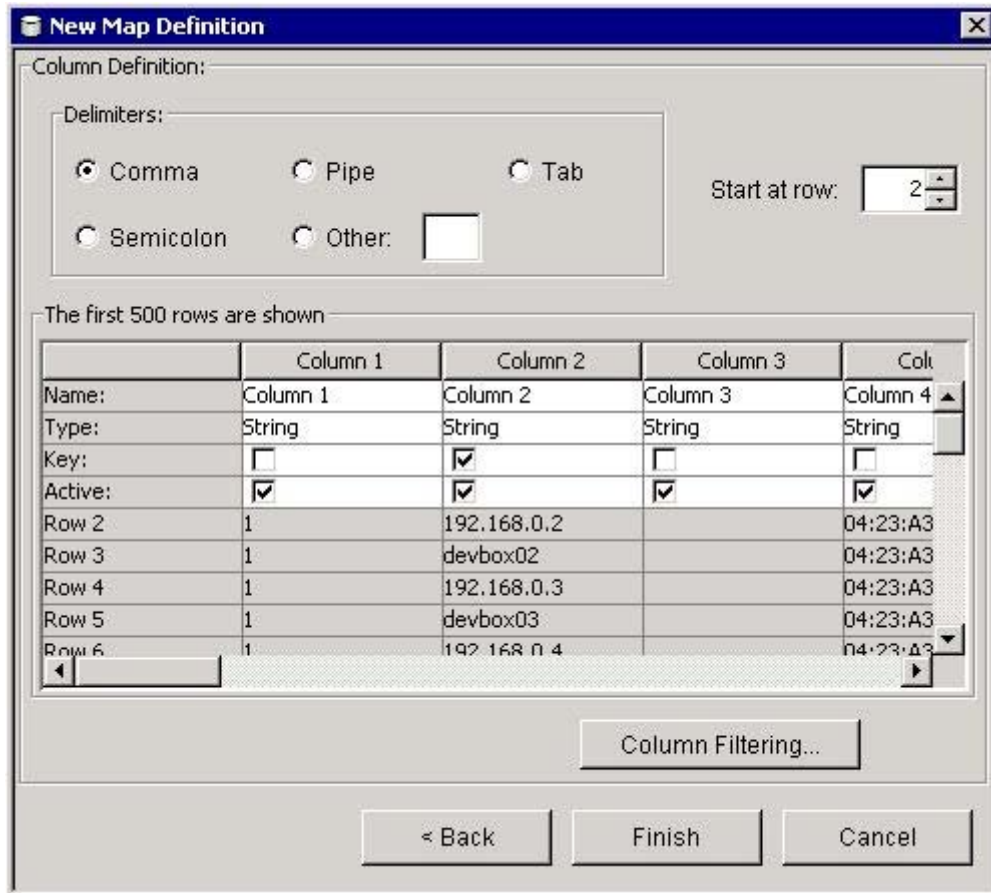
NOTA: Para los archivos de asignación que contienen más de 500 líneas, no todas las líneas se mostrarán en el SDM.

8. En la ventana Definición de asignación nueva, defina los elementos siguientes:

- El delimitador (conducto, coma, punto y coma, etc.) de datos en las filas del archivo de origen de datos.
- Empezar en la fila: el número de filas que se deben omitir a partir del principio del archivo de origen de datos.

- Los nombres de columna.
- Tipos de columna: a continuación se enumeran los tipos de columna admitidos.
 - *Cadena*: una cadena es un grupo de caracteres utilizado como un objeto único por un equipo. Una cadena puede consistir en una letra, una palabra o un número. La palabra FINANCE o la dirección IP 192.168.2.40 puede ser una cadena. Una cadena también puede estar formada por una combinación de palabras, espacios y números. La dirección de la calle 1313 LION DOG TOWER puede ser una cadena.
 - *Rango de números*: un rango de números (NumberRange) es un intervalo de números. Por ejemplo, el rango entre el 10 y el 200 puede representarse como 10-200. Para utilizar la funcionalidad de asignación de rangos, una definición de asignación debe tener exactamente una columna de clave y ésta debe ser del tipo NumberRange. Si hay otras columnas de clave, o bien si la columna de clave es de un tipo distinto, el servicio de asignación no considerará la asignación como una asignación de rango.
- Columnas activas: cuando una columna se marca como activa, los datos que contiene se distribuirán a los procesos mediante asignaciones. Todas las columnas de clave deben estar activas. Sólo las columnas que no contienen claves que están activas pueden seleccionarse como *Asignar columna* en la pestaña Eventos.
- Columnas de clave: una clave es un identificador exclusivo para la fila de datos en los datos de la asignación. Si se selecciona más de una columna como clave, la clave global de la asignación incluirá todas las columnas seleccionadas como claves.
- Filtrado de columnas: es posible incluir o excluir explícitamente una fila en función de los criterios de concordancia para una columna en particular. Esta opción puede utilizarse para excluir filas de los datos de origen de la asignación que no son necesarias o que interfieren con la asignación.

A medida que configure cada valor y filtro, la tabla de datos se actualizará automáticamente y podrá obtener una vista previa de los datos y comprobar que éstos se están analizando según lo esperado.



9. Cuando haya terminado de configurar todos los parámetros y filtros de la definición, haga clic en *Finalizar*.
10. Si en el paso 7 anterior ha seleccionado Archivo local, se le solicitará al usuario que cargue el archivo a la carpeta virtual Archivos remotos que se encuentra en el directorio siguiente: %ESEC_HOME%\sentinel\bin\map_data. Introduzca un nombre de archivo y haga clic en *Aceptar*.

Adición de una definición de asignación de rango de números

Para utilizar la funcionalidad de asignación de rangos, una definición de asignación debe tener exactamente una columna de clave y ésta debe ser del tipo NumberRange. Si hay otras columnas de clave, o bien si la columna de clave es de un tipo distinto, el servicio de asignación no considerará la asignación como una asignación de rango.

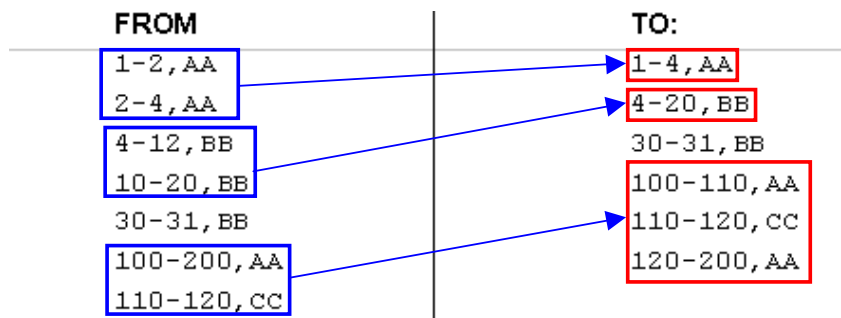
Para crear una asignación de rango, seleccione una sola columna como la clave de la asignación y *NumberRange* como el tipo de columna. El formato de los datos de una columna tipo *NumberRange* debe ser “m-n”, donde m representa el número mínimo del rango y n el número máximo (p. ej., 10-200). El número máximo de un rango no se incluye en el rango (p. ej., [m,n]). Esto significa que un rango de 10-200 sólo proporcionará números entre 10 y 199. Un conjunto de datos de ejemplo es con la primera columna como clave:

1-2 , AA
 2-4 , AA
 4-12 , BB
 10-20 , BB
 30-31 , BB
 100-200 , AA
 110-120 , CC

The first 500 rows are shown

	Column 1	Column 2
Name:	Range	Value
Type:	NumberRange	String
Key:	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Active:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Row 0	1-4	AA
Row 1	4-20	BB
Row 2	30-31	BB
Row 3	100-110	AA
Row 4	110-120	CC
Row 5	120-200	AA

Observe como se transforma la tabla de ejemplo.



Una configuración de evento de ejemplo sobre la asignación anterior puede tener el aspecto siguiente:

CustomerVar82
CustomerVar83
CustomerVar84
CustomerVar85
CustomerVar86
CustomerVar87
CustomerVar88
CustomerVar89
SARBOX
HIPAA
GLBA
FISMA

Data Source

External

Referenced from Map

Map Name:

Map Column:

Key Configuration:

Map Key Field	Event Tag
Range	CustomerVar97

Se espera que CustomerVar97 contenga un valor numérico o bien sea de un tipo que se pueda convertir en un valor numérico como, por ejemplo, una dirección IP o una fecha.

Al realizar búsquedas en la asignación de rangos de ejemplo, el valorCustomerVar97 utilizará la asignación de rangos y buscará el rango al que pertenece el valor (si lo hay). Entre algunos ejemplos y sus resultados se incluyen:

```
CustomerVar97 = 1; CustomerVar89 se definirá en AA
CustomerVar97 = 4; CustomerVar89 se definirá en BB
CustomerVar97 = 300; CustomerVar89 no se definirá
```

Internamente, Sentinel convierte las direcciones IP y las fechas en un número entero para las etiquetas de tipo IPv4 y fecha.

Las etiquetas IPv4 son las siguientes:

- DestinationIP (dip)
- SourceIP (sip)

Las etiquetas de fecha son las siguientes:

- De CustomerVar11 a CustomerVar20 (de cv11 a cv20)
- DateTime (dt)
- De ReservedVar11 a ReservedVar20 (de rv11 a rv20)

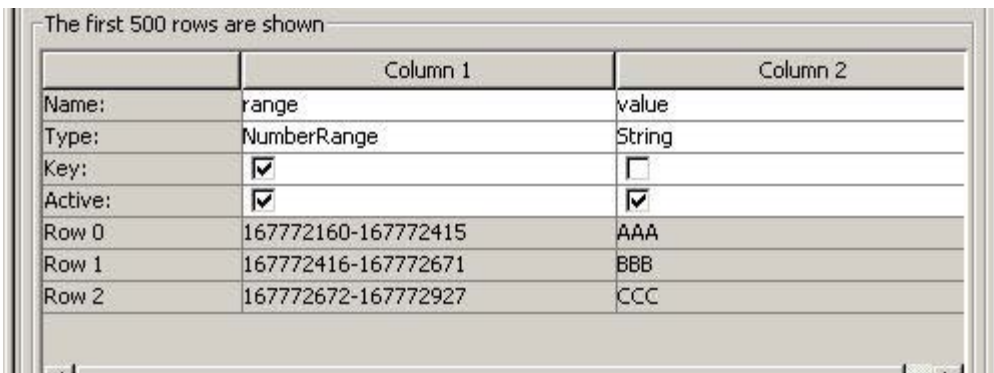
Para obtener más información sobre las meta-etiquetas, consulte el capítulo 5 sobre asistentes y meta-etiquetas de Sentinel en la Guía de referencia de Sentinel.

Por ejemplo, en la tabla siguiente, la columna 1 es un rango numérico equivalente a un rango de direcciones IP de 10.0.0.0 a 10.0.2.255.

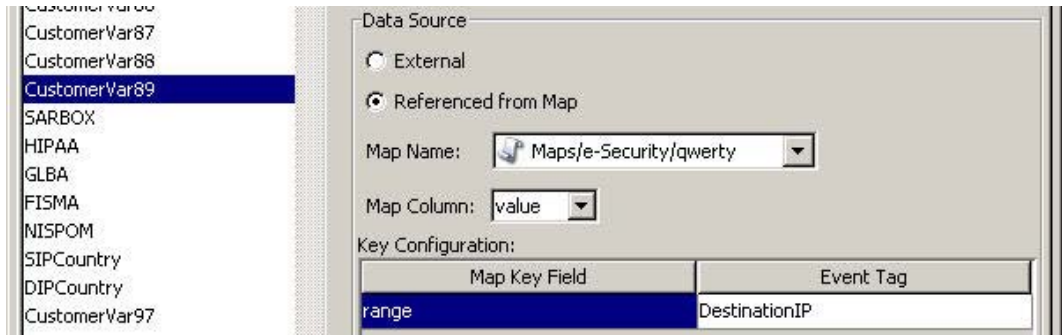
```
167772160-167772415 ,AAA
167772416-167772671 ,BBB
167772672-167772927 ,CCC
```

Utilizando la misma configuración que la del ejemplo anterior, si:

- la etiqueta Event se define como DestinationIP y la columna 1 se define como la columna de claves (rango).
- la columna se asigna a la columna 2 (valor). Los valores de salida para CustomerVar89.



	Column 1	Column 2
Name:	range	value
Type:	NumberRange	String
Key:	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Active:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Row 0	167772160-167772415	AAA
Row 1	167772416-167772671	BBB
Row 2	167772672-167772927	CCC



Si un evento contiene una dirección IP de destino de 10.0.1.14 (equivalente al valor numérico 167772430), el resultado de la columna CustomerVar89 en el evento será BBB.

Sentinel admite los rangos de números siguientes:

- Rango de un número negativo a un número negativo (p. ej., “-234--34”).
- Rango de un número negativo a un número positivo (p. ej., “-234-34”).
- Rango de un número positivo a un número positivo (p. ej., “234-236”).
- Rango de un solo número (negativo) (p. ej., “-234”). En este caso, tanto el número mínimo como el máximo serán -234.
- Rango de un solo número (positivo) (p. ej., “234”). En este caso, tanto el número mínimo como el máximo serán 234.
- Rango de un número negativo a un número máximo (p. ej., “-234-”). En este caso, el número mínimo será -234 y el máximo será $(2^{63} - 1)$.
- Rango de un número positivo a un número máximo (p. ej., “234-”). En este caso, el número mínimo será 234 y el máximo será $(2^{63} - 1)$.

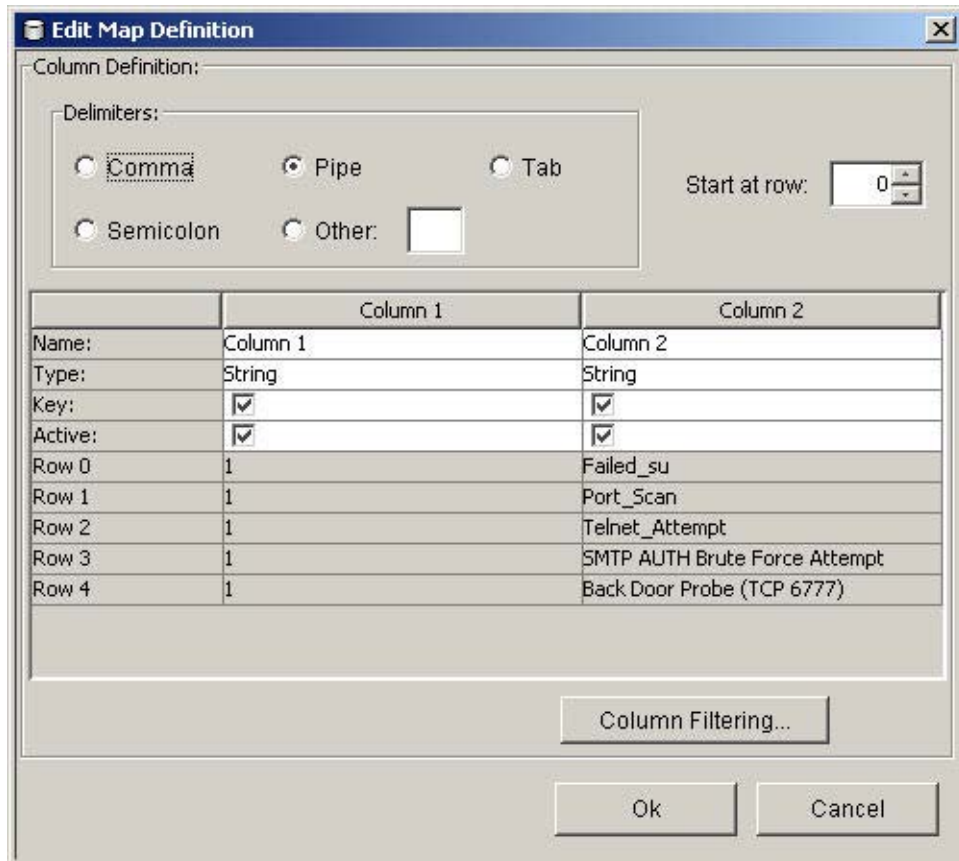
NOTA: En todos los casos, el número mínimo debe ser menor que o igual al número máximo (p. ej., “-234—235” NO es válido).

Edición de definiciones de asignación

Para editar una definición de asignación:

1. Haga clic en la pestaña *Asignación*.
2. Expanda la carpeta deseada.
3. Resalte una definición de asignación y haga clic en *Editar*.

NOTA: Para las definiciones de asignación de la carpeta del sistema, la función de edición estará inhabilitada.



La función de edición permite realizar las operaciones siguientes:

- Definir los delimitadores
- Definir la fila a partir de la cual se iniciará la asignación
- Cambiar el nombre de las columnas
- Activar o desactivar una columna
- Definir las claves de columna
- Definir los filtros de columna

4. Tras realizar los cambios, haga clic en *Aceptar*.

Supresión de definiciones de asignación

Para suprimir una definición de asignación

1. Haga clic en la pestaña *Asignación*.
2. Expanda la carpeta deseada.
3. Resalte la definición de asignación que se debe suprimir.
4. Haga clic en *Suprimir*.

NOTA: Las definiciones de asignación de la carpeta de Sentinel no se pueden suprimir.

Actualización de los datos de asignación

La actualización permite sustituir el archivo de datos de origen de asignación de una asignación en el servidor que ejecuta DAS por otro archivo. Para que la asignación funcione correctamente después de la actualización, el nuevo archivo de datos de origen de asignación debe tener el mismo delimitador, número de columnas y estructura global que el archivo existente. La única diferencia entre el archivo de datos de origen de asignación y el archivo existente son los valores que aparecen en las columnas. Si la estructura del nuevo archivo de datos de origen de asignación es distinta de la estructura del archivo existente, utilice la función [Editar](#) de la GUI del SDM para actualizar la definición de asignación.

Para actualizar los datos de asignación

1. Si aún no ha creado un archivo que contenga los nuevos datos de origen de asignación en el equipo en el que se ejecuta el SDM, hágalo ahora. Este archivo se puede generar (p. ej., a partir de un guión de volcado de datos), crearse manualmente desde cero o bien ser una versión modificada del archivo de origen de datos de asignación existente. Si fuera necesario, el archivo de origen de datos de asignación existente se puede obtener en la ubicación siguiente:

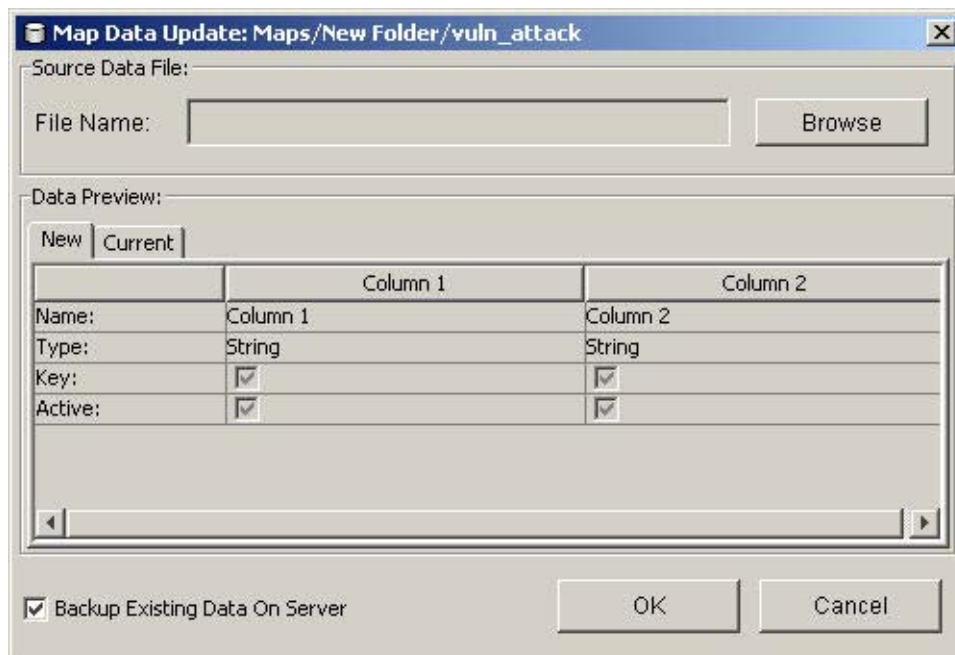
En Windows:

```
%ESEC_HOME%\sentinel\bin\map_data
```

En UNIX:

```
$(ESEC_HOME)/sentinel/bin/map_data
```

2. Haga clic en la pestaña *Asignación*.
3. Expanda la carpeta deseada. Resalte la asignación que se debe actualizar. Haga clic en *Actualizar*.



4. Para seleccionar el nuevo archivo de origen de datos de asignación, haga clic en *Examinar* y seleccione el archivo que contiene los nuevos datos de asignación. Tras seleccionar el archivo, los datos del archivo nuevo aparecerán en la pestaña *Nuevo*. Los datos de asignación que se están sustituyendo se encuentran en la pestaña *Actual*.
5. Desmarque o deje el valor por defecto *Copia de seguridad de los datos existentes en el servidor*. Si se habilita esta opción, se creará una copia de seguridad del archivo de origen de datos de asignación existente en la carpeta %ESEC_HOME%\sentinel\bin\map_data (Windows) o \$ESEC_HOME/sentinel/bin/map_data (UNIX). El prefijo del nombre de la copia de seguridad del archivo de origen de datos de asignación será el nombre del archivo existente. El final del nombre de archivo contendrá un conjunto de números aleatorios seguido del sufijo.bak. Por ejemplo:vuln_attacks10197.bak.
6. Haga clic en *Aceptar*.
7. Los datos del nuevo archivo de origen de datos de asignación se cargarán en el servidor y sustituirán el contenido del archivo existente. Una vez que los datos de origen se hayan cargado por completo, los datos de asignación se volverán a generar y se distribuirán a los clientes de asignación (p. ej., el Gestor de recopiladores).

Pestaña Eventos

NOTA: Para poder utilizar la pestaña *Eventos*, el archivo configuration.xml debe apuntar a un servidor de comunicaciones que tenga conectado DAS_Binary y DAS_Query. Esto suele ser el caso por defecto, siempre y cuando el servidor de comunicaciones y los procesos de DAS se estén ejecutando.

Asignación de eventos

La asignación de eventos es un mecanismo que permite añadir datos a un evento utilizando los datos que ya existen en el evento al que se debe hacer referencia y obtener datos desde un origen externo. El origen de datos externo es una asignación, que se define mediante la [pestaña Asignación](#). Los datos que ya se encuentran en el evento que deben utilizarse como referencia en la asignación y los datos que se deben obtener de la asignación para colocarse el evento se especifican mediante la pestaña *Eventos*.

Puesto que casi cualquier conjunto de datos puede convertirse en una asignación, la asignación de eventos es de gran utilidad a la hora de incorporar en el evento datos de flujo de otra área de la organización. Entre algunas de las oportunidades que ofrece la asignación de eventos se incluyen:

- Monitorización del cumplimiento con las normas
- Conformidad con directivas
- Definición de prioridades de las respuestas
- Análisis de datos de seguridad en relación con las operaciones comerciales
- Mejora de la responsabilidad

Cuando se define una asignación de eventos, ésta se aplica en todo el sistema a todos los eventos y desde todos los recopiladores. Además, Sentinel distribuirá automáticamente los datos de asignación a todos los procesos que realizan asignaciones de evento y los mantendrá actualizados en los mismos. Por estos motivos, la asignación de eventos proporciona importantes capacidades para admitir implantaciones empresariales.

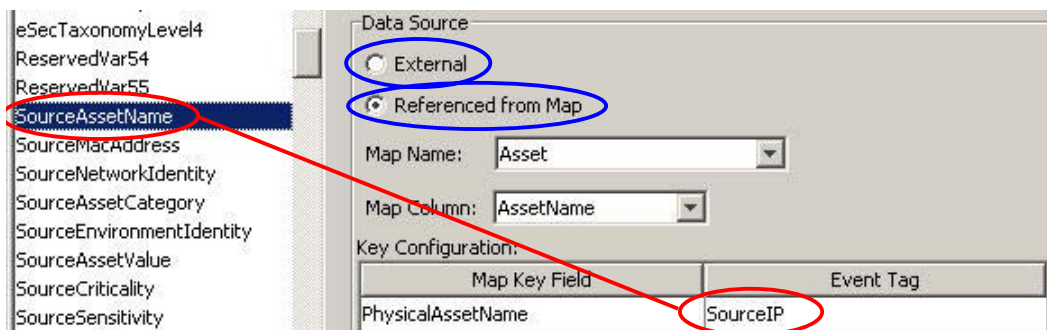
La asignación de eventos comprende cuatro elementos principales:

- Controlador: almacena toda la información de asignación.
- Distribuidor: redistribuye automáticamente las asignaciones modificadas a los procesos registrados para la asignación.
- Monitor: monitor para detectar los cambios en los datos de origen de asignación.
- Generador: genera asignaciones a partir de datos de origen.

Una aplicación de la asignación de eventos es la funcionalidad Datos del activo de Sentinel. Por ejemplo, la información sobre el activo se recopila y almacena en el esquema de activos de la base de datos de Sentinel y se representa mediante una entrada de activo físico. Los activos abstractos como, por ejemplo, servicios y aplicaciones, se representan mediante una entrada vinculada a un activo físico. El principal mecanismo de actualización automatizada para los datos de activo es a través de un recopilador de activos que realiza una lectura de los datos mediante un explorador como, por ejemplo, Nmap. El recopilador de activos automatiza la recuperación de la información sobre activos leyendo los datos de activos desde el explorador y rellenando las tablas de esquema de activos con dichos datos. Para la asignación de eventos, la información sobre activos se asigna desde la IP de destino y la IP de origen.

Existen dos tipos de orígenes de datos:

- Externos: un recopilador incluye dicho valor en la etiqueta del evento.
- Con referencia desde la asignación: los datos se recuperan desde un archivo de asignaciones para rellenar la etiqueta.



En la ilustración anterior, la etiqueta SourceAssetName se ha rellenado a partir de la asignación denominada Asset (que tiene asset.csv como archivo de origen de datos de asignación). El valor específico de SourceAssetName se obtiene de la columna AssetName de la asignación Asset. La columna PhysicalAssetName se ha definido como la clave. Cuando la etiqueta SourceIP del evento concuerda con uno de los valores de la IP de origen en la columna PhysicalAssetName de la asignación, la fila con la clave que concuerda se utiliza para cruzar la columna AssetName. Por ejemplo, en el ejemplo siguiente, IP 198.168.1.100 corresponde a AssetName Finance35.

NOTA: Si una columna se define como una clave, ésta no aparecerá en el campo desplegable Columna.

PhysicalAssetName	CustomerID	MacAddress	AssetName
198.168.1.91	Key		Marketing01
198.168.1.95			Marketing02
198.168.1.96		SourceAssetName	ProgramMgmt03
198.168.1.98			Finance34
198.168.1.100			Finance35

Es posible que haya más de una columna definida como una clave, ya que no se desea que la asignación sea una asignación de rangos, que sólo pueden tener una columna de clave con ese tipo de columna definida como NumberRange. Por ejemplo, (con el tipo de columna definido como Cadena) la etiqueta AttackId tiene las columnas DeviceName (nombre del dispositivo de seguridad) y DeviceAttackName (nombre de ataque de dispositivo) definidas como claves y utiliza la columna NormalizedAttackID de la asignación AttackNormalization para su valor. En una fila en la que la etiqueta del evento DeviceName concuerda con los datos de la columna de asignación Device y DeviceAttackName concuerda con los datos de la columna de asignación AttackSignature, el valor de AttackId será el valor de la columna NormalizedAttackID. La configuración de la asignación de eventos que se acaba de describir es la siguiente:

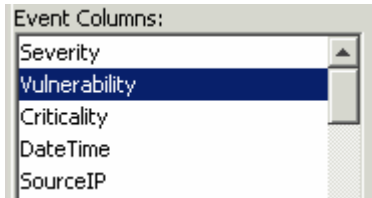


Key	Key	NormalizedAttackId	AttackId entry
Secure	BackDoorProbe (TCP 1234)	3	Trojan: Backdoor.SubSeven
Secure	BackDoorProbe (TCP 1999)	3	Trojan: Backdoor.SubSeven
Dragon	RWALLD:SYLOG-FORMAT	4	Sun Microsystems Solaris rwall Elevated F
Snort	RPC TCP rwall request	4	Sun Microsystems Solaris rwall Elevated F
Snort	RPC UDP rwall request	4	Sun Microsystems Solaris rwall Elevated F
Snort	WEB-IIS foxweb.dll access	12	Microsoft Exchange Server Arbitrary Code
RealSecure	SMTP_Exchange_Verb_DoS	12	Microsoft Exchange Server Arbitrary Code

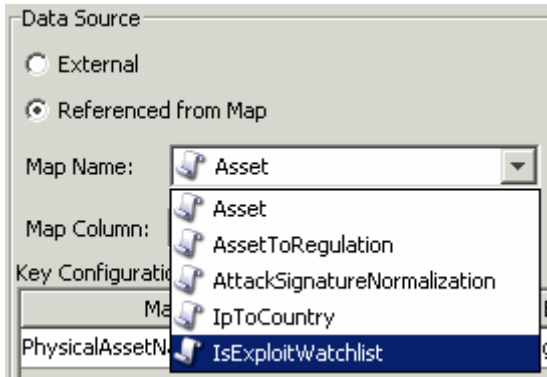
Configuración de etiquetas (columnas) de evento para utilizar la asignación

1. Haga clic en la pestaña *Eventos*.
2. En la lista Columnas de eventos, resalte una entrada de etiqueta de evento.

NOTA: El nombre original de la etiqueta de evento aparecerá encima del campo Etiqueta. Además, se proporciona la descripción de la columna de eventos.



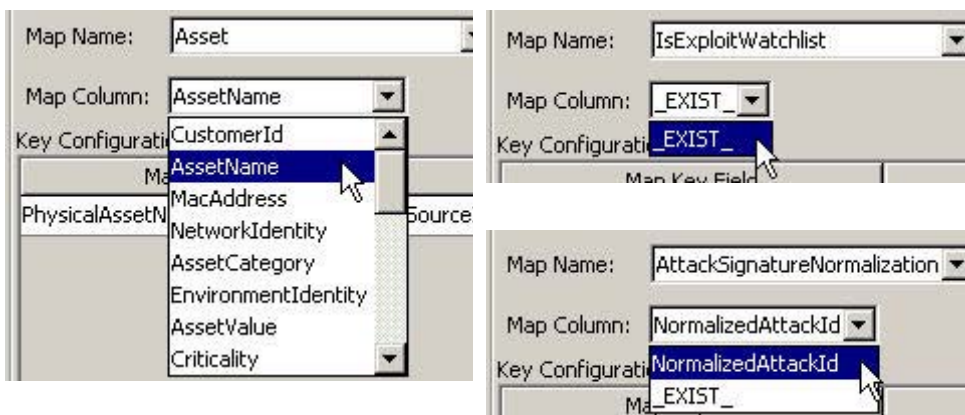
3. Haga clic en *Con referencia desde la asignación* para configurar la etiqueta de evento que debe rellenarse con los datos de la asignación. Haga clic en *Externo* para conservar el valor que el recopilador haya colocado en la etiqueta de evento (si lo hay).
4. Haga clic en la flecha hacia abajo del campo *Nombre de asignación*.



Seleccione una de las asignaciones por defecto siguientes o una asignación creada por el usuario:

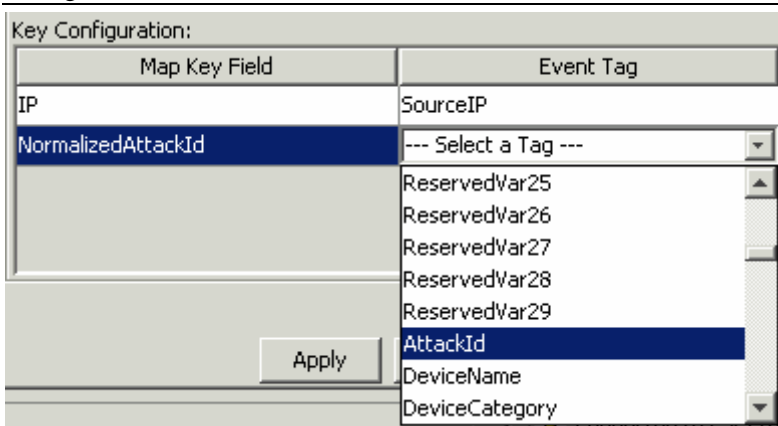
- **Asset:** contiene los datos del archivo de origen de datos de asignación *asset.csv*. Este archivo se genera automáticamente a partir de datos de activo desde la base de datos de Sentinel cuando se ejecuta un recopilador de activos. Si lo desea, este archivo puede rellenarse manualmente.
- **AssetToRegulation:** contiene los datos del archivo de origen de datos de asignación *AssetToRegulation.csv*. Este archivo debe alimentarse manualmente.
- **AttackSignatureNormalization:** contiene los datos del archivo de origen de datos de asignación *attackNormalization.csv* (firmas IDS). El archivo *attackNormalization.csv* se genera automáticamente a partir de los datos del asesor de la base de datos de Sentinel cuando se haya finalizado la inserción de los datos del asesor.
- **IpToCountry:** contiene los datos del archivo de origen de datos de asignación *IpToCountry.csv*. Este archivo debe alimentarse manualmente.
- **IsExploitWatchlist:** contiene los datos del archivo de origen de datos de asignación *exploitDetection.csv* (vulnerabilidades y amenazas). El archivo *exploitDetection.csv* se genera automáticamente a partir de datos de asesor y de vulnerabilidades de la base de datos de Sentinel cuando se haya finalizado la inserción de datos del asesor o se haya ejecutado un recopilador de vulnerabilidades.

- Haga clic en la flecha de campo hacia abajo *Asignar columna* y seleccione un nombre de *columna de asignación*. Estos valores variarán en función de la selección de la asignación de nombre realizada en el paso anterior.



- **_EXIST_:** una columna de asignación especial que existe en todas las asignaciones. Si se selecciona esta columna de asignación, se colocará el valor “1” en todas las etiquetas cuando la clave se encuentre en los datos de asignación. Si la clave no se encuentra en los datos de asignación, se colocará el valor “0” en la etiqueta de evento.
 - Todas las demás opciones: los nombres de las columnas activas en la definición de la asignación que no se define como clave (p. ej., la columna CustomerId en Asset o la columna NormalizedAttackId en AttackNormalization).
- En la columna Configuración clave, para cada fila de la tabla, seleccione la etiqueta de evento en la columna correspondiente que se hará concordar con la columna de clave de asignación especificada en la columna Asignar campo de claves correspondiente. Las filas de la tabla Configuración clave dependerán del nombre de asignación seleccionado.

NOTA: Una clave es un identificador exclusivo para la fila de datos en los datos de la asignación.



- Haga clic en *Aplicar*.

NOTA: Al hacer clic en *Aplicar*, en el buffer temporal, se guardarán los cambios realizados en la columna de eventos seleccionada. Si no se hace clic en *Aplicar*, al seleccionar otra columna de eventos, se perderán los cambios realizados en la columna de eventos seleccionada anteriormente. Los cambios no se guardarán en el servidor hasta que haga clic en *Guardar*.

- Si desea editar la *asignación de eventos* de otra columna de *eventos*, repita los pasos anteriores. No olvide hacer clic en *Aplicar* tras editar la *asignación de eventos* para cada columna de *eventos*.

- Haga clic en *Guardar*.

NOTA: Al hacer clic en *Guardar*, se guardarán los cambios en el servidor. Esta función guarda todos los cambios almacenados en el buffer temporal (al hacer clic en *Aplicar*).

Cambio del nombre de las etiquetas

La pestaña *Eventos* también permite asignar nombres a etiquetas de evento existentes. Por ejemplo, puede renombrar la etiqueta de la etiqueta de evento Ct2 a City. De este modo, la etiqueta de evento que aparecía en el Centro de control de Sentinel como “Ct2” ahora aparecerá como “City”. Entre algunos de los lugares en los que las etiquetas de evento aparecen en el Centro de control de Sentinel se incluyen los filtros, las reglas de correlación y las vistas Active Views.

Sin embargo, la operación de renombrar etiquetas no cambia el nombre de la variable en los guiones del recopilador. Por lo tanto, incluso si el nombre de la etiqueta de evento Ct2 se cambia a City, la variable que debe utilizarse en un guión de recopilador para hacer referencia a esta metaetiqueta seguirá siendo s_CT2.

A continuación se incluye una ilustración (antes y después) de esta función en una vista Active Views.

The image shows two screenshots of the Sentinel Active Views interface. The top screenshot shows a table with columns: SourceIP, DestinationIP, EventName, Ct2, Vulnerability, and Criticality. The bottom screenshot shows the same table after the column 'Ct2' has been renamed to 'City'.

SourceIP	DestinationIP	EventName	Ct2	Vulnerability	Criticality
172.16.2.107		Drop	Orlando	0	6
172.16.2.105		Drop	Orlando	0	7
172.16.2.106		Drop	Orlando	0	7
172.16.2.105		Drop	Orlando	0	7
172.16.5.103		Drop	Cupertino	0	7
172.16.5.103		Drop	Cupertino	0	7
172.16.7.105		Drop	Chicago	0	4
172.16.7.105		Drop	Chicago	0	4
172.30.2.211		EventInsertionFailed			

SourceIP	DestinationIP	EventName	City	Vulnerability	Criticality
172.16.2.107		Drop	Orlando	0	6
172.16.2.105		Drop	Orlando	0	7
172.16.2.106		Drop	Orlando	0	7
172.16.2.105		Drop	Orlando	0	7
172.16.5.103		Drop	Cupertino	0	7
172.16.5.103		Drop	Cupertino	0	7
172.16.7.105		Drop	Chicago	0	4
172.16.7.105		Drop	Chicago	0	4
172.30.2.211		EventInsertionFailed			

Cambio de nombre de una columna de eventos

- Haga clic en la pestaña *Eventos*.

NOTA: El nombre original de la columna de eventos aparecerá encima del campo *Etiqueta*. Además, se proporciona la descripción de la columna de eventos.

- Resalte una entrada de columna de eventos.

3. En el campo Etiqueta, introduzca un valor nuevo para la columna de eventos.



4. Haga clic en *Aplicar*.

NOTA: Al hacer clic en *Aplicar*, en el buffer temporal, se guardarán los cambios realizados en la etiqueta de evento seleccionada. Si no se hace clic en *Aplicar*, al seleccionar otra etiqueta de eventos, se perderán los cambios realizados en la etiqueta de eventos seleccionada anteriormente. Los cambios no se guardarán en el servidor hasta que haga clic en *Guardar*.

5. Haga clic en *Guardar*.

NOTA: Al hacer clic en *Guardar*, se guardarán los cambios en el servidor. Esta función guarda todos los cambios almacenados en el buffer temporal (al hacer clic en *Aplicar*).

6. Para que los cambios sean visibles en el Centro de control de Sentinel, éste debe cerrarse y volver a abrirse.

Pestaña Datos de informes

NOTA: Para poder utilizar la pestaña Datos de informes, el archivo configuration.xml debe apuntar a un servidor de comunicaciones que tenga conectado DAS_Binary y DAS_Query. Esto suele ser el caso por defecto, siempre y cuando el servidor de comunicaciones y los procesos de DAS se estén ejecutando.

La pestaña *Datos de informes* es una *interfaz de gestión de resúmenes* para Sentinel que permite habilitar e inhabilitar los **resúmenes**. Al habilitar un resumen, la función de adición puede comenzar a calcular los conteos para dicho resumen.

Un resumen es un conjunto definido de atributos que componen la clave para la que debe calcularse el número de sucesos exclusivos (conteo de eventos) en intervalos de media hora (tiempo del evento). En el caso de *EventSevDestPortSummary*, cuando se encuentre *activo*, guardará el conteo de eventos para cada combinación exclusiva de puerto de destino y gravedad durante un período de una hora. Estos cálculos guardados de los datos de eventos permiten una generación más rápida de informes y consultas de resumen. Estos informes los utiliza Crystal Reports. Consulte los capítulos sobre la instalación de Crystal Reports de la Guía de instalación de Sentinel para obtener más información. Para garantizar la precisión de los informes de resumen, algunos resúmenes deberán estar *activos*.

La función de adición es el proceso de calcular el conteo en ejecución de todos los resúmenes activos a medida que los eventos pasan por el sistema. Estos conteos en ejecución se guardan en la tabla correspondiente de resúmenes de la base de datos.

Ventajas de los resúmenes:

- Importante reducción del conjunto de datos de eventos
- Dimensiones conformadas que permiten realizar búsquedas detalladas y horizontales, así como transferencias ascendentes de los datos de eventos
- Ejecución mucho más rápida de los informes de resumen con resúmenes precalculados

Ventajas de la función de adición:

- Sólo procesa los resúmenes activos.
- No afecta a la inserción de eventos en la base de datos en tiempo real.

La pestaña Datos de informes permite realizar las operaciones siguientes:

- Habilitar/inhabilitar los resúmenes predefinidos
- Ver los atributos de cada resumen
- Ver la validez de un resumen para un período de tiempo
- Consultar los *archivos de eventos* que deben ejecutarse para que se complete el resumen

En la tabla siguiente se incluyen todos los resúmenes ya definidos en el sistema. Se incluye el nombre del resumen, el nombre de la tabla de base de datos y sus atributos en una descripción breve del resumen.

Nombre del resumen	Tabla/Descripción
EventSrcSummary	EVT_SRC_SMRY_1 En este resumen se realiza una suma del conteo de eventos por IP de origen, información de activo de origen, puerto de origen, usuario de origen, taxonomía, nombre de evento, recurso, recopilador, protocolo, gravedad y tiempo de evento por hora.
EventDestSummary	EVT_DEST_SMRY_1 En este resumen se realiza una suma del conteo de eventos por IP de destino, información de activo de destino, puerto de destino, usuario de destino, taxonomía, nombre de evento, recurso, recopilador, protocolo, gravedad y tiempo de evento por hora.
EventSevDestTxnmySummary	EVT_DEST_TXNMY_SMRY_1 En este resumen se realiza una suma del conteo de eventos por IP de destino, información de activo de destino, taxonomía, gravedad y tiempo de evento por hora.
EventSevDestEvtSummary	EVT_DEST_EVT_NAME_SMRY_1 En este resumen se realiza una suma del conteo de eventos por IP de destino, activo de evento destino, taxonomía, nombre de evento, gravedad y tiempo de evento por hora.
EventSevDestPortSummary	EVT_PORT_SMRY_1 En este resumen se realiza una suma del conteo de eventos por puerto de destino, gravedad y tiempo de evento por hora.
EventSevSummary	EVT_SEV_SMRY_1 En este resumen se realiza una suma del conteo de eventos por gravedad y tiempo de evento por hora.

Habilitación/inhabilitación del resumen

1. Haga clic en la pestaña *Datos de informes*.
2. Para inhabilitar un resumen, haga clic en el botón *Activo* de la columna Estado hasta que cambie a *Inactivo*.
3. Para habilitar un resumen, haga clic en *Inactivo* de la columna Estado hasta que cambie a *Activo*.

Source	Status
formedEvent	InActive
formedEvent	InActive
formedEvent	InActive
formedEvent	InActive
formedEvent	InActive
formedEvent	InActive

Para habilitar la *adición para los primeros 10 informes* de Crystal Reports:

- Habilite los tres resúmenes siguientes:
 - EventDestSummary
 - EventSevSummary
 - EventSrcSummary
- Habilite EventFileRedirectService en el archivo das_binary.xml que se encuentra en las ubicaciones siguientes:

En UNIX:

```
$ESEC_HOME/sentinel/config/das_binary.xml
```

En Windows:

```
%ESEC_HOME%\sentinel\config\das_binary.xml
```

Visualización de la información para un resumen

1. Haga clic en la pestaña *Datos de informes*.
2. Haga clic en el botón “...” de la columna Atributos para ver los atributos que componen un resumen.

Attributes	
IME.EVT_CNT	...
CUST_ID.DES	...
CUST_ID.DES	...
SEV.DEST_POI	...
CUST_ID.SEV	...
CUST_ID.RSR	...

Summary Attributes		
Summary Name: EventDestSummary		
SNo	Attribute	Attribute Type
1	CUST_ID	attribute
2	RSRC_ID	attribute
3	DEST_EVT_ASSET_ID	attribute
4	DEST_IP	attribute
5	DEST_PORT	attribute
6	DEST_USR_ID	attribute
7	TXNMY_ID	attribute
8	SEV	attribute
9	AGENT_ID	attribute
10	EVT_NAME_ID	attribute
11	PRTCL_ID	attribute
12	EVT_TIME	attribute

OK

Comprobación de la validez de un resumen

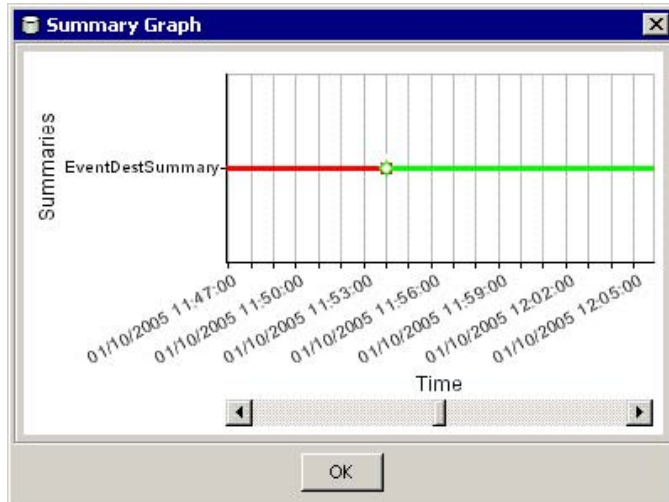
1. Haga clic en la pestaña *Datos de informes*.
2. Seleccione *Estado*.
3. Seleccione los resúmenes que desea consultar.

Summary Status	
Summary Name	
<input checked="" type="checkbox"/>	EventDestSummary
<input type="checkbox"/>	EventSevDestTxnmySummary
<input type="checkbox"/>	EventSevDestEvtSummary
<input type="checkbox"/>	EventSevDestPortSummary
<input type="checkbox"/>	EventSevSummary
<input type="checkbox"/>	EventSrcDestSummary

Time Interval

Between

4. Seleccione un intervalo de tiempo.
5. Haga clic en *Mostrar el gráfico*.
6. Las barras de color verde indican que el resumen se ha completado para el período de tiempo correspondiente. Las secciones de color rojo indican que al resumen le faltan datos durante el período de tiempo correspondiente.



NOTA: Para completar los resúmenes, consulte la sección sobre la *ejecución de archivos de eventos para un resumen*.

Consulta de los archivos de eventos para un resumen

1. Haga clic en la pestaña *Datos de informes*.
2. Seleccione *Estado*.
3. Seleccione los resúmenes que desea consultar.

Summary Name	
<input checked="" type="checkbox"/>	EventDestSummary
<input type="checkbox"/>	EventSevDestTxnmySummary
<input type="checkbox"/>	EventSevDestEvtSummary
<input type="checkbox"/>	EventSevDestPortSummary
<input type="checkbox"/>	EventSevSummary
<input type="checkbox"/>	EventSrcDestSummary

Time Interval
Between [] []

Show Event Show Graph Cancel

4. Seleccione un intervalo de tiempo.
5. Haga clic en *Mostrar el evento*.
6. Los archivos de eventos necesarios para completar el resumen aparecerán en formato de lista.

NOTA: Para completar los resúmenes, consulte la sección sobre la *ejecución de archivos de eventos para un resumen*.

Processed Summary Status					
	Summary	File Name	Min Event Time	Max Event Time	Process
1	EventDestSummary	events_20050110_1...	Mon Jan 10 13:27:02 EST...	Mon Jan 10 13:57:02 EST 2005	<input type="checkbox"/>
2	EventDestSummary	events_20050110_1...	Mon Jan 10 13:57:03 EST...	Mon Jan 10 14:27:03 EST 2005	<input type="checkbox"/>
3	EventDestSummary	events_20050110_1...	Mon Jan 10 14:27:53 EST...	Mon Jan 10 14:43:12 EST 2005	<input type="checkbox"/>
4	EventDestSummary	events_20050110_1...	Mon Jan 10 14:48:25 EST...	Mon Jan 10 15:19:17 EST 2005	<input type="checkbox"/>
5	EventDestSummary	events_20050110_1...	Mon Jan 10 15:15:17 EST...	Mon Jan 10 23:44:00 EST 2005	<input type="checkbox"/>
6	EventDestSummary	events_20050110_1...	Mon Jan 10 15:50:33 EST...	Mon Jan 10 16:20:33 EST 2005	<input type="checkbox"/>
7	EventDestSummary	events_20050110_1...	Mon Jan 10 16:20:40 EST...	Mon Jan 10 16:50:40 EST 2005	<input type="checkbox"/>
8	EventDestSummary	events_20050110_1...	Mon Jan 10 16:46:31 EST...	Mon Jan 10 17:20:40 EST 2005	<input type="checkbox"/>
9	EventDestSummary	events_20050110_1...	Mon Jan 10 17:16:32 EST...	Mon Jan 10 17:50:40 EST 2005	<input type="checkbox"/>
10	EventDestSummary	events_20050110_1...	Mon Jan 10 17:46:42 EST...	Mon Jan 10 18:20:49 EST 2005	<input type="checkbox"/>
11	EventDestSummary	events_20050110_1...	Mon Jan 10 18:20:38 EST...	Mon Jan 10 18:50:40 EST 2005	<input type="checkbox"/>
12	EventDestSummary	events_20050110_1...	Mon Jan 10 18:50:40 EST...	Mon Jan 10 19:20:41 EST 2005	<input type="checkbox"/>
13	EventDestSummary	events_20050110_1...	Mon Jan 10 19:20:42 EST...	Mon Jan 10 19:50:43 EST 2005	<input type="checkbox"/>
14	EventDestSummary	events_20050110_1...	Mon Jan 10 19:50:44 EST...	Mon Jan 10 20:20:44 EST 2005	<input type="checkbox"/>
15	EventDestSummary	events_20050110_1...	Mon Jan 10 20:20:45 EST...	Mon Jan 10 20:50:46 EST 2005	<input type="checkbox"/>
16	EventDestSummary	events_20050110_1...	Mon Jan 10 20:50:47 EST...	Mon Jan 10 21:20:46 EST 2005	<input type="checkbox"/>
17	EventDestSummary	events_20050110_1...	Mon Jan 10 21:20:48 EST...	Mon Jan 10 21:50:49 EST 2005	<input type="checkbox"/>

Ejecución de archivos de eventos para un resumen

1. Haga clic en la pestaña *Datos de informes*.
2. Seleccione *Estado*.
3. Seleccione los *resúmenes* que desea consultar.
4. Seleccione un intervalo de tiempo.
5. Haga clic en *Mostrar el evento*.
6. Los *archivos de eventos* necesarios para completar el resumen aparecerán en formato de lista.
7. Seleccione los *archivos de eventos* que desea ejecutar para completar el resumen.

ie	Min Even...	Max Eve...	Process
...	Mon Jan ...	Mon Jan ...	<input checked="" type="checkbox"/>
...	Mon Jan ...	Mon Jan ...	<input checked="" type="checkbox"/>
...	Mon Jan ...	Mon Jan ...	<input checked="" type="checkbox"/>
...	Mon Jan ...	Mon Jan ...	<input checked="" type="checkbox"/>
...	Mon Jan ...	Mon Jan ...	<input type="checkbox"/>

8. Haga clic en *Proceso*.

Línea de comando del SDM

NOTA: Si el equipo no dispone de acceso a DAS_Binary ni DAS_Query, se puede utilizar la línea de comando del SDM en lugar de la GUI del SDM.

Cómo guardar las propiedades de conexión para el Gestor de datos de Sentinel

Esta operación debe realizarse antes de utilizar cualquier acción de la línea de comando del Gestor de datos de Sentinel distintas de la acción saveConnection.

Si ha ejecutado la GUI del SDM, puede utilizar el archivo sdm.connect que se ha creado en la GUI. Este archivo se encuentra en el directorio %ESEC_HOME%\sdm en Windows y \$ESEC_HOME/sdm en UNIX.

La función de guardado de la conexión guarda la información siguiente sobre la conexión junto con la contraseña cifrada en el archivo especificado (mediante el almacén de claves que se especifica en el archivo configuration.xml).

Este comando utiliza los indicadores siguientes:

-action	saveConnection
-server	<oracle o mssql>
-host	<dirección IP del host de la base de datos o nombre de host al que se conectará>
-port	<número de puerto de la base de datos al que se conectará [Oracle, por defecto:1521/SQL Server, por defecto:1433]>
-database	<nombre de la base de datos/SID al que conectarse>
-user	<nombre de usuario de la base de datos>
-password	<contraseña de la base de datos>
-winAuth	Utilizado para la autenticación de Windows. Si utiliza esta opción, no utilice -user ni -password.
-connectFile	<nombre de archivo para guardar la información de conexión [nombre de archivo de su elección]>

La aplicación guarda toda la información anterior junto con la contraseña cifrada en el archivo especificado y utiliza la información de conexión guardada para ejecutar las demás acciones de la línea de comando. Este paso debe efectuarse la primera vez que se inicia la aplicación y cada vez que desee cambiar la información de conexión que emplea la aplicación.

Ejecución de saveConnection

1. Ejecute el comando según se indica a continuación:

```
sdm -action saveConnection -server <oracle/mssql> -  
host <IPhost/NombreHost> -port <NúmPuerto> -  
database <NombreBDD/SID> [-driverProps  
<ArchivoPropiedades>] {-user <UsuarioBDD> -password  
<ContraseñaBDD> | -winAuth} -connectFile  
<NombreArchivoGuardarConexión>
```

En el ejemplo siguiente, se guardarán las conexiones para un host con una dirección IP de 172.16.0.36 en el puerto 1521 (por defecto para Oracle, para SQL Server, el puerto por defecto es 1433).

▪ Ejemplo para Oracle:

```
./sdm -action saveConnection -server oracle -host  
172.16.0.36 -port 1521 -database esec -user esecdba  
-password XXXXXX -connectFile sdm.connect
```

▪ Ejemplo para SQL Server:

```
sdm -action saveConnection -server mssql -host  
172.16.0.36 -port 1433 -database esec -user esecdba  
-password XXXXXX -connectFile sdm.connect
```


En el ejemplo siguiente, se guardarán las conexiones para un host con una dirección IP de 172.16.0.36 en el puerto 1433 con el nombre de base de datos esec_51 para la autenticación de Windows.

- Ejemplo para SQL Server (autenticación de Windows):

```
sdm -action saveConnection -server mssql -host
    172.16.1.3 -port 1433 -database esec_51 -winAuth -
    connectFile %ESEC_HOME%\sdm\sdm.connect
```

Esta operación hará que la información de conexión se guarde en el archivo sdm.connect. El resto de los comandos tomará este nombre de archivo como entrada con el fin de conectarse a la base de datos designada y efectuar sus acciones.

Gestión de particiones

Configuración de particiones

Esta opción sólo se aplica a Oracle. Esta acción (partitionConfig) se utiliza para configurar las particiones de la base de datos. Esta configuración controla el modo de adición de particiones a todas las tablas con particiones de Sentinel. Esta acción utiliza los indicadores siguientes:

```
-action      partitionConfig
-freq        <o bien "3D" o "2D", o bien "1D" o "1W">
```

Las opciones siguientes son las únicas admitidas

3D: tres particiones por día

2D: dos particiones por día

1D: una partición por día

1W: una partición por semana

```
-days       <Número de días que se deben añadir cuando se selecciona addPartitions>
-connectFile <Vía al nombre de archivo que se guarda mediante saveConnection>
```

Ejecución de partitionConfig

1. Ejecute este comando según se indica a continuación:

```
./sdm -action partitionConfig -freq <o bien 3D o 2D, o
    bien 1D o 1W> -days <número de días que se deben
    añadir cuando se selecciona "addPartitions">
    -connectFile <vía al nombre de archivo que se
    guarda mediante "saveConnection" (por
    defecto: %ESEC_HOME/sdm/sdm.connect)>
```

En el ejemplo siguiente, el sistema añadirá treinta particiones (3 particiones por 1 DÍA = 3 * 10).

```
./sdm -action partitionConfig -freq 3D -days 10 -
    connectFile sdm.connect
```

En el ejemplo siguiente, el sistema añadirá diez particiones (1 partición por 1 DÍA = 1 * 10).

```
./sdm -action partitionConfig -freq 1D -days 10 -  
connectFile sdm.connect
```

En el ejemplo siguiente, el sistema añadirá una partición (1 partición por 7 días = 1 * 10/7).

```
./sdm -action partitionConfig -size 1W -days 10 -  
connectFile sdm.connect
```

Adición de particiones

Esta acción (addPartitions) añade el número necesario de particiones de acuerdo con la configuración de particiones de las tablas siguientes:

- Oracle:
 - EVENTS
 - CORRELATED_EVENTS
 - EVT_DEST_EVT_NAME_SMRY_1
 - EVT_DEST_SMRY_1
 - EVT_DEST_TXNMY_SMRY_1
 - EVT_PORT_SMRY_1
 - EVT_SEV_SMRY_1
 - EVT_SRC_SMRY_1
- SQL Server
 - EVENTS
 - CORRELATED_EVENTS
 - EVT_DEST_EVT_NAME_SMRY_1
 - EVT_DEST_SMRY_1
 - EVT_DEST_TXNMY_SMRY_1
 - EVT_PORT_SMRY_1
 - EVT_SEV_SMRY_1
 - EVT_SRC_SMRY_1

Si el sistema está configurado para tener diez días de particiones, cada vez que se ejecute *addPartitions*, se comprobará para ver si hay diez días de particiones por delante. Si hay suficientes particiones para los próximos diez días, no se realizará ninguna acción. De lo contrario, la acción añadirá el número necesario de particiones para diez días.

Esta acción utiliza los indicadores siguientes:

```
-action          addPartitions  
-connectFile    <vía al nombre de archivo que se guarda mediante "saveConnection">
```

Ejecución de addPartitions

1. Ejecute este comando según se indica a continuación:

```
sdm -action addPartitions -connectFile <vía al nombre  
de archivo que se guarda mediante "saveConnection">
```

Ejemplo para Oracle:

```
./sdm -action addPartitions -connectFile sdm.connect
```

Ejemplo para SQL Server:

```
sdm -action addPartitions -connectFile sdm.connect
```

Particiones abandonadas

Esta acción (dropPartition) abandona de las tablas siguientes todas las particiones con una antigüedad superior al indicador keepDays:

- Oracle:
 - EVENTS
 - CORRELATED_EVENTS
 - EVT_DEST_EVT_NAME_SMRY_1
 - EVT_DEST_SMRY_1
 - EVT_DEST_TXNMY_SMRY_1
 - EVT_PORT_SMRY_1
 - EVT_SEV_SMRY_1
 - EVT_SRC_SMRY_1
- SQL Server
 - EVENTS
 - CORRELATED_EVENTS
 - EVT_DEST_EVT_NAME_SMRY_1
 - EVT_DEST_SMRY_1
 - EVT_DEST_TXNMY_SMRY_1
 - EVT_PORT_SMRY_1
 - EVT_SEV_SMRY_1
 - EVT_SRC_SMRY_1

Esta acción no abandona ninguna partición que no esté archivada. Para suprimir particiones no archivadas, utilice el indicador *forceDelete*. Si se utiliza forceDelete:

false o sin especificar	Se abandonan solamente las particiones con una antigüedad superior al valor de keepDays y las que se han archivado.
true	Se abandonan todas las particiones con una antigüedad superior al valor de keepDays, incluidas las particiones sin archivar.

Esta acción utiliza los indicadores siguientes:

-action	dropPartitions
-keepDays	<número de días que se conservará>
[-forceDelete]	<“true” o “false”>
-connectFile	<vía al nombre de archivo que se guarda mediante “ saveConnection ”>

NOTA: Si se abandona una partición que no se ha archivado, ésta no se podrá importar.

Ejecución de dropPartition

1. Ejecute este comando según se indica a continuación:

```
sdm -action dropPartitions [-forceDelete <>false>] -  
keepDays <número> -connectFile <vía al nombre de  
archivo que se guarda mediante el comando  
“saveConnection”>
```

En los ejemplos siguientes, se abandonan todas las particiones con una antigüedad superior a 30 días, con lo que se garantiza el archivado de éstas. Al final de la operación se indicarán todas las particiones que se han omitido (no eliminado) debido a que aún no se han archivado.

Ejemplo para Oracle:

```
./sdm -action dropPartitions -keepDays 30 -connectFile  
sdm.connect
```

```
./sdm -action dropPartitions -forceDelete false -  
keepDays 30 -connectFile sdm.connect
```

Ejemplo para SQL Server:

```
sdm -action dropPartitions -keepDays 30 -connectFile  
sdm.connect
```

```
sdm -action dropPartitions -forceDelete false -  
keepDays 30 -connectFile sdm.connect
```

Visualización de los resúmenes de las particiones

Esta acción (ViewPartitions) muestra el resumen de la partición de las siguientes tablas admitidas:

- Oracle:
 - EVENTS
 - CORRELATED_EVENTS
 - EVT_DEST_EVT_NAME_SMRY_1
 - EVT_DEST_SMRY_1
 - EVT_DEST_TXNMY_SMRY_1
 - EVT_PORT_SMRY_1
 - EVT_SEV_SMRY_1
 - EVT_SRC_SMRY_1
- SQL Server
 - EVENTS
 - CORRELATED_EVENTS
 - EVT_DEST_EVT_NAME_SMRY_1
 - EVT_DEST_SMRY_1
 - EVT_DEST_TXNMY_SMRY_1
 - EVT_PORT_SMRY_1
 - EVT_SEV_SMRY_1
 - EVT_SRC_SMRY_1

Este comando utiliza los indicadores siguientes:

```
-action          startGui  
-tableName      <nombre de una de las tablas anteriores>  
-connectFile    <vía al nombre de archivo que se guarda mediante "saveConnection">
```

Para visualizar los resúmenes de las particiones

1. Ejecute este comando según se indica a continuación:

```
sdm -action viewPartitions -tableName <nombre de la  
tabla> -connectFile <vía al nombre de archivo que  
se guarda mediante el comando "saveConnection">
```

En el ejemplo siguiente, se muestra una lista de las particiones de la tabla EVENTS y el estado de cada una de ellas.

- Ejemplo para Oracle:

```
./sdm -action viewPartitions -tableName EVENTS -
      connectFile sdm.connect
```

- Ejemplo para SQL Server:

```
sdm -action viewPartitions -tableName EVENTS -
     connectFile sdm.connect
```

Gestión de los archivos de reserva

Configuración de los archivos de reserva

Esta acción (archiveConfig) se utiliza para configurar la operación de archivado. En esta configuración se indica cómo se archivan los datos desde las tablas de Sentinel.

Esta acción utiliza los indicadores siguientes:

-action	archiveConfig
-dirPath	<vía al directorio válida en la que se escribirán los archivos archivados>
-keepDays	<número de días que se conservará>
-fileSize	(Sólo Oracle) <tamaño máximo de cada archivo archivado. Especificar KB, MB o GB>
-connectFile	<vía al nombre de archivo que se guarda mediante " saveConnection ">

Para Oracle, la vía al directorio dirPath debe especificarse como el parámetro UTL_FILE_DIR en el archivo init.ora según los requisitos de Oracle. Se debe disponer de uno de los elementos siguientes:

- UTL_FILE_DIR = *
- UTL_FILE_DIR = directorio específico en el que desea escribir los archivos en el archivo init.ora

Ejecución de archiveConfig

1. Ejecute este comando según se indica a continuación:

```
sdm -action archiveConfig -dirPath <vía al directorio
en el que se escribirán los archivos archivados> -
keepDays <número de días que se conservarán> -
fileSize <tamaño máximo de cada archivo archivado,
especificado en KB, MB o GB> -connectFile <vía al
nombre de archivo que se guarda mediante
"saveConnection">
```

- Ejemplo para Oracle:

En el ejemplo siguiente se archivan todos los datos de más de 13 días al directorio /tmp en segmentos con un tamaño superior a 1 GB.

```
./sdm -action archiveConfig -dirPath /tmp -keepDays 13
      -fileSize 1GB -connectFile sdm.connect
```

En el ejemplo siguiente se archivan todos los datos de más de 13 días al directorio /tmp en segmentos con un tamaño superior a 40 MB.

```
./sdm -action archiveConfig -dirPath /tmp -keepDays 13
      -fileSize 40MB -connectFile sdm.connect
```

Archivado de datos

Ejecute esta acción (archiveData) después de establecer la configuración del archivado (archiveConfig). Esta acción archiva los datos del nombre de tabla especificado según la configuración del archivado. Archiva los datos de las tablas siguientes:

- Oracle:
 - EVENTS
 - CORRELATED_EVENTS
- SQL Server
 - EVENTS
 - CORRELATED_EVENTS

NOTA: Las tablas de adición no se archivan.

Este comando utiliza los indicadores siguientes:

-action archiveData
-connectFile <vía al nombre de archivo que se guarda mediante “[saveConnection](#)”>

Ejecución de archiveData

1. Ejecute este comando según se indica a continuación:

```
sdm -action archiveData -connectFile <vía al nombre de
    archivo que se guarda mediante “saveConnection”>
```

- Ejemplo para Oracle:

En el ejemplo siguiente se archivan los eventos, sus valores personalizados y reservados y los eventos correlacionados desde la tabla EVENTS, EVT_RESERVED_VALUES, EVT_CUSTOM_VALUES y ASSOCIATIONS según el valor definido en la configuración del archivado ([archiveConfig](#)). El uso del valor definido en el ejemplo que se indica en la sección [Gestión de los archivos de reserva](#) archivará los datos con una antigüedad superior a 13 días.

```
./sdm -action archiveData -connectFile sdm.connect
```

- Ejemplo para SQL Server:

En el ejemplo siguiente se archivan los eventos y los eventos correlacionados según el valor definido en la configuración del archivado ([archiveConfig](#)). El uso del valor definido en el ejemplo que se indica en la sección [Gestión de los archivos de reserva](#) archivará los datos con una antigüedad superior a 13 días.

```
sdm -action archiveData -connectFile sdm.connect
```

Supresión de datos

Esta acción (`deleteData`) suprime los datos con una antigüedad superior al valor de “`keepDays`” del nombre de tabla especificado. Suprime los datos de las tablas siguientes:

- Oracle:
 - EVENTS
 - CORRELATED_EVENTS
 - EVT_DEST_EVT_NAME_SMRY_1
 - EVT_DEST_SMRY_1
 - EVT_DEST_TXNMY_SMRY_1
 - EVT_PORT_SMRY_1
 - EVT_SEV_SMRY_1
 - EVT_SRC_SMRY_1

- SQL Server
 - EVENTS
 - CORRELATED_EVENTS
 - EVT_DEST_EVT_NAME_SMRY_1
 - EVT_DEST_SMRY_1
 - EVT_DEST_TXNMY_SMRY_1
 - EVT_PORT_SMRY_1
 - EVT_SEV_SMRY_1
 - EVT_SRC_SMRY_1

Esta acción no abandona ninguna partición que no esté archivada. Si desea suprimir particiones sin archivar, el indicador opcional *forceDelete* tiene que tener especificado con el valor `true`. Si se utiliza *forceDelete*:

<code>false</code> o sin especificar	Se abandonan solamente las particiones con una antigüedad superior al valor de <code>keepDays</code> y las que se han archivado.
<code>true</code>	Se abandonan todas las particiones con una antigüedad superior al valor de <code>keepDays</code> , incluidas las particiones sin archivar.

Este comando utiliza los indicadores siguientes:

<code>-action</code>	<code>deleteData</code>
<code>-keepDays</code>	<número de días que se conservará>
<code>[-forceDelete]</code>	< <code>true</code> o <code>false</code> >
<code>-connectFile</code>	<vía al nombre de archivo que se guarda mediante “ saveConnection ”>

Ejecución de `deleteData`

1. Ejecute este comando según se indica a continuación:

```
sdm -action deleteData -keepDays <número de días que se conservará> -connectFile <vía al nombre de archivo que se guarda mediante “saveConnection”>
```

- Ejemplo para Oracle:

En el ejemplo siguiente se abandonan las particiones de las tablas EVENTS y CORRELATED_EVENTS con una antigüedad superior a 13 días, con lo que se garantiza el archivado de éstas. Al final, se genera una lista de todas las particiones que no se han suprimido si no se han archivado.

```
./sdm -action deleteData -keepDays 13 -connectFile
sdm.connect
```

- Ejemplo para SQL Server:

En el ejemplo siguiente se abandonan las particiones de todas las tablas con una antigüedad superior a 13 días, con lo que se garantiza el archivado de éstas. Al final, se ofrece una lista de todas las particiones que no se ha suprimido si no se han archivado.

```
sdm -action deleteData -keepDays 13 -connectFile
sdm.connect
```

Gestión de la importación

Listado de archivos para importar

Esta acción (filesToImport) se utiliza para enumerar los archivos en los que se deben importar los datos entre fechas específicos de las siguientes tablas admitidas:

- Oracle:
 - HIST_EVENTS
 - HIST_CORRELATED_EVENTS
- SQL Server
 - HIST_EVENTS
 - HIST_CORRELATED_EVENTS

Este comando utiliza los indicadores siguientes:

```
-action      filesToImport
-startDate   <mm/dd/aaaa hh24:mi:ss>
-endDate     <mm/dd/aaaa hh24:mi:ss>
-connectFile <vía al nombre de archivo que se guarda mediante "saveConnection">
```

NOTA: hh24 representa las horas en el formato de 24 horas. Por ejemplo, 1:15:00 p.m. es 13:15:00 y 3:00:00 a.m. es 03:00:00.

Ejecución de filesToImport

1. Ejecute este comando según se indica a continuación:

```
sdm -action filesToImport -startDate <mm/dd/aaaa
hh24:mi:ss> -endDate <mm/dd/aaaa hh24:mi:ss> -
connectFile <vía al nombre de archivo que se guarda
mediante "saveConnection">
```

En el ejemplo siguiente se enumeran todos los archivos que contienen datos entre las fechas "09/25/2003 00:00:00" (25 de septiembre a la medianoche) y "09/26/2003 00:00:00" (26 de septiembre a la medianoche) y que se han archivado en una fecha anterior y pueden volver a importarse.

- Ejemplo para Oracle:

```
./sdm -action filesToImport -startDate 09/25/2003
      00:00:00 -endDate 09/26/2003 00:00:00 -connectFile
      sdm.connect
```

- Ejemplo para SQL Server:

```
sdm -action filesToImport -startDate 09/25/2003
     00:00:00 -endDate 09/26/2003 00:00:00 -connectFile
     sdm.connect
```

En el ejemplo siguiente se enumeran todos los archivos que contienen datos entre las fechas “09/25/2003 16:00:00” (25 de septiembre a las cuatro de la tarde) y “09/26/2003 18:00:00” (26 de septiembre a las seis de la tarde) y que se han archivado en una fecha anterior y pueden volver a importarse.

- Ejemplo para Oracle:

```
./sdm -action filesToImport -startDate 09/25/2003
      16:00:00 -endDate 09/26/2003 18:00:00 -connectFile
      sdm.connect
```

- Ejemplo para SQL Server:

```
sdm -action filesToImport -startDate 09/25/2003
     16:00:00 -endDate 09/26/2003 18:00:00 -connectFile
     sdm.connect
```

Importación de datos

Esta acción (importData) importa los datos entre fechas específicas en las siguientes tablas admitidas:

- Oracle:
 - HIST_EVENTS
 - HIST_CORRELATED_EVENTS
- SQL Server
 - HIST_EVENTS
 - HIST_CORRELATED_EVENTS

Si los datos ya se han importado o bien no se han encontrado datos archivados entre las fechas especificadas, aparecerá un mensaje.

La aplicación importa cada archivo en una tabla y genera la vista histórica sobre todas las tablas históricas. La vista del informe se une en la tabla original y en la vista histórica. Todos los informes utilizan la vista de informe; por lo tanto, se verán todos los datos importados.

Este comando utiliza los indicadores siguientes:

-action	importData
-startDate	<mm/dd/aaaa hh24:mi:ss>
-endDate	<mm/dd/aaaa hh24:mi:ss>
-dirPath	<directorio desde el que se importarán los archivos>
-connectFile	<vía al nombre de archivo que se guarda mediante “ saveConnection ”>

NOTA: hh24 representa las horas en el formato de 24 horas. Por ejemplo, 1:15:00 p.m. es 13:15:00 y 3:00:00 a.m. es 03:00:00.

Ejecución de importData

1. Coloque todos los archivos que se deben importar en un directorio específico (por ejemplo, dirPath - <directorio desde el que se importarán los archivos>).
2. Ejecute este comando según se indica a continuación:

```
sdm -action importData -dirPath <directorio desde el
que se importarán los archivos> -startDate
<mm/dd/aaaa hh24:mi:ss> -endDate <mm/dd/aaaa
hh24:mi:ss> -vía al nombre de archivo que se guarda
mediante "saveConnection">
```

En el ejemplo siguiente se importan los archivos archivados desde el directorio tmp que contienen datos entre las fechas "09/25/2003 00:00:00" (25 de septiembre a la medianoche) y "09/26/2003 00:00:00" (26 de septiembre a la medianoche) a las tablas mencionadas anteriormente.

- Ejemplo para Oracle:

```
./sdm -action importData -dirPath /tmp -startDate
09/25/2003 00:00:00 -endDate 09/26/2003 00:00:00
-connectFile sdm.connect
```

- Ejemplo para SQL Server:

```
sdm -action importData -dirPath c:\tmp -startDate
09/25/2003 00:00:00 -endDate 09/26/2003 00:00:00
-connectFile sdm.connect
```

En el ejemplo siguiente se importan los archivos archivados desde el directorio tmp que contienen datos entre las fechas "09/25/2003 08:30:00" (25 de septiembre a las 8.30 de la mañana) y "09/26/2003 20:00:00" (26 de septiembre a las 8.00 de la noche) a las tablas mencionadas anteriormente.

- Ejemplo para Oracle:

```
./sdm -action importData -dirPath /tmp -startDate
09/25/2003 08:00:00 -endDate 09/26/2003 20:00:00
-connectFile sdm.connect
```

- Ejemplo para SQL Server:

```
sdm -action importData -dirPath c:\tmp -startDate
09/25/2003 08:00:00 -endDate 09/26/2003 20:00:00
-connectFile sdm.connect
```

Supresión de datos importados

Esta acción (dropImported) suprime los datos importados entre las fechas especificadas de las siguientes tablas admitidas:

- Oracle:
 - HIST_EVENTS
 - HIST_CORRELATED_EVENTS
- SQL Server
 - HIST_EVENTS
 - HIST_CORRELATED_EVENTS

Si no existen datos importados entre las dos fechas especificadas, aparecerá un mensaje.

Este comando utiliza los indicadores siguientes:

```
-action          dropImported
-startDate       <mm/dd/aaaa hh24:mi:ss>
-endDate         <mm/dd/aa hh24:mi:ss>
-connectFile     <vía al nombre de archivo que se guarda mediante “saveConnection”>
```

NOTA: hh24 representa las horas en el formato de 24 horas. Por ejemplo, 1:15:00 p.m. es 13:15:00 y 3:00:00 a.m. es 03:00:00.

Ejecución de dropImported

1. Ejecute este comando según se indica a continuación:

```
sdm -action dropImported -startDate <mm/dd/aaaa
    hh24:mi:ss> -endDate <mm/dd/aaaa hh24:mi:ss> -
    connectFile <vía al nombre de archivo que se guarda
    mediante “saveConnection”>
```

En el ejemplo siguiente se suprimen los datos importados entre las fechas especificadas de las tablas mencionadas anteriormente:

- Ejemplo para Oracle:

```
./sdm -action dropImported -startDate 09/25/2003
    00:00:00 -endDate 09/26/2003 00:00:00 -connectFile
    sdm.connect
```

- Ejemplo para SQL Server:

```
sdm -action dropImported -startDate 09/25/2003
    00:00:00 -endDate 09/26/2003 00:00:00 -connectFile
    sdm.connect
```

Gestión de los espacios de tabla

En la gestión de los espacios de tabla se incluye una opción de línea de comando y una opción de la GUI. La línea de comando permite realizar las operaciones siguientes:

- Ver el uso del espacio de la base de datos de Sentinel

La GUI permite realizar las operaciones siguientes:

- Ver particiones
- Ver particiones archivadas
- Ver particiones de importación
- Ver el uso del espacio

Visualización del uso del espacio de la base de datos de Sentinel (línea de comando)

Esta acción (dbstats) muestra el uso de la base de datos de Sentinel de todos los espacios de tabla de Sentinel en Oracle y grupos de archivos de Sentinel en MS SQL.

Este comando utiliza los indicadores siguientes:

```
-action          dbstats
-connectFile     <vía al nombre de archivo que se guarda mediante “saveConnection”>
```

Visualización del uso del espacio de la base de datos de Sentinel (línea de comando)

1. Ejecute el comando siguiente:

```
sdm -action dbStats -connectFile <vía al nombre de
      archivo que se guarda mediante "saveConnection">
```

- Ejemplo para Oracle:

En el ejemplo siguiente se muestran los espacios de tabla de la base de datos de Sentinel con su espacio total, el espacio utilizado y el espacio libre disponible.

```
./sdm -action dbStats -connectFile sdm.connect
```

- Ejemplo para SQL Server:

En el ejemplo siguiente se muestran los grupos de archivos de la base de datos de Sentinel con su espacio total, el espacio utilizado y el espacio libre disponible.

```
sdm -action dbStats -connectFile sdm.connect
```

Actualización de asignaciones (línea de comando)

Esta acción (updateMapData) permite sustituir el archivo de datos de origen de asignación por otro. El nuevo archivo de origen de datos debe tener los mismos delimitadores, columnas de claves y columna activada que la asignación anterior. De no ser así, utilice la función [Editar](#) de la GUI del SDM.

Este comando utiliza los indicadores siguientes:

```
-action      updateMapData
-map         <nombre de la asignación>
-file       <nombre de archivo>
-backup     <true/false> (por defecto:true)
-connectFile <vía al nombre de archivo que se guarda mediante "saveConnection">
```

El indicador `-backup` permite crear una copia de seguridad del archivo de asignaciones original en la carpeta `map_data`. La copia de seguridad del archivo de asignaciones de datos se guardará como un archivo `.bak` con un conjunto de números aleatorios al final del archivo. Por ejemplo: `threat10197.bak`.

Actualización (sustitución) de una asignación

1. Ejecute el comando siguiente:

```
sdm -action updateMapData -map <nombre de la
      asignación> -file <nombre de archivo> [-backup
      <true/false> (por defecto:true)] -connectFile <vía
      al nombre de archivo que se guarda mediante
      "saveConnection">
```

En el ejemplo siguiente se sustituyen las asignaciones de la asignación "threat" por las asignaciones del archivo de asignaciones "vuln_attacks.txt".

```
sdm -action updateMapData -map threat -file
      vuln_attacks.txt -connectFile sdm.connect
```

Dado que no se ha utilizado el indicador `-backup`, la operación por defecto creará una copia de seguridad de la asignación original antes de actualizarla con el archivo "vuln_attack.txt".

Uso del guión de gestión automática Novell suministrado (sólo para Windows)

Novell ha desarrollado un archivo por lotes que se puede programar de modo que muchas de las acciones de gestión del SDM se puedan realizar automáticamente.

NOTA: Si el equipo no dispone de acceso a DAS_Binary ni DAS_Query, se puede utilizar la línea de comando del SDM en lugar de la GUI del SDM.

Este procedimiento sólo se aplica para entornos de Windows. Al efectuar las tareas previas a la configuración y la configuración, asegúrese de llevar a cabo las operaciones siguientes:

- Compruebe que se ha inicializado sdm.connect mediante la GUI de SDM o la línea de comando.
- Compruebe que existe el directorio de archivado.
- Compruebe que los días de archiveConfig y dropPartitions son iguales.
- Compruebe que el archivo por lotes se ejecuta correctamente en el indicador de comandos al menos una vez antes de programarlo para que se ejecute automáticamente.

NOTA: Si se produce un error en la tarea programada, no se enviará ninguna notificación. Se registrará en SDM_*.log.

Configuración del archivo Manage_data.bat para el archivado de datos y la adición de particiones

Tareas previas a la configuración

Antes de ajustar automáticamente las opciones de archivado de datos y adición de particiones, se deben realizar las operaciones siguientes:

- [Guardar las propiedades de la conexión](#)
- [Establecer los parámetros de archivado](#)

NOTA: Si un archivo de conexión se ha guardado en una ubicación diferente o con un nombre diferente del valor por defecto (%ESEC_HOME%\sdm\sdm.connect), se deberá editar el archivo manage_data.bat para actualizar la vía a dicho archivo.

Establecimiento de los parámetros de archivado

Esta operación se puede realizar mediante la línea de comando.

Esta acción (archiveConfig) se utiliza para configurar el archivado. En esta configuración se indica cómo se archivan los datos desde las tablas de Sentinel.

Esta acción utiliza los indicadores siguientes:

-action	archiveConfig
-dirPath	<vía al directorio válida en la que se escribirán los archivos archivados>
-keepDays	<número de días que se conservará>
-connectFile	<vía al nombre de archivo que se guarda mediante " saveConnection ">

Establecimiento de los parámetros de archivado a través de la línea de comando

1. Cree un directorio de salida de archivo en la raíz denominado SDM_archivo_de_reserva (c:\SDM_archivo_de_reserva).

NOTA: Si crea un directorio de salida o una ubicación distinta, deberá editar el archivo `manage_data.bat`.

2. Ejecute este comando según se indica a continuación:

```
sdm -action archiveConfig -dirPath <vía al directorio
en el que se guardarán los archivos archivados> -
keepDays <número de días que se conservarán> -
connectFile <vía al nombre de archivo que se guarda
mediante "saveConnection">
```

En el ejemplo siguiente se archivarán todos los datos con una antigüedad superior a 30 días en el directorio `c:\SDM_archivo_de_reserva`.

```
sdm -action archiveConfig -dirpath c:\SDM_archive -
keepDays 30 -connectFile sdm.connect
```

Establecimiento de los parámetros de archivado a través de la GUI

1. Cree un directorio de salida de archivo en la raíz denominado `SDM_archivo_de_reserva` (`c:\SDM_archivo_de_reserva`).

NOTA: Si crea un directorio de salida o una ubicación distinta, deberá editar el archivo `manage_data.bat`.

2. La GUI del SDM no requiere parámetros de archivado, ya que puede archivar datos directamente sin necesidad de establecer dichos parámetros.

Supresión de datos (abandonar particiones)

Esta acción (`deleteData`) suprime los datos con una antigüedad superior al valor de “`keepDays`” del nombre de tabla especificado. Suprime los datos de las tablas siguientes:

- EVENTS
- CORRELATED_EVENTS
- EVT_DEST_EVT_NAME_SMRY_1
- EVT_DEST_SMRY_1
- EVT_DEST_TXNMY_SMRY_1
- EVT_PORT_SMRY_1
- EVT_SEV_SMRY_1
- EVT_SRC_SMRY_1

Esta acción no abandona ninguna partición que no esté archivada. Si desea suprimir particiones sin archivar, el indicador opcional *forceDelete* tiene que tener especificado con el valor `true`. Si se utiliza `forceDelete`:

false o sin especificar	Se abandonan solamente las particiones con una antigüedad superior al valor de <code>keepDays</code> y las que se han archivado.
true	Se abandonan todas las particiones con una antigüedad superior al valor de <code>keepDays</code> , incluidas las particiones sin archivar.

Este comando utiliza los indicadores siguientes:

-action	<code>deleteData</code>
-keepDays	<número de días que se conservará>
[-forceDelete]	<true o false>
-connectFile	<vía al nombre de archivo que se guarda mediante " saveConnection ">

Ejecución de deleteData

1. Ejecute este comando según se indica a continuación:

```
sdm -action deleteData -keepDays <número de días que se conservará> -connectFile <vía al nombre de archivo que se guarda mediante "saveConnection">
```

En el ejemplo siguiente se abandonan las particiones de las tablas con una antigüedad superior a 30 días, con lo que se garantiza el archivado de éstas. Al final, se ofrece una lista de todas las particiones que no se ha suprimido si no se han archivado.

```
sdm -action deleteData -keepDays 30 -connectFile sdm.connect
```

Programación del archivo Manage_data.bat para el archivado de datos y la adición de particiones

NOTA: El archivo manage_data.bat se define con un valor de keepDay de 30, una salida de archivo en c:\SDM_archivo_de_reserva y el archivo de conexión en %ESEC_HOME%\SDM\sdm.connect. Si los valores que utiliza no son los mismos, deberá editar el archivo manage_data.bat.

Si ha definido las propiedades de conexión y los parámetros de archivado, ejecute el archivo manage_data.bat desde el indicador de comandos para asegurarse de que funciona.

Para programar automáticamente el archivado de datos y la adición de particiones

NOTA: Los pasos siguientes son para Windows 2000 Professional. Los pasos para Windows 2000 Server y XP pueden variar, pero son similares.

1. En Windows, haga clic en *Inicio* > *Configuración* > *Panel de control*.
2. Haga doble clic en *Tareas programadas*.
3. Haga doble clic en *Agregar tarea programada*. Haga clic en *Siguiente*.
4. Haga clic en *Examinar* y busque el archivo manage_data.bat.
5. Introduzca un nombre para la tarea programada como, por ejemplo, SDM_Archivo_de_reserva. En la sección *Realizar esta tarea*:, seleccione *Diariamente*. Haga clic en *Siguiente*.
6. Seleccione una hora y un día en los que desea ejecutar esta tarea. Haga clic en *Siguiente*.
7. Introduzca la fecha y la hora que desee. Haga clic en *Siguiente*.



8. Introduzca el usuario bajo el que se ejecutará esta tarea. El usuario no puede ser la cuenta del sistema local. Debe ejecutarse como un usuario específico. Haga clic en *Siguiente*.
9. Haga clic en *Finalizar* para finalizar la tarea programada.

11

Utilidades

Inicio y detención del servidor de Sentinel y del Gestor de recopiladores en UNIX

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

Inicio del servidor de Sentinel para UNIX

En un entorno UNIX, al iniciar el servidor de Sentinel también se inicia el servidor de comunicaciones.

Inicio del servidor de Sentinel para UNIX

1. Como usuario esecadm, cambie al directorio \$ESEC_HOME/sentinel/scripts.
2. Ejecute el comando siguiente:

```
./sentinel.sh start
```

Detención del servidor de Sentinel para UNIX

En un entorno UNIX, al cerrarse el servidor de Sentinel también se cierra el servidor de comunicaciones.

Cierre del servidor de Sentinel para UNIX

1. Como usuario esecadm, cambie al directorio \$ESEC_HOME/sentinel/scripts.
2. Ejecute el comando siguiente:

```
./sentinel.sh stop
```

Inicio del Gestor de recopiladores para UNIX

Inicio del Gestor de recopiladores para UNIX

1. Como usuario esecadm, cambie al directorio \$WORKBENCH_HOME.
2. Ejecute el comando siguiente:

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

Detención del Gestor de recopiladores para UNIX

Cierre del Gestor de recopiladores para UNIX

1. Como usuario esecadm, cambie al directorio \$WORKBENCH_HOME.
2. Ejecute el comando siguiente:

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

Inicio y detención del servidor de Sentinel y del Gestor de recopiladores en Windows

Según la configuración de la instalación, puede haber hasta tres servicios de Sentinel en ejecución en el equipo. Son los siguientes:

- Sentinel: vigilancia, este servicio se inicia en todos los demás procesos del servidor de Sentinel.
- Comunicación de Sentinel: este servicio representa el servidor de comunicaciones cifrado.
- Gestor de recopiladores: este servicio es el asistente.

En los Servicios de Windows, se puede iniciar, reiniciar o detener manualmente cualquiera de estos servicios.

Inicio del Gestor de recopiladores para Windows

Inicio del Gestor de recopiladores para Windows

1. Haga clic en *Inicio > Configuración > Panel de control*.
2. Haga doble clic en *Herramientas administrativas*.
3. Haga doble clic en *Servicios*.
4. Haga clic con el botón derecho del ratón en *Gestor de recopiladores > Iniciar*.

Detención del Gestor de recopiladores para Windows

Detención del Gestor de recopiladores para Windows

1. Haga clic en *Inicio > Configuración > Panel de control*.
2. Haga doble clic en *Herramientas administrativas*.
3. Haga doble clic en *Servicios*.
4. Haga clic con el botón derecho del ratón en *Gestor de recopiladores > Detener*.

Inicio del servidor de Sentinel para Windows

Inicio del servidor de Sentinel para Windows

1. Haga clic en *Inicio > Configuración > Panel de control*.
2. Haga doble clic en *Herramientas administrativas*.
3. Haga doble clic en *Servicios*.
4. En la ventana Servicios, resalte *Sentinel*.
5. Haga clic con el botón derecho del ratón en *> Iniciar* o bien, haga clic en *Iniciar* de la barra de herramientas.

Detención del servidor de Sentinel para Windows

Detención del servidor de Sentinel para Windows

1. Haga clic en *Inicio > Configuración > Panel de control*.
2. Haga doble clic en *Herramientas administrativas*.
3. Haga doble clic en *Servicios*.
4. En la ventana Servicios, resalte *Sentinel*.
5. Haga clic con el botón derecho del ratón en *> Detener* o bien, haga clic en *Detener* de la barra de herramientas.

Inicio del servidor de comunicaciones de Sentinel para Windows

Inicio del servidor de comunicaciones de Sentinel para Windows

1. Haga clic en *Inicio > Configuración > Panel de control*.
2. Haga doble clic en *Herramientas administrativas*.
3. Haga doble clic en *Servicios*.
4. En la ventana Servicios, resalte *Comunicación de Sentinel*.
5. Haga clic con el botón derecho del ratón en *> Iniciar* o bien, haga clic en *Iniciar* de la barra de herramientas.

Detención del servidor de comunicaciones de Sentinel para Windows

Cierre del servidor de comunicaciones de Sentinel para Windows

1. Haga clic en *Inicio > Configuración > Panel de control*.
2. Haga doble clic en *Herramientas administrativas*.
3. Haga doble clic en *Servicios*.
4. En la ventana Servicios, resalte *Comunicación de Sentinel*.
5. Haga clic con el botón derecho del ratón en *> Detener* o bien, haga clic en *Detener* de la barra de herramientas.

Archivos de guión de Sentinel

Según la configuración de la instalación, el directorio \$ESEC_HOME/sentinel/scripts o %ESEC_HOME%\sentinel\scripts pueden contener algunos o todos los archivos de guión siguientes:

Archivo de guión:	Descripción:	
▪ remove_sonic_lock.bat	Este guión permite eliminar los archivos de bloqueo del servidor de comunicaciones.	
▪ start_broker.bat	Estos guiones permiten iniciar el servidor de comunicaciones en la línea de comando en modo de consola.	
▪ start_broker.sh		
▪ stop_broker.bat	Estos guiones permiten detener el servidor de comunicaciones en la línea de comando en modo de consola.	
▪ stop_broker.sh		
▪ stop_container.bat	Estos guiones permiten reiniciar los contenedores siguientes:	
▪ stop_container.sh		
		▪ DAS_Aggregation
		▪ DAS_RT
		▪ DAS_iTRAC
	▪ DAS_Binary	
	▪ DAS_Query	
▪ sentinel.sh	Este guión cierra o inicia el servidor de Sentinel. Consulte Inicio del servidor de Sentinel para UNIX o Detención del servidor de Sentinel para UNIX .	

Eliminación de los archivos de bloqueo del servidor de comunicaciones

En el caso de que el sistema se apague de forma incorrecta, es posible que el servidor de comunicaciones se bloquee. Tras eliminar los archivos de bloqueo, deberá reiniciarse el servidor de comunicaciones. Estos archivos se encuentran en las ubicaciones siguientes:

En Windows:

```
%ESEC_HOME%\3rdparty\SonicMQ\MQ6.1\esecDomain\data\_MFSys  
tem\lock  
%ESEC_HOME%\3rdparty\SonicMQ\MQ6.1\SonicMQStore\db.lck
```

En UNIX:

```
$ESEC_HOME/3rdparty/SonicMQ/MQ6.1/esecDomain/data/_MFSys  
tem/lock  
$ESEC_HOME /3rdparty/SonicMQ/MQ6.1/SonicMQStore/db.lck
```

Eliminación del archivo de bloqueo del servidor de comunicaciones (Windows)

1. Cambie al directorio siguiente o utilice Windows Explorer para dirigirse a la ubicación siguiente:

```
%ESEC_HOME%\sentinel\scripts
```

2. Haga doble clic en el nombre de guión (en Windows Explorer) o bien ejecute el archivo siguiente:

```
remove_sonic_lock.bat
```

Eliminación del archivo de bloqueo del servidor de comunicaciones (UNIX)

Normalmente, no es necesario eliminar el archivo de bloqueo en un entorno UNIX, ya que este archivo suele eliminarse automáticamente cuando se inicia el servidor de Sentinel. Si hay que eliminarlos manualmente, deben eliminarse mediante los comandos estándar del sistema de archivos UNIX (por ejemplo, rm).

Inicio del servidor de comunicaciones en modo de consola

Estos guiones permiten iniciar el servidor de comunicaciones en la línea de comando en modo de consola y son de gran utilidad a la hora de depurar el servidor de comunicaciones sin tener que ejecutar el resto del servidor de Sentinel. Durante el funcionamiento normal, estos guiones no deben utilizarse (en su lugar, deben utilizarse las instrucciones que se describen en [Inicio del servidor de Sentinel para UNIX](#) o [Inicio del servidor de Sentinel para Windows](#)).

Inicio del servidor de comunicaciones (Windows)

NOTA: Al iniciar este guión en Windows, no se indicará como iniciado en la ventana Servicios y sólo se ejecutará si la ventana del indicador de comandos permanece abierta.

1. Cambie al directorio o utilice Windows Explorer para dirigirse a la ubicación siguiente:

```
%ESEC_HOME%\sentinel\scripts
```

2. Haga doble clic en la dirección anterior (en Windows Explorer) o bien ejecute el archivo siguiente:

```
start_broker.bat
```

Inicio del servidor de comunicaciones (UNIX)

1. Entre a la sesión como el usuario esecadm.
2. Cambie al directorio siguiente:

```
$ESEC_HOME/sentinel/scripts
```

3. Introduzca:

```
./start_broker.sh
```

Detención del servidor de comunicaciones en modo de consola

Estos guiones permiten detener el servidor de comunicaciones en la línea de comando en modo de consola y son de gran utilidad a la hora de depurar el servidor de comunicaciones sin tener que detener el resto del servidor de Sentinel. Durante el funcionamiento normal, estos guiones no deben utilizarse (en su lugar, deben utilizarse las indicaciones que se describen en [Detención del servidor de Sentinel para UNIX](#) o [Inicio del servidor de Sentinel para Windows](#)).

Detención del servidor de comunicaciones (Windows)

1. Cambie al directorio o utilice Windows Explorer para dirigirse a la ubicación siguiente:

```
%ESEC_HOME%\sentinel\scripts
```

2. Haga doble clic en el nombre de guión (en Windows Explorer) o bien ejecute el archivo siguiente:

```
stop_broker.bat
```

Detención del servidor de comunicaciones (UNIX)

1. Entre a la sesión con el usuario esecadm.
2. Cambie al directorio siguiente:

```
$ESEC_HOME/sentinel/scripts
```

3. Introduzca:

```
./stop_broker.sh
```

Reinicio de los contenedores de Sentinel

Los siguientes guiones reinician los contenedores que se indican a continuación y envían un mensaje al servicio especificado para que se apague. A continuación, la vigilancia de Sentinel reinicia el servicio.

El método preferido para detener, iniciar o reiniciar estos servicios de contenedor es mediante el uso de las vistas del servidor de la pestaña Admin del Centro de control de Sentinel.

Nombre	Descripción
▪ DAS_Aggregation	(das_aggregation.xml) se utiliza para ejecutar y configurar el servicio de adición.
▪ DAS_RT	(das_rt.xml) se utiliza para ejecutar y configurar el servicio de vistas en tiempo real.
▪ DAS_iTRAC	(das_itrac.xml) se utiliza para configurar el servicio iTRAC.
▪ DAS_Binary	(das_binary.xml) se utiliza para la operación de inserción de eventos y de eventos correlacionados.
▪ DAS_Query	(das_query.xml) todas las demás operaciones de base de datos.

Reinicio de un contenedor de Sentinel (Windows)

1. Cambie al directorio siguiente:

```
%ESEC_HOME%\sentinel\scripts
```

2. Introduzca:

```
stop_container.bat <equipo host> <nombre del  
contenedor>
```

Por ejemplo:

```
stop_container.bat localhost DAS_RT
```

Reinicio de un contenedor de Sentinel (UNIX)

1. Entre a la sesión como el usuario esecadm.
2. Cambie al directorio siguiente:

```
$ESEC_HOME/sentinel/scripts
```

3. Introduzca:

```
./stop_container <equipo host> <nombre del contenedor>
```

Por ejemplo:

```
./stop_container localhost DAS_RT
```

Información sobre la versión

Información sobre la versión del servidor de Sentinel

El servidor de Sentinel dispone de una opción de línea de comando para visualizar la información sobre la versión de los procesos siguientes:

- watchdog
- rulelg_checker
- correlation_engine
- data_synchronizer
- query_manager
- DAS

Cómo obtener la información sobre la versión de Sentinel (UNIX)

1. Cambie al directorio siguiente:

```
$ESEC_HOME/sentinel/bin
```

2. Introduzca:

```
./<proceso> -version
```

Por ejemplo:

```
./correlation_engine -version
```

Cómo obtener la información sobre la versión de Sentinel (Windows)

1. Cambie al directorio siguiente:

```
%ESEC_HOME%\sentinel\bin
```

2. Introduzca:

```
<proceso> -version
```

Por ejemplo:

```
correlation_engine -version
```

Información sobre la versión de los archivos .dll y .exe de Sentinel

Cómo obtener información sobre la versión de los archivos .dll y .exe de Sentinel

1. Cambie el directorio %ESEC_HOME%.
2. En los distintos subdirectorios, haga clic con el botón derecho del ratón en un archivo .dll o .exe y seleccione Propiedades.
3. Haga clic en la pestaña Versión.
4. En el panel Nombre del elemento, seleccione Versión del producto. El número de la versión del archivo aparecerá en el panel Valor.

Información sobre la versión del archivo .jar de Sentinel

Cómo obtener la información sobre la versión del archivo .jar de Sentinel

1. En el servidor de Sentinel, entre a la sesión como el usuario siguiente:

En UNIX:

```
esecadm
```

En Windows, entre a la sesión como usuario con derechos sobre el servidor de Sentinel.

2. Cambie al directorio siguiente:

En UNIX:

```
$ESEC_HOME/utilities
```

En Windows:

```
%ESEC_HOME%\utilities
```

3. O bien, escriba lo siguiente en la línea de comando:

En UNIX:

```
./versionreader.sh <v 徹/nombre del archivo jar>
```

En Windows:

```
versionreader <vía/nombre del archivo jar>
```

Configuración del correo electrónico de Sentinel

Los valores de configuración del correo electrónico de Sentinel se almacenan en el archivo `execution.properties` durante la instalación. Este archivo se puede editar después de la instalación y se encuentra en el equipo en el que está instalado DAS en la ubicación siguiente:

En Windows:

```
%ESEC_HOME%\sentinel\config
```

En UNIX:

```
$ESEC_HOME/sentinel/config
```

Existen dos guiones (`mailconfig.sh` y `mailconfigtest.sh` para UNIX, y `mailconfig.bat` y `mailconfigtest.bat` para Windows) que modifican y prueban los valores de configuración del correo electrónico dentro del archivo `execution.properties`. El guión `mailconfig.*` modifica los valores de configuración del correo electrónico y el guión `mailconfigtest.*` realiza una prueba de éstos. Las áreas en negrita representan una configuración del correo electrónico que se puede modificar.

Las propiedades en el archivo `execution.properties` son las siguientes:

mail.authentication.user=<dominio\usuario>

`correlated events retry wait=5000`

mail.smtp.host=<HOST_SMTP>

El host SMTP que se utilizará para enviar correo electrónico.

mail.events.max=1000

Número máximo de eventos que se enviarán en un mensaje de correo electrónico que active automáticamente el motor de correlación. Está diseñado para limitar el tamaño de los mensajes de correo electrónico para los eventos correlacionados con un conjunto importante de eventos de activación.

correlated events retry count=10

mail.address.from=
<SMTP_DIRECCIÓN_ORIGEN>

La dirección de correo electrónico que aparecerá en el campo De del mensaje de correo electrónico enviado desde DAS.

mail.authentication.password=<contraseña>

Contraseña para mail.authentication.user.

Los guiones mailconfig.sh y mailconfig.bat utilizan los argumentos siguientes:

-host Nombre del host SMTP o dirección IP
-from Campo De del mensaje de correo electrónico
-user El usuario de autenticación de correo
-password Contraseña para el usuario de autenticación de correo

NOTA: No introduzca la contraseña después del argumento `-password`, ya que el sistema le solicitará una nueva contraseña tras introducir el comando. La salida de la consola se ocultará mediante asteriscos (*).

Los archivos mailconfigtest.sh y mailconfig.bat utilizan el argumento siguiente:

-to Dirección de correo electrónico de destino

Para definir las propiedades de correo electrónico en el archivo execution.properties

1. En el equipo en el que está instalado DAS, cambie al directorio siguiente:

En UNIX:

```
$ESEC_HOME/sentinel/config
```

En Windows:

```
%ESEC_HOME%\sentinel\config
```

2. Ejecute mailconfig tal como se indica a continuación:

En UNIX:

```
./mailconfig.sh -host <servidor SMTP> -from <dirección  
de correo electrónico de origen> -user <usuario de  
autenticación de correo> -password
```

En Windows:

```
mailconfig.bat -host <servidor SMTP> -from <dirección  
de correo electrónico de origen> -user <usuario de  
autenticación de correo> -password
```

Ejemplo para UNIX:

```
./mailconfig.sh -host 10.0.1.14 -from  
mi_nombre@dominio.com -user mi_nombre_usuario -  
password
```

Ejemplo para Windows:

```
mailconfig.bat -host 10.0.1.14 -from  
mi_nombre@dominio.com -user mi_nombre_usuario -  
password
```

Tras introducir este comando, el sistema le solicitará una contraseña nueva.

```
Introducir contraseña:*****
```

```
Confirmar contraseña:*****
```

NOTA: Si se utiliza la opción de contraseña, ésta debe ser el último argumento.

Para realizar una prueba de la configuración del correo electrónico en el archivo `execution.properties`

1. En el equipo en el que está instalado DAS, cambie al directorio siguiente:

En UNIX:

```
$ESEC_HOME/sentinel/config
```

En Windows:

```
%ESEC_HOME%\sentinel\config
```

2. Ejecute `mailconfigtest` tal como se indica a continuación:

En UNIX:

```
./mailconfigtest.sh -to <dirección de correo  
electrónico de destino>
```

En Windows:

```
mailconfigtest.bat -to <dirección de correo  
electrónico de destino>
```

Si el mensaje se envía correctamente, aparecerá el mensaje siguiente en la pantalla y el mensaje de correo electrónico se habrá recibido en la dirección de destino.

```
El mensaje de correo electrónico se ha enviado correctamente.
```

Compruebe el buzón de entrada del correo electrónico de destino para confirmar la recepción del mensaje. La línea de tema y el contenido deben ser:

```
Tema: Prueba de las propiedades del correo de Sentinel
```

```
Esta es una prueba para la configuración de las  
propiedades del correo de Sentinel. Si ha recibido  
este mensaje, significa que las propiedades del  
correo de Sentinel se han configurado correctamente  
para enviar mensajes de correo electrónico.
```

Actualización de la clave de licencia

Si ha caducado la clave de licencia de Sentinel y Novell ha emitido una nueva, ejecute el programa de clave de software para actualizarla.

Cómo actualizar la clave de licencia (UNIX)

1. Entre a la sesión como el usuario esecadm.
2. Diríjase a \$ESEC_HOME/utilities.
3. Introduzca el comando siguiente:

```
./softwarekey
```
4. Introduzca el número 1 para definir la clave principal. Pulse la tecla Intro.

Cómo actualizar la clave de licencia (Windows)

1. Entre a la sesión como usuario con derechos administrativos.
2. Diríjase a %ESEC_HOME%\utilities.
3. Escriba el comando siguiente:

```
softwarekey.exe
```
4. Introduzca el número 1 para definir la clave principal. Pulse la tecla Intro.

12 Inicio rápido

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

En este capítulo se tratan los procedimientos de inicio rápido para los elementos siguientes:

- [Analistas de seguridad](#)
- [Analistas de informes](#)
- [Administradores](#)

Se tratarán los temas siguientes:

- [Vistas Active Views™](#)
- [Detección de explotaciones](#)
- [Datos del activo](#)
- [Consulta de eventos](#)
- [Informes de análisis a través de Crystal Reports](#)
- [Correlación básica](#)

Analistas de seguridad

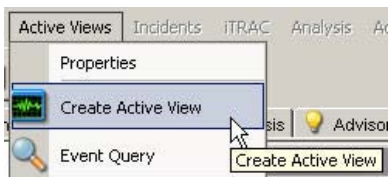
NOTA: Se presupone que el administrador de seguridad o el usuario han generado los filtros necesarios y configurado los recopiladores requeridos para el sistema.

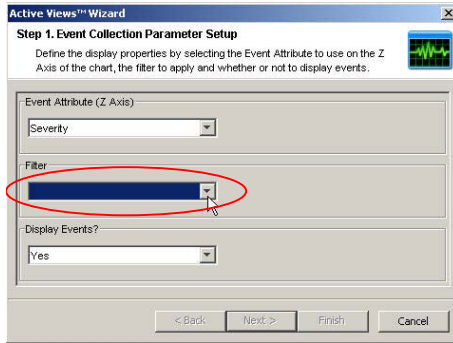
Pestaña Vistas Active Views

En la pestaña Vistas Active Views, se pueden monitorizar los eventos a medida que se producen y realizar consultas en éstos. Estos eventos se pueden monitorizar en forma de tabla o a través de una representación gráfica tridimensional.

Para iniciar los eventos en tiempo real

1. Haga clic en *Vistas Active Views* > *Crear una vista Active Views*, en la sección Filtro, haga clic en la flecha hacia abajo; seleccione un filtro y haga clic en Seleccionar.

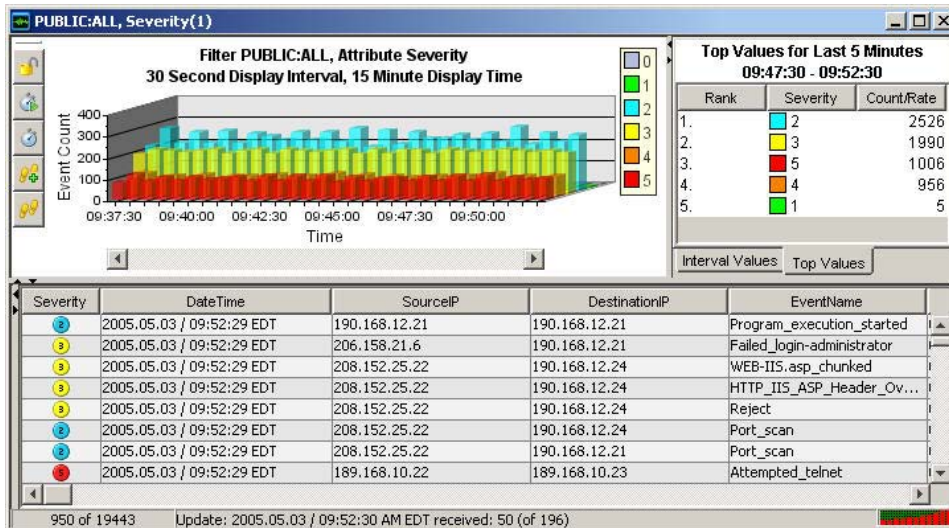




Propietario	Nombre del filtro	Cadena de expresiones
PUBLIC	Operating_System_E	filter(e.DeviceCategory = "OS")
PUBLIC	IDS_Events	filter(e.DeviceCategory = "IDS")
PUBLIC	Database_Events	filter(e.DeviceCategory = "DB")
PUBLIC	High_Severity	filter(e.Severity >= 3)
PUBLIC	Low_Severity	filter(e.Severity <= 2)
PUBLIC	Firewall_Events	filter(e.DeviceCategory = "FW")
PUBLIC	Correlation	filter((e.SensorType = "C") or (e.SensorType = "M"))
PUBLIC	Exploit_Detection	filter(e.Vulnerability = 1)
PUBLIC	External_Events	filter((e.SensorType = "I") and (e.SensorType != "P"))
PUBLIC	ALL	filter(1=1)
PUBLIC	Scan_Events	filter(e.DeviceCategory = "SCAN")
PUBLIC	Severe_Internal	filter((e.SensorType = "I") and (e.Severity >= 3))
PUBLIC	Internal_Events	filter(e.SensorType = "I")

- Haga clic en *Finalizar*. Si dispone de una red activa, es posible que vea algo similar a la imagen siguiente:

NOTA: Para visualizar un gráfico tridimensional sin eventos en tiempo real, haga clic en la flecha hacia abajo ¿Desea visualizar los eventos? y seleccione *No*.



Detección de explotaciones

Para ver los eventos que indican una posible explotación, debe disponer de los elementos siguientes:

- Datos del asesor
- Detección de intrusiones
- Exploración de vulnerabilidades

Severity	Vulnerability	AttackId
2	0	
3	0	

Dentro de un evento, cuando el campo Vulnerabilidad (*vul*) es igual a 1, se explota el activo o el dispositivo de destino. Si el campo Vulnerabilidad es igual a 0, no se explota el activo ni el dispositivo de destino. Si el campo Vulnerabilidad se deja en blanco, no se activará la función de detección de explotaciones de Sentinel.

Para ver los eventos que indican una posible explotación, utilice un filtro para crear una vista Active Views en el que el campo Vulnerabilidad sea igual a 1. Si dispone de Nmap y se ha ejecutado el recopilador Nmap, la información sobre el activo se podrá ver en el activo explotado o en cualquier activo.

Si desea obtener más información sobre cómo funciona la detección de explotaciones y los sistemas de detección de intrusiones y los exploradores de vulnerabilidades compatibles, consulte el *capítulo 1, Introducción*, o el *capítulo 10, Gestor de datos de Sentinel*.

Datos del activo

Para ver la información de activo de cualquier evento, haga clic con el botón derecho del ratón en un evento o eventos > *Análisis* > *Datos del activo*; aparecerá una ventana similar a la siguiente.

Asset Report

desk.acmeinc.net					
Hardware	MAC Address	A0:12:56:78:90:00			
	Name	Build Machine	Value	500	
	Type	Server	Criticality	High	
	Vendor	Dell	Sensitivity	Low	
	Product	Precision	Environment	Production	
	Version	360	Location	Internal	
Network	IP	199.16.2.23			
	Hostname	desk.acmeinc.net			
Software	Name	Type	Vendor	Product	Version
	ClearCase	APPLICATION	IBM	ClearCase	5.0
	C++	APPLICATION	Microsoft	Visual C++	6.0
Contacts	Order	Name	Role	Email	Phone Number
	1	Erickson, Stein	USER	serickson@acmedomain.net	(703) 555-8865
	2	IT	Administrator	LAN_FOLKS@acmedomain.net	(703) 555-9876
Location	Room	server room			
	Rack	#17			
	Address	HQ			
		Agent 86 Security Circle Suite 86 Washington DC 12345 USA			

Consulta de eventos

Caso de ejemplo: durante la monitorización, se detectan varios intentos de Telnet de la dirección IP de origen 189.168.10.22. Los intentos de Telnet pueden ser un ataque. Telnet permite potencialmente que un atacante se conecte de manera remota a un equipo remoto como si estuviese conectado de manera local. Esto puede resultar en modificaciones no autorizadas en la configuración, la instalación de programas, virus, etc.

Puede utilizar la opción Consulta de eventos para determinar el número de veces que un posible atacante ha intentado realizar una operación de Telnet y configurar un filtro para realizar una consulta sobre este atacante en particular. Por ejemplo, se conoce la información siguiente:

- IP de origen:189.168.10.22
- IP de destino:189.168.10.23
- Gravedad:5
- Nombre del evento:Attempted_telnet
- Tipo de sensor:H (detección de intrusiones host)

Para realizar una consulta de eventos

1. Haga clic en *Consulta de eventos* (icono de lupa) y haga clic en la flecha hacia abajo del campo Filtro.
2. Haga clic en *Añadir*, introduzca "telnet SIP 189_168_10_22" como nombre del filtro. En el campo situado debajo del campo Filtro, introduzca los valores siguientes:
 - IP de origen = 189.168.10.22
 - Gravedad = 5
 - Nombre del evento = Attempted_telnet
 - Tipo de sensor = H
 - Correlacionar si, seleccione (and)
 - IP de destino = 189.168.10.23
3. Haga clic en *Guardar*. Resalte el filtro y haga clic en *Seleccionar*.
4. Introduzca el período de tiempo deseado y haga clic en *Buscar* (icono de lupa). Aparecerán los resultados de la consulta.

Severity	DateTime	SourceIP	DestinationIP	EventName
5	2005.05.03 / 09:25:24 EDT	189.168.10.22	189.168.10.23	Attempted_telnet
5	2005.05.03 / 09:25:22 EDT	189.168.10.22	189.168.10.23	Attempted_telnet
5	2005.05.03 / 09:25:20 EDT	189.168.10.22	189.168.10.23	Attempted_telnet
5	2005.05.03 / 09:25:18 EDT	189.168.10.22	189.168.10.23	Attempted_telnet
5	2005.05.03 / 09:25:16 EDT	189.168.10.22	189.168.10.23	Attempted_telnet
5	2005.05.03 / 09:25:14 EDT	189.168.10.22	189.168.10.23	Attempted_telnet
5	2005.05.03 / 09:25:12 EDT	189.168.10.22	189.168.10.23	Attempted_telnet
5	2005.05.03 / 09:25:10 EDT	189.168.10.22	189.168.10.23	Attempted_telnet
5	2005.05.03 / 09:25:08 EDT	189.168.10.22	189.168.10.23	Attempted_telnet
5	2005.05.03 / 09:25:06 EDT	189.168.10.22	189.168.10.23	Attempted_telnet

Si desea ver la frecuencia general con la que este usuario intenta realizar una operación telnet, quite las opciones IP de destino, Tipo de sensor y Gravedad del filtro o bien cree un filtro nuevo. Los filtros mostrarán todas las direcciones IP de destino a las que el usuario intenta realizar una operación de Telnet.

Si alguno de los eventos son eventos correlacionados (Tipo de sensor = C o W), puede hacer clic con el botón derecho del ratón en *> Ver los eventos activadores* para buscar los eventos que han activado dicho evento correlacionado.

Otro evento que puede ser de interés es una cantidad excesiva de eventos FTP. Esto también puede tratarse de una conexión remota que permite la transferencia, copia y supresión de archivos.

A continuación se incluye una lista breve de los ataques que pueden ser de interés.

Los tipos de ataques es una lista extensa. Si desea obtener más información sobre los ataques de red y host, existe una gran cantidad de recursos disponibles (como Internet y libros) que explican con detalle los distintos tipos de ataques.

- Inundación SYN
- Rastreo de paquetes
- Smurf y Fraggle
- Inundación ICMP y UDP
- Denegación de servicio
- Ataque de diccionarios

Analista de informes

NOTA: Se presupone que el administrador de seguridad ha configurado el servidor Web de Crystal Enterprise y publicado una lista de los informes disponibles.

Pestaña Análisis

La pestaña Análisis permite generar informes históricos. Los informes históricos y de vulnerabilidades se publican en un servidor Web Crystal y se ejecutan directamente contra la base de datos de Sentinel. Estos informes son de gran utilidad para monitorizar e investigar las actividades durante un período de tiempo prolongado como, por ejemplo, una semana o un mes. Además, se pueden utilizar como método de generación de informes de alto nivel destinados a los supervisores. Si el servidor Web de generación de informes se encuentra instalado, consulte la barra de navegación para ver los informes disponibles.

NOTA: A continuación se incluye un ejemplo de Crystal 9. Los procedimientos de Crystal 11 son iguales excepto que los nombres de los informes son diferentes.

Por ejemplo, si el usuario es el responsable de generar informes destinados a la dirección superior de la organización, es probable que ejecute SourceDestinationReports. Este tipo de informes son los primeros 10 pares de IP de origen y destino en los nombres de host, puertos, direcciones IP y usuarios. Para ejecutar este informe, realice lo siguiente:

Ejecución de un informe Crystal Report

1. Expanda la opción Primeros 10 y seleccione Resumen de los primeros 10 pares de IP de origen y destino; haga clic en *Crear un informe* (lupa).
2. Introduzca `esecrpt` (para la autenticación de SQL y Oracle) como nombre de usuario o bien el nombre de usuario de la autenticación de Windows y, a continuación, introduzca la contraseña.
3. En Tipo de informe, seleccione *Informe semanal* (seleccione un rango de fechas específico para indicar un rango de fechas específico).

NOTA: Es posible que otros informes tengan parámetros adicionales como, por ejemplo, nombre del origen y rango de gravedad.

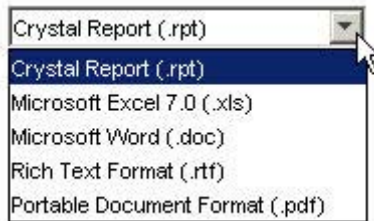
4. Haga clic en *Ver informe*.

Top 10 Source to Destination IP Pairs: Weekly

Report Description: This report summarizes the Top 10 Pairs of Source IP Addresses and Destination IP Addresses for the **last full week** from all sensors (i.e., event sources) monitored by e-Security Agents.

Source IP	Destination IP	Number of Occurrences
206.158.21.6	189.168.10.22	4,174
206.158.23.8	192.168.11.23	2,880
208.152.25.22	190.168.12.21	1,154
10.0.20.5	192.168.0.1	1,152
10.0.20.7	192.168.0.4	579
10.0.20.4	192.168.0.7	577
207.25.71.204	207.25.71.204	576
199.168.10.25	199.168.11.22	576
199.168.10.22	199.168.10.22	576
190.168.12.21	190.168.12.21	576

5. Para exportar este archivo en formato Word, PDF, rtf, Excel o como un informe de Crystal Report, haga clic en *Exportar* (sobre).



Consulta de eventos

Al igual que el analista de seguridad, si existe un evento o eventos de interés dentro de los informes, se puede ejecutar la opción Consulta de eventos de la pestaña Análisis. Para ejecutar una consulta, seleccione Eventos históricos > Consultas de eventos históricos y haga clic en *Crear un informe* (lupa). Si desea obtener más información, consulte [Analista de seguridad, caso de ejemplo de consulta de eventos](#).

Administradores

Correlación básica

La correlación es el proceso de analizar eventos de seguridad para identificar posibles relaciones entre dos o más eventos. La correlación permite establecer una asociación rápida de ataques de prioridad según elementos comunes de datos de evento.

Al hacer referencia en el escenario de telnet en la sección [Analista de seguridad, caso de ejemplo de consulta de eventos](#), se podrá crear una regla de correlación básica que activará un evento correlacionado cuando se produzcan cuatro eventos de Telnet en un plazo de 10 segundos.

Para crear una regla de correlación

1. Vaya a la pestaña Admin y seleccione Reglas de correlación de la barra de navegación.
2. Cree una nueva carpeta y coloque la regla en ella. Para ello, utilice la opción correspondiente del menú contextual.
3. Seleccione Correlación básica, introduzca un nombre y haga clic en *Siguiente*. En el panel siguiente, haga clic en la flecha hacia abajo y seleccione *Gestor de filtros*. En el panel Selección del filtro, haga clic en la flecha hacia abajo del campo Filtro seleccionado y seleccione *Añadir*.
4. Introduzca la información siguiente:
 - Nombre: telnet_attemp_189_168_10_22
 - Nombre del filtro: telnet attempt 189_168_10_22
 - IP de origen = 189.168.10.22
 - Nombre del evento = Attempted_telnet
 - Seleccione *And*
 - Gravedad = 5
 - Tipo de sensor = H
 - IP de destino = 189.168.10.23

5. Haga clic en *Guardar*. Resalte el filtro y haga clic en *Seleccionar*.
6. Haga clic en *Siguiente*, introduzca un valor de 4 para cuando se cumpla la condición y 10 segundos en el panel Criterios de grupo y umbral. Haga clic en *Siguiente*.
7. En el panel Evento y acciones correlacionados, cambie el nivel de gravedad a 2 (haga clic en la flecha hacia abajo). Haga clic en *Finalizar*.
8. Para distribuir esta regla, seleccione Gestor de motores de correlación del panel de navegación, seleccione un motor de correlación y haga clic con el botón derecho del ratón en *Distribuir las reglas*. En el panel Distribuir las reglas, busque la regla correspondiente y coloque una marca de verificación en ella. Haga clic en *Aceptar*. Compruebe que las opciones Motores de correlación y Reglas de correlación incluyen marcas de verificación de color verde que indican que están habilitadas. Para ello, haga clic con el botón derecho del ratón.
9. Si hay eventos correlacionados, existen varios métodos diferentes para visualizarlos, entre los cuales se incluyen los siguientes:
 - Crear una ventana de eventos de vista Active Views utilizando el filtro de correlación que se acaba de crear.
 - Crear una ventana de eventos de vista Active Views utilizando el filtro de correlación proporcionado.
 - Crear una ventana de eventos de vista Active Views utilizando el filtro Todo proporcionado, crear una instantánea y ordenar por tipo de sensor; a continuación, visualizar todos los eventos con la opción Tipo de sensor igual a C.
 - Realizar una consulta rápida utilizando el filtro creado o el filtro de correlación.

Haga clic con el botón derecho del ratón en el evento correlacionado y seleccione .

Ver los eventos activadores para ver el número de eventos de Telnet (puede haber más de 4) que han activado esta regla de correlación.

The screenshot displays two windows from a network management system. The top window is a table of events with a context menu open over one of the rows. The bottom window shows the configuration for a specific correlation rule, including a list of triggering events.

SensorType	Severity	DateTime	SourceIP	DestinationIP	Correlate
C		2005.05.03 / 12:22:56 EDT	189.168.10.22	189.168.10.23	Correlate
H	Show Details	12:22:58 EDT	190.168.12.21	190.168.12.21	Program
H	Email	12:22:58 EDT	206.158.21.6	190.168.12.21	Failed_lo
H		12:22:58 EDT	189.168.10.22	189.168.10.23	Attempt
H	Create Incident	12:22:58 EDT	206.158.21.6	189.168.10.22	Successf
H	Add To Incident	12:22:58 EDT	199.168.10.25	199.168.11.22	Repeate
H		12:22:58 EDT	206.158.21.6	199.168.10.25	Failed_si
H	View Trigger Events	12:22:58 EDT	199.168.10.22	199.168.10.22	Failed_si
H		12:22:58 EDT	206.158.21.6	199.168.10.22	Repeate
H	Investigate	12:22:58 EDT	206.158.21.6	199.168.10.25	Repeate
H	Analysis	12:22:58 EDT	207.25.71.204	207.25.71.204	Security
H	ping	12:22:58 EDT	207.25.71.204	207.25.71.204	Successf
H	nslookup	12:22:58 EDT	206.158.23.8	207.25.71.204	Successf
H		12:22:58 EDT	206.158.23.8	207.25.71.203	Failed_lo
H	tracert	12:22:58 EDT	206.158.23.8	207.25.71.202	Failed_lo
H		12:22:58 EDT	206.158.23.8	207.25.71.201	Failed_lo

SensorType	Severity	DateTime	SourceIP	DestinationIP	Attempt
H	●	2005.05.03 / 12:25:47 EDT	189.168.10.22	189.168.10.23	Attempt
H	●	2005.05.03 / 12:25:45 EDT	189.168.10.22	189.168.10.23	Attempt
H	●	2005.05.03 / 12:25:43 EDT	189.168.10.22	189.168.10.23	Attempt
H	●	2005.05.03 / 12:25:41 EDT	189.168.10.22	189.168.10.23	Attempt
H	●	2005.05.03 / 12:25:39 EDT	189.168.10.22	189.168.10.23	Attempt
H	●	2005.05.03 / 12:25:37 EDT	189.168.10.22	189.168.10.23	Attempt
H	●	2005.05.03 / 12:25:35 EDT	189.168.10.22	189.168.10.23	Attempt
H	●	2005.05.03 / 12:25:32 EDT	189.168.10.22	189.168.10.23	Attempt

Event Id: 22411B3E-955E-1027-9B6C-000874483C3C Correlation rule: telnet_attempt_189_168_10_22 Batch size: 100

Search complete. Count: 85

A

Eventos del sistema para Sentinel 5

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

En las tablas de descripción que aparecen a continuación, las palabras en cursiva entre <...> se sustituyen por los valores pertinentes en los mensajes reales.

Eventos de autenticación

Error en la autenticación

Cuando se produce un error en la autenticación del usuario, se genera el evento siguiente.

Etiqueta	Valor
Severity	4
Event Name	AuthenticationFailed
Resource	UserAuthentication
SubResource	Authenticate
Message	Error en la autenticación del usuario <nombre> con nombre de SO <dominio usuario> desde <IP>.

Evento de usuario de tipo incorrecto

Cuando un usuario intenta entrar en una aplicación y la autenticación es correcta pero el usuario no es un usuario de Sentinel, se genera el evento siguiente.

Etiqueta	Valor
Severity	4
Event Name	NoSuchUser
Resource	UserAuthentication
SubResource	Authenticate
Message	No existe el usuario con el nombre <nombre>.

Objetos Usuario duplicados

Cuando existe un segundo objeto Usuario activo inesperado, que no debería ocurrir, se genera el evento siguiente. Es un error interno.

Etiqueta	Valor
Severity	4
Event Name	TooManyActiveUsers
Resource	UserAuthentication
SubResource	Authenticate
Message	Error en la tabla de usuario:Existen varios usuarios con el nombre <nombre>.

Cuenta bloqueada

Cuando una cuenta de usuario bloqueada intenta entrar a la sesión, se genera el evento siguiente.

Etiqueta	Valor
Severity	4
Event Name	LockedUser
Resource	UserAuthentication
SubResource	Autenticación
Message	<i>Se ha intentado entrar a la sesión con la cuenta bloqueada < cuenta >.</i>

Sesiones de usuario

Salida del usuario

Cuando un usuario sale de la sesión, se genera el siguiente evento interno.

Etiqueta	Valor
Severity	1
Event Name	UserLoggedOut
Resource	UserSessionManager
SubResource	User
Message	El cierre de sesión para < usuario > con nombre de SO < nombre_so > desde < IP > estaba activo desde < fecha >; actualmente hay < número > usuarios activos.

Entrada del usuario

Cuando un usuario entra a la sesión, se genera el siguiente evento interno.

Etiqueta	Valor
Severity	1
Event Name	UserLoggedIn
Resource	UserSessionManager
SubResource	User
Message	Usuario < usuario > con nombre de SO < nombre_so > conectado a < IP >; actualmente hay < número > usuarios activos.

Usuario descubierto

Si el servidor se reinicia, éste pierde la información de la sesión. A continuación, dicho servidor reconstruye la sesión cuando recibe mensajes de usuarios activos. Cuando descubre un usuario conectado, se genera el siguiente evento interno.

Etiqueta	Valor
Severity	1
Event Name	UserLoggedIn
Resource	UserSessionManager

Etiqueta	Valor
SubResource	User
Message	Usuario activo descubierto <usuario> con nombre de SO <nombre_so> conectado a <IP>; actualmente hay <número> usuarios activos.

Evento

Error al mover el archivo finalizado

Cuando se finaliza un archivo de eventos, se mueve al directorio de salida. Si se produce un error en el desplazamiento, se genera el siguiente evento interno.

Etiqueta	Valor
Severity	3
Event Name	MoveArchiveFileFailed
Resource	<nombre de DAS>
SubResource	ArchiveFile
Message	Error al mover el archivo de reserva completado <nombre archivo> a <directorio>.

Error al insertar eventos

Si se produce un error al insertar eventos en la base de datos, se genera el siguiente evento interno.

Etiqueta	Valor
Severity	5
Event Name	InsertEventsFailed
Resource	EventSubsystem
SubResource	Events
Message	Error al introducir eventos en la base de datos; los eventos pueden haberse perdido permanentemente. Compruebe los registros del servidor de la base de datos y del sistema de apoyo <excepción>.

Error al abrir el archivo de reserva

Si se produce un error al abrir un archivo de reserva para almacenar los eventos para la adición, se genera el siguiente evento interno.

Etiqueta	Valor
Severity	3
Event Name	OpenArchiveFileFailed
Resource	<Nombre de Das>
SubResource	ArchiveFile
Message	Error al abrir el archivo de reserva <nombre> en <directorio>.

Error al escribir el archivo de reserva

Si se produce un error al abrir un archivo de reserva para almacenar los eventos para la adición, se genera el siguiente evento interno.

Etiqueta	Valor
Severity	3
Event Name	WriteArchiveFileFailed
Resource	<nombre de Das>
SubResource	ArchiveFile
Message	Error al escribir eventos recibidos recientemente en el archivo de reserva de adición <nombre archivo>.

Escritura en la partición desbordada (P_MAX)

Se envía un evento aproximadamente cada 5 minutos en el que se notifica al usuario cuándo se escriben los eventos en la partición desbordada (P_MAX). Cuando esto sucede, el administrador debe utilizar el SDM y añadir más particiones, de lo contrario, el rendimiento irá disminuyendo.

Etiqueta	Valor
Severity	5
Event Name	InsertIntoOverflowPartition
Resource	EventSubSystem
SubResource	Events
Message	Error:se están insertando en las particiones del flujo de datos (P_MAX); añada más particiones.

La inserción de eventos está bloqueada

Si DAS está escribiendo en la partición desbordada y el usuario intenta añadir particiones, el SDM enviará una petición a DAS para detener temporalmente la inserción de eventos en la base de datos. Si sucede esto, DAS envía eventos internos cada vez que intente insertar eventos en la base de datos.

Etiqueta	Valor
Severity	4
Event Name	EventInsertionIsBlocked
Resource	EventSubSystem
SubResource	Events
Message	La inserción de eventos se ha bloqueado, espere <número> seg.

La inserción de eventos se reanuda

Cuando la inserción de eventos se reanuda después de haber sido bloqueada, se envía el evento siguiente.

Etiqueta	Valor
Severity	2
Event Name	EventInsertionResumed
Resource	EventSubSystem
SubResource	Events
Message	La inserción de eventos se ha reanudado tras ser bloqueada.

El espacio de la base de datos ha alcanzado el umbral de tiempo especificado

Cuando la inserción de eventos se reanuda después de haber sido bloqueada, se envía el evento siguiente.

Etiqueta	Valor
Severity	0
Event Name	DbSpaceReachedTimeThrshld
Resource	Database
SubResource	Database
Message	El espacio de tabla <cadena> tiene <número> MB libres y está aumentando <número> bytes por segundo. Se quedará sin espacio en el umbral de tiempo especificado de <número> segundos.

El espacio de la base de datos ha alcanzado el umbral de porcentaje especificado

Cuando la inserción de eventos se reanuda después de haber sido bloqueada, se envía el evento siguiente.

Etiqueta	Valor
Severity	0
Event Name	DbSpaceReachedPercentThrshld
Resource	Database
SubResource	Database
Message	El espacio de tabla <cadena> tiene el tamaño actual de <número> MB con un tamaño máximo de <número> MB. Ha alcanzado el umbral del porcentaje de <número> %.

Poco espacio en la base de datos

Cuando la inserción de eventos se reanuda después de haber sido bloqueada, se envía el evento siguiente.

Etiqueta	Valor
Severity	5
Event Name	DbSpaceVeryLow
Resource	Database
SubResource	Database
Message	El espacio de tabla <cadena> tiene el tamaño actual de <número> MB y ha alcanzado el umbral físico de <número> MB.

Adición

Error al insertar datos de resumen en la base de datos

Si se produce un error mientras se escriben los datos de adición en la base de datos, se genera el siguiente evento interno.

Etiqueta	Valor
Severity	4
Event Name	SummaryUpdateFailure
Resource	Aggregation
SubResource	Summary
Message	Error al guardar la revisión del resumen en la base de datos del resumen <nombre_resumen>.

Servicio de asignación

Error al inicializar una asignación con ID

Este evento interno se ha generado desde el cliente del servicio de asignación (el que forma parte del Gestor de recopiladores). Este error se genera si el Gestor de recopiladores intenta recuperar una asignación que no existe. Esto no debería pasar pero puede pasar si se crean y se suprimen asignaciones.

Etiqueta	Valor
Severity	4
Event Name	ErrorNoSuchMap
Resource	MappingService
SubResource	ReferentialDataObjectMap
Message	Error al inicializar una asignación con ID <ID>:no existe la asignación.

Actualización de la asignación desde el caché

Este evento interno se ha generado desde el cliente del servicio de asignación (el que forma parte del Gestor de recopiladores). Cuando el Gestor de recopiladores debe actualizar la asignación porque se ha modificado o su definición ha cambiado, envía un evento interno. Esto significa que su caché está actualizado y que está actualizando la asignación desde el caché.

Etiqueta	Valor
Severity	1
Event Name	LoadingMapFromCache
Resource	MappingService
SubResource	ReferentialDataObjectMap
Message	Carga desde el caché <versión> de la asignación <nombre_asignación> (ID <ID>).

Actualización de la asignación desde el servidor

Este evento interno se ha generado desde el cliente del servicio de asignación (el que forma parte del Gestor de recopiladores). Cuando el Gestor de recopiladores debe actualizar la asignación porque se ha modificado o ha cambiado su definición, envía un evento interno. Esto significa que la asignación no estaba en el caché o que la versión del caché no estaba actualizada y que el Gestor de recopiladores está recuperando la asignación desde el servidor.

Etiqueta	Valor
Severity	1
Event Name	RefreshingMapFromServer
Resource	MappingService
SubResource	ReferentialDataObjectMap
Message	Actualización desde asignación de servidor <nombre> con ID <ID>.

Tiempo límite de actualización de asignación

Este evento interno se ha generado desde el cliente del servicio de asignación (el que forma parte del Gestor de recopiladores). Cuando el Gestor de recopiladores debe actualizar la asignación porque se ha modificado o su definición ha cambiado, envía un evento interno. Esto significa que el Gestor de recopiladores ha intentado recuperar la asignación del servidor y el servidor no ha reconocido la petición ni el tiempo límite. Este error se considera transitorio y el Gestor de recopiladores lo volverá a intentar.

Etiqueta	Valor
Severity	4
Event Name	TimeoutRefreshingMap
Resource	MappingService
SubResource	ReferentialDataObjectMap
Message	Petición interrumpida mientras se actualizaba la asignación <nombre>:<excepción>.

Error al actualizar la asignación

Este evento interno se ha generado desde el cliente del servicio de asignación (el que forma parte del Gestor de recopiladores). Cuando el Gestor de recopiladores debe actualizar la asignación porque se ha modificado o su definición ha cambiado, envía un evento interno. Esto significa que se ha producido un error no transitorio inesperado mientras intentaba actualizar la asignación. El Gestor de recopiladores esperará 15 minutos y volverá a intentarlo. Si esto sucede durante la inicialización, la inicialización continuará y esta asignación se ignorará hasta que pueda cargarse correctamente.

Etiqueta	Valor
Severity	4
Event Name	ErrorRefreshingMapData
Resource	MappingService
SubResource	ReferentialDataObjectMap
Message	Error al actualizar la asignación <nombre_asignación>:<excepción>.

Asignación grande cargada

Este evento interno es un evento de información enviado por el servicio de asignación que indica que se ha cargado una asignación grande en el Gestor de recopiladores. Una asignación se considera grande si el número de filas supera las 100.000.

Etiqueta	Valor
Severity	0
Event Name	LoadedLargeMap
Resource	MappingService
SubResource	ReferentialDataObjectMap
Message	Carga de asignación <nombre> finalizada con ID <ID>, <número> entradas y un tamaño total de <#> Kb en <##>seg.

La carga de la asignación tarda mucho tiempo

Este evento interno es un evento de información enviado por el servicio de asignación para informar que la carga de la asignación ha tardado un período de tiempo prolongado inusual (más de un minuto).

Etiqueta	Valor
Severity	0
Event Name	LongTimeToLoadMap
Resource	MappingService
SubResource	ReferentialDataObjectMap
Message	Ha tardado <##> seg. en cargar la asignación <nombre> con ID <ID>, <número> entradas y un tamaño total de <##> Kb.

TimeoutWaitingForCallback

Si el Gestor de recopiladores necesita actualizar una asignación, envía una petición al sistema de apoyo. Esta petición contiene una devolución de llamada. El sistema de apoyo genera la asignación y cuando está listo la envía al Gestor de recopiladores utilizando la devolución de llamada. Si la respuesta tarda mucho tiempo en llegar (más de diez minutos), el Gestor de recopiladores enviará una segunda petición porque supone que la primera se ha perdido. Cuando esto sucede, se genera el siguiente evento interno.

Etiqueta	Valor
Severity	2
Event Name	TimeoutWaitingForCallback
Resource	MappingService
SubResource	ReferentialDataObjectMap
Message	La asignación <nombre> se ha interrumpido al esperar la llamada de devolución con nuevos datos de asignación--reintentando.

ErrorApplyingIncrementalUpdate

Este evento se envía cuando el servicio de asignación no consigue aplicar una actualización en una asignación de cliente existente.

Etiqueta	Valor
Severity	4
Event Name	ErrorApplyingIncrementalUpdate
Resource	MappingService
SubResource	ReferentialDataObjectMap
Message	El error <error> se ha producido mientras se aplicaban las actualizaciones a la asignación <nombre asignación> (ID <ID asignación>) v.<versión>. Se está volviendo a programar una actualización para finalizar la actualización de la asignación.

OutOfSyncDetected

Este evento se envía cuando el servicio de asignación detecta que hay una asignación sin actualizar. El servicio de asignación programará automáticamente una actualización.

Etiqueta	Valor
Severity	2
Event Name	OutOfSyncDetected
Resource	MappingService
SubResource	ReferentialDataObjectMap
Message	La asignación <nombre asignación> que ha detectado los datos de asignación no está sincronizada, probablemente debido a una notificación de actualización que falta – programando una actualización.

Router de eventos

El router de eventos está en ejecución

El router de eventos es el componente principal del Gestor de recopiladores (el que realiza las asignaciones, aplica filtros globales y publica los eventos). Este evento interno se envía cuando el router de eventos está listo durante la inicialización. Cuando se reinicia el Gestor de recopiladores, se envía otro evento cuando está listo.

Este evento no se envía hasta que el router del evento no carga correctamente todos los filtros globales y la información de asignación.

Etiqueta	Valor
Severity	1
Event Name	EventRouterIsRunning
Resource	AgentManager
SubResource	EventRouter
Message	El router de eventos ha finalizado la inicialización en modo <modo>.

El router de eventos se está inicializando

Este evento se envía cuando un router de eventos empieza la inicialización. El router de eventos se inicializa cuando ha establecido una conexión con el sistema de apoyo (consulta de DAS).

Etiqueta	Valor
Severity	1
Event Name	EventRouterInitializing
Resource	AgentManager
SubResource	EventRouter
Message	El router de eventos se está inicializando en modo <modo>.

El router de eventos se está deteniendo

Este evento se envía cuando se recibe una petición del router de eventos para que se detenga durante el apagado.

Etiqueta	Valor
Severity	2
Event Name	EventRouterStopping
Resource	AgentManager
SubResource	EventRouter
Message	El router de eventos se está deteniendo.

El router de eventos está terminando

Este evento se envía cuando se recibe una petición del router de eventos para que se detenga durante el apagado.

Etiqueta	Valor
Severity	2
Event Name	EventRouterTerminating
Resource	AgentManager
SubResource	EventRouter
Message	El router de eventos está terminando.

Motor de correlación

El motor de correlación está en ejecución

El puede detener el proceso del motor de correlación. El estado en ejecución determina si el proceso activo está procesando eventos o no. El proceso se inicia en estado inactivo (detenido) y espera a recuperar la configuración desde la base de datos. Este evento se envía cuando el motor cambia el estado de detenido a en ejecución.

Etiqueta	Valor
Severity	1
Event Name	EngineRunning
Resource	CorrelationEngine
SubResource	CorrelationEngine
Message	El motor de correlación está procesando eventos.

El motor de correlación se ha detenido

Este evento se envía cuando el motor cambia el estado de en ejecución a detenido.

Etiqueta	Valor
Severity	1
Event Name	EngineStopped
Resource	CorrelationEngine
SubResource	CorrelationEngine
Message	El motor de correlación ha detenido el proceso de eventos.

La distribución de reglas se ha iniciado

Este evento se envía cuando un motor carga correctamente una distribución de reglas. Este mensaje se envía independientemente del estado en el que se encuentre el motor.

Etiqueta	Valor
Severity	1
Event Name	DeploymentStarted
Resource	CorrelationEngine
SubResource	Deployment
Message	La distribución <nombre> se ha iniciado.

La distribución de reglas se ha detenido

Este evento se envía cuando un motor descarga correctamente una distribución de reglas. Este mensaje se envía independientemente del estado en el que se encuentre el motor.

Etiqueta	Valor
Severity	1
Event Name	DeploymentStopped
Resource	CorrelationEngine
SubResource	Deployment
Message	La distribución <nombre> se ha detenido.

La distribución de reglas se ha modificado

Este evento se envía cuando un motor vuelve a cargar correctamente una distribución de reglas. Este mensaje se envía independientemente del estado en el que se encuentre el motor.

Etiqueta	Valor
Severity	1
Event Name	DeploymentModified
Resource	CorrelationEngine
SubResource	Deployment
Message	La distribución <nombre> se ha modificado.

Vigilante

El proceso controlado se ha iniciado

El vigilante se ejecuta como un servicio. Su objetivo principal es mantener los procesos de Sentinel en ejecución. Si un proceso finaliza, éste reiniciará automáticamente el proceso. Este evento se envía cuando se inicia un proceso.

Etiqueta	Valor
Severity	1
Event Name	ProcessStart
Resource	WatchDog
SubResource	Process
Message	El proceso <nombre_programa> ha generado (<pid>).

El proceso controlado se ha detenido

Este evento se envía cuando se detiene un proceso. La gravedad se ajusta en 5 si el proceso se ha definido para que se regenere (p. ej., no se espera que finalice). La gravedad se ajusta en 1 si el proceso se ha definido para que funcione una vez.

Etiqueta	Valor
Severity	1/5
Event Name	ProcessStop
Resource	WatchDog
SubResource	Process
Message	Se ha salido del proceso <nombre_programa> con el código <código_salida>.

El proceso de vigilancia se ha iniciado

Mientras se inicia el proceso de vigilancia, se genera el siguiente evento interno.

Etiqueta	Valor
Severity	1
Event Name	ProcessStart
Resource	WatchDog
SubResource	WatchDog
Message	El servicio de vigilancia se está iniciando.

El proceso de vigilancia se ha detenido

Cuando se detiene el servicio de vigilancia, se genera el siguiente evento interno.

Etiqueta	Valor
Severity	5
Event Name	ProcessStop
Resource	WatchDog
SubResource	WatchDog
Message	El servicio de vigilancia ha finalizado.

Gestor y motor del recopilador

Inicio del puerto

El Gestor de recopiladores envía este evento cuando se inicia un puerto.

Etiqueta	Valor
Severity	1
Event Name	PortStart
Resource	AgentManager
SubResource	AgentManager
Message	Se ha iniciado el proceso del puerto <ID_puerto>.

Detención del puerto

El Gestor de recopiladores envía este evento cuando un puerto se detiene.

Etiqueta	Valor
Severity	1
Event Name	PortStop
Resource	AgentManager
SubResource	AgentManager
Message	Se ha detenido el proceso del puerto <ID_puerto>.

El proceso permanente se ha cancelado

El motor del recopilador envía este evento cuando el conector del proceso permanente detecta que el proceso controlado se ha cancelado.

Etiqueta	Valor
Severity	5
Event Name	PersistentProcessDied
Resource	AgentManager
SubResource	AgentManager
Message	El proceso permanente en el puerto <ID_puerto> se ha cancelado.

El proceso permanente se ha reiniciado

El motor del recopilador envía este evento cuando el conector del proceso permanente es capaz de reiniciar el proceso controlado que se ha cancelado.

Etiqueta	Valor
Severity	1
Event Name	PersistentProcessRestarted
Resource	AgentManager
SubResource	AgentManager
Message	El proceso permanente en el puerto <ID_puerto> se ha reiniciado.

Servicio de eventos

Dependencia cíclica

El servicio de eventos envía este evento cuando detecta un ciclo en la definición de eventos (en dependencias entre etiquetas debido a asignaciones referenciales). Compruebe la configuración del evento en SDM y solucione la dependencia.

Etiqueta	Valor
Severity	5
Event Name	CyclicalDependency
Resource	EventService
SubResource	ObjectAttrInfos
Message	Se ha detectado una dependencia cíclica en las transformaciones del evento. Compruebe la configuración del evento.

Vista Active Views

Vista Active Views creada

DAS_Binary envía este evento cuando se crea una vista Active Views.

Etiqueta	Valor
Severity	1
Event Name	RtChartCreated
Resource	RealTimeSummaryService
SubResource	ChartManager
Message	Se está creando una nueva vista Active Views con el filtro <filtro> y el atributo <atributo> para usuarios con el filtro de seguridad <filtro_seguridad>. Actualmente se están recuperando <n> vistas Active Views.

Vista Active Views unida

DAS_Binary envía este evento cuando un usuario se conecta a una vista Active Views existente.

Etiqueta	Valor
Severity	1
Event Name	RtChartJoiningExistingData
Resource	RealTimeSummaryService
SubResource	ChartManager
Message	Se está uniendo la vista Active Views existente con el filtro <filtro> y el atributo <atributo> para usuarios con el filtro de seguridad <filtro_seguridad>. Actualmente, se están recopilando <n> vistas Active Views.

Vista Active Views inactiva eliminada

DAS_Binary envía este evento cuando se elimina una vista Active Views no permanente debido a inactividad.

Etiqueta	Valor
Severity	1
Event Name	RtChartInactiveAndRemoved
Resource	RealTimeSummaryService
SubResource	ChartManager
Message	Se ha eliminado una vista Active Views inactiva con el filtro <filtro> y el atributo <atributo> para usuarios con el filtro de seguridad <filtro_seguridad>. Actualmente, se están recopilando <n> vistas Active Views.

Vista Active Views permanente inactiva eliminada

DAS_Binary envía este evento cuando se elimina una vista Active Views permanente debido a inactividad. Las vistas Active Views permanentes son las que se guardan en las preferencias del usuario y se interrumpen tras unos días de inactividad por defecto.

Etiqueta	Valor
Severity	1
Event Name	RtPermanentChartRemoved
Resource	RealTimeSummaryService
SubResource	ChartManager
Message	Se ha eliminado una vista Active Views permanente inactiva con el filtro <filtro> y el atributo <atributo> para usuarios con el filtro de seguridad <filtro_seguridad>. Actualmente, se están recopilando <n> vistas Active Views.

Vista Active Views ahora permanente

DAS_Binary envía este evento cuando detecta una vista Active Views que ahora es permanente. Esta comprobación se realiza periódicamente, de modo que pueden pasar unos minutos tras guardar una vista Active Views en las preferencias antes de que se genere el evento.

Etiqueta	Valor
Severity	1
Event Name	RtChartIsNowPermanent
Resource	RealTimeSummaryService
SubResource	ChartManager
Message	La vista Active Views con el filtro <filtro> y el atributo <atributo> para usuarios con el filtro de seguridad <filtro_seguridad> ahora es permanente.

La vista Active Views ya no es permanente

DAS_Binary envía este evento cuando detecta que una vista Active Views permanente ya no es permanente. Esta comprobación se realiza periódicamente, de modo que pueden pasar unos minutos tras eliminar una vista Active Views de las preferencias antes de que se genere el evento.

Etiqueta	Valor
Severity	1
Event Name	RtChartNotPermanent
Resource	RealTimeSummaryService
SubResource	ChartManager
Message	La vista Active Views con el filtro <filtro> y el atributo <atributo> para usuarios con el filtro de seguridad <filtro_seguridad> ya no es permanente.

Resumen

Nombre de evento	Gravedad	Recurso	Subrecurso	Componente
AuthenticationFailed	4	UserAuthentication	Authenticate	Authentication
NoSuchUser	4	UserAuthentication	Authenticate	Authentication
TooManyActiveUsers	4	UserAuthentication	Authenticate	Authentication
LockedUser	4	UserAuthentication	Authenticate	Authentication
UserLoggedOut	1	UserSessionManager	User	User Session
UserLoggedIn	1	UserSessionManager	User	User
UserLoggedIn	1	UserSessionManager	User	User
MoveArchiveFileFailed	3	<i>DAS Name</i>	ArchiveFile	Event
InsertEventsFailed	5	EventSubSystem	Events	Event
OpenArchiveFileFailed	3	<i>DAS Name</i>	ArchiveFile	Event
WriteArchiveFileFailed	3	<i>DAS Name</i>	ArchiveFile	Event
SummaryUpdateFailure	4	Aggregation	Summary	Aggregation
InsertIntoOverflowPartition	5	EventSubSystem	Events	Event
EventInsertionIsBlocked	4	EventSubSystem	Events	Event
EventInsertionResumed	2	EventSubSystem	Events	Event
EventRouterIsRunning	1	AgentManager	EventRouter	EventRouter
EventRouterInitializing	1	AgentManager	EventRouter	EventRouter
EventRouterStopping	2	AgentManager	EventRouter	EventRouter
EventRouterTerminating	2	AgentManager	EventRouter	EventRouter
ErrorNoSuchMap	4	MappingService	ReferentialDataObjectMap	Mapping
LoadingMapFromCache	1	MappingService	ReferentialDataObjectMap	Mapping
RefreshingMapFromServer	1	MappingService	ReferentialDataObjectMap	Mapping
TimeoutRefreshingMapData	4	MappingService	ReferentialDataObjectMap	Mapping
ErrorRefreshingMapData	4	MappingService	ReferentialDataObjectMap	Mapping
LoadedLargeMap	0	MappingService	ReferentialDataObjectMap	Mapping
LongTimeToLoadMap	0	MappingService	ReferentialDataObjectMap	Mapping
TimeoutWaitingForCallback	2	MappingService	ReferentialDataObjectMap	Mapping
ErrorApplyingIncrementalUpdate	4	MappingService	ReferentialDataObjectMap	Mapping

Nombre de evento	Gravedad	Recurso	Subrecurso	Componente
OutOfSyncDetected	2	MappingService	ReferentialDataObjectMap	Mapping
EngineRunning	1	CorrelationEngine	CorrelationEngine	
EngineStopped	1	CorrelationEngine	CorrelationEngine	
DeploymentStarted	1	CorrelationEngine	Deployment	
DeploymentStopped	1	CorrelationEngine	Deployment	
DeploymentModified	1	CorrelationEngine	Deployment	
ProcessStart	1	WatchDog	Process	
ProcessStop	1/5	WatchDog	Process	
ProcessStart	1	WatchDog	WatchDog	
ProcessStop	5	WatchDog	WatchDog	
PortStart		AgentManager	AgentManager	
PortStop		AgentManager	AgentManager	
PersistentProcessDied	5	AgentManager	AgentManager	
PersistentProcessRestarted	1	AgentManager	AgentManager	
SortDependencies	5	EventService	ObjectAttrInfo	EventService
DbSpaceReachedTimeThrshld	0	Database	Database	Event
DbSpaceReachedPercentThrshld	0	Database	Database	Event
DbSpaceVeryLow	5	Database	Database	Event
RtChartCreated	1	RealTimeSummaryService	ChartManager	Active Views
RtChartJoiningExistingData	1	RealTimeSummaryService	ChartManager	Active Views
RtChartInactiveAndRemoved	1	RealTimeSummaryService	ChartManager	Active Views
RtChartPermanentAndRemoved	1	RealTimeSummaryService	ChartManager	Active Views
RtChartIsNowPermanent	1	RealTimeSummaryService	ChartManager	Active Views
RtChartNotPermanent	1	RealTimeSummaryService	ChartManager	Active Views

abandonar particiones.....	10-32
abrir	
Gestor de usuarios, ventana	9-28
regla de correlación, ventana.....	9-8
activar	
opción del menú Configuración del menú.....	9-23
actividad	
clic con el botón derecho	5-9, 5-10
creación	5-12
exportación.....	5-14
importación.....	5-14
modificación	5-14
actualización de la clave de licencia	
ID de host (UNIX).....	11-11
ID de host (Windows).....	11-11
addPartitions	10-31, 10-32
adición.....	10-23
consulta de los archivos de eventos para un resumen.....	10-27
ejecución de archivos de eventos para un resumen.....	10-28
habilitación del resumen	10-25
inhabilitación del resumen	10-25
validez de un resumen	10-26
visualizar información del resumen ...	10-25
agentes véase recopilador	
añadir	
filtro privado	9-17
filtro público.....	9-17
función de navegador a la opción del menú Configuración del menú	9-24
opción al menú Configuración del menú.....	9-21
añadir eventos a una incidencia.....	3-26
añadir particiones, GUI.....	10-5, 10-6
añadir particiones, línea de comando.....	10-31
anular una sesión activa	9-31
archivar datos.....	10-35
archivar particiones, GUI.....	10-5, 10-6
archiveConfig	10-34, 10-35
archiveData.....	10-35

archivo de bloqueo	
eliminar.....	11-4
archivo de guión.....	11-3
agent-manager.sh.....	11-1
remove_sonic_lock.bat.....	11-3
remove_sonic_lock.sh	11-3
sentinel.sh.....	11-1, 11-3
start_broker.bat	11-3
start_broker.sh	11-3
stop_broker.bat	11-3
stop_broker.sh.....	11-3
stop_container.bat	11-3
stop_container.sh.....	11-3
arquitectura.....	1-4
asesor	
actualización	7-1, 7-3
actualización, descarga de transmisión de Internet	7-3
actualización, descarga directa de Internet	7-3
asignación.....	10-8, 10-14
actualización	10-16
actualización(línea de comando)	10-41
añadir.....	10-8, 10-14
supresión	10-15
asignación de eventos..	10-8, 10-14, 10-17
asignación de gráficos	3-13, 3-15
Asistente	
reinicio.....	8-1
carpeta de reglas	
crear.....	9-8
carpeta de reglas de correlación	
exportar	9-9
importar.....	9-9
carpetas de reglas	9-3
Centro de control de Sentinel	
cerrar ventana.....	2-8
contraseña	2-9
disponer en mosaico.....	2-8
disponer ventanas en cascada.....	2-7
inicio (UNIX)	2-2
inicio en Windows	2-2
minimizar ventana	2-8
posición de la pestaña	2-7
restaurar ventana	2-8
ventana del navegador, anclar	2-7
ventana del navegador, flotar.....	2-7

ventana del navegador, mostrar	2-7		
ventana del navegador, ocultar.....	2-7		
clave de licencia			
actualizar.....	11-11		
clonar			
cuentas de usuario.....	9-30		
filtro privado	9-19		
filtro público.....	9-19		
opción del menú Configuración			
del menú.....	9-22		
columnas de eventos			
alias	10-22		
asignar	10-19		
reasignar	10-19		
renombrar	10-22		
condición lógica			
igual a	9-6		
igual a metaetiqueta.....	9-7		
igual a Regex	9-7		
igual a Subnet.....	9-7		
inferior a.....	9-6		
inferior a metaetiqueta.....	9-7		
inferior o igual a metaetiqueta	9-7		
inferior o igual a=	9-7		
no es igual a metaetiqueta.....	9-7		
no igual a=	9-6		
superior a.....	9-7		
superior a metaetiqueta.....	9-7		
superior o igual a	9-7		
superior o igual a metaetiqueta	9-7		
configuración de correo electrónico..	11-8		
configuración de eventos.....	10-22		
descripción	10-22		
configuración de particiones	10-30		
configuración del correo electrónico.	3-10		
configurar			
Informe de análisis.....	9-1		
Informe de asesor	9-1		
configurar el encabezado de la			
columna de eventos	10-22		
configurar el visor de adjuntos	4-7		
conjunto de reglas de correlación			
suprimir.....	9-8		
consulta de eventos.....	3-16		
ejecución de un informe	6-2		
contenedor			
reiniciar (UNIX).....	11-6		
reiniciar (Windows)	11-6		
Contenedor de Sentinel			
reiniciar (UNIX).....	11-6		
reiniciar (Windows)	11-6		
contraseña			
Centro de control de Sentinel.....	2-9		
contraseña del asesor			
descarga directa7-3			
controlador de datosvéase sincronizador			
de datos			
correlación	1-2		
correlación avanzada			
definición	9-5		
correlación básica			
definición	9-5		
correlación RuleLg de regla sin formato			
definición	9-5		
correlation_engine	1-15		
correo electrónico			
execution.properties	4-8		
incidencia.....	4-8		
correo electrónico del asesor	7-4		
crear			
carpeta de reglas	9-8		
cuentas de usuario.....	9-29		
filtro global	9-15		
incidencia.....	4-6		
incidencias.....	3-12		
informe de análisis	6-2		
informe de asesor.....	7-1		
regla.....	9-8		
vista de recopilador.....	8-3		
Crystal Report			
ejecución.....	6-2		
los diez informes más habituales	6-1		
cuentas de usuario			
clonar.....	9-30		
crear.....	9-29		
modificar	9-30		
suprimir	9-31		
visualizar	9-30		
DAS	1-15		

data_synchronizer	1-15	enviar por correo electrónico	
datos del activo	3-18	incidencia	4-8
datos del asesor	3-16, 7-4	etiquetas	
dbstats	10-40, 10-41	reasignar	10-19
definición de asignaciones	10-8, 10-14	evento1-2	
definición del proceso		evento correlacionado	3-13
modificación	5-3, 5-5	eventos	
deleteData	10-36, 10-43	investigación	3-13
desactivar		relación con incidencias	4-2
opción del menú Configuración		visualización de eventos que han	
del menú	9-23	activado un evento correlacionado..	3-13
desplazar		execution.properties	4-8
opción del menú Configuración		exportar	
del menú	9-23	carpeta de reglas de correlación	9-9
detalles		filesToImport	10-37
filtro privado	9-19	filtro global	9-15
filtro público	9-19	abandonar	9-16
detalles de la función		base de datos	9-16
visualizar	9-31	base de datos y GUI	9-16
detección de explotaciones	1-7	crear	9-15
detención del nivel de comunicación	11-5	reorganizar	9-16
detención del nivel de comunicación		suprimir	9-16
(UNIX)	11-5	filtro privado	9-14
diagrama de barras 3D		añadir	9-17
rotación	3-8	clonar	9-19
diagrama de cintas 3D		detalles	9-19
rotación	3-8	modificar	9-19
distribuir reglas de correlación	9-10	suprimir	9-19
dropImported	10-33, 10-39, 10-40	filtro público	9-14
dropPartition	10-32	añadir	9-17
editar		clonar	9-19
ventana de correlación	9-9	detalles	9-19
ejecución		modificar	9-19
informe de eventos correlacionados	6-3	suprimir	9-19
ejecutar		filtros	9-14
Crystal Report	6-2, 7-1	globales	9-15
informe de consulta de eventos	6-2	privados	9-14
eliminar particiones, GUI	10-6	públicos	9-14
		flujo de trabajo Véase iTRAC	
		gestión de base de datos	
		abandonar particiones, línea	
		de comando	10-32
		deleteData	10-36
		dropPartition	10-32
		suprimir datos, línea de comando	10-36

gestión de la base de datos	
actualización de asignaciones	10-16
actualización de asignaciones, línea de comando	10-41
addPartition	10-31
adición	10-25
añadir particiones, línea de comando	10-31
archivar datos, línea de comando.....	10-35
archiveConfig	10-34
archiveData	10-35
archivos para importar, línea de comando	10-37
asignación.....	10-19
configuración de particiones, línea de comando	10-30
gestión de los archivos de reserva, línea de comando	10-34
gestión de particiones	10-30
guardar conexión	10-29
importar datos, línea de comando	10-39
listado de archivos para importar.....	10-37
partitionConfig.....	10-30
reasignación	10-19
renombrar columnas de eventos	10-22
supresión de asignaciones	10-15
supresión de datos importados, línea de comando.....	10-40
uso del espacio de la base de datos, línea de comando	10-41
visualización de particiones.....	10-7, 10-8
visualización de particiones, línea de comando.....	10-33
gestión de los archivos de reserva ..	10-34
gestor de consultas	1-16
Gestor de datos de sentinel	
archivos para importar, línea de comando	10-37
Gestor de datos de Sentinel	10-1
abandonar particiones, línea de comando	10-32
actualización de los datos de asignación, línea de comando.....	10-41
actualización de una asignación.....	10-16
adición.....	10-23, 10-25
adición de archivo de asignaciones	10-8
adición, información de los archivos de eventos	10-27
adición, información del resumen	10-25, 10-26
adición, resumen de los archivos de eventos	10-28
añadir archivo de asignaciones	10-14
añadir particiones, GUI	10-5, 10-6
añadir particiones, línea de comando	10-31
archivar datos, línea de comando.....	10-35
archivar particiones, GUI	10-5, 10-6
archiveConfig.....	10-34
archiveData	10-35
asignación.....	10-19
asignación de eventos	10-8, 10-14, 10-17
conectar a la base de datos.....	10-2
configuración de eventos	10-22
configuración de eventos, descripción.....	10-22
configuración de particiones, línea de comando.....	10-30
dbstats.....	10-41
definición de asignaciones.....	10-8, 10-14
deleteData	10-36
dropImported	10-40
filesToImport.....	10-37
fileToImport.....	10-37
gestión de los archivos de reserva.....	10-34
guardar las propiedades de conexión en la base de datos.....	10-29
importar datos, línea de comando	10-39
importar particiones, GUI	10-5, 10-6
importData	10-39
iniciar (UNIX).....	10-2
iniciar (Windows).....	10-2
partitionConfig.....	10-30
reasignación	10-19
renombrar una columna de eventos...	10-22
sdm.connect	10-28
supresión de datos importados, línea de comando.....	10-40
supresión de una asignación	10-15
suprimir datos, línea de comando	10-36
suprimir particiones, GUI.....	10-5, 10-6
updateMapData.....	10-41
uso del espacio, línea de comando	10-41
viewPartition	10-33
visualización de particiones, GUI.....	10-7
visualización de particiones, línea de comando.....	10-33
visualizar particiones, GUI.....	10-4
Gestor de la base de datos	
visualización de particiones, GUI.....	10-8
Gestor de recopiladores	
cerrar (UNIX)	11-1
detención (Windows)	11-2
iniciar (Windows).....	11-2
inicio (UNIX)	11-1
reinicio.....	8-1
reinicio (UNIX).....	11-1
Gestor de usuarios, ventana	
abrir	9-28

gestor de vistas	
adición de una vista	4-4
guardar adjuntos.....	4-6
guardar preferencias	2-9
hora de los datos	
cambio.....	7-4
host del asistente	
creación de un visor del Gestor de recopiladores.....	8-3
creación de una vista de recopilador	8-3
modificación de una vista de recopilador	8-4
monitorización.....	8-1, 8-3
importar	
carpeta de reglas de correlación	9-9
importar datos	10-39
importar particiones, GUI.....	10-5, 10-6
importData	10-38, 10-39
incidencia	
adición de eventos.....	3-26
adición de una vista de incidencia	4-4
configuración del visor de adjuntos.....	4-7
creación	3-12, 4-6
envío por correo electrónico	4-8
guardado de adjuntos	4-6
modificación	4-8
opción de vista	4-2, 4-4
relación con eventos.....	4-2
supresión	4-9
supresión del flujo de trabajo	4-9
visualización.....	4-2
visualización de adjuntos.....	4-6
información de eventos	
instantánea	3-9
navegador visual	3-9
Informe de análisis	
configurar URL	9-1
informe de asesor	
creación	7-1
Informe de asesor	
configurar URL	9-1
informe de eventos correlacionados	
ejecución.....	6-3
inicio del nivel de comunicación.....	11-4

inicio del nivel de comunicación (UNIX)	11-5
inicio rápido	
consulta de eventos	12-4, 12-6
Crystal Report.....	12-5
datos del activo	12-3
detección de explotaciones.....	12-2
regla de correlación	12-6
vista Active Views	12-1
instantánea	
cierre.....	3-25
información de eventos	3-9
ocultación de información de eventos	3-10
ordenar	3-25
organización de columnas	3-24
supresión	3-26
tabla en tiempo real de eventos	3-25
integración con productos de otros fabricantes	
HP Service Desk	3-23
Remedy	3-23
iTRAC	
actividad, opción de clic con el botón derecho.....	5-9, 5-10
añadir.....	9-31
creación de una actividad.....	5-12
exportación de una actividad	5-14
importación de una actividad	5-14
incidencia asociada.....	5-9, 5-10
Inicio del proceso	5-12
modificación de la definición de un proceso	5-3
modificación de una actividad	5-14
modificación de una definición del proceso.....	5-4, 5-5
monitorización de un proceso.....	5-10
Monitorización de un proceso, definición de una opción	5-11
suprimir	9-31
Terminación del proceso	5-12
lista de vigilancia	
definición	9-4
listado de archivos para importar	10-37
mensaje de evento	
por correo electrónico	3-10
mensaje de incidencia	
por correo electrónico	3-11
modificación de la definición del proceso.....	5-4

modificar		modificar	9-23
cuentas de usuario.....	9-30	suprimir	9-23
filtro privado	9-19	uso	3-23
filtro público.....	9-19	operaciones con HP-OpenView	3-23
incidencia.....	4-8	parámetros de una opción del menú	
opción del menú Configuración		Configuración del menú	
del menú.....	9-23	visualizar	9-23
vista de recopilador	8-4	partitionConfig	10-30
monitorización de un proceso	5-10	posición de la pestaña	
definición de una opción	5-11	Control de control de Sentinel.....	2-7
motor de correlación	1-15, 9-5	prácticas recomendadas	
detener	9-9	añadir particiones.....	10-42
iniciar.....	9-9	archivar datos	10-42
navegador visual		preferencias	
cierre	3-25	guardar	2-9
información de eventos	3-9	proceso	
ocultación de información de eventos .	3-10	inicio	5-12
organización de columnas	3-24	terminación	5-12
supresión	3-26	procesos	1-13
nivel de comunicación		DAS.....	1-15
detención (UNIX)	11-5	data_synchronizer.....	1-15
detención (Windows)	11-5	gestor de consultas.....	1-16
eliminar el archivo de bloqueo (UNIX)..	11-4	motor de correlación.....	1-15
eliminar el archivo de bloqueo		verificador RuleLg	1-15
(Windows)	11-4	vigilancia	1-14
inicio (UNIX).....	11-5	recopilador	
inicio (Windows).....	11-4	detención	8-4
Nivel de comunicación de Sentinel		inicio	8-4
detención (UNIX)	11-5	mostrar información.....	8-4
detención (Windows)	11-5	Recopilador	
eliminación del archivo de bloqueo		monitorización	8-1
(UNIX).....	11-4	regla	
eliminación del archivo de bloqueo		crear.....	9-8
(Windows)	11-4	regla de correlación, ventana	
inicio (UNIX).....	11-5	abrir	9-8
inicio (Windows).....	11-4	reglas	9-3
ocultar información de eventos		reglas de correlación	9-3
instantánea	3-10	distribuir.....	9-10
navegador visual	3-10	exportar	9-6
opción al menú Configuración del menú		importar	9-6
añadir	9-21	reglas de evento	9-3
opción de vista		Remedy	3-23
incidencia.....	4-2, 4-4		
opción del menú Configuración del menú			
activar.....	9-23		
añadir función de navegador	9-24		
clonar	9-22		
desactivar.....	9-23		
desplazar.....	9-23		

renombrar encabezados de la columna de eventos	10-22	tiempo real del evento	
rotar		navegador visual	3-4
diagrama de barras 3D.....	3-8	número máximo de eventos	3-3
diagrama de cintas 3D	3-8	valor en caché.....	3-3
rulelg_checker.....	1-15	visualización	3-4
saveConnection		updateMapData.....	10-41
ejecutar	10-29	uso del espacio de la base de datos	10-41
Sentinel		usuario por defecto	
arquitectura.....	1-4	ESEC_CORR	9-28
descripción	1-3	esecadm	9-28
procesos	1-13	esecapp	9-28
Sentinel Data Manager		esecdba	9-28
starting (UNIX)	10-1	esecrpt.....	9-28
Servicio de acceso a los datos véase DAS		usuarios	
servicio de asignación.....	1-7	por defecto <i>Consulte</i> usuario por defecto	
servicio de asignaciones.....	10-7	ventana de correlación	
servicio eSecurity véase <i>vigilancia</i>		editar.....	9-9
servidor de Sentinel		verificador de reglas de correlación véase <i>verificador RuleLg</i>	
inicio (UNIX).....	11-3	verificador RuleLg.....	1-15
Servidor de Sentinel		Versión de Sentinel	
cerrar (UNIX)	11-1	archivos .dll	11-7
cerrar (Windows)	11-3	archivos .exe.....	11-7
detención (Windows)	11-2	archivos .jar	11-8
iniciar (Windows).....	11-3	Versión de Sentinel (UNIX)).....	11-7
inicio (UNIX).....	11-1	Versión de Sentinel (Windows))	11-7
inicio (Windows).....	11-2	vigilancia	1-14
sesión de usuario		vista Active Views	
anular	9-31	ajuste de la tabla de eventos.....	3-7
sinronizador de datos.....	1-15	cambio del tipo de diagrama	3-7
supresión de datos importados	10-40	filtrado de una tabla de eventos	
suprimir		en tiempo real	3-7
conjunto de reglas de correlación	9-8	navegador visual	3-4
cuentas de usuario.....	9-31	propiedades	3-3
filtro global.....	9-16	reajustar los parámetros.....	3-7
filtro privado	9-19	toma de una instantánea	3-25
filtro público.....	9-19	visualización	3-4
incidencia.....	4-9	vista de recopilador	
opción del menú Configuración		creación.....	8-3
del menú.....	9-23	modificación	8-4
regla de correlación	9-8	visualización de particiones,	
suprimir particiones, GUI	10-5, 10-6	GUI.....	10-7, 10-8
tabla en tiempo real de eventos		visualización de particiones, línea de comando	10-33
toma de una instantánea	3-25		

visualizar		
cuentas de usuario.....	9-30	
incidencia.....	4-2	
parámetros de una opción del menú		
Configuración del menú.....	9-23	
visualizar adjuntos.....	4-6	
		visualizar particiones, GUI 10-4
		vulnerabilidad
		datos del asesor 3-16
		exploración 3-22
		SmartViews 3-18