Guía de instalación

Novell®
Sentinel 6.1 Rapid Deployment

SP2

Abril de 2011

www.novell.com

Información 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.

Los productos o la información técnica que se proporcionan bajo este Acuerdo pueden estar sujetos a los controles de exportación de Estados Unidos o a la legislación sobre comercio de otros países. Usted acepta acatar las regulaciones de los controles de exportación y obtener todas las licencias necesarias para exportar, reexportar o importar bienes. También se compromete a no exportar ni reexportar el producto a entidades que figuren en las listas de exclusión de exportación de Estados Unidos, ni a países sometidos a embargo o sospechosos de albergar terroristas, tal y como se especifica en las leyes de exportación de los Estados Unidos. Asimismo, se compromete a no usar el producto para fines prohibidos, como la creación de misiles o armas nucleares, químicas o biológicas. Consulte la página Web sobre servicios de comercio internacional de Novell (http://www.novell.com/info/exports/) para obtener más información sobre la exportación del software de Novell. Novell no se responsabiliza de la posibilidad de que el usuario no pueda obtener los permisos de exportación necesarios.

Copyright © 1999-2011 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.
404 Wyman Street, Suite 500
Waltham, MA 02451
EE. UU.
www.novell.com

Documentación en línea: para acceder a la documentación en línea más reciente acerca de este y otros productos de Novell, visite la página Web de documentación de Novell (http://www.novell.com/documentation).

Marcas comerciales de Novell

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

Materiales de otros fabricantes

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

Tabla de contenido

Acerca de esta guía

El objetivo de esta guía es proporcionar una introducción a Novell Sentinel 6.1 Rapid Deployment Service Pack 2 y describir los procedimientos de instalación.

Usuarios a los que va dirigida

Esta documentación va dirigida a profesionales en seguridad de la información.

Comentarios

Nos gustaría recibir sus comentarios y sugerencias acerca de este manual y del resto de la documentación incluida con este producto. Utilice la función de comentarios del usuario, situada en la parte inferior de cada página de la documentación en línea, para escribir sus comentarios.

Documentación adicional

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

- *Guía de instalación de Novell Sentinel Rapid Deployment* (http://www.novell.com/documentation/sentinel61rd/s61rd_install/data/index.html)
- *Novell Sentinel Rapid Deployment User Guide (Guía del usuario de Novell Sentinel 6.1 Rapid Deployment)* (http://www.novell.com/documentation/sentinel61rd/s61rd_user/data/bookinfo.html)
- *Novell Sentinel Rapid Deployment Reference Guide (Guía de referencia de Novell Sentinel 6.1 Rapid Deployment)* (http://www.novell.com/documentation/sentinel61rd/s61rd_reference/data/bookinfo.html)
- *Guía de instalación de Novell Sentinel* (http://www.novell.com/documentation/sentinel61/s61_install/?page=/documentation/sentinel61/s61_install/data/)
- *Novell Sentinel User Guide (Guía del usuario de Novell Sentinel)* (http://www.novell.com/documentation/sentinel61/s61_user/?page=/documentation/sentinel61/s61_user/data/)

- *Novell Sentinel Reference Guide (Guía de referencia de Novell Sentinel)* (http://www.novell.com/documentation/sentinel61/s61_reference/?page=/documentation/sentinel61/s61_reference/data/)
- *Sentinel SDK* (http://www.novell.com/developer/develop_to_sentinel.html)

  El sitio del SDK de Sentinel ofrece información detallada acerca del desarrollo de recopiladores (propietarios o JavaScript) y de acciones de correlación de JavaScript.

Comunicación con Novell

- *Sitio Web de Novell* (http://www.novell.com)
- *Asistencia técnica de Novell* (http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup)
- *Novell Self Support* (http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog)
- *Sitio de descarga de parches* (http://download.novell.com/index.jsp)
- *Asistencia técnica 24x7 de Novell* (http://www.novell.com/company/contact.html)
- *Sentinel TIDS* (http://support.novell.com/products/sentinel)
- Foros de asistencia de la comunidad de Sentinel (http://forums.novell.com/novell-product-support-forums/sentinel/)
- Sitio Web del módulo auxiliar (plug-in) de Sentinel (http://support.novell.com/products/sentinel/secure/sentinelplugins.html)
- Boletín electrónico de notificación: inscríbase en el sitio Web del módulo auxiliar (plug-in) de Sentinel

Descripción general del producto 1

Sentinel 6.1 Rapid Deployment es una versión simplificada de Novell Sentinel que emplea componentes de código abierto, como PostgreSQL, activeMQ y JasperReports.

Las secciones siguientes le ayudarán a comprender los principales componentes del sistema Sentinel 6.1 Rapid Deployment. Esta *Guía de instalación de Sentinel Rapid Deployment* contiene información detallada sobre los procedimientos de instalación y configuración. La *Sentinel Rapid Deployment User Guide* (Guía del usuario de Sentinel Rapid Deployment) (http://www.novell.com/documentation/sentinel61rd/s61rd_user/?page=/documentation/sentinel61rd/s61rd_user/data/bookinfo.html) contiene datos sobre arquitectura, funcionamiento y procedimientos administrativos.

1.1 Descripción de Sentinel 6.1 Rapid Deployment

Sentinel es una solución de gestión de eventos y de información de seguridad que recibe información de muchos orígenes en toda la empresa, la estandariza, asigna prioridades y, finalmente, se la presenta a usted para que tome decisiones relacionadas con amenazas, riesgos y directivas.

Sentinel automatiza los procesos de recopilación, análisis y generación de informes de registros con el fin de asegurar que los controles de TI sean eficaces para detectar amenazas y cumplir requisitos de auditoría. Sentinel sustituye los procesos manuales tan laboriosos mediante una monitorización continua y automatizada de la seguridad, así como de los eventos de conformidad y de los controles de TI.

Sentinel también recopila y asocia información, tanto de seguridad como de cualquier otro tipo, por medio de la infraestructura de red de una organización, además de sistemas, dispositivos y aplicaciones de otros fabricantes. Sentinel presenta los datos recopilados en una interfaz gráfica del usuario, identifica cuestiones de seguridad y conformidad y realiza un seguimiento de las actividades de corrección para perfilar los procesos que tienen tendencia a errores y generar un sistema de gestión más riguroso y seguro.

La gestión automatizada de respuestas a incidencias le permite documentar y formalizar el proceso de seguimiento, escala y respuesta a incidencias y violaciones de directivas. Además, proporciona dos formas de integración con sistemas de tratamiento de incidencias. Sentinel le permite reaccionar rápidamente y solucionar incidencias de forma eficaz.

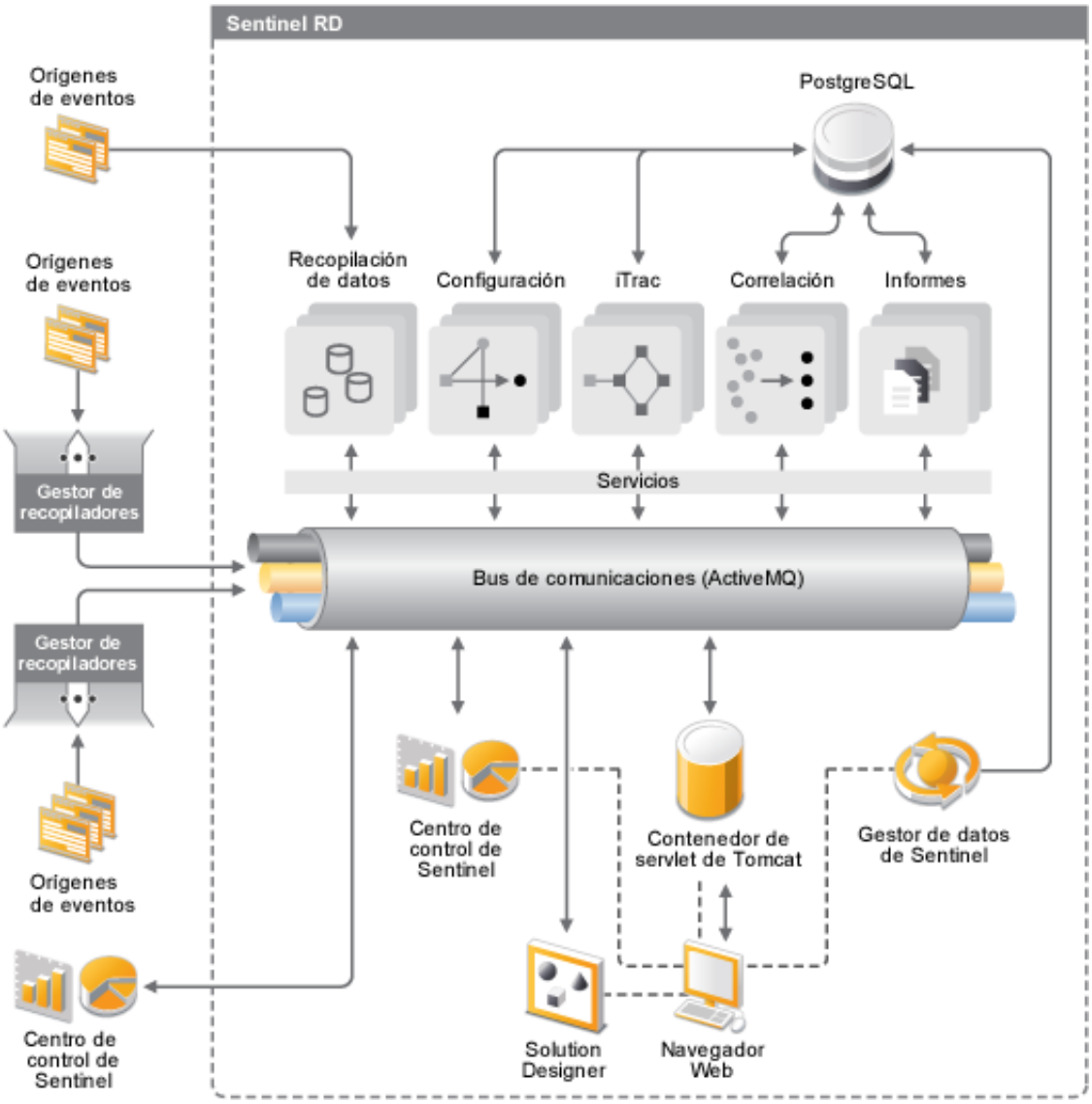
Los paquetes de soluciones constituyen una forma sencilla de distribuir e importar reglas de correlación de Sentinel, listas dinámicas, mapas, informes y flujos de tareas iTRAC en controles. Estos controles pueden diseñarse para cumplir requisitos reguladores específicos, como el Payment Card Industry Data Security Standard, o pueden estar relacionados con un origen de datos específico, como eventos de autenticación de usuarios para una base de datos de Oracle.

Con Sentinel Rapid Deployment recibe:

- Gestión de la seguridad en tiempo real, integrada y automatizada, y monitorización de conformidad en todos los sistemas y redes.
- Un marco de trabajo que permite que las directivas de la empresa cumplan con las directivas y los procedimientos de TI.
- Documentación e información automática sobre seguridad, sistemas y eventos de acceso en la empresa.
- La corrección y gestión de incidencias están incorporadas.
- Capacidad para demostrar y supervisar la conformidad con las directivas internas y las regulaciones gubernamentales, como Sarbanes-Oxley, HIPAA, GLBA y FISMA. El contenido requerido para implementar estos controles se distribuye y se implementa mediante paquetes de soluciones.

En la ilustración siguiente se describe una arquitectura conceptual de Sentinel Rapid Deployment, que muestra los componentes utilizados para realizar la gestión de seguridad y conformidad.

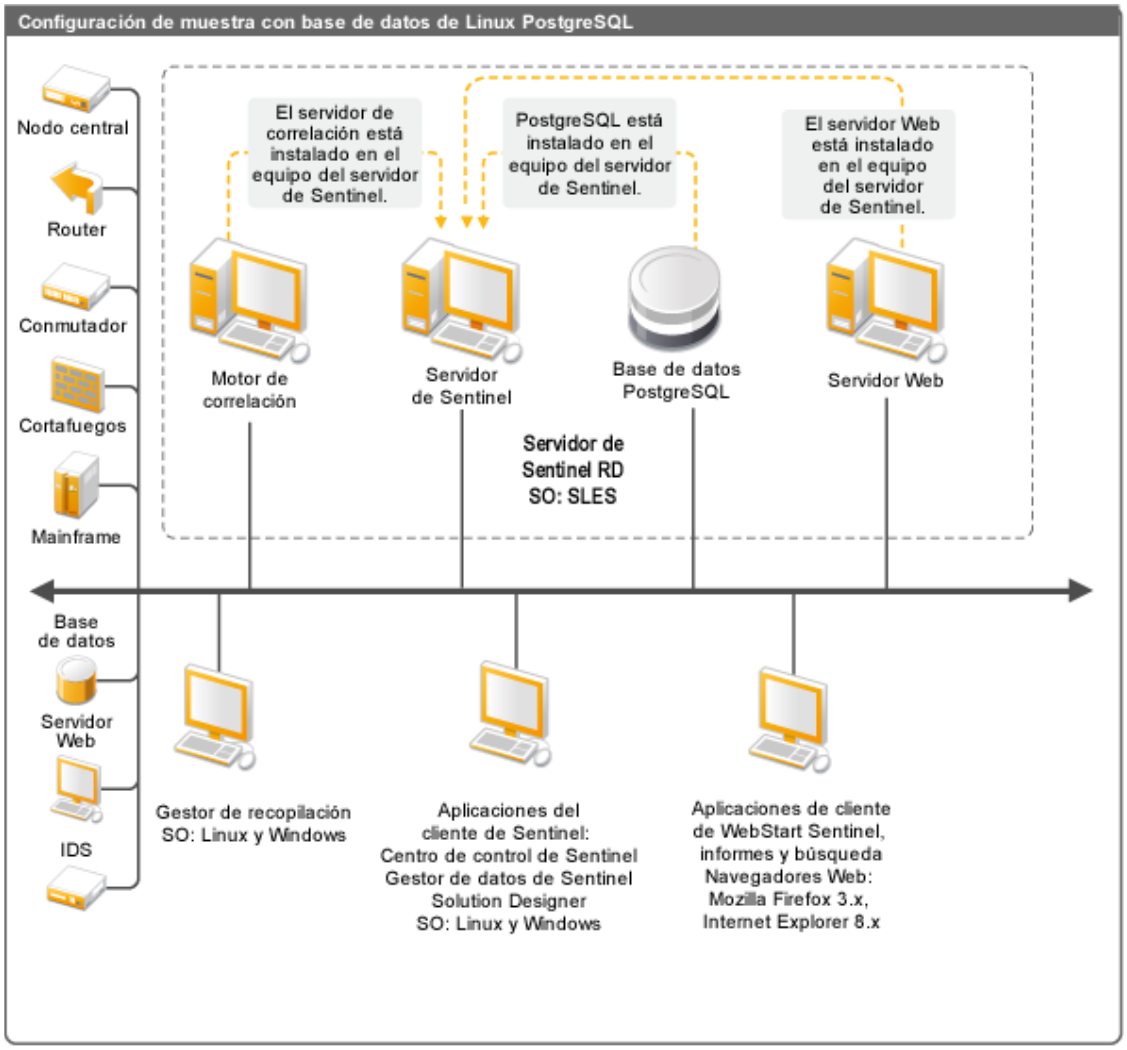
Figura 1-1 *Arquitectura conceptual de Sentinel*



1.2 Configuración de Sentinel 6.1 Rapid Deployment

La ilustración siguiente muestra la configuración de Sentinel 6.1 Rapid Deployment.

Figura 1-2 *Configuración de Sentinel 6.1 Rapid Deployment*



1.3 Interfaces de usuario de Rapid Deployment

Sentinel incluye las siguientes interfaces de usuario fáciles de utilizar:

- Interfaz Web de Sentinel 6.1 Rapid Deployment
- Centro de control de Sentinel
- Gestor de datos de Sentinel
- Solution Designer de Sentinel
- SDK del módulo auxiliar (plug-in) de Sentinel

1.3.1 Interfaz Web de Sentinel 6.1 Rapid Deployment

Con la interfaz Web de Novell Sentinel 6.1 Rapid Deployment puede gestionar informes, así como lanzar el Centro de control de Sentinel (SCC), el gestor de datos de Sentinel y Solution Designer. También puede descargar el instalador del gestor de recopiladores y el instalador del cliente desde la página *Aplicaciones* de la interfaz Web de Sentinel 6.1 Rapid Deployment.

Para obtener más información, consulte "Managing Sentinel Rapid Deployment Through the Web Interface" (Gestión de Sentinel Rapid Deployment mediante la interfaz Web) en la *Sentinel Rapid Deployment User Guide* (Guía del usuario de Sentinel Rapid Deployment).

1.3.2 Centro de control de Sentinel

El Centro de control de Sentinel ofrece una consola integrada de gestión de seguridad que permite a los analistas identificar rápidamente las nuevas tendencias o ataques, manipular e interactuar con información gráfica en tiempo real y responder a las incidencias.

Puede lanzar SCC bien como aplicación cliente o con Java Webstart.

Las funciones claves del Centro de control de Sentinel son:

- **Vistas Active Views:** proporciona datos de análisis y vistas en tiempo real.
- **Análisis:** permite ejecutar y guardar consultas desconectadas.
- **Incidencias:** permite la creación y gestión de incidencias.
- **Correlación:** permite la definición y gestión de definiciones de reglas de correlación.
- **iTRAC:** permite la gestión de procesos para documentar, aplicar y realizar un seguimiento de procesos de resolución de incidencias.
- **Generación de informes:** ofrece informes y medidas de historial.
- **Gestión de orígenes de eventos:** permite la distribución y la supervisión del recopilador.
- **Gestor de soluciones:** permite instalar, implementar y probar el contenido del paquete de soluciones.

Para obtener más información, consulte "Sentinel Control Center" (Centro de control de Sentinel) en la *Sentinel Rapid Deployment User Guide* (Guía del usuario de Sentinel Rapid Deployment).

1.3.3 Gestor de datos de Sentinel

El gestor de datos de Sentinel permite gestionar la base de datos de Sentinel. Es posible realizar las siguientes operaciones en el gestor de datos de Sentinel:

- Monitorizar la utilización del espacio de la base de datos.
- Ver y gestionar las particiones de la base de datos.
- Gestionar los archivos de la base de datos.
- Importar datos archivados a la base de datos.

Para obtener más información, consulte "Sentinel Data Manager" (Gestor de datos de Sentinel) en la *Sentinel Rapid Deployment User Guide* (Guía del usuario de Sentinel 6.1 Rapid Deployment).

1.3.4 Solution Designer de Sentinel

Solution Designer de Sentinel se utiliza para crear y modificar los paquetes de soluciones, que son conjuntos empaquetados de contenido de Sentinel, como reglas de correlación, acciones, flujos de tareas iTRAC e informes.

El contenido de Sentinel conforma la función ampliada del sistema Sentinel. Este contenido incluye lo siguiente: acciones de Sentinel, integradores y módulos auxiliares (plug-ins) de Sentinel, como recopiladores, conectores y paquetes de soluciones, que también pueden incluir muchos tipos distintos de módulos auxiliares (plug-ins) Estos componentes modulares se usan para realizar la integración con sistemas de otros fabricantes, para instalar una solución de seguridad completa basada en controles y para proporcionar una solución automatizada a las incidencias detectadas.

Para obtener más información, consulte "Solution Packs" (Paquetes de soluciones) en la *Sentinel Rapid Deployment User Guide* (Guía del usuario de Sentinel Rapid Deployment).

1.3.5 SDK del módulo auxiliar (plug-in) de Sentinel

El SDK del módulo auxiliar (plug-in) de Sentinel incluye bibliotecas y código desarrollado por Novell Engineering, así como la plantilla y el código de ejemplo que puede utilizar para desarrollar sus propios proyectos. Para obtener más información, consulte el SDK de Sentinel (http://www.novell.com/developer/develop_to_sentinel.html).

1.4 Componentes del servidor de Sentinel

Sentinel consta de los siguientes componentes:

1.4.1 Servicio de acceso a los datos

El servicio de acceso a los datos de Sentinel es el principal componente utilizado para comunicarse con la base de datos de Sentinel. El servidor de acceso a datos y otros componentes de servidor trabajan conjuntamente para almacenar los eventos recibidos desde los gestores de recopiladores en la base de datos, filtrar datos, procesar presentaciones de Active Views, ejecutar consultas en la base de datos y procesar los resultados, así como gestionar tareas como la autenticación y la autorización de los usuarios. Para obtener más información, consulte "Data Access Service" (Servicio de acceso a los datos) en la *Sentinel Rapid Deployment User Guide* (Guía del usuario de Sentinel Rapid Deployment).

1.4.2 Bus de mensajes

Sentinel 6.1 Rapid Deployment utiliza un intermediario de mensajes de código abierto denominado Apache Active MQ. El bus de mensajes puede mover miles de paquetes de mensajes en un segundo entre los componentes de Sentinel. La arquitectura de Apache Active MQ está construida en torno a Java Message Oriented Middleware (JMOM), que admite llamadas asíncronas entre las aplicaciones cliente y servidor. Las colas de mensajes proporcionan un almacenamiento temporal cuando el programa de destino está ocupado o no está conectado. Para obtener más información, consulte "Communication Server" (Servidor de comunicaciones) en la *Sentinel Rapid Deployment User Guide* (Guía del usuario de Sentinel Rapid Deployment).

1.4.3 Base de datos de Sentinel

El producto Sentinel se genera en torno a una base de datos de un sistema secundario que almacena los eventos de seguridad y todos los metadatos de Sentinel. Sentinel 6.1 Rapid Deployment admite PostgreSQL. Los eventos se almacenan de forma normalizada, junto con datos de los activos y de vulnerabilidad, información de identidades, estados del flujo de trabajo y de las incidencias y muchos otros tipos de datos. Para obtener más información, consulte "Sentinel Data Manager" (Gestor de datos de Sentinel) en la *Sentinel Rapid Deployment User Guide* (Guía del usuario de Sentinel 6.1 Rapid Deployment).

1.4.4 Gestor de recopiladores de Sentinel

El gestor de recopiladores de Sentinel gestiona la recopilación de datos, supervisa los mensajes de estado del sistema y realiza un filtrado de eventos según sea necesario. Las principales funciones del gestor de recopiladores son 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 el envío de mensajes de la actividad al servidor de Sentinel. El gestor de recopiladores de Sentinel se conecta directamente con el bus de mensajes. Para obtener más información, consulte "Collector Manager" (Gestor de recopiladores) en la *Sentinel Rapid Deployment User Guide* (Guía del usuario de Sentinel Rapid Deployment).

1.4.5 Motor de correlación

El motor de correlación añade inteligencia a la gestión de eventos de seguridad mediante la automatización del 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. Para obtener más información, consulte "Correlation Tab" (Pestaña Correlación) en la *Sentinel Rapid Deployment User Guide* (Guía del usuario de Sentinel Rapid Deployment).

1.4.6 iTRAC

Sentinel proporciona un sistema de gestión del flujo de tareas iTRAC para definir y automatizar procesos para las respuestas a incidencias. Aquellas incidencias que Sentinel identifique, bien manualmente o mediante una regla de correlación, pueden asociarse con un flujo de tareas iTRAC. Para obtener más información, consulte "iTRAC Workflows" (Flujos de tareas iTRAC) en la *Sentinel Rapid Deployment User Guide* (Guía del usuario de Sentinel Rapid Deployment).

1.4.7 Asesor de Sentinel y detección de exploits

El Asesor de Sentinel es un servicio de suscripción de datos opcional que incluye ataques conocidos, vulnerabilidades e información sobre la solución. Estos datos, combinados con las vulnerabilidades conocidas y la detección de intrusiones en tiempo real o la información de prevención del entorno, proporciona una detección de exploits proactiva y la capacidad de actuar de inmediato cuando tiene lugar un ataque contra un sistema vulnerable.

Junto a Sentinel 6.1 Rapid Deployment se instala por defecto una instantánea de datos del asesor. Necesita una licencia del asesor para poder suscribirse a las actualizaciones continuas de datos del asesor. Para obtener más información, consulte "Advisor Usage and Maintenance" (Uso del asesor y mantenimiento) en la *Sentinel Rapid Deployment User Guide* (Guía del usuario de Sentinel Rapid Deployment).

1.4.8 Servidor Web

Sentinel Rapid Deployment utiliza Apache Tomcat como servidor Web para permitir la conexión segura con la interfaz Web de Sentinel Rapid Deployment.

1.5 Módulos auxiliares (plug-ins) de Sentinel

Sentinel admite diversos módulos auxiliares (plug-ins) para ampliar y mejorar la funcionalidad del sistema. Algunos de estos módulos auxiliares ya están preinstalados. Hay disponibles módulos auxiliares y actualizaciones para descargar en el sitio Web de módulos auxiliares (plug-ins) de Sentinel 6.1 (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

Algunos módulos auxiliares (plug-ins) como Remedy Integrator, el conector de mainframes de IBM y el conector para SAP XAL requieren una licencia adicional para su descarga.

1.5.1 Recopiladores

Sentinel recopila datos de dispositivos de origen y ofrece un flujo de eventos más intenso aplicando taxonomía, detección de exploits 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.

Los recopiladores de Sentinel pueden analizar datos de los siguientes tipos de dispositivos, entre otros:

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

Se pueden escribir los recopiladores de JavaScript utilizando las herramientas de desarrollo estándar de JavaScript y el SDK de recopiladores.

1.5.2 Conectores e integradores

Los conectores proporcionan conectividad desde el gestor de recopiladores a los orígenes de eventos mediante protocolos estándar, como JDBC y Syslog. Los eventos se pasan del conector al recopilador para su análisis.

Los integradores habilitan las acciones de soluciones en los sistemas fuera de Sentinel. Por ejemplo, una acción de correlación puede usar el integrador SOAP para iniciar un flujo de trabajo del Gestor de identidades de Novell.

El integrador AR de soluciones opcional proporciona la capacidad de crear un ticket de solución desde eventos o incidencias de Sentinel. Para obtener más información, consulte "Action Manager and Integrator" (Gestor de acciones e integrador) en la *Sentinel Rapid Deployment User Guide* (Guía del usuario de Sentinel Rapid Deployment).

1.5.3 Reglas y acciones de correlación

Las reglas de correlación identifican patrones importantes en el flujo de eventos. Cuando se activa una regla, inicia acciones de correlación, como el envío de notificaciones por correo electrónico, el inicio de un flujo de tareas iTRAC o la ejecución de una acción utilizando un integrador. Para obtener más información, consulte "Correlation Tab" (Pestaña Correlación) en la *Sentinel Rapid Deployment User Guide* (Guía del usuario de Sentinel Rapid Deployment).

1.5.4 Informes

Con JasperReports puede ejecutar una amplia variedad de informes operativos y de consola desde la interfaz Web de Sentinel Rapid Deployment. Los informes se distribuyen por lo general a través de paquetes de soluciones.

1.5.5 Flujos de tareas iTRAC

Los flujos de tareas iTRAC proporcionan procesos consistentes y reiterativos para la gestión de incidencias. Las plantillas de flujos de trabajo se distribuyen por lo general a través de paquetes de soluciones. iTRAC incluye un conjunto de plantillas por defecto que se pueden modificar para

adaptarse a sus necesidades. Para obtener más información, consulte "iTRAC Workflows" (Flujos de tareas iTRAC) en la *Sentinel Rapid Deployment User Guide* (Guía del usuario de Sentinel Rapid Deployment).

1.5.6 Paquetes de soluciones

Los paquetes de soluciones son conjuntos empaquetados de contenido de Sentinel relacionado, como reglas de correlación, acciones, flujos de tareas iTRAC e informes. Novell proporciona paquetes de soluciones que se centran en necesidades comerciales específicas, como el paquete de soluciones PCI-DSS, que aborda la conformidad con Payment Card Industry Data Security Standard. Novell también crea paquetes de recopiladores, que incluyen el contenido centrado en un origen de eventos específico, como Windows Active Directory. Para obtener más información, consulte "Solution Packs" (Paquetes de soluciones) en la *Sentinel Rapid Deployment User Guide* (Guía del usuario de Sentinel Rapid Deployment).

1.6 Asistencia para el idioma

Los componentes de Sentinel están disponibles en los siguientes idiomas:

- Alemán
- Checo
- Chino simplificado
- Chino tradicional
- Español
- Francés
- Inglés
- Italiano
- Japonés
- Neerlandés
- Polaco
- Portugués

Requisitos del sistema

2

Para conseguir un mejor rendimiento y mayor fiabilidad, debe instalar los componentes de Sentinel Rapid Deployment en un equipo con software y hardware aprobado, como se muestra en esta sección. La calidad de los requisitos mencionados en esta sección se ha garantizado y certificado.

2.1 Plataformas compatibles

La Tabla 2-1 muestra las combinaciones de software y sistemas operativos certificadas o admitidas por Novell. Las combinaciones certificadas se han probado con el paquete de prueba completo de Novell Engineering. Se espera que las combinaciones compatibles sean completamente funcionales.

2.1.1 Sistemas operativos compatibles

Novell admite la ejecución de Sentinel Rapid Deployment en las versiones de los sistemas operativos descritas en esta sección. Novell también admite la ejecución en sistemas con actualizaciones menores de esos sistemas operativos, como parches de seguridad o Hot Fix. Sin embargo, no es posible ejecutar Sentinel Rapid Deployment en sistemas con actualizaciones mayores o menores de estos sistemas operativos hasta que Novell haya probado y certificado dichas actualizaciones.

Los componentes del servidor de Sentinel Rapid Deployment son el servidor de comunicaciones, el motor de correlación, el servicio de acceso a los datos (DAS), el servidor Web y el servicio de suscripción a los datos del asesor.

Las aplicaciones cliente de Sentinel son el Centro de control de Sentinel (SCC), el gestor de datos de Sentinel (SDM) y Solution Designer de Sentinel (SSD).

Para el gestor de recopiladores existen requisitos específicos de plataforma.

Tabla 2-1 *Sistemas operativos compatibles y certificados*

Plataformas	Componentes del servidor	Aplicaciones cliente de Sentinel	Gestor de recopiladores
SUSE Linux Enterprise Server (SLES) 11 SP1 (64 bits)	Certificado	Certificado	Certificado
SUSE Linux Enterprise Server (SLES) 11 SP1 (32 bits)	No compatible	Compatible	Compatible

Plataformas	Componentes del servidor	Aplicaciones cliente de Sentinel	Gestor de recopiladores
SUSE Linux Enterprise Server (SLES) 10 SP3 (64 bits)	Certificado	Compatible	Compatible
SUSE Linux Enterprise Server (SLES) 10 SP3 (32 bits)	Compatible	Compatible	Compatible
Windows Server 2008 R2 (64 bits)	No compatible	Certificado	Certificado
Windows Server 2003 R2 (64 bits)	No compatible	Compatible	Compatible
Windows Server 2003 R2 (32 bits)	No compatible	Compatible	Compatible
Windows XP SP3 (32 bits)	No compatible	Compatible	No compatible
Windows Vista SP2 (32 bits)	No compatible	Compatible	No compatible
Windows 7	No compatible	Certificado	No compatible

Siga estas directrices para obtener un rendimiento, una estabilidad y una fiabilidad óptimos.

- En el caso de SLES, el sistema operativo del equipo servidor de Sentinel Rapid Deployment debe incluir al menos los componentes Base Server y X Window de SLES.
- Para el servidor de Sentinel Rapid Deployment, utilice el sistema de archivos ext3. Para obtener más información sobre los sistemas de archivos, consulte Overview of File Systems in Linux (http://www.novell.com/documentation/sles11/stor_admin/data/filesystems.html) (Descripción de los sistemas de archivos en Linux) en la *Storage Administration Guide* (Guía de administración del almacenamiento).

Nota:

- Sentinel Rapid Deployment no se admite en las instalaciones Open Enterprise Server de SLES.
- La versión de 32 bits del servidor de Sentinel 6.1 Rapid Deployment está diseñada para entornos de demostración y pruebas a escala limitada mediante el uso de sistemas operativos y hardware de 32 bits. Los clientes o socios con un contrato de asistencia para Sentinel 6.1 Rapid Deployment pueden recibir asistencia técnica limitada en esta plataforma por parte del servicio de Asistencia técnica de Novell para los problemas que se puedan reproducir en la plataforma de producción de 64 bits. Debido a las limitaciones inherentes del hardware de 32 bits, la Asistencia técnica de Novell no realiza solución de problemas de rendimiento o capacidad de ampliación en la versión de demostración de 32 bits. Las versiones de demostración de 32 bits no son compatibles con un entorno de producción.

2.2 Requisitos del hardware

Los componentes del servidor de Sentinel Rapid Deployment se ejecutan en un equipo con hardware x86-64 (64 bits), con algunas excepciones según el sistema operativo, como se describe en la Sección 2.1.1, “Sistemas operativos compatibles”, en la página 19. Sentinel está certificado para hardware AMD Opteron e Intel Xeon. No se admiten los servidores Itanium.

En esta sección se incluyen algunas recomendaciones generales de hardware para el diseño del sistema de Sentinel. Las recomendaciones para el diseño del sistema se basan en los rangos de la velocidad de los eventos. Sin embargo, estas recomendaciones se basan en los siguientes supuestos:

- La velocidad de los eventos se encuentra en el límite superior del rango de eventos por segundo.
- El tamaño medio de los eventos es de 1 KB.
- Todos los eventos se almacenan en la base de datos (es decir, no hay filtros para soltar eventos).
- En la base de datos se almacenará una acumulación de datos durante un período de noventa días.
- El espacio de almacenamiento para los datos del asesor no se incluye en las especificaciones de Tabla 2-2 en la página 22 ni de Tabla 2-3 en la página 22.
- Por defecto, el servidor de Sentinel tiene un espacio de disco de 5 GB para el almacenamiento temporal en caché de los datos de eventos que no se pueden introducir de inmediato en la base de datos.
- Este servidor también dispone de un espacio de disco de 5 GB por defecto para los eventos que no se pueden insertar de inmediato en los archivos de eventos de adición.
- La suscripción opcional del asesor requiere 1 GB adicional de espacio de disco en el servidor.

Las recomendaciones de hardware para una implementación de Sentinel pueden variar en función de la implementación individual, de forma que se recomienda consultar con los Servicios de consultoría de Novell o con algún socio de Novell Sentinel antes de finalizar la arquitectura de Sentinel. Las recomendaciones que se mencionan a continuación pueden utilizarse como guía.

En la versión de SLES, la base de datos está incrustada con el servidor de Sentinel Rapid Deployment y se instala en el mismo equipo que el servidor.

Nota: debido a la gran carga de eventos y la necesidad de almacenar gran cantidad de datos en caché, el servidor de Sentinel requiere una matriz (RAID) repartida, ya sea compartida o local, con al menos cuatro discos.

Tabla 2-2 *Configuración en un equipo (hasta 2.000 eps)*

Componentes	RAM	Espacio	CPU
Equipo 1: servidor de Sentinel Rapid Deployment ◆ Base de datos PostgreSQL incrustada (3 GB) ◆ Gestor de recopiladores (1228 MB) ◆ DAS_Core (1579 MB) ◆ DAS_Binary (1404 MB) ◆ Motor de correlación (1073 MB) ◆ 4 recopiladores (Genérico, Cisco, Snort e IBM, cada uno genera 500 eps) ◆ 10 reglas de correlación implantadas ◆ 10 vistas Active Views únicas ◆ 3 usuarios simultáneos ◆ 2 asignaciones implantadas	16 GB	Discos duros 1 TB, SAS (15.000 rpm) RAID de hardware 10	Dell PowerEdge 2900, 2 x Intel Xeon E5310 de núcleo cuádruple (1,6 GHz) con Gigabit Ethernet NIC

Tabla 2-3 *Configuración en tres equipos (hasta 5.000 eps)*

Componentes	RAM	Espacio	CPU
Equipo 1: servidor de Sentinel Rapid Deployment ◆ Base de datos PostgreSQL incrustada (3 GB) ◆ Gestor de recopiladores (1228 MB) ◆ DAS_Core (1579 MB) ◆ DAS_Binary (1404 MB) ◆ Motor de correlación (1073 MB) ◆ 4 recopiladores (cada uno genera 500 eps), 1.500 eps del gestor de recopiladores remoto 1 y 1500 eps del gestor de recopiladores remoto 2.	16 GB	Discos duros 1 TB, SAS (15.000 rpm) RAID de hardware 10	Dell PowerEdge 2900, 2 x Intel Xeon E5310 de núcleo cuádruple (1,6 GHz) con Gigabit Ethernet NIC
Equipo 2: Gestor de recopiladores ◆ Gestor de recopiladores / recopiladores ◆ 3 recopiladores (generan 500 eps cada uno)	4 GB	Disco duro 300 GB, SATA (3 Gbit/s)	Intel Core 2 Duo E6750 (2,66 GHz) con Gigabit Ethernet NIC
Equipo 3: Gestor de recopiladores ◆ Gestor de recopiladores / recopiladores ◆ 3 recopiladores (generan 500 eps cada uno)	4 GB	Disco duro 300 GB, SATA (3 Gbit/s)	Intel Core 2 Duo E6750 (2,66 GHz) con Gigabit Ethernet NIC

2.3 Navegadores Web compatibles

- Mozilla Firefox 3.*x*
- Internet Explorer 8.*x*

2.4 Entorno virtual

Sentinel Rapid Deployment se ha probado de forma exhaustiva en el servidor VMWare ESX y Novell ofrece asistencia técnica completa de Sentinel Rapid Deployment en este entorno. Para obtener resultados de rendimiento comparables a los resultados de pruebas en equipos físicos en ESX o en otro entorno virtual, éste debe contar con la misma memoria, CPU, espacio en disco y opciones de E/S que las recomendaciones del equipo físico.

Para obtener más información sobre las recomendaciones físicas del equipo para un sistema SLES, consulte la Sección 2.2, “Requisitos del hardware”, en la página 20.

2.5 Límites recomendados

Los límites mencionados en esta sección son recomendaciones basadas en las pruebas de rendimiento realizadas en Novell o en instalaciones de clientes. No se trata de límites estrictos. Estas recomendaciones son aproximadas. En sistemas muy dinámicos, es recomendable instalar en un buffer y dejar espacio para la expansión.

2.5.1 Límites del gestor de recopiladores

A no ser que se indique otra cosa, los límites del gestor de recopiladores son para sistemas de 4 núcleos de CPU a 2,2 GHz cada uno, 4 GB de RAM con el sistema operativo SLES 11.

Tabla 2-4 *Datos de rendimiento del gestor de recopiladores*

Atributo	Límite	Comentarios
Número máximo de gestores de recopiladores	20	En este límite se supone que el gestor de recopiladores tiene un número bajo de eps (por ejemplo, menos de 100). El límite se reduce a medida que aumentan los eventos por segundo.
Número máximo de conectores (utilizados por completo) en un único gestor de recopiladores	1 por núcleo de CPU, con al menos 1 núcleo de CPU reservado para el sistema operativo y otros procesos	Un conector utilizado por completo es aquel en el que se producen el máximo posible de eps para dicho tipo de conector.
Número máximo de recopiladores (utilizados por completo) en un único gestor de recopiladores	1 por núcleo de CPU, con al menos 1 núcleo de CPU reservado para el sistema operativo y otros procesos	Un recopilador utilizado por completo es aquel en el que se producen el máximo posible de eps para dicho tipo de recopilador.

Atributo	Límite	Comentarios
Número máximo de dispositivos en un único gestor de recopiladores	2.000	El límite del servidor de Sentinel Rapid Deployment es también de 2.000. Por lo tanto, si hay 2.000 dispositivos en un único gestor de recopiladores, el límite de dispositivos para todo el sistema Sentinel se alcanza con ese gestor.
Número máximo de dispositivos en el servidor de Sentinel Rapid Deployment	2.000	El límite máximo de dispositivos en el servidor de Sentinel Rapid Deployment es de 2.000.

2.5.2 Límites de informes

Tabla 2-5 *Datos de rendimiento de los informes*

Atributo	Límite	Comentarios
Número máximo de informes guardados	200	Este límite puede aumentar o disminuir según el tamaño de los informes y el espacio disponible en el disco del servidor que no utilice el resto del sistema.
Número máximo de informes que se pueden ejecutar de forma simultánea	3	En este límite se presupone que el servidor no se utiliza a capacidad máxima para realizar la recopilación de datos u otras tareas.

2.6 Resultados de las pruebas

Sentinel Rapid Deployment permite contar con distintas configuraciones según las necesidades del entorno. La información siguiente de pruebas de rendimiento es resultado de las pruebas de Novell en las configuraciones concretas mostradas en las tablas siguientes.

Las recomendaciones de hardware para una implementación de Sentinel pueden variar; por lo tanto, es recomendable consultar a los servicios de consultoría de Novell o a los socios de Novell Sentinel antes de completar la arquitectura de Sentinel. La información de pruebas siguiente se puede usar como guía.

Las pruebas de Linux se realizaron para conseguir el número máximo de eps con cantidades distintas de dispositivos y el número máximo de dispositivos para un valor de eps específico. Se ha utilizado la siguiente configuración de hardware:

- **Número de núcleos de CPU:** 4
- **Modelo de CPU:** CPU Intel Xeon X5770 a 2,93 GHz
- **RAM:** 16 GB
- **Capacidad del disco duro (tipo +RAID y número de discos en RAID):** 1,7 TB (RAID 5, 6 discos)

Nota: todas las pruebas se han realizado con orígenes de eventos basados en syslog. Otros conectores pueden tener un rendimiento distinto.

En la tabla siguiente se muestra el número máximo de eps que se pueden obtener con distintas cantidades de dispositivos en un sistema SLES:

Tabla 2-6 *Eps máximos en un sistema SLES*

Configuración del sistema	Dispositivos	Eps máximos
4 gestores de recopiladores (uno local y tres remotos) con 10 recopiladores (generan 500 eps cada uno)	25	5.000
4 gestores de recopiladores (uno local y tres remotos) con 10 recopiladores (generan 500 eps cada uno)	100	5.000
4 gestores de recopiladores (uno local y tres remotos) con 10 recopiladores (generan 500 eps cada uno)	1.000	5.000

En la tabla siguiente se muestra el número máximo de dispositivos que se pueden obtener con distintas velocidades de eps en un sistema SLES:

Tabla 2-7 *Dispositivos máximos en un sistema SLES*

Configuración del sistema	Eps	Máximo de dispositivos
1 gestor de recopiladores con 1 recopilador que genera 500 eps	500	2.000
1 gestor de recopiladores con 2 recopiladores que generan 500 eps cada uno	1.000	2.000
1 gestor de recopiladores con 3 recopiladores que generan 500 eps cada uno	1.500	2.000

Nota:

- Si quiere obtener más eps o dispositivos, instale gestores de recopiladores adicionales.
- Los límites máximos de dispositivos no son fijos. Se trata de recomendaciones basadas en las pruebas de rendimiento llevadas a cabo por Novell. En ellas se aplica una tasa media baja de eventos por segundo por dispositivo (menos de 3 eps). Una velocidad de eps más alta da lugar a valores máximos de dispositivos sostenibles más bajos. Puede usar la ecuación (dispositivos máximos) x (media de eps por dispositivo) = velocidad máxima de eventos para obtener los límites aproximados de la velocidad media de eps específica o el número de dispositivos, siempre que el número máximo de dispositivos no supere el límite indicado anteriormente.

Instalación

3

En esta sección se recogen datos sobre la instalación de Sentinel Rapid Deployment y los componentes del cliente.

3.1 Descripción general

El paquete de instalación de Sentinel proporciona un instalador del servidor simplificado para un equipo que permite instalar todo lo que necesita para ejecutar Sentinel Rapid Deployment. El instalador del servidor de Sentinel Rapid Deployment instala los componentes siguientes:

3.1.1 Componentes del servidor

Tabla 3-1 *Componentes y aplicaciones del servidor de Sentinel*

Componente	Descripción
	La base de datos de Sentinel almacena la configuración y datos de eventos.
Bus de mensajes	Un bus de mensajes basado en JMS controla la comunicación entre los distintos componentes del sistema Sentinel.
Motor de correlación	El motor de correlación realiza un análisis de eventos en tiempo real.
Asesor	El asesor proporciona una correlación en tiempo real entre los ataques IDS detectados y la salida del análisis de vulnerabilidad para indicar de inmediato un mayor riesgo para una organización.
Servicio de acceso a los datos	Incluye los componentes de almacenamiento de datos, consultas, visualización y procesamiento.
Servidor Web	Admite la interfaz Web para Sentinel Rapid Deployment.

Componente	Descripción
Gestor de recopiladores	Servicio que gestiona conexiones a orígenes de eventos, análisis de datos, asignaciones, etc. Puede distribuir el gestor de recopiladores a otras ubicaciones, otros equipos y otros sistemas operativos por medio del instalador del gestor de recopiladores disponible mediante la interfaz Web de Sentinel Rapid Deployment. Por ejemplo, puede instalar un gestor de recopiladores adicional en un equipo Windows.
iTRAC	Sentinel proporciona un sistema de gestión del flujo de tareas iTRAC para definir y automatizar procesos para las respuestas a incidencias. Aquellas incidencias que Sentinel identifique, bien manualmente o mediante una regla de correlación, pueden asociarse con un flujo de tareas iTRAC.

3.1.2 Aplicaciones cliente

Las aplicaciones cliente (el Centro de control de Sentinel, el gestor de datos de Sentinel y Solution Designer) se instalan por defecto en el servidor de Sentinel Rapid Deployment. Puede lanzar las aplicaciones cliente mediante estos métodos:

- Con la interfaz Web de Sentinel Rapid Deployment. Los sistemas cliente deben tener instalado Java 1.6.0_20 o posterior y debe definirse la vía de JRE para lanzar las aplicaciones de Sentinel mediante WebStart.

  Defina la variable de entorno `JAVA_HOME` para que señale a la ubicación de la carpeta `JRE 6`. Defina la vía de exportación para que señale a la carpeta `bin` en la ubicación de JRE 6.
- Si se usa `<directorio_de_instalación>/bin` como usuario propietario de los archivos de instalación de Sentinel Rapid Deployment. Por ejemplo:

  `./bin/<client_application>.sh`

Tabla 3-2 *Aplicaciones cliente de Sentinel*

Componente	Descripción
Centro de control de Sentinel	Consola principal para analistas de seguridad o de conformidad.
Gestor de datos de Sentinel	Utilidad de gestión de la base de datos.
Solution Designer	Aplicación para la creación de paquetes de soluciones.
Gestor de recopiladores de Sentinel	Servicio que gestiona conexiones a orígenes de eventos, análisis de datos, asignaciones, etc. En el servidor de Sentinel hay instalado un gestor de recopiladores, pero se pueden instalar gestores de recopiladores adicionales en equipos Windows o Linux remotos mediante un instalador descargable.

3.2 Instalación en SUSE Linux Enterprise Server

- Sección 3.2.1, “Requisitos previos”, en la página 29
- Sección 3.2.2, “Instalación de Sentinel Rapid Deployment”, en la página 30

3.2.1 Requisitos previos

Asegúrese de cumplir los siguientes requisitos previos antes de instalar Sentinel Rapid Deployment. Para obtener más información sobre estos requisitos previos (incluyendo la lista de plataformas certificadas), consulte el Capítulo 2, “Requisitos del sistema”, en la página 19

- “Servidor” en la página 29
- “Cliente” en la página 29
- “Asesor” en la página 30

Importante: las instalaciones de Sentinel Rapid Deployment llevadas a cabo con el instalador siempre deberían realizarse en un sistema limpio. Si ya tiene instalada otras versiones de Sentinel, como Sentinel Classic o Sentinel Log Manager, en cualquiera de los equipos, en primer lugar debe desinstalarlas. Para obtener información sobre cómo desinstalar las versiones anteriores de Sentinel, consulte las guías de instalación relevantes:

- Para desinstalar Sentinel Classic, consulte el capítulo “Desinstalación de Sentinel” en la Guía de instalación de Sentinel (http://www.novell.com/documentation/sentinel61/s61_install/?page=/documentation/sentinel61/s61_install/data/bgpq4la.html).
- Para desinstalar Sentinel Log Manager, consulte el capítulo “Uninstalling Sentinel Log Manager” (Desinstalación de Sentinel Log Manager) en la Sentinel Log Manager 1.1 Installation Guide (http://www.novell.com/documentation/novelllogmanager11/log_manager_install/?page=/documentation/novelllogmanager11/log_manager_install/data/bor9aaf.html) (Guía de instalación de Sentinel Log Manager 1.1).

Servidor

- Asegúrese de que todos los equipos del servidor cumplen los requisitos mínimos del sistema. Para obtener más información acerca de los estados individuales, consulte el Capítulo 2, “Requisitos del sistema”, en la página 19.
- Configure el sistema operativo de manera que el comando `hostname -f` devuelva un nombre de host válido.
- Instale y configure un servidor SMTP si desea poder enviar notificaciones de correo electrónico desde el sistema Sentinel.

Cliente

- Asegúrese de que todos los equipos cliente cumplen los requisitos mínimos del sistema. Para obtener más información sobre estos requisitos previos, consulte el Capítulo 2, “Requisitos del sistema”, en la página 19.
- Asegúrese de crear un directorio cuyo nombre solo incluya caracteres ASCII (sin caracteres especiales) desde el que se ejecutará el instalador.
- Cuando instale el gestor de recopiladores remoto o las aplicaciones cliente en equipos Linux, asegúrese de que no hay ninguna restricción a nivel de carpeta definida en la carpeta `/tmp` para el usuario admin.

- Asegúrese de proporcionar privilegios de superusuario al usuario del dominio para el gestor de recopiladores en Windows, ya que los derechos de usuario normal no son suficientes para la instalación de este componente.
- Si instala el gestor de recopiladores en un equipo de 64 bits, asegúrese de que estén disponibles las bibliotecas de 32 bits. Las bibliotecas de 32 bits se requieren cuando se ejecuta un recopilador que está escrito en el lenguaje exclusivo del recopilador (que incluye casi todos los recopiladores escritos antes de junio de 2008) así como cuando se ejecutan ciertos conectores (como el conector LEA). Los recopiladores basados en JavaScript y el resto de Sentinel están habilitados para 64 bits. Es particularmente importante comprobar en las plataformas de Linux que estas bibliotecas están disponibles, ya que es posible que no se incluyan por defecto.

Asesor

Si desea instalar el asesor, debe adquirir una suscripción de detección de exploits de Sentinel de los datos del asesor. Después de adquirir la suscripción, utilice sus datos de inicio de sesión en Novell para descargar y actualizar los datos del asesor. Para obtener más información, consulte el capítulo "Advisor Usage and Maintenance" (Uso del asesor y mantenimiento) en la *Sentinel Rapid Deployment User Guide* (Guía del usuario de Sentinel Rapid Deployment).

3.2.2 Instalación de Sentinel Rapid Deployment

El servidor de Sentinel Rapid Deployment se puede instalar de estas formas:

- "Instalación de un único guión con privilegios "root"" en la página 30
- "Instalación distinta al root" en la página 32

El guion del instalador de Sentinel Rapid Deployment proporciona las siguientes opciones durante la instalación:

- **-all:** debe ser el usuario `root` para poder emplear esta opción. Esta opción crea un usuario (por defecto: `novell`) y un grupo de usuarios (por defecto: `novell`) e instala el servidor de Sentinel Rapid Deployment. También ejecuta los servicios de Sentinel Rapid Deployment de forma automática al iniciar el sistema.
- **-install:** esta opción sólo instala el servidor de Sentinel Rapid Deployment.
- **-createuser:** debe ser el usuario `root` para poder emplear esta opción. Esta opción sólo crea el usuario (por defecto: `novell`) y el grupo de usuarios (por defecto: `novell`).
- **-createservice:** debe ser el usuario `root` para poder emplear esta opción. Esta opción sólo habilita los servicios de Sentinel Rapid Deployment para que se ejecuten de forma automática al iniciar el sistema.
- **-help:** esta opción muestra ayuda sobre cómo usar las opciones del guion de instalación.

Instalación de un único guión con privilegios "root"

1. Entre como usuario `root`.

   El usuario que va a realizar la instalación debe contar con acceso de escritura al directorio temporal donde se descargarán los archivos del instalador.
2. Descargue el instalador `sentinel6_rd_linux_x86-64.tar.gz` del sitio de descargas de Novell (http://download.novell.com/) a un directorio temporal.
3. Extraiga el instalador:

```
tar zxvf sentinel6_rd_linux_x86-64.tar.gz
```

4 Acceda al directorio en el que ha extraído el instalador:

```
cd sentinel6_rd_linux_x86-64
```

5 Ejecute el guion `install.sh` con la opción `-all`:

```
./install.sh -all
```

El guion de instalación comprueba primero si hay memoria y espacio disponibles en el disco. Si hay menos de 1 GB de memoria disponible, el guion cierra la instalación de forma automática. Si hay entre 1 GB y 4 GB de memoria disponible, el guion muestra un mensaje que indica que hay menos memoria de la recomendada. También pregunta si desea continuar con la instalación. Escriba `y` (sí) si desea continuar con la instalación o `n` si no es así.

6 Especifique el nombre de usuario o pulse la tecla Intro para seleccionar el nombre de usuario por defecto. El nombre de usuario por defecto es `novell`.

Si el nombre de usuario especificado ya existe, el instalador muestra un mensaje para indicar esta situación y muestra el grupo en el que se encuentra el usuario. Pase al Paso 8.

Si el nombre de usuario no existe, el instalador lo crea. Pase al Paso 7.

7 Especifique el nombre del grupo o pulse Intro para seleccionar el nombre del grupo por defecto. El nombre del grupo por defecto es `novell`.

Si el nombre del grupo especificado ya existe, el instalador continúa con la instalación. Si el nombre del grupo especificado no existe, el instalador crea el grupo y muestra un mensaje que indica que el nombre de usuario especificado se ha creado en el grupo.

El usuario especificado y el grupo poseen los procesos de instalación y ejecución de Sentinel.

8 Especifique la vía de instalación o pulse Intro para seleccionar la vía por defecto. La vía por defecto es `/opt/novell`.

La vía de instalación que especifique no debe contener espacios. Si hay espacios, el guion de instalación pide que proporcione otra vía sin ellos.

9 Elija uno de los idiomas siguientes introduciendo el número correspondiente:

Número de serie	Idioma
1	Checo
2	Inglés
3	Francés
4	Alemán
5	Italiano
6	Japonés
7	Neerlandés
8	Polaco
9	Portugués
10	Chino simplificado
11	Español
12	Chino tradicional

El acuerdo de licencia de usuario final se muestra en el idioma seleccionado.

10 Lea el acuerdo de licencia de usuario final e introduzca `1` si está de acuerdo con los términos y desea continuar la instalación. Si desea salir de la instalación, escriba `2`.

El instalador empieza a extraer los archivos y pide la licencia.

11 Escriba `1` para usar la clave de licencia de evaluación de 90 días o `2` para usar una clave de licencia válida.

Si escribe `2`, el instalador le pedirá que introduzca una clave de licencia válida para Sentinel RD. Si la clave de licencia que especifique no es válida, el instalador le pedirá que la vuelva a indicar. Si la clave de licencia no es válida la segunda vez, se instalará automáticamente la clave de licencia de evaluación de 90 días. Puede introducir una licencia válida más tarde.

El guion carga la licencia de prueba o la licencia válida.

12 Especifique una contraseña para el usuario `dbauser` y confírmela introduciéndola de nuevo.

Las credenciales de `dbauser` se emplean para crear tablas y particiones en la base de datos PostgreSQL.

13 Especifique una contraseña para el usuario `admin` y confírmela introduciéndola de nuevo.

Cuando se le pida que especifique contraseñas para los usuarios `admin` y `dbauser`, no utilice los caracteres de barra invertida (\) ni apostrofe ('), ya que la base de datos PostgreSQL no los permite.

El guion de instalación instala la base de datos PostgreSQL, crea tablas y particiones y, a continuación, instala el servidor de Sentinel Rapid Deployment.

Después de la instalación, puede:

- Lanzar la interfaz Web de Sentinel Rapid Deployment dirigiéndose a: `https://<IP_SERVIDOR>:8443/sentinel`. *<IP_SERVIDOR>* es la dirección IP del equipo donde se instala Sentinel Rapid Deployment.
- Lanzar el Centro de control de Sentinel ejecutando `<directorio_de_instalación>/bin/control_center.sh` como el usuario que creó en el Paso 6.

Instalación distinta al root

Si la directiva administrativa prohíbe la ejecución del proceso de instalación completo como usuario `root`, la instalación puede completarse en dos partes. La primera parte del proceso de instalación debe desarrollarse con privilegios de `root` y la segunda se lleva a cabo como usuario administrativo de Sentinel (creado durante la primera parte).

1 Entre en el servidor donde desea instalar Sentinel Rapid Deployment.

El usuario que va a realizar la instalación debe contar con acceso de escritura al directorio temporal donde se descargarán los archivos del instalador.

2 Descargue el instalador `sentinel6_rd_linux_x86-64.tar.gz` del sitio de descargas de Novell (http://download.novell.com/) a un directorio temporal.

3 Extraiga el instalador:

```
tar zxvf sentinel6_rd_linux_x86-64.tar.gz
```

4 Entre como usuario `root`.

5 Acceda al directorio en el que ha extraído el instalador:

```
cd sentinel6_rd_linux_x86-64
```

6 Ejecute el guion `install.sh` con la opción `-createuser`:

```
./install.sh -createuser
```

7 Especifique el nombre de usuario o pulse la tecla Intro para seleccionar el nombre de usuario por defecto. El nombre de usuario por defecto es `novell`.

Si el nombre de usuario especificado ya existe, el instalador muestra un mensaje para indicar esta situación y muestra el grupo en el que se encuentra el usuario. Pase al Paso 9.

Si el nombre de usuario no existe, el instalador lo crea. Pase al Paso 8.

8 Especifique el nombre del grupo o pulse Intro para seleccionar el nombre del grupo por defecto. El nombre del grupo por defecto es `novell`.

Si el nombre del grupo especificado ya existe, el instalador continúa con la instalación. Si el nombre del grupo especificado no existe, el instalador crea el grupo y muestra un mensaje que indica que el nombre de usuario especificado se ha creado en el grupo.

El usuario especificado y el grupo poseen los procesos de instalación y ejecución de Sentinel.

9 Especifique la vía de instalación o pulse Intro para seleccionar la vía por defecto. La vía por defecto es `/opt/novell`.

La vía de instalación que especifique no debe contener espacios. Si hay espacios, el guion de instalación pide que proporcione otra vía sin ellos.

10 Entre como usuario distinto al root. Por ejemplo.

```
su - novell
```

11 Ejecute el guion de instalación con la opción `-install`:

```
./install.sh -install
```

El guion de instalación comprueba primero si hay memoria y espacio disponibles en el disco. Si hay menos de 1 GB de memoria disponible, el guion cierra la instalación de forma automática. Si hay entre 1 GB y 4 GB de memoria disponible, el guion muestra un mensaje que indica que hay menos memoria de la recomendada. También pregunta si desea continuar con la instalación. Escriba `y` (sí) si desea continuar con la instalación o `n` si no es así.

12 Especifique la vía de instalación o pulse Intro para seleccionar la vía por defecto. La vía por defecto es `/opt/novell`.

La vía de instalación que especifique no debe contener espacios. Si hay algún espacio, el guion de instalación pide que proporcione otra vía sin espacios.

13 Elija uno de los idiomas siguientes introduciendo el número correspondiente:

Número de serie	Idioma
1	Checo
2	Inglés
3	Francés
4	Alemán
5	Italiano
6	Japonés
7	Neerlandés
8	Polaco

Número de serie	Idioma
9	Portugués
10	Chino simplificado
11	Español
12	Chino tradicional

El acuerdo de licencia de usuario final se muestra en el idioma seleccionado.

14 Lea el acuerdo de licencia de usuario final e introduzca `1` si está de acuerdo con los términos y desea continuar la instalación. Si desea salir de la instalación, escriba `2`.

El instalador empieza a extraer los archivos y pide la licencia.

15 Escriba `1` para usar la clave de licencia de evaluación de 90 días o `2` para usar una clave de licencia válida.

Si escribe `2`, el instalador le pedirá que introduzca una clave de licencia válida para Sentinel RD. Si la clave de licencia que especifique no es válida, el instalador le pedirá que la vuelva a indicar. Si la clave de licencia no es válida la segunda vez, se instalará automáticamente la clave de licencia de evaluación de 90 días. Puede introducir una licencia válida más tarde.

El guion carga la licencia de prueba o la licencia válida.

16 Especifique una contraseña para el usuario `dbauser` y confírmela introduciéndola de nuevo.

Las credenciales de `dbauser` se emplean para crear tablas y particiones en la base de datos PostgreSQL.

17 Especifique una contraseña para el usuario `admit` y confírmela introduciéndola de nuevo.

Cuando se le pida que especifique contraseñas para los usuarios `admin` y `dbauser`, no utilice los caracteres de barra invertida (\) ni apostrofe ('), ya que la base de datos PostgreSQL no los permite.

18 (Condicional) Cuando se complete la instalación, si desea ejecutar automáticamente los servicios de Sentinel Rapid Deployment al iniciar el sistema, ejecute el guion `install.sh` con la opción `-createservice` como usuario `root`:

```
./install.sh -createservice
```

Después de la instalación, puede:

- Lanzar la interfaz Web de Sentinel Rapid Deployment dirigiéndose a: `https://<IP_SERVIDOR>:8443/sentinel`. *<IP_SERVIDOR>* es la dirección IP del equipo donde se instala Sentinel Rapid Deployment.
- Lanzar el Centro de control de Sentinel ejecutando `<directorio_de_instalación>/bin/control_center.sh` como el usuario que creó en el Paso 7.

3.3 Instalación del gestor de recopiladores y de las aplicaciones del cliente

Utilice la interfaz Web de Novell Sentinel Rapid Deployment para descargar el instalador del gestor de recopiladores y el instalador del cliente.

- Sección 3.3.1, “Descarga de los instaladores”, en la página 35

- Sección 3.3.2, “Números de puerto para los componentes del cliente de Sentinel Rapid Deployment”, en la página 35
- Sección 3.3.3, “Instalación de aplicaciones del cliente de Sentinel”, en la página 36
- Sección 3.3.4, “Instalación del gestor de recopiladores de Sentinel en SLES o Windows”, en la página 38

3.3.1 Descarga de los instaladores

1. Abra un navegador Web en la siguiente dirección URL:

   `https://<svrname.example.com>:8443/sentinel`

   Sustituya `<svrname.example.com>` con el nombre DNS real o dirección IP del servidor donde se está ejecutando Sentinel. La dirección URL distingue entre mayúsculas y minúsculas.
2. Si se le solicita verificar los certificados, revise la información del certificado y, a continuación, haga clic en *Sí*, si es válido.
3. Especifique el nombre de usuario y la contraseña para acceder a la cuenta de Sentinel.
4. Utilice la lista desplegable *Idiomas* para seleccionar el idioma.

   Se trata del mismo idioma que el código de idioma del servidor de Sentinel Rapid Deployment y del equipo local. Asegúrese de que los valores de idiomas de su navegador están configurados para admitir el idioma deseado.
5. Haga clic en *Entrar*.
6. Seleccione *Aplicaciones*.

   Puede descargar los siguientes instaladores:

Opciones	Descripción	Acción:
Instalador del gestor de recopiladores	El instalador del gestor de recopiladores permite instalar el gestor de recopiladores de Sentinel en plataformas Windows y Linux compatibles.	Haga clic en *Descargar instalador del gestor de recopiladores* y siga las instrucciones que aparecen en pantalla.
Instalador del cliente	El instalador del cliente permite instalar el Centro de control de Sentinel, Solution Designer de Sentinel y el gestor de datos de Sentinel en las plataformas admitidas.	Haga clic en *Descargar el instalador de cliente* y siga las instrucciones que aparecen en pantalla.

Para obtener más información sobre cómo instalar el gestor de recopiladores, consulte la Sección 3.3.4, “Instalación del gestor de recopiladores de Sentinel en SLES o Windows”, en la página 38. Para el instalador del cliente, consulte la Sección 3.3.3, “Instalación de aplicaciones del cliente de Sentinel”, en la página 36.

3.3.2 Números de puerto para los componentes del cliente de Sentinel Rapid Deployment

Utilice los puertos siguientes para configurar el cortafuego de forma que permita la comunicación entre Sentinel Rapid Deployment y los componentes del cliente.

Tabla 3-3 *Números de puerto compatibles para los componentes de Sentinel Rapid Deployment*

Número de puerto	Descripción
61616	Los gestores de recopiladores remotos usan este puerto para conectar con el servidor de Sentinel Rapid Deployment mediante ActiveMQ.
10013	El Centro de control de Sentinel usa este puerto para conectar con el servidor de Sentinel Rapid Deployment mediante un servidor proxy.
5432	El gestor de datos de Sentinel usa este puerto para conectar con la base de datos PostgreSQL.
8443	Los clientes Web usan este puerto para conectar con el servidor de Sentinel Rapid Deployment.

3.3.3 Instalación de aplicaciones del cliente de Sentinel

Es posible instalar la aplicación cliente de Sentinel en sistemas Linux o Windows. Para instalar las aplicaciones del cliente:

1. Diríjase a la carpeta donde ha descargado el instalador del cliente.
2. Extraiga el guión de instalación del archivo:

Plataforma	Acción:
Windows	Descomprima el archivo `client_installer.zip`. Los archivos se descomprimen en un directorio denominado `disk1`.
Linux	Ejecute el siguiente comando con privilegios “root”: `unzip client_installer.zip` Los archivos se descomprimen en un directorio denominado `disk1`.

3. Desplácese al directorio de instalación y comience la instalación:

Plataforma	Acción:
Windows	Ejecute `disk1\setup.bat` **Nota:** en un equipo con Windows Vista, lance el indicador de comandos utilizando la opción *Ejecutar como administrador* en las opciones del menú contextual.
Linux	◆ **Modo GUI:** `<directorio_instalación>/disk1/setup.sh` ◆ **Modo de consola:** `<directorio_instalación>/disk1/setup.sh –console`

Los pasos siguientes sólo son válidos para el modo de interfaz gráfica.

4. Haga clic en la flecha abajo y seleccione uno de los idiomas.

5 En la pantalla de bienvenida, haga clic en *Siguiente*.

6 Lea y acepte el Acuerdo de licencia del usuario final. Haga clic en *Siguiente*.

7 Acepte el directorio de instalación por defecto o haga clic en *Examinar* para especificar la ubicación de la instalación. Haga clic en *Siguiente*.

Importante: no es posible instalar en directorios que incluyan caracteres especiales o caracteres que no son ASCII en su nombre. Por ejemplo, al instalar Sentinel Rapid Deployment en Windows x86-64, la vía por defecto es `C:\\Archivos de programa (x86)`. Si desea continuar la instalación, debe cambiar esta vía por defecto para evitar los caracteres especiales, como los paréntesis de (x86).

---

8 Seleccione las aplicaciones de Sentinel que desee instalar.

Están disponibles las siguientes opciones:

Componente	Descripción
Centro de control de Sentinel	La consola principal para analistas de seguridad o de conformidad.
Gestor de datos de Sentinel (SDM)	Utilizado para las actividades manuales de gestión de bases de datos.
Solution Designer	Le ayuda a crear paquetes de soluciones.

9 Si decide instalar el Centro de control de Sentinel, el instalador le solicita el máximo espacio de memoria para asignarla al Centro de control. Especifique el tamaño máximo de la pila JVM (MB) que va a utilizar sólo el Centro de control de Sentinel.

El rango permitido es 64-1.024 MB.

Esta opción no está disponible si ya está instalada alguna aplicación de Sentinel.

10 Especifique el nombre del usuario o pulse Intro para seleccionar el nombre del usuario por defecto. El nombre del usuario por defecto es `esecadm`.

Éste es el nombre de usuario del usuario al que pertenece el producto Sentinel instalado. Si el usuario todavía no existe, debe crear uno junto con un directorio personal en el directorio especificado.

11 Especifique el directorio personal del usuario o pulse Intro para seleccionar el directorio por defecto. El directorio por defecto es `/export/home`.

Si el usuario es `esecadm`, el directorio personal correspondiente es `/export/home/esecadm`.

12 Especifique la contraseña del usuario que ha entrado como usuario `esecadm` en caso de que haya seleccionado el nombre de usuario por defecto en el Paso 10. Si no es así, defina la contraseña para el usuario que ha creado en el Paso 10.

13 Especifique la siguiente información:

- **Puerto del bus de mensajes:** el puerto en el que está escuchando el servidor de comunicaciones. Los componentes que están conectados directamente al servidor de comunicaciones utilizan este puerto. El número de puerto por defecto es 61616.

- **Puerto del servidor proxy del Centro de control de Sentinel:** el puerto en el que escucha el servidor proxy SSL (servidor proxy de acceso a datos) para aceptar el nombre de usuario y la contraseña. El servidor proxy SSL acepta las credenciales basadas en las conexiones autenticadas. El Centro de control de Sentinel utiliza este puerto para conectarse al servidor de Sentinel. El número de puerto por defecto es `10013`.
- **Nombre de host del servidor de comunicaciones:** la dirección IP del equipo o el nombre de host donde está instalado el servidor de Sentinel Rapid Deployment.

Asegúrese de que los números de puerto sean los mismos que los del servidor de Sentinel Rapid Deployment en `<directorio_instalación>/config/configuration.xml` para poder habilitar las comunicaciones. Anote estos puertos para instalaciones futuras en otros equipos. Para obtener más información acerca de los números de puertos, consulte la Sección 3.3.2, “Números de puerto para los componentes del cliente de Sentinel Rapid Deployment”, en la página 35.

14 Haga clic en *Siguiente.*

Se muestra un resumen de la instalación.

15 Haga clic en *Install* (Instalar).

16 Haga clic en *Finalizar* para terminar la instalación de

Nota: cuando vuelva a entrar a la sesión, utilice el nombre de usuario que haya especificado en Paso 10.

Si ha olvidado el nombre de usuario definido, abra una consola de terminal e introduzca el siguiente comando como usuario `root`:

```
env | grep ESEC_USER
```

Este comando devuelve el nombre de usuario si el usuario ya está creado y las variables de entorno ya están definidas.

3.3.4 Instalación del gestor de recopiladores de Sentinel en SLES o Windows

El instalador del gestor de recopiladores de Sentinel está disponible para su descarga en la página de aplicaciones de la interfaz Web de Sentinel Rapid Deployment. Para instalar el gestor de recopiladores:

1 Diríjase a la carpeta donde ha descargado el instalador del gestor de recopiladores.

2 Extraiga el guión de instalación del archivo:

Plataforma	Acción:
Windows	Descomprima el archivo `scm_installer.zip`.
	Los archivos se descomprimen en un directorio denominado `disk1`.
Linux	Ejecute el siguiente comando con privilegios “root”:
	`unzip scm_installer.zip`
	Los archivos se descomprimen en un directorio denominado `disk1`.

3 Diríjase al directorio `disk1` y comience la instalación:

Plataforma	Acción:
Windows	Ejecute el comando siguiente: `disk1\setup.bat`
Linux	◆ **Modo GUI:** `<directorio_instalación>/disk1/setup.sh` ◆ **Modo de consola:** `<directorio_instalación>/disk1/setup.sh -console`

4 Seleccione un idioma para continuar con la instalación.

5 Lea la pantalla de bienvenida y haga clic en *Siguiente*.

6 Lea y acepte el Acuerdo de licencia del usuario final. Haga clic en *Siguiente*.

7 Acepte el directorio de instalación por defecto o haga clic en *Examinar* para especificar la ubicación de la instalación y, a continuación, haga clic en *Siguiente*.

Importante: no es posible instalar en directorios que incluyan caracteres especiales o caracteres que no son ASCII en su nombre. Por ejemplo, al instalar Sentinel en Windows x86-64, la vía por defecto es `C:\\Archivos de programa (x86)`. Si desea continuar la instalación, debe cambiar la vía por defecto para evitar los caracteres especiales, como los paréntesis de (x86).

8 Especifique el nombre de usuario del administrador de Sentinel y la vía al directorio personal correspondiente.

Esta opción no está disponible si ya está instalada alguna aplicación de Sentinel.

- **Nombre de usuario administrador de Sentinel:** el valor por defecto es `esecadm`.

  Éste es el nombre de usuario del usuario al que pertenece el producto Sentinel instalado. Si el usuario todavía no existe, se debe crear uno junto con un directorio personal en el directorio especificado.

- **Directorio personal del usuario administrador de Sentinel:** por defecto es `/export/home`. Si `esecadm` es el nombre de usuario, el directorio personal correspondiente es `/export/home/esecadm`.

Para entrar como usuario `esecadm`, primero tiene que definir su contraseña.

9 Especifique la siguiente información:

- **Puerto del bus de mensajes:** el puerto en el que está escuchando el servidor de comunicaciones. Los componentes que están conectados directamente al servidor de comunicaciones utilizan este puerto. El número de puerto por defecto es 61616.
- **Nombre de host del servidor de comunicaciones:** la dirección IP del equipo o nombre de host donde está instalado el servidor de Sentinel Rapid Deployment.

Asegúrese de que los números de puertos son los mismos en todos los equipos del sistema de Sentinel para habilitar las comunicaciones. Anote estos puertos para instalaciones futuras en otros equipos.

10 Haga clic en *Siguiente.*

11 Especifique la siguiente información:

- **Configuración automática de la memoria:** seleccione la cantidad total de memoria que se va a asignar en el gestor de recopiladores. El instalador determina automáticamente la distribución óptima de memoria en todos los componentes teniendo en cuenta la sobrecarga estimada de la base de datos y del sistema operativo.

  Importante: puede modificar el valor de -Xmx en el archivo `configuration.xml` para cambiar la RAM asignada al proceso del gestor de recopiladores. El archivo `configuration.xml` está situado en `<directorio_instalación>/config` en Linux o en `<directorio_instalación>\config` en Windows.

- **Configuración personalizada de la memoria:** haga clic en *Configurar* para ajustar las asignaciones de memoria. Esta opción sólo está disponible si hay suficiente memoria en el equipo.

12 Haga clic en *Siguiente.*

Se muestra una pantalla de resumen con las funciones seleccionadas para la instalación.

13 Haga clic en *Instalar.*

14 Cuando termine la instalación, se le solicitará que introduzca el nombre de usuario y la contraseña que utiliza la estrategia JMS de ActiveMQ para conectarse al intermediario.

Utilice el nombre de usuario `collectormanager` y su contraseña correspondiente disponible en el archivo `<directorio_instalación>/config/activemqusers.properties` del servidor de Sentinel.

A continuación se muestra un ejemplo de las credenciales disponibles en el archivo `activemqusers.properties`:

```
collectormanager=cefc76062c58e2835aa3d777778f9295
```

`collectormanager` es el nombre de usuario y `cefc76062c58e2835aa3d777778f9295` la contraseña correspondiente.

Debe utilizar el usuario collectormanager y su correspondiente contraseña durante la instalación del servicio del gestor de recopiladores. En este caso, el usuario `collectormanager` tiene derechos de acceso sólo a los canales de comunicación necesarios para las operaciones del gestor de recopiladores.

Cuando termine la instalación, se le solicitará que reinicie o que vuelva a entrar a la sesión y que inicie manualmente los servicios de Sentinel.

15 Haga clic en *Finalizar* para reiniciar el sistema.

16 Vuelva a entrar con el nombre de usuario especificado en el Paso 8.

Si ha olvidado el nombre de usuario, abra una consola de terminal e introduzca el siguiente comando con credenciales `root`.

```
env | grep ESEC_USER
```

Este comando devuelve el nombre de usuario si el usuario ya está creado y las variables de entorno ya están definidas.

Nota: existen algunos problemas con la instalación del gestor de recopiladores en la plataforma Windows 2008, así como en los gestores de recopiladores cuya imagen se ha generado. Para obtener información sobre cómo resolver estos problemas, consulte el Apéndice B, “Sugerencias para la resolución de problemas”, en la página 89.

3.4 Inicio y detención manual de los servicios de Sentinel

Para iniciar manualmente los servicios de Sentinel, utilice uno de los comandos siguientes:

Plataforma	Comando
Linux	`<install_directory>/bin/sentinel.sh start`
Windows	`<install_directory>/bin/sentinel.bat start`

Para detener manualmente los servicios de Sentinel, utilice uno de los comandos siguientes:

Plataforma	Comando
Linux	`<install_directory>/bin/sentinel.sh stop`
Windows	`<install_directory>/bin/sentinel.bat stop`

También puede usar el comando siguiente para iniciar o detener los servicios de Sentinel.

```
/etc/init.d/sentinel.sh stop|start
```

3.5 Actualización manual de Java

La versión 1.6.0_24 de Java se incluye con el programa de instalación del servidor de Sentinel Rapid Deployment y se instala junto a este servidor. Sin embargo, si actualiza Java a la versión más reciente en el servidor, debe llevar a cabo los pasos siguientes para que Sentinel Rapid Deployment la use:

1. Descargue los lotes de jre del sistema operativo en el que se instale el servidor de Sentinel Rapid Deployment.

   El usuario que realiza la actualización debe tener permiso de escritura en el directorio de instalación de Sentinel Rapid Deployment y también en el directorio donde se descargan los archivos de actualización.

   - Si ha instalado Sentinel Rapid Deployment en SUSE Linux Enterprise Server, descargue los lotes de jre de 32 y 64 bits del sitio de descargas de Java (http://www.java.com/en/download/manual.jsp).

2. Cambie el nombre de las carpetas `jre` y `jre64` del directorio de instalación de Sentinel Rapid Deployment a `jre_old` y `jre64_old`, respectivamente.

   ```
   cd <install_path>/sentinel_rd
   mv jre jre_old
   mv jre64 jre64_old
   ```

   Nota: es preciso realizar el cambio de nombre para poder revertir a la versión anterior si la actualización de Java no funciona correctamente. Es posible suprimir las carpetas renombradas si Java funciona correctamente tras la actualización.

3. Extraiga los lotes de jre descargados.

4. Renombre la carpeta de 32 bits a `jre` y el directorio de 64 bits a `jre64`.

5 Copie las carpetas `jre` y `jre64` renombradas al directorio de instalación de Sentinel Rapid Deployment.

```
copy jre <install_path>/sentinel_rd/
copy jre64 <install_path>/sentinel_rd/
```

6 (Condicional) Asegúrese de definir la propiedad y los permisos necesarios de las carpetas `jre` y`jre64` para el usuario que va a ejecutar el servidor de Sentinel Rapid Deployment.

7 Reinicie el servidor de Sentinel Rapid Deployment, reinicie el navegador y compruebe si Java se ha instalado correctamente.

3.6 Configuración posterior a la instalación

Esta sección le ayudará a comprender la configuración posterior a la instalación para los servicios de Sentinel Rapid Deployment.

3.6.1 Cambio de los ajustes de fecha y hora

El formato de fecha y hora por defecto del Centro de control de Sentinel se puede anular. Para obtener más información sobre cómo personalizar el formato de fecha y hora y cambiarlo a la zona horaria local, consulte el sitio Web de Java (http://java.sun.com/j2se/1.6.0/docs/api/java/text/SimpleDateFormat.html).

1 Edite el archivo `SentinelPreferences.properties`.

`<install_directory>/config/SentinelPreferences.properties`

2 Elimine el comentario de la siguiente línea y personalice el formato de fecha y hora para los campos de fecha y hora de eventos del Centro de control de Sentinel:

```
com.eSecurity.Sentinel.event.datetimeformat=yyyy-MM-dd'T'HH:mm:ss.SSSZ
```

3.6.2 Configuración del integrador de SMTP para enviar notificaciones de Sentinel

En Sentinel Rapid Deployment, la acción SendEmail de JavaScript funciona con el integrador de SMTP para enviar mensajes de correo desde varios contextos en la interfaz de Sentinel a los destinatarios de correo. El integrador de SMTP debe estar configurado con información de conexión válida para que funcione. Para obtener más información, consulte “Sending an E-mail” (Envío de correo electrónico) en la *Sentinel Rapid Deployment User Guide* (Guía del usuario de Sentinel Rapid Deployment).

En cada instalación de Sentinel, se crea automáticamente una única instancia del módulo auxiliar (plug-in) de la acción SendEmail. No es necesaria configuración alguna para la acción SendEmail, excepto indicar los destinatarios del mensaje de correo y el contenido del mensaje, que se configuran en los parámetros de la acción.

Sentinel activa la acción SendEmail de forma interna para enviar correo en las siguientes situaciones:

- Si se genera una regla de correlación, se activa una acción SendEmail. Esta acción SendEmail es la que se indica en el icono de la herramienta, que es la única válida para la correlación (al contrario de la acción SendEmail de JavaScript, que se indica mediante el icono JS JavaScript).
- Si un flujo de trabajo incluye una actividad o un paso de correo configurado para enviar correo electrónico.
- Si un usuario abre una incidencia y selecciona ejecutar una actividad configurada para enviar correos electrónicos.
- Si un usuario hace clic con el botón derecho en un evento y selecciona *Correo electrónico.*
- Si un usuario abre una incidencia y selecciona *Enviar incidencia por correo electrónico.*

3.6.3 Servicios del gestor de recopiladores

- "Instalación de un gestor de recopiladores adicional" en la página 43
- "Uso del recopilador genérico" en la página 43

Instalación de un gestor de recopiladores adicional

Los gestores de recopiladores administran todos los procesos de recopilación y análisis de datos. De vez en cuando, puede ser necesario agregar un nodo del gestor de recopiladores de Sentinel adicional al entorno de Sentinel para equilibrar la carga entre equipos. Los gestores de recopiladores remotos presentan varias ventajas:

- Permiten el análisis de eventos y el procesamiento distribuidos para mejorar el rendimiento del sistema.
- Permiten filtrar, cifrar y comprimir datos en el sistema de origen si concurren con los orígenes de eventos. Se reducen así los requisitos de ancho de banda de la red y se ofrece seguridad adicional a los datos.
- Permiten instalar en sistemas operativos adicionales. Por ejemplo, se puede instalar un nodo del gestor de recopiladores en Microsoft Windows para permitir la recopilación de datos mediante el protocolo WMI.
- Permiten el almacenamiento en caché de archivos, lo que habilita al gestor de recopiladores remoto para almacenar en caché grandes cantidades de datos si el servidor está ocupado temporalmente archivando o procesando un pico de eventos. Esto supone una ventaja para los protocolos como, por ejemplo, syslog, que no admiten de forma nativa el almacenamiento en caché de eventos.

Los componentes del gestor de recopiladores pueden equilibrar la carga mediante la instalación de instancias de estos componentes en equipos adicionales. Es posible instalar gestores de recopiladores adicionales ejecutando el instalador en un equipo nuevo. Para obtener más información acerca de la instalación del gestor de recopiladores, consulte la Sección 3.3.4, "Instalación del gestor de recopiladores de Sentinel en SLES o Windows", en la página 38.

Uso del recopilador genérico

Durante la instalación del servidor de Sentinel Rapid Deployment, se configurará un recopilador denominado recopilador genérico. Por defecto, crea eventos a una velocidad de 5 eventos por segundo (eps).

Si desea recopiladores adicionales para el sistema, puede descargarlos del sitio Web de Novell (http://support.novell.com/products/sentinel/collectors.html).

3.6.4 Gestión del tiempo

Debe conectar el servidor de Sentinel a un servidor NTP (Protocolo de hora de la red) o a otro tipo de servidor de hora. Si el tiempo del sistema en todas las máquinas no está sincronizado, el Motor de correlación de Sentinel y las vistas Active Views no funcionarán correctamente. Los eventos de los gestores de recopiladores no se consideran de tiempo real y, por tanto, se envían directamente a la base de datos de Sentinel, omitiendo los centros de control de Sentinel y los motores de correlación.

Por defecto, el umbral para los datos en tiempo real es de 120 segundos. Esto se puede modificar cambiando el valor de `esecurity.router.event.realtime.expiration` en el archivo `event-router.properties`. El tiempo de los eventos de Sentinel se rellena basándose en la hora del dispositivo de confianza o en la hora del gestor de recopiladores. Puede seleccionar la hora del dispositivo de confianza mientras configura un recopilador. La hora del dispositivo de confianza es la hora a la que el dispositivo generó el registro y la hora del gestor de recopiladores es la hora del sistema local del sistema del gestor de recopiladores.

3.7 Autenticación LDAP

Sentinel Rapid Deployment es compatible tanto con la autenticación LDAP como con la autenticación de la base de datos. Puede permitir que los usuarios entren en Sentinel Rapid Deployment con sus credenciales de Novell eDirectory o de Microsoft Active Directory configurado un servidor de Sentinel Rapid Deployment para la autenticación LDAP.

- Sección 3.7.1, “Descripción general”, en la página 44
- Sección 3.7.2, “Requisitos previos”, en la página 45
- Sección 3.7.3, “Configuración del servidor de Sentinel para la autenticación LDAP”, en la página 46
- Sección 3.7.4, “Configuración de varios servidores LDAP para failover”, en la página 48
- Sección 3.7.5, “Configuración de la autenticación LDAP para varios dominios de Active Directory”, en la página 51
- Sección 3.7.6, “Entrada mediante las credenciales de usuario LDAP”, en la página 52

3.7.1 Descripción general

Puede configurar el servidor de Sentinel Rapid Deployment para la autenticación LDAP en una conexión SSL segura. En el directorio LDAP se pueden usar búsquedas anónimas, o no.

Nota: si las búsquedas anónimas están inhabilitadas en el directorio LDAP, no debe configurar el servidor de Sentinel Rapid Deployment para que las use.

- **Búsqueda anónima:** cuando cree las cuentas de usuario LDAP de Sentinel Rapid Deployment, debe especificar el nombre de usuario del directorio, pero no es necesario indicar el nombre completo (DN) del usuario.

Si el usuario de LDAP entra en Sentinel Rapid Deployment, el servidor de Sentinel Rapid Deployment realiza una búsqueda anónima en el directorio LDAP según el nombre de usuario especificado, busca el DN correspondiente y autentica los datos del usuario con el directorio LDAP mediante el DN.

- **Búsqueda no anónima:** cuando cree las cuentas de usuario LDAP de Sentinel Rapid Deployment, debe especificar tanto el nombre de usuario del directorio como el nombre completo (DN) del usuario.

  Cuando el usuario de LDAP entra en Sentinel Rapid Deployment, el servidor de Sentinel Rapid Deployment autentica los datos del usuario con el directorio LDAP mediante el DN de usuario especificado y no realiza ninguna búsqueda anónima en el directorio LDAP.

  Existe un método adicional sólo aplicable en el caso de Active Directory. Para obtener más información, consulte la Autenticación LDAP no anónima mediante el atributo UserPrincipalName en Active Directory.

3.7.2 Requisitos previos

- "Exportación del certificado de CA del servidor LDAP" en la página 45
- "Habilitación de la búsqueda anónima en el directorio LDAP" en la página 45

Exportación del certificado de CA del servidor LDAP

La conexión SSL segura con el servidor LDAP requiere el certificado de CA del servidor LDAP, que debe exportar a un archivo codificado en base64.

- **eDirectory:** consulte Exporting an Organizational CA's Self-Signed Certificate (http://www.novell.com/documentation/edir88/edir88/?page=/documentation/edir88/edir88/data/a7elxuq.html) (Exportación del certificado autofirmado de CA de una organización).

  Para exportar un certificado de CA de eDirectory a iManager, los módulos auxiliares (plug-ins) del servidor de certificados de Novell para iManager deben estar instalados.

- **Active Directory:** consulte How to enable LDAP over SSL with a third-party certification authority (http://support.microsoft.com/kb/321051) (Habilitación de LDAP en SSL con una autoridad certificadora de otro fabricante).

Habilitación de la búsqueda anónima en el directorio LDAP

Para realizar la autenticación LDAP utilizando la búsqueda anónima, se deben habilitar éstas en el directorio LDAP. La búsqueda anónima está habilitada por defecto en eDirectory e inhabilitada en Active Directory.

Para habilitar la búsqueda anónima en el directorio LDAP, consulte lo siguiente:

- **eDirectory:** consulte el apartado ldapBindRestrictions en la sección Attributes on the LDAP Server Object (http://www.novell.com/documentation/edir88/edir88/?page=/documentation/edir88/edir88/data/agq8auc.html) (Atributos del objeto de servidor LDAP).

- **Active Directory:** el objeto de usuario ANONYMOUS LOGON debe recibir los permisos de lista y los acceso de lectura apropiados para los atributos `sAMAccountName` y `objectclass`. Para obtener más información, consulte Configuring Active Directory to Allow Anonymous Queries (http://support.microsoft.com/kb/320528) (Configuración de Active Directory para permitir las consultas anónimas).

  En Windows Server 2003 hay que realizar una configuración adicional. Para obtener más información, consulte Configuring Active Directory on Windows Server 2003 (http://support.microsoft.com/kb/326690/en-us) (Configuración de Active Directory en Windows Server 2003).

3.7.3 Configuración del servidor de Sentinel para la autenticación LDAP

1. Asegúrese de que cumple los requisitos previos descritos en la Sección 3.7.2, “Requisitos previos”, en la página 45.
2. Entre al servidor de Sentinel Rapid Deployment como usuario `root`.
3. Copie el archivo de certificado de CA del servidor LDAP exportado a `<directorio_instalación>/config`.
4. Defina la propiedad y los permisos del archivo de certificado de la siguiente forma:

   ```
   chown novell:novell <directorio_instalación>/config/<archivo-certificado>
   chmod 700 <directorio_instalación>/config/<archivo-certificado>
   ```

5. Cambie al usuario `novell`:

   ```
   su - novell
   ```

6. Cambie al directorio `<directorio_instalación>/bin`.
7. Ejecute el guion de configuración de la autenticación LDAP:

   ```
   ./ldap_auth_config.sh
   ```

   El guion realiza una copia de seguridad de los archivos de configuración `auth.login` y `configuration.xml` en el directorio `config` como `auth.login.sav` y `configuration.xml.sav` antes de modificarlos para la autenticación LDAP.
8. Especifique la siguiente información:

   Pulse Intro para aceptar el valor por defecto o especifique un valor nuevo para anularlo.

   - **Ubicación de instalación de Sentinel:** el directorio de instalación en el servidor de Sentinel.
   - **Nombre de host o dirección IP del servidor LDAP:** el nombre del host o la dirección IP del equipo donde está instalado el servidor LDAP. El valor por defecto es localhost. Sin embargo, no debería instalar el servidor LDAP en el mismo equipo que el servidor de Sentinel
   - **Puerto del servidor LDAP:** el número de puerto de una conexión LDAP segura. El número de puerto por defecto es 636.
   - **Búsquedas anónimas en el directorio LDAP:** especifique `y` (sí) para realizar búsquedas anónimas. Si no desea hacerlo, indique `n`. El valor por defecto es `y`.

     Si especifica `n`, complete la configuración de LDAP y lleve a cabo los pasos mencionados en la sección “Autenticación LDAP sin realizar búsquedas anónimas” en la página 47.

- **Directorio LDAP usado:** este parámetro sólo se muestra si ha especificado la opción afirmativa (y) para las búsquedas anónimas. Indique 1 para Novell eDirectory o 2 para Active Directory. El valor por defecto es 1.
- **Subárbol LDAP para buscar usuarios:** este parámetro sólo se muestra si ha especificado la opción afirmativa (y) para las búsquedas anónimas. Es el subárbol del directorio que contiene los objetos de usuario. A continuación se muestran algunos ejemplos para indicar el subárbol en eDirectory y Active Directory:
  - eDirectory:

    ```
    ou=users,o=novell
    ```

    Nota: en el caso de eDirectory, si no se especifica ningún subárbol, la búsqueda se realiza en todo el directorio.
  - Active Directory:

    ```
    CN=users,DC=TESTAD,DC=provo, DC=novell,DC=com
    ```

    Nota: en el caso de Active Directory, el subárbol no puede dejarse vacío.
- **Nombre de archivo del certificado del servidor LDAP:** el nombre de archivo del certificado de CA de eDirectory o Active Directory que ha copiado en el Paso 3.

9 Introduzca uno de estos comandos:

- `y` para aceptar los valores introducidos.
- `n` para introducir valores nuevos.
- `q` para salir de la configuración.

Si la configuración es correcta:

- El certificado del servidor LDAP se añade a un almacén de claves denominado `<directorio_instalación>/config/ldap_server.keystore`.
- Los archivos de configuración `auth.login` y `configuration.xml` de `<directorio_instalación>/config` se actualizan para habilitar la autenticación LDAP.

10 Indique `y` (sí) para reiniciar el servicio Sentinel.

Importante: si se produce algún error, revierta los cambios realizados a los archivos de configuración `auth.login` y `configuration.xml` del directorio `config`:

```
cp -p auth.login.sav auth.login
cp -p configuration.xml.sav configuration.xml
```

11 (Condicional) Si ha especificado `n` para Búsquedas anónimas en el directorio LDAP:, continúe en "Autenticación LDAP sin realizar búsquedas anónimas" en la página 47.

Autenticación LDAP sin realizar búsquedas anónimas

Al configurar Sentinel Rapid Deployment para la autenticación LDAP, si ha especificado la opción negativa (n) para las búsquedas anónimas en el directorio LDAP, la autenticación LDAP no realiza búsquedas anónimas.

Si crea la cuenta de usuario LDAP mediante el Centro de control de Sentinel, asegúrese de especificar *DN de usuario LDAP* para la autenticación LDAP no anónima. Puede usar este enfoque tanto para eDirectory como para Active Directory.

Para obtener más información, consulte “Creating an LDAP User Account for Sentinel” (Creación de una cuenta de usuario LDAP para Sentinel) en la *Sentinel Rapid Deployment User Guide* (Guía del usuario de Sentinel Rapid Deployment).

Asimismo, en el caso de Active Directory existe un enfoque alternativo para realizar la autenticación LDAP sin búsquedas anónimas. Para obtener más información, consulte la Autenticación LDAP no anónima mediante el atributo UserPrincipalName en Active Directory.

Autenticación LDAP no anónima mediante el atributo UserPrincipalName en Active Directory

En el caso de Active Directory también es posible realizar la autenticación LDAP sin búsquedas anónimas mediante el atributo userPrinicipalName:

1. Asegúrese de que el atributo userPrinicipalName está definido como <*sAMNombreCuenta@dominio*> para el usuario de Active Directory.

   Para obtener más información, consulte User-Principal-Name Attribute (http://msdn.microsoft.com/en-us/library/ms680857(VS.85).aspx) (Atributo User-Principal-Name).

2. Asegúrese de haber realizado del Paso 1 en la página 46 al Paso 10 en la página 47 y de que ha respondido negativamente (`n`) en “Búsquedas anónimas en el directorio LDAP:” en la página 46.

3. En el servidor de Sentinel, edite la sección `LdapLogin` del archivo <*directorio_instalación*>`/config/auth.login`:

   ```
   LdapLogin {
    com.sun.security.auth.module.LdapLoginModule required
    userProvider="ldap://LDAP server IP:636/DN of the Container that contains
   the user objects"
    authIdentity="{USERNAME}@Domain Name"
    userFilter="(&(sAMAccountName={USERNAME})(objectclass=user))"
    useSSL=true;
    };
   ```

   Por ejemplo:

   ```
   LdapLogin {
    com.sun.security.auth.module.LdapLoginModule required
    userProvider="ldap://137.65.151.12:636/DC=Test-
   AD,DC=provo,DC=novell,DC=com"
    authIdentity="{USERNAME}@Test-AD.provo.novell.com"
    userFilter="(&(sAMAccountName={USERNAME})(objectclass=user))"
    useSSL=true;
    };
   ```

4. Reinicie el servicio Sentinel:

   ```
   /etc/init.d/sentinel stop
   ```

   ```
   /etc/init.d/sentinel start
   ```

3.7.4 Configuración de varios servidores LDAP para failover

Para configurar uno o varios servidores LDAP como servidores de failover (relevo de funciones multinodo) para la autenticación LDAP:

1. Asegúrese de haber seguido del Paso 2 en la página 46 al Paso 10 en la página 47 para configurar el servidor de Sentinel para la autenticación LDAP en el servidor LDAP primario.

2. Entre en el servidor de Sentinel como el usuario `novell`.
3. Detenga el servicio de Sentinel.

   ```
   /etc/init.d/sentinel stop
   ```
4. Cambie al directorio `<directorio_instalación>/config`.

   ```
   cd <install_directory>/config
   ```
5. Abra el archivo `auth.login` para editarlo.

   ```
   vi auth.login
   ```
6. Actualice el `userProvider` (proveedor del usuario) en la sección LdapLogin para especificar varias URL de LDAP. Separe cada URL con un espacio en blanco.

   Por ejemplo:

   ```
   userProvider="ldap://ldap-url1 ldap://ldap-url2"
   ```

   En Active Directory, asegúrese de que el subárbol de la URL de LDAP no está vacío.

   Para obtener más información sobre cómo especificar varias URL de LDAP, consulte la descripción de la opción `userProvider` en Class LdapLogin Module (http://java.sun.com/javase/6/docs/jre/api/security/jaas/spec/com/sun/security/auth/module/LdapLoginModule.html) (Módulo LdapLogin de clase).
7. Guarde los cambios.
8. Exporte el certificado de cada servidor LDAP de failover y copie el archivo de certificado en `<directorio_instalación>/config` en el servidor de Sentinel.

   Para obtener más información, consulte "Exportación del certificado de CA del servidor LDAP" en la página 45.
9. Asegúrese de definir la propiedad y los permisos necesarios del archivo de certificado de cada servidor LDAP de failover.

   ```
   chown novell:novell <install_directory>/config/<cert-file>
   chmod 700 <install_directory>/config/<cert-file>
   ```
10. Añada los certificados de servidor LDAP de failover al almacén de claves `ldap_server.keystore` creado en el Paso 8 de la sección "Configuración del servidor de Sentinel para la autenticación LDAP" en la página 46.

    ```
    <install_directory>/jre64/bin/keytool -importcert -noprompt -trustcacerts
    -file <certificate-file> -alias <alias_name> -keystore
    ldap_server.keystore -storepass sentinel
    ```

    Sustituya `<certificate-file>` por el nombre del archivo de certificado LDAP en formato con código base64 y `<alias_name>` por el nombre del alias del certificado que se va a importar.

    Importante: asegúrese de especificar el alias. Si no se especifica ningún alias, la herramienta de claves toma `mykey` como alias por defecto. Si importa varios certificados en el almacén de claves sin especificar ningún alias, la herramienta de claves muestra un error que indica que el alias ya existe.

    ---
11. Inicie el servicio de Sentinel.

    ```
    /etc/init.d/sentinel start
    ```

Puede que el servicio no esté conectado al servidor LDAP de failover si el servidor de Sentinel supera el tiempo límite antes de descubrir que el servidor LDAP está apagado. Para garantizar que el servidor de Sentinel se conecta con el servidor LDAP de failover sin que se supere el tiempo límite:

1. Entre al servidor de Sentinel como usuario `root`.
2. Abra el archivo `sysct1.conf` para editarlo:

   ```
   vi /etc/sysctl.conf
   ```

3. Asegúrese de que el valor de `net.ipv4.tcp_syn_retries` es 3. Si la entrada no existe, añádala. Guarde el archivo:

   ```
   net.ipv4.tcp_syn_retries = 3
   ```

4. Ejecute el comando para que los cambios surtan efecto:

   ```
   /sbin/sysctl -p
   ```

   ```
   /sbin/sysctl -w net.ipv4.route.flush=1
   ```

5. Defina el valor de tiempo límite del servidor de Sentinel añadiendo el parámetro `-Desecurity.remote.timeout=60` a `control_center.sh` y `solution_designer.sh` en <*directorio_instalación*>/bin:

   control_center.sh:

   ```
   "<install_directory>/jre/bin/java" $MEMORY -
   Dcom.esecurity.configurationfile=$ESEC_CONF_FILE -
   Desecurity.cache.directory="<install_directory>/data/
   control_center.cache" -Desecurity.communication.service="sentinel_client"
   -Dfile.encoding=UTF8 -Desecurity.dataobjects.config.file="/xml/
   BaseMetaData.xml,/xml/WorkflowMetaData.xml,/xml/ActMetaData.xml" -
   Djava.util.logging.config.file="<install_directory>/config/
   control_center_log.prop" -
   Djava.security.auth.login.config="<install_directory>/config/auth.login"
   $SENTINEL_LANG_PROP $SENTINEL_CTRY_PROP -
   Dice.pilots.html4.baseFontFamily="Arial Unicode MS" -
   Desecurity.remote.timeout=60 -jar ../lib/console.jar
   ```

   solution_designer.sh:

   ```
   "<install_directory>/jre/bin/java" -classpath $LOCAL_CLASSPATH $MEMORY -
   Dcom.esecurity.configurationfile="$ESEC_CONF_FILE" -
   Dsentinel.installer.jar.location="<install_directory>/lib/
   contentinstaller.jar" -Desecurity.communication.service="sentinel_client"
   -Dfile.encoding=UTF8 -Desecurity.dataobjects.config.file="/xml/
   BaseMetaData.xml,/xml/WorkflowMetaData.xml,/xml/ActMetaData.xml" -
   Djava.util.logging.config.file="<install_directory>/config/
   solution_designer_log.prop" -
   Djava.security.auth.login.config="<install_directory>/config/auth.login"
   $SENTINEL_LANG_PROP $SENTINEL_CTRY_PROP -Desecurity.cache.directory=../
   data/solution_designer.cache -Desecurity.remote.timeout=60
   com.esecurity.content.exportUI.ContentPackBuilder
   ```

3.7.5 Configuración de la autenticación LDAP para varios dominios de Active Directory

Si los usuarios de LDAP que se van a autenticar se encuentran en varios dominios de Active Directory, es posible configurar el servidor de Sentinel Rapid Deployment para la autenticación LDAP de la siguiente forma:

1. Asegúrese de haber realizado del Paso 2 en la página 46 al Paso 10 en la página 47 para configurar el servidor de Sentinel para la autenticación LDAP con el controlador de dominios de Active Directory del primer dominio. Asegúrese también de haber especificado `n` para "Búsquedas anónimas en el directorio LDAP:" en la página 46.
2. Entre en el servidor de Sentinel como el usuario `novell`.
3. Detenga el servicio de Sentinel.

   ```
   /etc/init.d/sentinel stop
   ```
4. Cambie al directorio `<directorio_instalación>/config`.

   ```
   cd <install_directory>/config
   ```
5. Abra el archivo `auth.login` para editarlo.

   ```
   vi auth.login
   ```
6. Edite la sección `LdapLogin` e indique varias URL de LDAP separadas por un espacio en blanco.

   Por ejemplo:

   ```
   LdapLogin {
           com.sun.security.auth.module.LdapLoginModule required
           userProvider="ldap://<IP of the domain 1 domain controller>:636
   ldap://<IP of the domain 2 domain controller>:636"
           authIdentity="{USERNAME}"
           useSSL=true;
   };
   ```

   Para obtener más información sobre cómo especificar varias URL de LDAP, consulte la descripción de la opción `userProvider` en Class LdapLogin Module (http://java.sun.com/javase/6/docs/jre/api/security/jaas/spec/com/sun/security/auth/module/LdapLoginModule.html) (Módulo LdapLogin de clase).
7. Guarde los cambios.
8. Exporte el certificado del controlador de dominios de cada dominio y copie los archivos de certificado en el directorio `<directorio_de_instalación>/config` del servidor de Sentinel.

   Para obtener más información, consulte "Exportación del certificado de CA del servidor LDAP" en la página 45.
9. Asegúrese de definir la propiedad y los permisos necesarios de los archivos de certificado.

   ```
   chown novell:novell <install_directory>/config/<cert-file>
   ```

   ```
   chmod 700 <install_directory>/config/<cert-file>
   ```
10. Añada cada certificado al almacén de claves `ldap_server.keystore` creado en el Paso 8 de la sección "Configuración del servidor de Sentinel para la autenticación LDAP" en la página 46.

```
<install_directory>/jre64/bin/keytool -importcert -noprompt -trustcacerts
-file <certificate-file> -alias <alias_name> -keystore
ldap_server.keystore -storepass sentinel
```

Sustituya *<certificate-file>* por el nombre del archivo de certificado LDAP en formato con código base64 y *<alias_name>* por el nombre del alias del certificado que se va a importar.

Importante: asegúrese de especificar el alias. Si no se especifica ningún alias, la herramienta de claves toma `mykey` como alias por defecto. Si importa varios certificados en el almacén de claves sin especificar ningún alias, la herramienta de claves muestra un error que indica que el alias ya existe.

---

11 Inicie el servicio de Sentinel.

```
/etc/init.d/sentinel start
```

3.7.6 Entrada mediante las credenciales de usuario LDAP

Después de configurar correctamente el servidor de Sentinel para la autenticación LDAP, puede crear cuentas de usuario LDAP de Sentinel en el Centro de control de Sentinel. Para obtener más información sobre la creación de cuentas de usuario LDAP, consulte "Creating an LDAP User Account for Sentinel" (Creación de una cuenta de usuario LDAP para Sentinel) en la *Sentinel Rapid Deployment User Guide* (Guía del usuario de Sentinel Rapid Deployment).

Después de crear la cuenta de usuario LDAP, puede entrar a la interfaz Web de Sentinel Rapid Deployment, al Centro de control de Sentinel y a Solution Designer de Sentinel con el nombre de usuario y la contraseña LDAP.

Nota: para modificar una configuración de LDAP existente, vuelva a ejecutar el guion `ldap_auth_config` y especifique los valores nuevos de los parámetros.

3.8 Actualización de la clave de licencia desde una clave de evaluación a una clave de producción

En caso de que haya adquirido el producto después de la evaluación, siga el procedimiento siguiente para actualizar la clave de licencia con el fin de evitar que se vuelva a instalar:

1. Entre al equipo donde se ha instalado Sentinel Rapid Deployment como usuario administrador del sistema operativo de Sentinel (el usuario por defecto es `novell`).
2. En el indicador de comandos, cambie el directorio a *<directorio_instalación>*`/bin`.
3. Introduzca el siguiente comando:

   ```
   ./softwarekey.sh
   ```
4. Especifique 1 para definir la clave primaria. Pulse Intro.
5. Introduzca la clave de licencia válida nueva y siga las instrucciones en pantalla para salir después de actualizar la clave.

Actualización de Sentinel Rapid Deployment

4

Esta sección ofrece información sobre cómo actualizar una versión existente de Sentinel Rapid Deployment con el parche más reciente.

Nota: este parche sólo es aplicable a las instalaciones de 64 bits de Sentinel Rapid Deployment. Si se aplica el parche a un sistema de demostración de 32 bits, la instalación no funcionará.

4.1 Requisitos previos

- Asegúrese de que el sistema que actualiza ya tiene instalado Sentinel 6.1 Rapid Deployment SP1.
- Asegúrese de que los trabajos del gestor de datos de Sentinel están habilitados para que la partición Conexión actual no alcance nunca el valor de P_MAX. Si alcanza el valor de P_MAX y añade particiones manualmente, el Centro de control de Sentinel no se lanzará correctamente.

4.2 Instalación del parche en el servidor

1. Entre al servidor donde desea instalar el parche como usuario `novell`.

   Antes de instalar el parche, asegúrese de realizar una copia de seguridad de la base de datos de Sentinel, la carpeta Config y la carpeta Data con los siguientes comandos:

   Base de datos de Sentinel:

   ```
   tar -cf backup.tar <install_directory>/3rdparty/postgresql/database_files
   tar -cf backupdata.tar <install_directory>/3rdparty/postgresql/data
   ```

   Carpeta Config:

   ```
   tar -cf backupconfig.tar <install_directory>/config
   ```

   Carpeta Data:

   ```
   tar -cf backupdata.tar <install_directory>/data
   ```

   Para obtener más información sobre estos comandos, consulte File system level back up (http://www.postgresql.org/docs/8.1/static/backup-file.html) (Copia de seguridad del nivel del sistema de archivos) en el sitio Web de PostgreSQL.

2. Realice una copia de seguridad de la configuración del gestor de orígenes de eventos (ESM) y cree un archivo de exportación de ESM.

   Para obtener más información, consulte “Exporting a Configuration” (Exportación de configuraciones) en la *Sentinel Rapid Deployment User Guide* (Guía del usuario de Sentinel Rapid Deployment).

3 Descargue el instalador de parches para Sentinel Rapid Deployment del buscador de parches de Novell (http://download.novell.com/patch/finder/).

4 Copie el paquete del instalador descargado en un directorio temporal.

5 Detenga los servicios de Sentinel:

```
sentinel.sh stop
```

6 Especifique el comando siguiente para extraer los archivos del paquete del instalador:

```
unzip <install_filename>
```

Sustituya <*install_filename*> con el nombre del archivo de instalación.

7 Acceda al directorio en el que ha extraído los archivos del instalador:

```
cd <directory_name>
```

Sustituya <*directory_name*> por el nombre del directorio en el que se han extraído los archivos.

8 Especifique el comando siguiente para aplicar el parche al servidor y siga las instrucciones en pantalla:

```
./service_pack.sh
```

Después de la instalación, los servicios de Sentinel se inician de forma automática.

9 Aplique el parche en todos los equipos en los que se ejecute el gestor de recopiladores o las aplicaciones del cliente.

4.3 Actualización del gestor de recopiladores y de las aplicaciones del cliente

4.3.1 Actualización del gestor de recopiladores

Linux

1 Entre al equipo del gestor de recopiladores de Sentinel Rapid Deployment como usuario `root`.

2 Descargue el instalador de parches para Sentinel Rapid Deployment del buscador de parches de Novell (http://download.novell.com/patch/finder/).

3 Copie el archivo del instalador descargado en un directorio temporal.

4 Especifique el comando siguiente para extraer los archivos del paquete zip del instalador:

```
unzip <install_filename>
```

Reemplace <*install_filename*> por el nombre real del archivo de instalación.

5 Acceda al directorio en el que ha extraído los archivos del instalador:

```
cd <directory_name>
```

Sustituya <*directory_name*> por el nombre del directorio en el que se han extraído los archivos del instalador.

6 Detenga los servicios del gestor de recopiladores.

```
<install_directory>/bin/sentinel.sh stop
```

7 Ejecute el instalador del paquete de servicios y siga las instrucciones en pantalla:

```
./service_pack.sh
```

Después de la instalación, los servicios del gestor de recopiladores se inician de forma automática.

Windows

1 Entre al equipo del gestor de recopiladores de Sentinel Rapid Deployment como usuario admin.

2 Descargue el instalador de parches para Sentinel Rapid Deployment del buscador de parches de Novell (http://download.novell.com/patch/finder/).

3 Copie el archivo del instalador en un directorio temporal.

4 Extraiga los archivos del paquete del instalador.

5 Detenga los servicios del gestor de recopiladores.

```
<install_directory>\bin\sentinel.bat stop
```

6 Acceda al directorio en el que ha extraído los archivos del instalador.

7 Lleve a cabo una de estas acciones para ejecutar el instalador:

- Haga doble clic en el archivo `service_pack.bat` y siga las instrucciones en pantalla.
- En el indicador de comandos, ejecute el archivo `service_pack.bat` y siga las instrucciones en pantalla.

Después de la instalación, los servicios del gestor de recopiladores se inician de forma automática.

4.3.2 Actualización de las aplicaciones cliente

- “Linux” en la página 55
- “Windows” en la página 56

Linux

1 Entre como usuario `root` en el equipo en el que se ejecutan las aplicaciones del cliente de Novell Sentinel Rapid Deployment.

2 Descargue el instalador de parches para Sentinel Rapid Deployment del buscador de parches de Novell (http://download.novell.com/patch/finder/).

3 Copie el paquete del instalador descargado en un directorio temporal.

4 Especifique el comando siguiente para extraer los archivos del paquete del instalador:

```
unzip <install_filename>
```

Reemplace <*install_filename*> por el nombre real del archivo de instalación.

5 Acceda al directorio en el que ha extraído los archivos del instalador:

```
cd <directory_name>
```

Sustituya <*directory_name*> por el nombre del directorio en el que se han extraído los archivos.

6 Ejecute el instalador y siga las instrucciones en pantalla:

```
./service_pack.sh
```

Windows

1 Entre como administrador en el equipo en el que se ejecutan las aplicaciones del cliente de Novell Sentinel Rapid Deployment.

2 Descargue el instalador de parches para Sentinel Rapid Deployment del buscador de parches de Novell (http://download.novell.com/patch/finder/).

3 Copie el archivo del instalador descargado en un directorio temporal.

4 Extraiga los archivos del paquete del instalador.

5 Acceda al directorio en el que ha extraído los archivos del instalador.

6 Lleve a cabo una de estas acciones para ejecutar el instalador:

- Haga doble clic en el archivo `service_pack.bat` y siga las instrucciones en pantalla.
- En el indicador de comandos, ejecute el archivo `service_pack.bat` y siga las instrucciones en pantalla.

Consideraciones de seguridad para Sentinel Rapid Deployment

5

Esta sección proporciona instrucciones específicas sobre cómo instalar, configurar y mantener con seguridad Novell Sentinel Rapid Deployment.

5.1 Protección

5.1.1 Protección predefinida

- Todos los puertos no necesarios están desactivados.
- Siempre que es posible, un puerto de servicio sólo escucha las conexiones locales y no permite las conexiones remotas.
- Los archivos se instalan con el mínimo de privilegios para que sólo unos pocos usuarios puedan leerlos.
- No se permiten las contraseñas por defecto.
- Los informes de la base de datos sólo se producen para usuarios que tienen permisos de selección en la base de datos.
- Todas las interfaces Web requieren HTTPS.
- Se ejecuta una exploración de vulnerabilidades en la aplicación y se solucionan todos los problemas potenciales de seguridad.
- Todas las comunicaciones en red usan SSL por defecto y están configuradas para que requieran autenticación.
- Las contraseñas de las cuentas de usuario están cifradas por defecto al almacenarse en el sistema de archivos o en la base de datos.

5.1.2 Protección de los datos de Sentinel Rapid Deployment

a causa de la naturaleza sumamente confidencial de los datos de Sentinel Rapid Deployment, debe proteger físicamente el equipo y mantenerlo en un área segura de la red. Para recopilar datos de orígenes de eventos que no están en la red segura, utilice un gestor de recopiladores remoto. Para obtener más información acerca de los gestores de recopiladores, consulte la "Sección 3.3, "Instalación del gestor de recopiladores y de las aplicaciones del cliente", en la página 34".

5.2 Protección de la comunicación a través de la red

La comunicación entre los distintos componentes de Sentinel Rapid Deployment se realiza a través de la red y se utilizan diferentes clases de protocolos de comunicación en todo el sistema.

5.2.1 Comunicación entre los procesos del servidor de Sentinel

Los procesos del servidor de Sentinel incluyen DAS Core, DAS Binary, el motor de correlación, el gestor de recopiladores y el servidor Web. Se comunican entre sí utilizando ActiveMQ.

Por defecto, la comunicación entre los procesos del servidor es sobre SSL, a través del bus de mensajes de ActiveMQ. Para configurar SSL, especifique la siguiente información en `<directorio_instalación>/configuration.xml`:

```
<jms brokerURL="failover://(ssl://
localhost:61616?wireFormat.maxInactivityDuration=30000)?randomize=false"
interceptors="compression" keystore="../config/.activemqclientkeystore.jks"
keystorePassword="password" password="374d9f338b4dc4b50e45b3822fc6be12"
username="system"/>
```

Para obtener más información sobre la configuración del servidor personalizado y los certificados del cliente, consulte "Processes" (Procesos) en la *Sentinel Rapid Deployment User Guide* (Guía del usuario de Sentinel Rapid Deployment).

5.2.2 Comunicación entre el servidor de Sentinel y las aplicaciones cliente de Sentinel

Las aplicaciones cliente de Sentinel como el Centro de control de Sentinel, el gestor de datos de Sentinel y Solution Designer utilizan por defecto la comunicación SSL a través del servidor proxy SSL.

Para habilitar la comunicación entre el servidor de Sentinel y el Centro de control de Sentinel, el gestor de datos de Sentinel y Solution Designer, cuando se ejecutan todos como aplicaciones cliente en el servidor, especifique la siguiente información en <directorio_de_instalación>/configuration.xml:

```
<strategy active="yes" id="proxied_client"
location="com.esecurity.common.communication.strategy.proxystrategy.ProxiedCl
ientStrategyFactory">
   <transport type="ssl">
    <ssl host="localhost" keystore="<install_directory>/config/
.proxyClientKeystore" port="10013" usecacerts="false"/>
   </transport>
  </strategy>
```

Para habilitar la comunicación entre el servidor de Sentinel y el Centro de control de Sentinel, el gestor de datos de Sentinel y Solution Designer si se ejecutan a través de WebStart, la estrategia de comunicación se define en el servidor en el archivo <*directorio_de_instalación*>/3rdparty/tomcat/webapps/ROOT/novellsiemdownloads/configuration.xml de la manera siguiente:

```
<strategy active="yes" id="proxied_client"
location="com.esecurity.common.communication.strategy.proxystrategy.ProxiedCl
ientStrategyFactory" >
   <transport type="ssl">
    <ssl host="127.0.0.1" port="10013" keystore="./.novell/sentinel/
.proxyClientKeystore" />
   </transport>
  </strategy>
```

Para obtener más información sobre la configuración del servidor personalizado y los certificados del cliente, consulte "Processes" (Procesos) en la *Sentinel Rapid Deployment User Guide* (Guía del usuario de Sentinel Rapid Deployment).

5.2.3 Comunicación entre el servidor y la base de datos

El protocolo usado para la comunicación entre el servidor y la base de datos se define mediante el controlador de JDBC. Algunos controladores son capaces de cifrar la comunicación con la base de datos.

Sentinel Rapid Deployment utiliza el controlador de PostgreSQL (postgresql-<versión>.jdbc3.jar) proporcionado en la página de descargas de PostgreSQL (http://jdbc.postgresql.org/download.html), para conectarse a la base de datos PostgreSQL, que es una implementación Java (Tipo IV). Este controlador admite el cifrado para la comunicación de datos. Para configurar el cifrado de la comunicación de datos, consulte las opciones del cifrado de PostgreSQL (http://www.postgresql.org/docs/8.1/static/encryption-options.html).

Nota: al activar el cifrado, el rendimiento del sistema se ve afectado. Por lo tanto, la comunicación con la base de datos no está cifrada por defecto. Sin embargo, no se trata de un problema de seguridad, ya que la comunicación entre la base de datos y el servidor se produce en una interfaz de red de retrobucle y no queda expuesta en una red abierta.

5.2.4 Comunicación entre los gestores de recopiladores y los orígenes de eventos

Es posible configurar Sentinel Rapid Deployment para recopilar de forma segura datos de varios orígenes de eventos. Sin embargo, la recopilación segura de datos viene determinada por los protocolos concretos admitidos por el origen de eventos. Por ejemplo, Check Point LEA, Syslog y los conectores de auditoría se pueden configurar para cifrar su comunicación con los orígenes de eventos.

Para obtener más información sobre las características de seguridad que es posible habilitar, consulte la documentación del proveedor del conector y el origen de eventos disponible en el sitio Web de módulos auxiliares (plug-ins) de Novell Sentinel (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

5.2.5 Comunicaciones con navegadores Web

El servidor Web está configurado por defecto para comunicarse a través de HTTPS. Para obtener más información, consulte la documentación de Tomcat (http://tomcat.apache.org/tomcat-4.0-doc/ssl-howto.html).

5.2.6 Comunicación entre la base de datos y otros clientes

Puede configurar la base de datos SIEM de PostgreSQL para permitir la conexión desde cualquier equipo cliente usando el gestor de datos de Sentinel o bien una aplicación de otro fabricante, como Pgadmin.

Para permitir que el gestor de datos de Sentinel se conecte desde cualquier equipo cliente, añada la línea siguiente en el archivo `<directorio_de_instalación>/3rdparty/postgresql/data/pg_hba.conf`:

```
host    all         all         0.0.0.0/0             md5
```

Si desea limitar las conexiones del cliente que pueden ejecutarse y conectarse a la base de datos a través del gestor de datos de Sentinel, sustituya la línea anterior por la dirección IP del host. La línea siguiente de `pg_hba.conf` es un indicador para que PostgreSQL acepte conexiones desde el equipo local para que el gestor de datos de Sentinel se pueda ejecutar sólo en el servidor.

```
host all all 127.0.0.1/32 md5
```

Para limitar las conexiones desde otros equipos cliente, debe añadir entradas de `host` adicionales.

5.3 Protección de usuarios y contraseñas

5.3.1 Usuarios de sistemas operativos

Instalación del servidor

La instalación del servidor de Sentinel Rapid Deployment crea un usuario de sistema y un grupo que son propietarios de los archivos instalados dentro del `<directorio_de_instalación>`. Si el usuario no existe, se crea y su directorio personal se define en `<directorio_de_instalación>`. Si se crea un usuario nuevo, la contraseña del usuario no se define por defecto, para maximizar la seguridad. Si desea entrar al sistema como un usuario creado durante la instalación, debe definir una contraseña para el usuario después de la instalación.

Instalación del gestor de recopiladores

Los usuarios del sistema pueden tener distintos niveles de seguridad, según el sistema operativo en el que esté instalado el gestor de recopiladores.

Linux: el instalador le solicita que especifique el nombre del usuario del sistema propietario de los archivos instalados, así como la ubicación para crear su directorio personal. Por defecto, el usuario del sistema es `esecadm`; sin embargo, puede cambiar ese nombre de usuario. Si el usuario no existe, se crea con su directorio personal. Si se crea un usuario nuevo, la contraseña del usuario no se define durante la instalación para maximizar la seguridad. Si desea entrar al sistema como ese usuario, debe definir una contraseña para el usuario después de la instalación. El grupo por defecto es `esec`

Durante la instalación del cliente, si el usuario ya existe, el instalador no vuelve a solicitar el usuario. Este comportamiento es similar al que ocurre durante la instalación o desinstalación del software. Sin embargo, puede hacer que el instalador vuelva a solicitar el usuario:

1. Suprima el usuario y el grupo creados durante la primera instalación.
2. Borre las variables de entorno ESEC_USER de `/etc/profile`.

Windows: no se ha creado ningún usuario.

Las directivas de contraseñas para los usuarios del sistema están definidas por el sistema operativo que se está utilizando.

5.3.2 Usuarios de la aplicación y de la base de datos de Sentinel

Todos los usuarios de la aplicación de Sentinel Rapid Deployment son usuarios de la base de datos original y sus contraseñas están protegidas utilizando los procedimientos seguidos por la plataforma de bases de datos originales. Estos usuarios sólo tienen acceso de lectura a ciertas tablas de la base de datos, de tal forma que pueden ejecutar consultas en la base de datos.

El instalador crea y configura una base de datos PostgreSQL con los usuarios siguientes:

- **admin:** el usuario admin es el administrador de entrada en todas la aplicaciones de Sentinel.
- **dbauser:** el usuario dbauser se crea como superusuario que puede gestionar la base de datos. La contraseña del usuario dbauser se define durante la instalación del servidor de Sentinel Rapid Deployment. Esta contraseña se almacena en el `<directorio personal del usuario>/.pgpass`. El sistema sigue las directivas de contraseña de la base de datos PostgreSQL. Para obtener más información, consulte la Sección 5.3.3, “Aplicación de una directiva de contraseñas para usuarios”, en la página 62.

- **appuser:** se trata de un usuario sin derechos de superusuario que las aplicaciones de Sentinel utilizan para conectar con la base de datos. Por defecto, el usuario appuser emplea una contraseña generada aleatoriamente durante la instalación y que se guarda cifrada en los archivos XML (`das_core.xml`, `das_binary.xml` y `advisor_client.xml`) en <*directorio_de_instalación*>/config. Para cambiar la contraseña del appuser, emplee la utilidad `<directorio_instalación>/bin/dbconfig`. Para obtener más información, consulte "DAS Container Files" (Archivos del contenedor DAS) en la *Sentinel Rapid Deployment User Guide* (Guía del usuario de Sentinel Rapid Deployment).

Nota: también hay un usuario de la base de datos PostgreSQL que posee toda la base de datos, incluyendo las tablas de base de datos del sistema. Por defecto, el usuario de la base de datos PostgreSQL está definido en NOLOGIN para que nadie pueda entrar en el sistema como usuario PostgreSQL.

5.3.3 Aplicación de una directiva de contraseñas para usuarios

Sentinel Rapid Deployment utiliza mecanismos basados en estándares para facilitar la aplicación de directivas de contraseña.

El instalador crea y configura una base de datos PostgreSQL con los usuarios siguientes:

dbauser: el propietario de la base de datos (usuario administrador de la base de datos). La contraseña se establece durante el proceso de instalación.

appuser: se trata del usuario de la aplicación que suele entrar en la base de datos desde Sentinel Rapid Deployment. La contraseña se genera de forma aleatoria durante el proceso de instalación y está diseñada para un uso exclusivo interno.

admin: se pueden usar las credenciales del administrador para entrar en la interfaz Web de Sentinel Rapid Deployment. La contraseña se establece durante el proceso de instalación.

Las contraseñas de los usuarios se guardan por defecto en la base de datos PostgreSQL, que está incrustada en Sentinel Rapid Deployment. PostgreSQL ofrece la opción de utilizar varios mecanismos de autenticación basados en estándares, como se describe en la sección Client Authentication (http://www.postgresql.org/docs/8.3/static/client-authentication.html) (Autenticación de clientes) de la documentación de PostgreSQL.

El uso de estos mecanismos afecta a todas las cuentas de usuario de Sentinel Rapid Deployment, incluidos los usuarios de la aplicación Web y las cuentas usadas sólo por los servicios de sistema secundario, como `dbauser` y `appuser`.

Una opción más sencilla es utilizar un directorio LDAP para autenticar a los usuarios de la aplicación Web. Para habilitar esta opción en el servidor de Sentinel Rapid Deployment, consulte la Sección 3.7, "Autenticación LDAP", en la página 44. Esta opción no tiene efecto en las cuentas usadas por los servicios de sistema secundario, que se siguen autenticando mediante PostgreSQL, a no ser que se cambie la configuración de PostgreSQL.

Se puede conseguir la aplicación de una directiva de contraseña robusta en Sentinel Rapid Deployment mediante el uso de estos mecanismos basados en estándares y de los mecanismos existentes en el entorno, como el directorio LDAP.

5.4 Protección de los datos de Sentinel

Importante: A causa de la naturaleza sumamente confidencial de los datos del servidor de Sentinel, debería proteger físicamente el equipo y mantenerlo en un área segura de la red. Para recopilar datos de orígenes de eventos que no están en la red segura, utilice un gestor de recopiladores remoto.

Para ciertos componentes, las contraseñas deben almacenarse para que estén disponibles cuando el sistema necesite conectarse a un recurso como la base de datos o a un origen de eventos. En este caso, cuando se almacena la contraseña, se cifra primero para evitar el acceso no autorizado a la contraseña de texto no cifrada.

Aunque la contraseña esté cifrada, debe procurar que el acceso a los datos almacenados de la contraseña están protegidos para evitar que ésta sea revelada. Por ejemplo, puede garantizar que otros usuarios no autorizados no pueden leer los permisos en los archivos con datos confidenciales.

ARCHIVOS

`advisor_client.xml`

Credenciales de la base de datos

Las credenciales de la base de datos se almacenan en el archivo `<directorio_de_instalación>/config/server.xml`.

```
<class>esecurity.base.ccs.comp.dataobject.ConnectionManager</class>
    <property name="username">appuser</property>
    <property name="password">7fA+ogBMeK7cRbJ+S6xJ/
InLBUi+sRVGK5qYycDxfIqGDHVX9FApWg==</property>
```

Credenciales del Asesor

```
<obj-component id="DownloadComponent">
          <class>esecurity.ccs.comp.advisor.feed.NewAdvClientDownload</class>
      <property name="advisor.downloadfrom.url">https://secure-www.novell.com/
sentinel/advisor/advisordata</property>
      <property name="username">admin</property>
      <!-- Set the password (encrypted) using the adv_change_password script -
->
      <property name="password">jqhlWIX8HD6GDHVX9FApWg==</property>
<property name="compression.enabled">true</property>
      <!--
        Set the following properties to connect through an HTTP proxy.
       Set the proxy password (encrypted) using the adv_change_password script
(make a
        copy of the script and add "-x" to the java cmd line to set the proxy
password
        instead of the advisor password.
      -->
      <!--
      <property name="proxy_host"></property>
      <property name="proxy_port"></property>
      <property name="proxy_username"></property>
      <property name="proxy_password"></property>
      -->
        </obj-component>
```

Configuration.xml

```
<strategy active="yes" id="jms"
location="com.esecurity.common.communication.strategy.jmsstrategy.activemq.Ac
tiveMQStrategyFactory" name="ActiveMQ">
<jms brokerURL="failover://(ssl://
localhost:61616?wireFormat.maxInactivityDuration=30000)?randomize=false"
interceptors="compression" keystore="../config/.activemqclientkeystore.jks"
keystorePassword="password" password="374d9f338b4dc4b50e45b3822fc6be12"
username="system"/>
    </strategy>
```

das_binary.xml

```
<class>esecurity.base.ccs.comp.dataobject.ConnectionManager</class>
    <property name="username">appuser</property>
    <property name="password">7fA+ogBMeK7cRbJ+S6xJ/
InLBUi+sRVGK5qYycDxfIqGDHVX9FApWg==</property>
```

das_core.xml

```
 <class>esecurity.base.ccs.comp.dataobject.ConnectionManager</class>
    <property name="username">appuser</property>
    <property name="password">7fA+ogBMeK7cRbJ+S6xJ/
InLBUi+sRVGK5qYycDxfIqGDHVX9FApWg==</property>
```

Algunas tablas de la base de datos almacenan contraseñas y certificados. Estos datos confidenciales están cifrados y se almacenan en las tablas indicadas más abajo. Debe limitar el acceso a estas tablas.

- **evt_src:** datos de la columna evt_src_config
- **evt_src_collector:** columnas: evt_src_collector_props
- **evt_src_grp (doubt):** columnas: evt_src_default_config
- **md_config:** columna: data
- **integrator_config:** columna: integrator_properties
- **md_view_config:** columna: view_data
- **esec_content:** columna: content_context, content_hash
- **esec_content_grp_content:** columnas: content_hash
- **sentinel_plugin:** columnas: content_pkg, file_hash

Sentinel Rapid Deployment almacena tanto datos de configuración como de eventos. Estos datos se almacenan en las siguientes ubicaciones:

Componentes	Ubicación de los datos de configuración	Ubicación de los datos de eventos
Servidor de Sentinel Rapid Deployment	Tablas de la base de datos y sistema de archivos (*<directorio_instalación>*/config) Esta información de configuración incluye la base de datos cifrada, el origen de eventos, integradores y contraseñas.	Base de datos (tablas EVENTS, CORRELATED_EVENTS y EVT_SMRY_, AUDIT_RECORD) y el sistema de archivos en *<directorio_instalación>*/data/eventdata y <*directorio_instalación*>/data/raw data Los datos de eventos se pueden archivar en el sistema de archivos como parte del trabajo de gestión de particiones.
Motor de correlación	Sistema de archivos (*<directorio_instalación>*/config). La única información de configuración confidencial es el par de claves del cliente utilizado para conectarse al bus de mensajes.	correlation_engine.cache
DAS Core	*<directorio_instalación>*/config	das_core.cache
DAS Binary	*<directorio_instalación>*/config	Los datos de eventos se pueden almacenar en el caché si la base de datos está inactiva. das_binary.cache
Gestor de recopiladores	Sistema de archivos (*<directorio_instalación>*/config). La única información de configuración confidencial es la contraseña del usuario del gestor de recopiladores utilizada para conectar al bus de mensajes.	Los datos de eventos se pueden almacenar en el caché en el sistema de archivos durante condiciones de error como que el bus de mensajes esté inactivo o haya una sobrecarga de eventos. Estos datos de eventos se almacenan en el directorio *<directorio_de_instalación>*/data/collector_mgr.cache.
Aplicaciones cliente	Sistema de archivos (*directorio_instalación*/config). Las aplicaciones cliente no almacenan información confidencial en sus archivos de configuración. Por ejemplo, las aplicaciones cliente pueden exportar datos de la gestión de orígenes de eventos a un sistema de archivos local. El archivo exportado contiene contraseñas cifradas, si están presentes en la configuración de los orígenes de eventos que se han exportado. Aunque las contraseñas estén cifradas, el permiso de exportación de ESM sólo debería otorgarse a aquellos usuarios que tengan un privilegio de confianza.	Ninguna

5.5 Copia de seguridad de la información

- Debe realizar copias de seguridad de los eventos con frecuencia. Los medios de copia de seguridad deben almacenarse en una instalación segura sin conexión.
- Realice una copia de seguridad de los datos del sistema. Para obtener más información, consulte "Backup and Restore Utility" (Utilidad de copia de seguridad y restauración) en la *Sentinel Rapid Deployment User Guide* (Guía del usuario de Sentinel Rapid Deployment).
- Para los datos confidenciales, utilice uno de los métodos siguientes para cifrar la copia de seguridad de los datos:
  - Cifre los mismos datos si la aplicación que crea los datos admite el cifrado. Por ejemplo, los productos de la base de datos y las herramientas de otros fabricantes admiten el cifrado de datos. Utilice un software de copia de seguridad que pueda cifrar los datos a medida que haga las copias de seguridad. Este método plantea desafíos de rendimiento y manejabilidad, sobre todo para la gestión de claves de cifrado.
  - Utilice una aplicación de cifrado que cifre los medios de copias de seguridad a medida que se hagan copias de seguridad de los datos.
- Si transporta y almacena medios sin conexión, utilice una empresa que esté especializada en el envío y almacenamiento de medios. Asegúrese de que se puede realizar el seguimiento de las cintas mediante códigos de barras, que estén almacenadas en un condiciones respetuosas con el medio ambiente y que las manipula una empresa cuya reputación reside en su capacidad de manipular correctamente los medios.
- Cargue los certificados de recuperación. Por defecto el servicio de Novel Sentinel no está configurado para el agente de recuperación. Durante la configuración del servidor a través de YaST, asegúrese de que se ha configurado la vía del agente de recuperación. Esta vía debería contener la lista de certificados que el servicio puede cargar para que elijan los usuarios.

  Para obtener más información, consulte "Certificate Management for Sentinel 6.1 Rapid Deployment Server" (Gestión de certificados para el servidor de Sentinel 6.1 Rapid Deployment) en la *Sentinel Rapid Deployment Reference Guide* (Guía de referencia de Sentinel Rapid Deployment).

  YaST contiene módulos para la gestión básica de los certificados X.509, lo que implica principalmente la creación de CA, CA secundarias y sus certificados. Para obtener más información sobre cómo gestionar y actualizar certificados, consulte la sección Managing X.509 Certification (http://www.novell.com/documentation/sles10/sles_admin/data/cha_yast_ca.html) (Gestión de certificados X.509) en la guía *SUSE Linux Enterprise Server 10 Installation and Administration Guide* (http://www.novell.com/documentation/sles10/sles_admin/data/bookinfo_book_sles_admin.html) (Guía de administración e instalación de SUSE Linux Enterprise Server 10).

5.6 Protección del sistema operativo

- Sentinel Rapid Deployment es compatible con SUSE Linux Enterprise Server (SLES) 10 SP3 o posterior. Para obtener más información sobre la protección de un equipo SLES, consulte la documentación de SUSE Linux Enterprise Server 10 (http://www.novell.com/documentation/sles10/sles_admin/data/part_security.html).
- Proteja el acceso al servidor de Sentinel Rapid Deployment con un cortafuegos. Si se puede acceder al servidor de Sentinel desde fuera de la red corporativa, debe emplearse un cortafuegos para evitar que un intruso pueda acceder directamente a él.

Habilite los puertos siguientes en el cortafuegos:

Componentes	Puerto
ActiveMQ	61616
PostgreSQL	5432
Tomcat	8443
Puerto del servidor proxy del Centro de control de Sentinel	10013
Cliente de confianza en módulo auxiliar (plug-in)	10014
internal_gateway_server e internal_gateway se usan entre el motor y el gestor	5556
internal_router_server e internal_router_client Utilizado entre el cliente del router de eventos y el servidor	5558
Puerto de escucha de eventos configurado en `config/collector_mgr.properties` como "`esecurity.agentmanager.event.port`"	35000

Nota: los puertos marcados con un asterisco pueden ser diferentes si ya se estaban utilizando durante la instalación. Si ya se estaban utilizando durante la instalación, sustituya los números de puerto que se solicitaron durante la instalación.

Para obtener más información sobre cómo habilitar un cortafuegos en SLES 10, consulte Configuring Firewalls with YaST (http://www.novell.com/documentation/sles10/sles_admin/data/sec_fire_suse.html) (Configuración de cortafuegos con YaST) en la guía *SLES 10 Administration Guide* (Guía de Administración de SLES 10).

5.7 Visualización de eventos de auditoría de Sentinel

Sentinel Rapid Deployment genera eventos de auditoría para muchas acciones realizadas por usuarios, así como para acciones realizadas de forma interna por las actividades del sistema. Estos eventos se pueden ver en vistas de Active Views o se puede acceder a ellos a través de una búsqueda o informe. Sin embargo, hay que contar con los permisos necesarios para poder ver los eventos del sistema.

Para obtener más información, consulte "System Events for Sentinel" (Eventos del sistema de Sentinel) en la *Sentinel Rapid Deployment User Guide* (Guía del usuario de Sentinel Rapid Deployment).

5.8 Uso de un certificado de CA

Puede sustituir el certificado autofirmado con un certificado firmado por una autoridad certificadora (CA) principal, como VeriSign, Thawte o Entrust. También puede sustituir el certificado autofirmado con un certificado firmado por una CA menos común, con una CA de su empresa u organización.

Para obtener más información, consulte “Certificate Management for Sentinel 6.1 Rapid Deployment Server” (Gestión de certificados para el servidor de Sentinel 6.1 Rapid Deployment) en la *Sentinel Rapid Deployment Reference Guide* (Guía de referencia de Sentinel Rapid Deployment).

Prueba de las funciones de Sentinel Rapid Deployment

6

Sentinel Rapid Deployment se instala con un recopilador genérico que se puede utilizar para probar muchas de las funciones básicas del sistema. Puede usar este recopilador para probar las Active Views, la creación de incidencias, las reglas de correlación y los informes.

6.1 Realización de pruebas en la instalación de Rapid Deployment

El siguiente procedimiento describe los pasos para probar el sistema Sentinel Rapid Deployment y los resultados esperados. Es posible que no pueda ver los mismos eventos, pero los resultados que obtenga serán parecidos a los resultados siguientes.

En el nivel básico, dichas pruebas le permiten confirmar lo siguiente:

- Los servicios de Sentinel están actualizados y en ejecución.
- La comunicación mediante el bus de mensajes es funcional.
- Se están enviando los eventos de auditoría interna.
- Los eventos se pueden enviar desde el gestor de recopiladores.
- Los eventos se insertan en la base de datos y se pueden recuperar utilizando un informe.
- Se pueden ver y crear las incidencias.
- Las reglas se evalúan y el Motor de correlación activa los eventos activados.
- El gestor de datos de Sentinel está conectado a la base de datos y puede leer información sobre particiones.

En caso de que alguna de estas pruebas falle, revise el registro de instalación y otros archivos de registro, y póngase en contacto con la Asistencia técnica de Novell (http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup) si es necesario.

Para probar la instalación:

1. Entre en la interfaz Web de Sentinel Rapid Deployment.

   Para obtener más información, consulte “Accessing the Novell Sentinel Web Interface” (Acceso a la interfaz Web de Novell Sentinel) en la *Sentinel Rapid Deployment User Guide* (Guía del usuario de Sentinel Rapid Deployment).
2. Seleccione la página de búsqueda y busque cualquier evento interno. Deben devolverse uno o más eventos.

   Por ejemplo, para buscar eventos internos con una gravedad de 3 a 5, seleccione *Incluir eventos del sistema* e introduzca *sev:[3 TO 5]* en el campo *Buscar.*

Para obtener más información sobre la búsqueda, consulte “Running an Event Search” (Ejecución de búsquedas de eventos) en la *Sentinel Rapid Deployment User Guide* (Guía del usuario de Sentinel Rapid Deployment).

La función de búsqueda no está habilitada por defecto en la versión SP2. Sin embargo, si desea habilitar la función, consulte “Enabling the Search Option in Web User Interface” (Habilitación de la opción de búsqueda en la interfaz Web del usuario) en la *Sentinel Rapid Deployment User Guide* (Guía del usuario de Sentinel Rapid Deployment).

3 Seleccione la página Informes, especifique los parámetros y ejecute un informe.

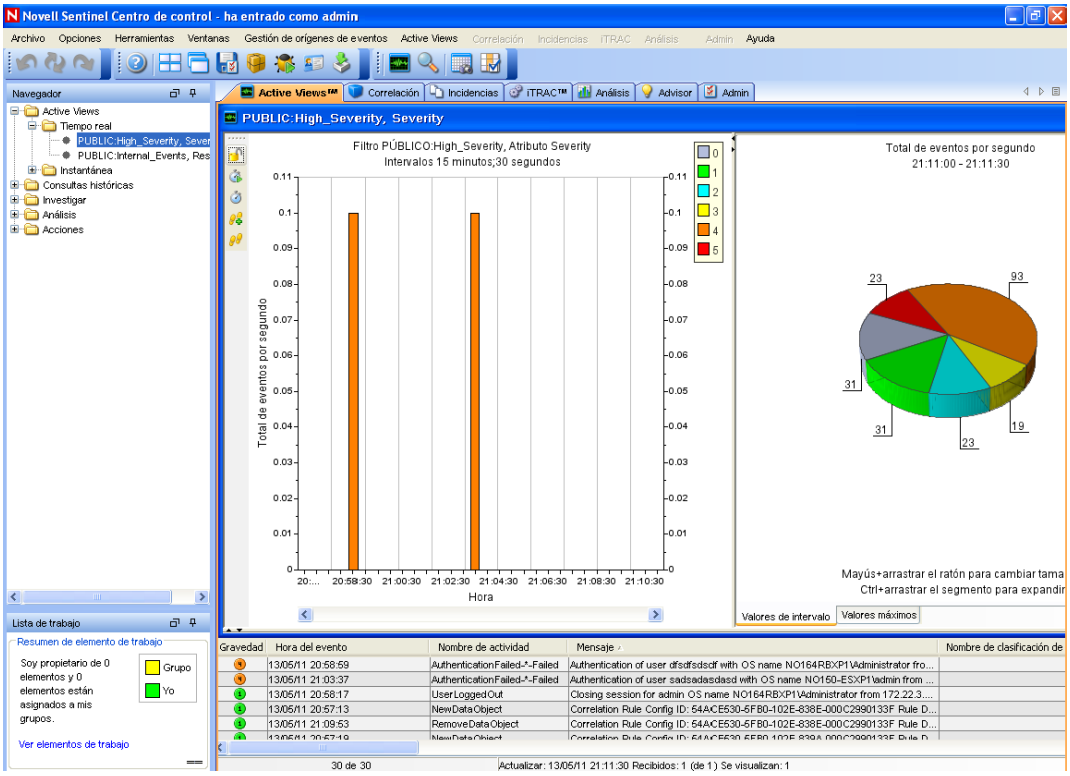
Por ejemplo, haga clic en el botón *Ejecutar* situado junto a la configuración de eventos principales de Sentinel, especifique los parámetros que desee y haga clic en *Ejecutar.*

Para obtener más información, consulte “Running Reports” (Ejecución de informes) en la *Sentinel Rapid Deployment User Guide* (Guía del usuario de Sentinel Rapid Deployment).

4 En la página Aplicaciones, haga clic en *Lanzar el Centro de control de Sentinel.*

5 Entre en el sistema utilizando el usuario administrativo de Sentinel especificado durante la instalación (admin por defecto).

Se abre el Centro de control de Sentinel y podrá ver la pestaña *Active Views* con los eventos filtrados por los filtros públicos *Eventos_internos* y *Gravedad_alta*.



6 Abra el menú *Gestión de orígenes de eventos* y seleccione la *Vista activa.*

7 En la vista gráfica, haga clic con el botón derecho en el *origen de eventos de 5 eps* y seleccione *Inicio.*

8 Cierre la ventana de la vista activa de la gestión del origen de eventos.

9 Haga clic en la pestaña *Active Views.*

Se abrirá la vista de la ventana Activo titulada PÚBLICO: Gravedad_alta, Gravedad. Es posible que el recopilador tarde en iniciarse y que los datos tarden en mostrarse en esta ventana.

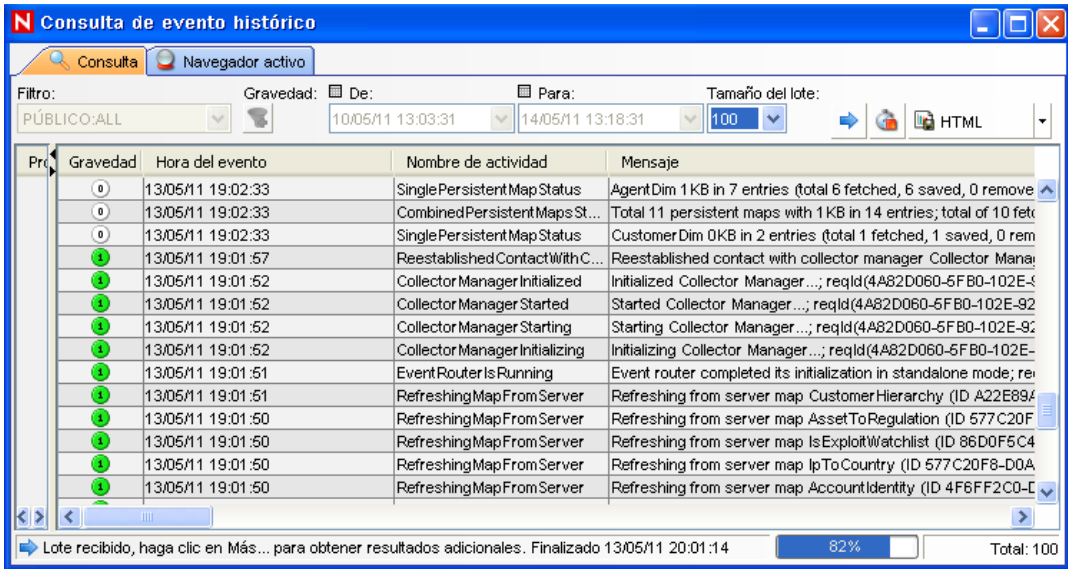
10 Haga clic en el botón *Consulta de eventos* de la barra de herramientas. Se muestra la ventana Consulta de evento histórico.

11 En la ventana Consulta de evento histórico, haga clic en la flecha hacia abajo *Filtro* para seleccionar el filtro correspondiente. Seleccione el filtro *Público: Todos.*

12 Seleccione un período de tiempo que cubra el tiempo de actividad del recopilador. Utilice las listas desplegables *Desde* y *Hasta* para seleccionar el intervalo de fechas.

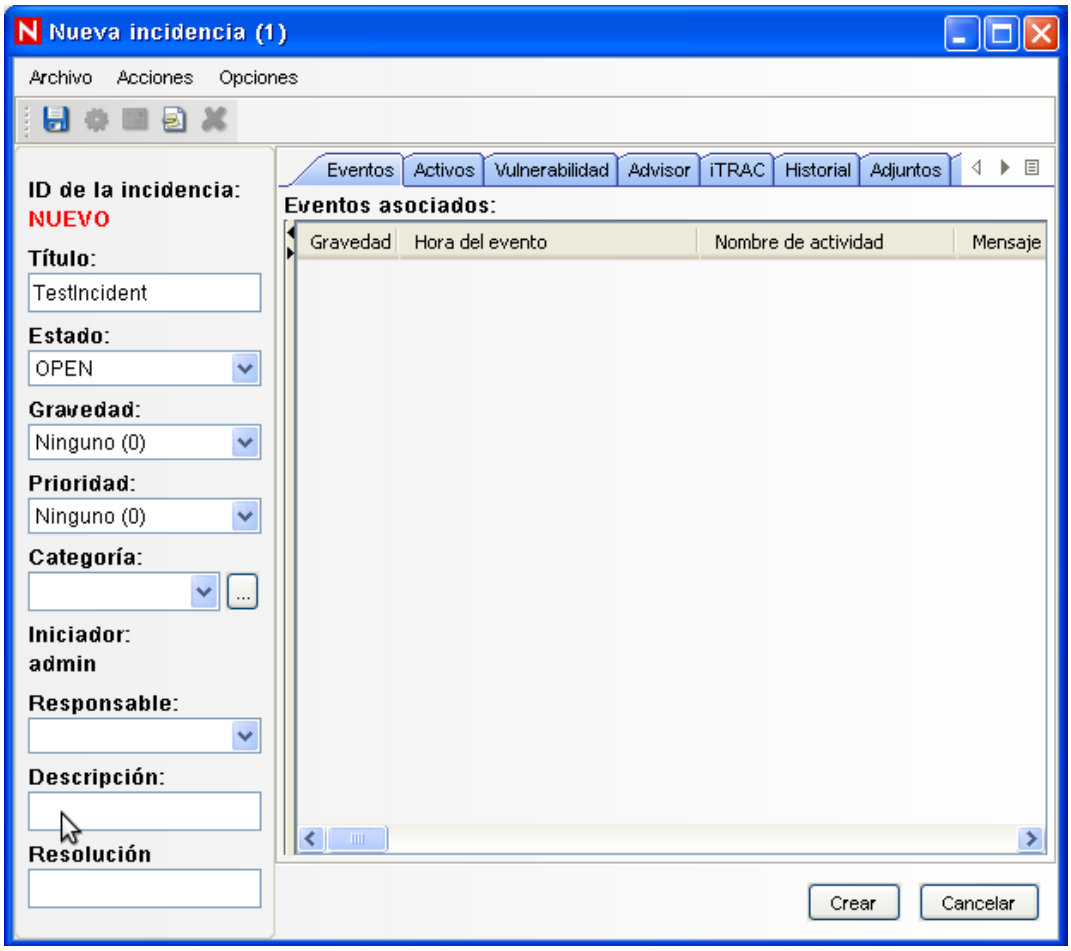
13 Seleccione el tamaño del lote.

14 Haga clic en el icono de la lupa para ejecutar la consulta.



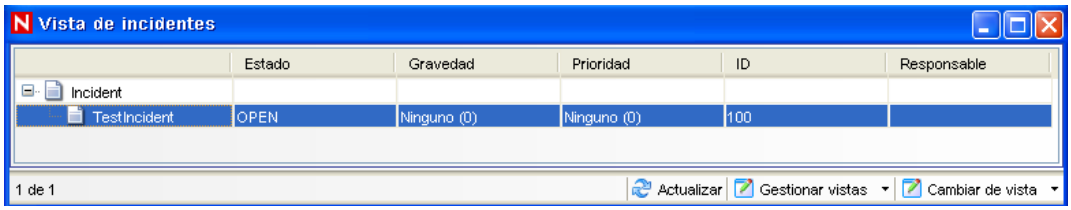
15 Mantenga pulsadas las teclas Ctrl o Mayús y seleccione varios eventos en la ventana de Consulta de evento histórico.

16 Haga clic con el botón derecho en la ventana y seleccione *Crear incidencia* para acceder a la ventana Nueva incidencia.

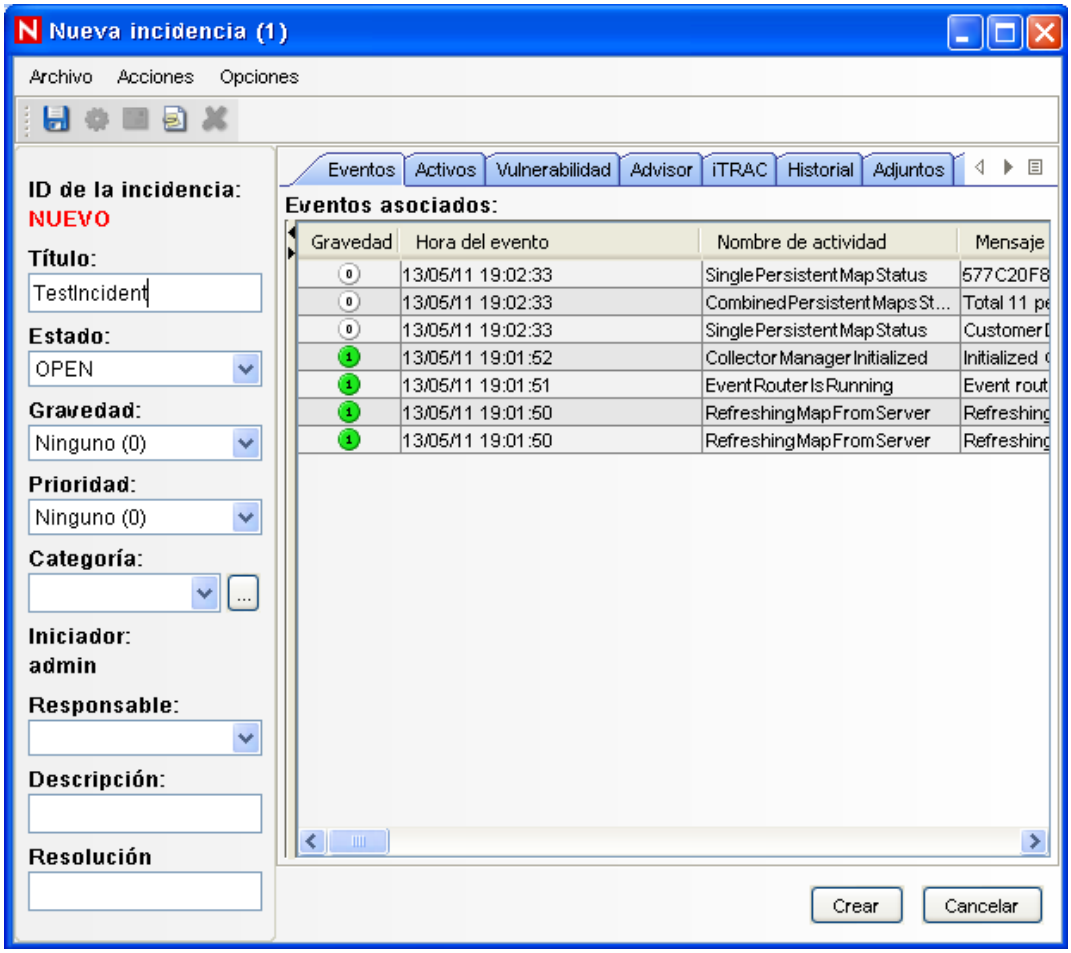


17 Asigne a la incidencia el nombre IncidenciaPrueba1 y haga clic en *Crear*. Cuando se muestre una notificación de proceso correcto, haga clic en *Guardar*.

18 Haga clic en la pestaña *Incidencia* para ver la incidencia que acaba de crear en el gestor de vistas de incidencias.



19 Haga doble clic en la incidencia para mostrar los eventos.



20 Cierre la ventana Incidencias.

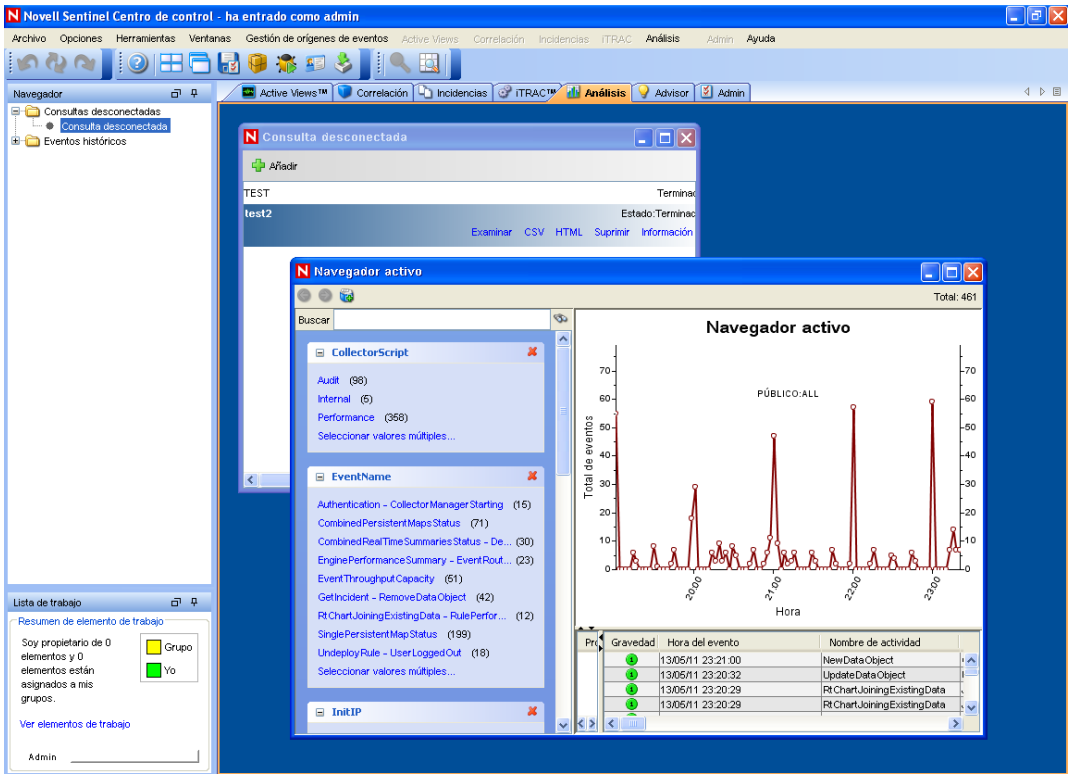
21 Haga clic en la pestaña *Análisis*.

22 Haga clic en *Consultas desconectadas* en el menú *Análisis* o en el navegador.

23 En la ventana Consulta desconectada, haga clic en *Añadir*.

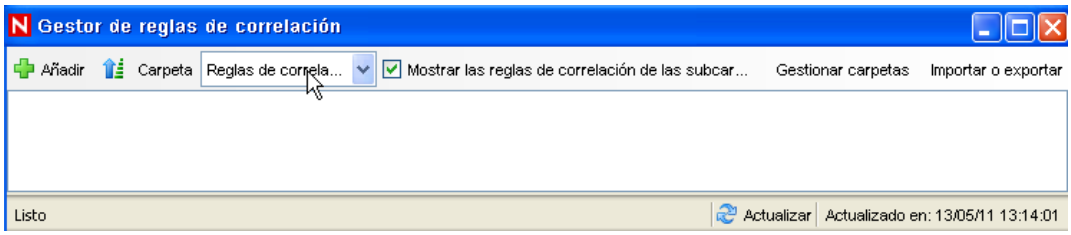
24 Especifique un nombre, seleccione un filtro y un periodo de tiempo y haga clic en *Aceptar*.

25 Haga clic en *Examinar* para ver la lista de eventos y detalles asociados en la ventana Navegador activo.

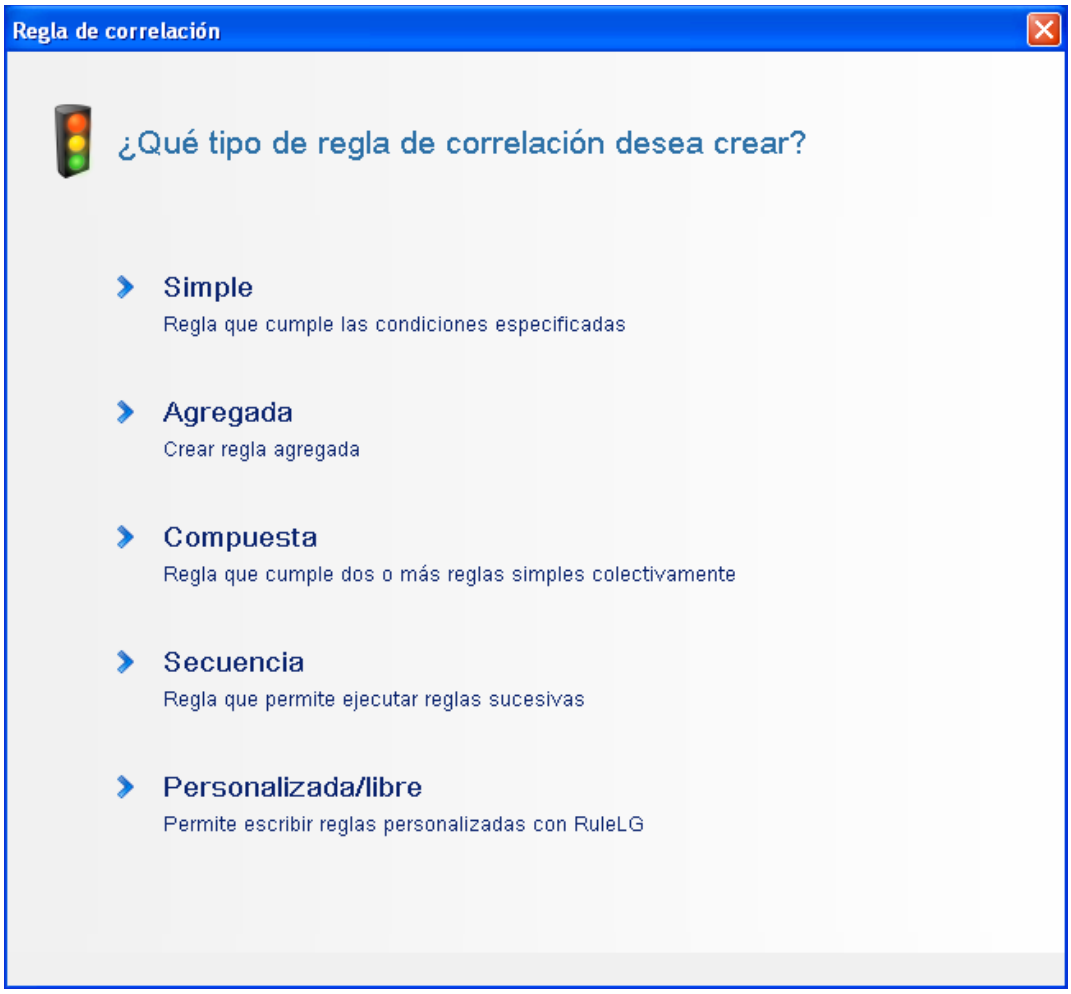


Puede ver detalles como el recopilador, la IP de destino, la gravedad, el puerto de servicio de destino y los recursos.

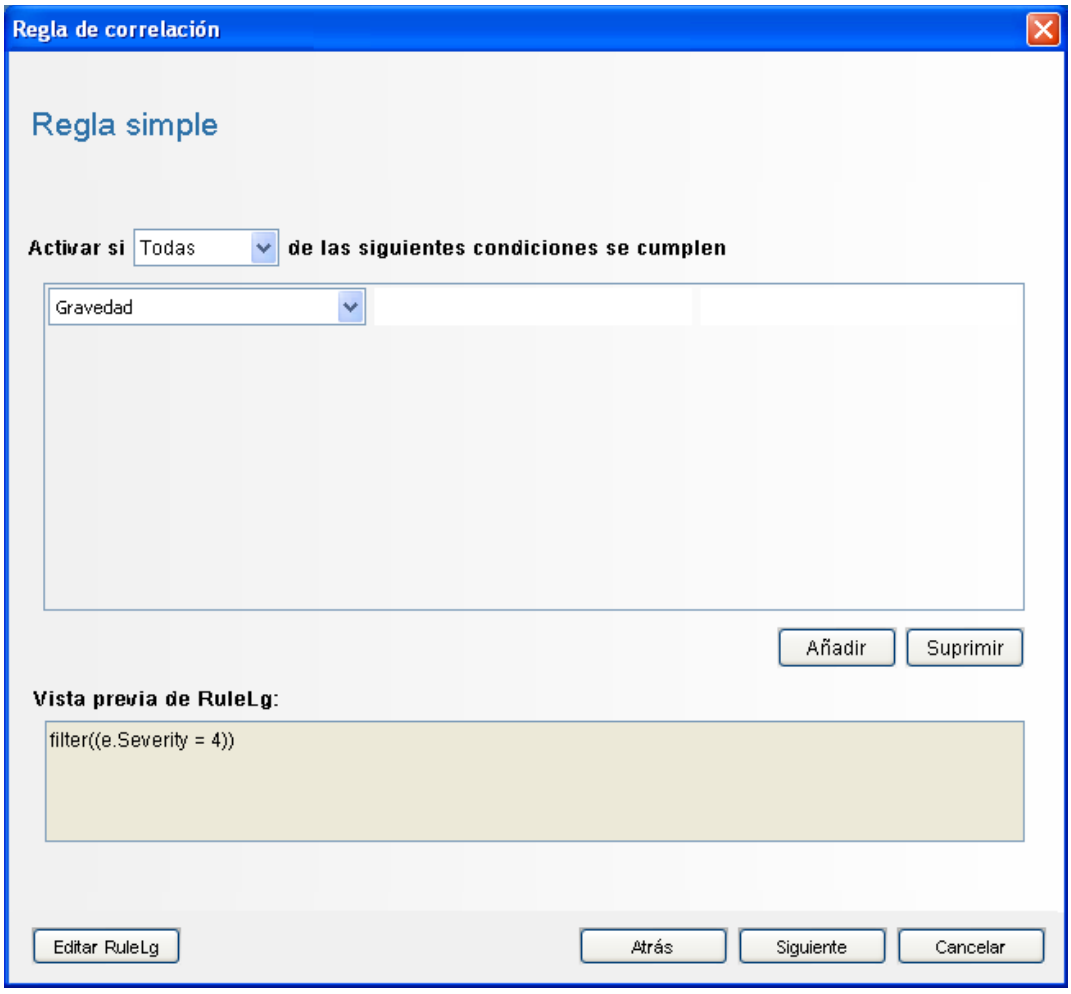
26 Seleccione la pestaña *Correlación*. Se muestra el gestor de reglas de correlación.



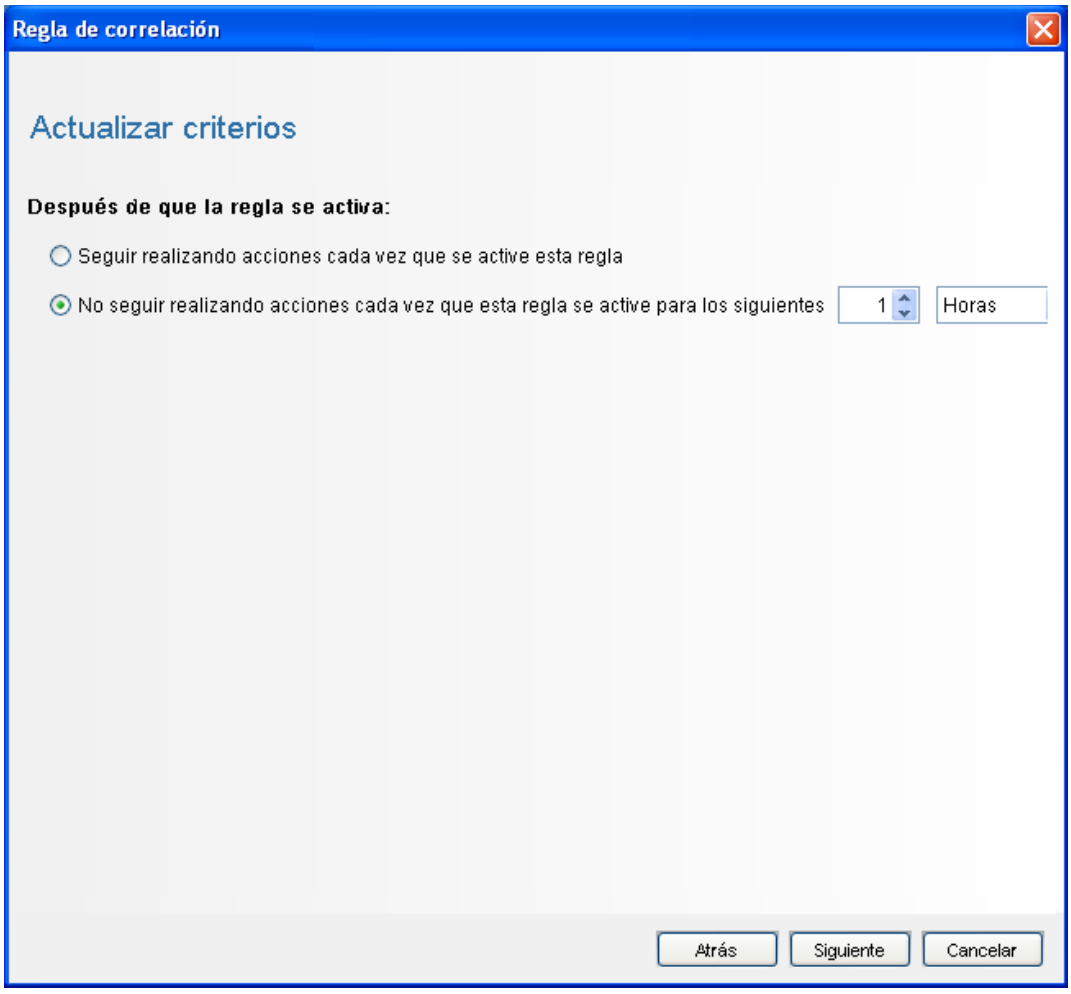
27 Haga clic en *Añadir*. Se muestra el Asistente para reglas de correlación.



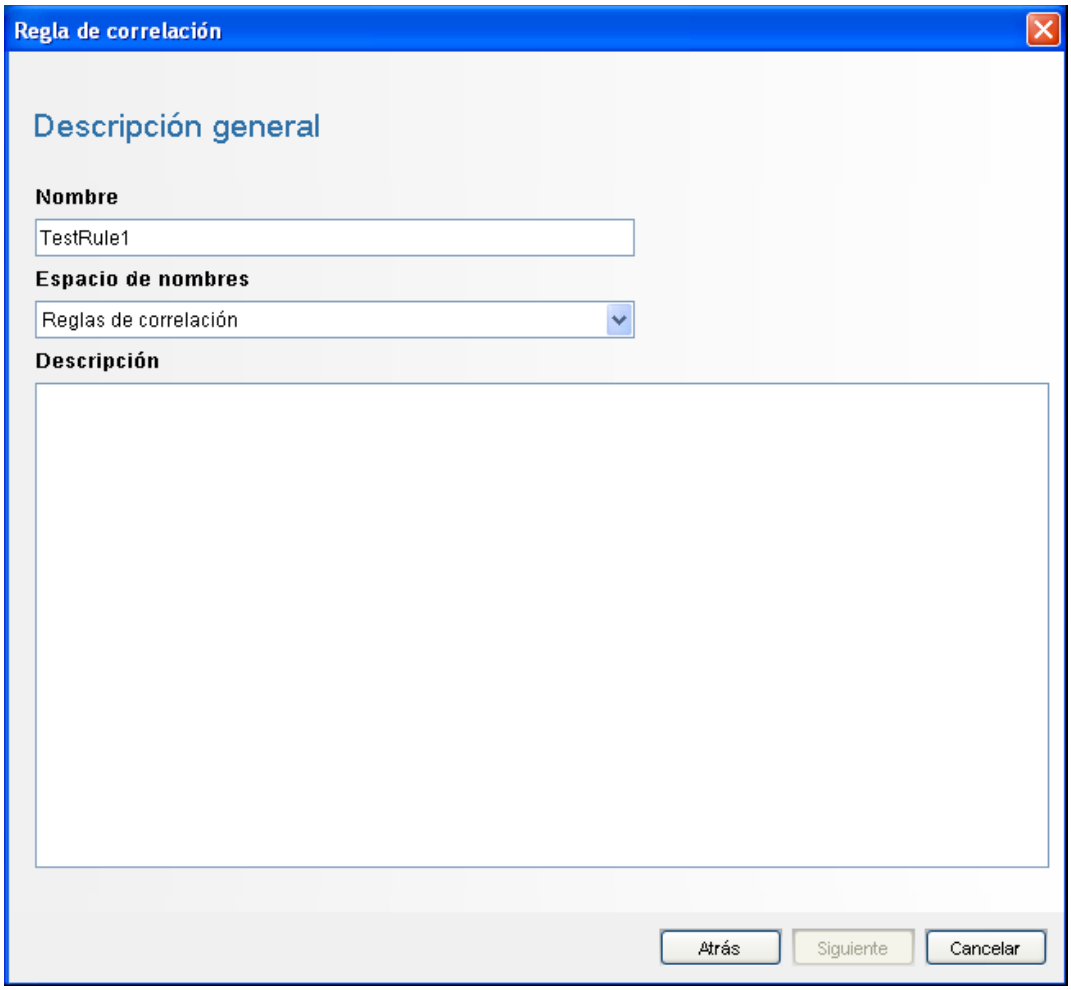
28 Haga clic en *Simple*. Se muestra la ventana Regla simple.



29 Utilice los menús desplegables para ajustar los criterios en Gravedad=4 y haga clic en *Siguiente.* Se muestra la ventana Actualizar criterios.



30 Seleccione *No seguir realizando acciones cada vez que esta regla se active para los siguientes*, use el menú desplegable para definir un periodo de 1 minuto y haga clic en *Siguiente.* Se muestra la ventana Descripción general.



31 Asigne a la regla el nombre *ReglaPrueba1*, introduzca la descripción y haga clic en *Siguiente.*

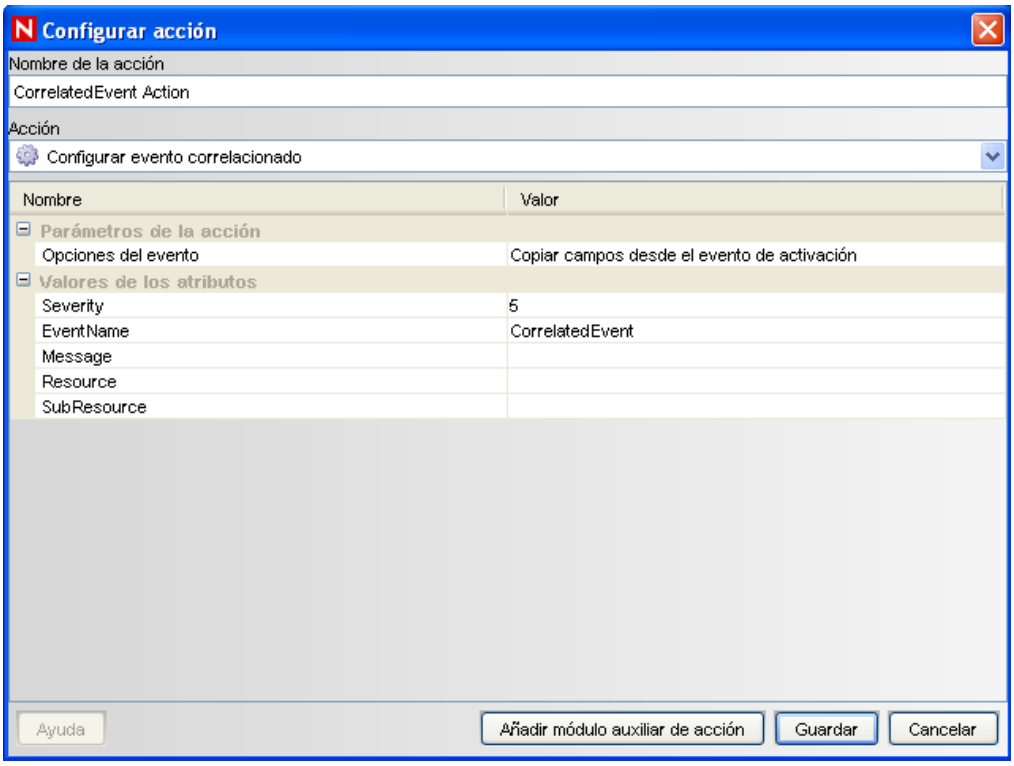
32 Seleccione *No crear otra regla* y haga clic en *Siguiente.*

33 Cree una acción para asociarla con la regla que ha creado:

33a Realice una de las siguientes acciones:

- Seleccione *Herramientas* > *Gestor de acciones* > *Añadir.*
- En la ventana Distribuir regla, haga clic en *Añadir acción.* Para obtener más información, consulte del Paso 34 al Paso 35 en la página 79.

Se muestra la ventana Configurar acción.



33b En la ventana Configurar acción, indique lo siguiente:

- Especifique el nombre de la acción, por ejemplo, la acción Evento correlacionado.
- Seleccione *Configurar evento correlacionado* en la lista desplegable *Acción.*
- Defina las *Opciones del evento.*
- Defina la *Gravedad* en 5.
- Especifique el *Nombre de evento,* por ejemplo, Evento correlacionado.
- Si fuera necesario, especifique un mensaje.

Para obtener más información sobre cómo crear una acción, consulte "Creating Actions" (Creación de acciones) en la *Sentinel Rapid Deployment User Guide* (Guía del usuario de Sentinel Rapid Deployment).

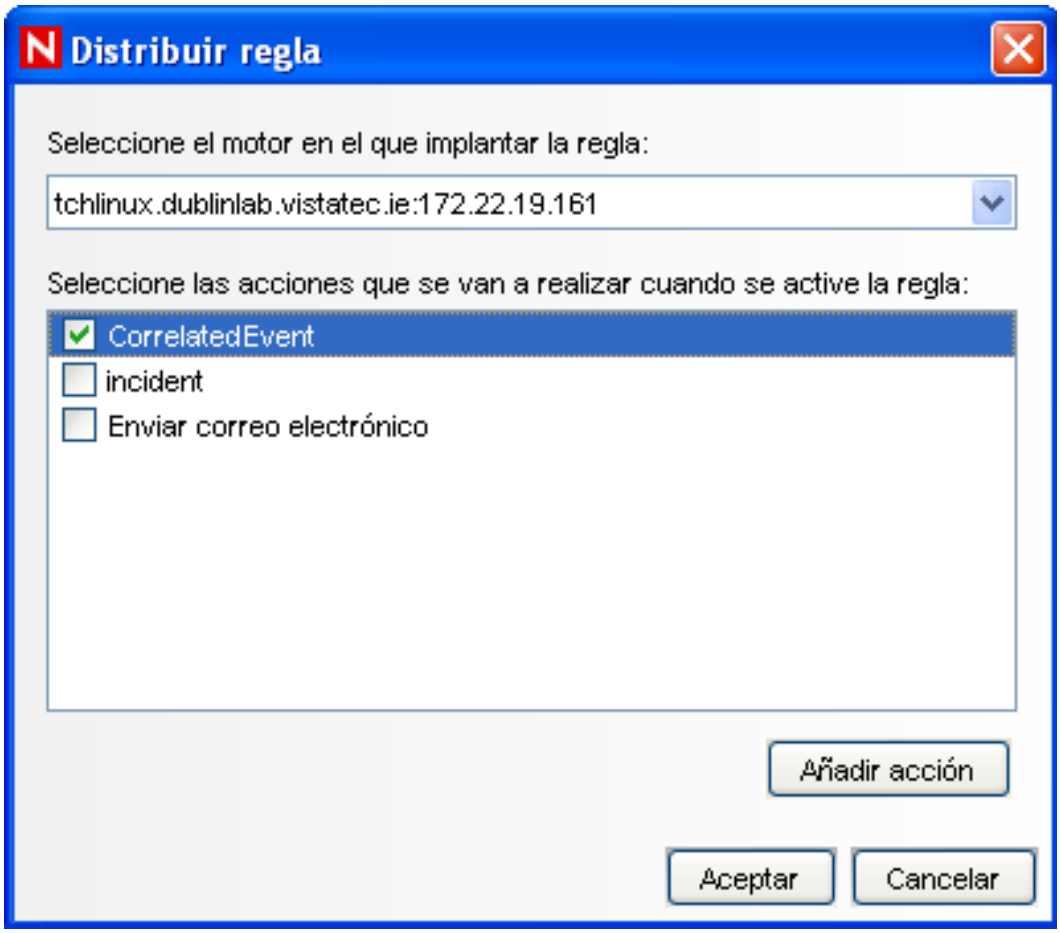
33c Haga clic en *Guardar*.

34 Abra la ventana Gestor de reglas de correlación.

35 Seleccione una regla y haga clic en el enlace *Distribuir las reglas.* Se muestra la ventana Distribuir regla.

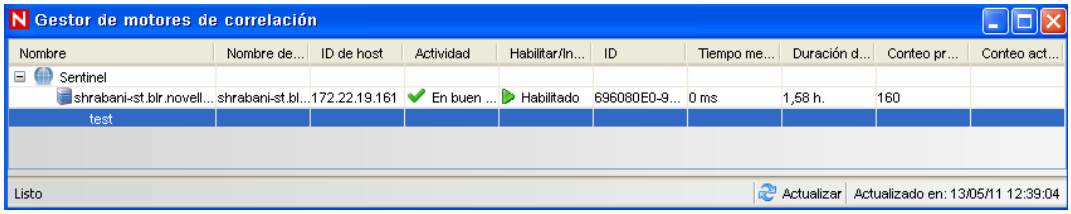
36 En la ventana Distribuir regla, seleccione el motor para distribuir la regla.

37 Seleccione la acción que ha creado en el Paso 33 en la página 78 para asociarla con la regla y haga clic en *Aceptar.*



38 Seleccione *Gestor de motores de correlación.*

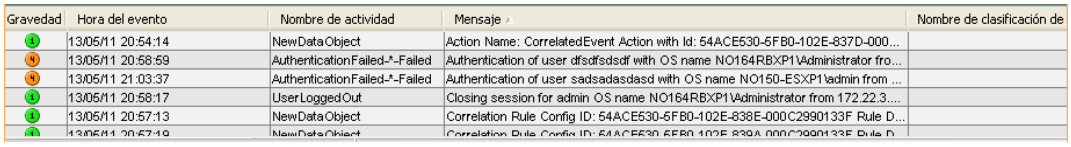
En el motor de correlación puede ver si la regla está distribuida y habilitada.



39 Active un evento de gravedad 4, como un fallo de autenticación, para desencadenar la regla de correlación distribuida.

Por ejemplo, abra una ventana de entrada al Centro de control de Sentinel y especifique unos datos de usuario incorrectos para generar un evento de este tipo.

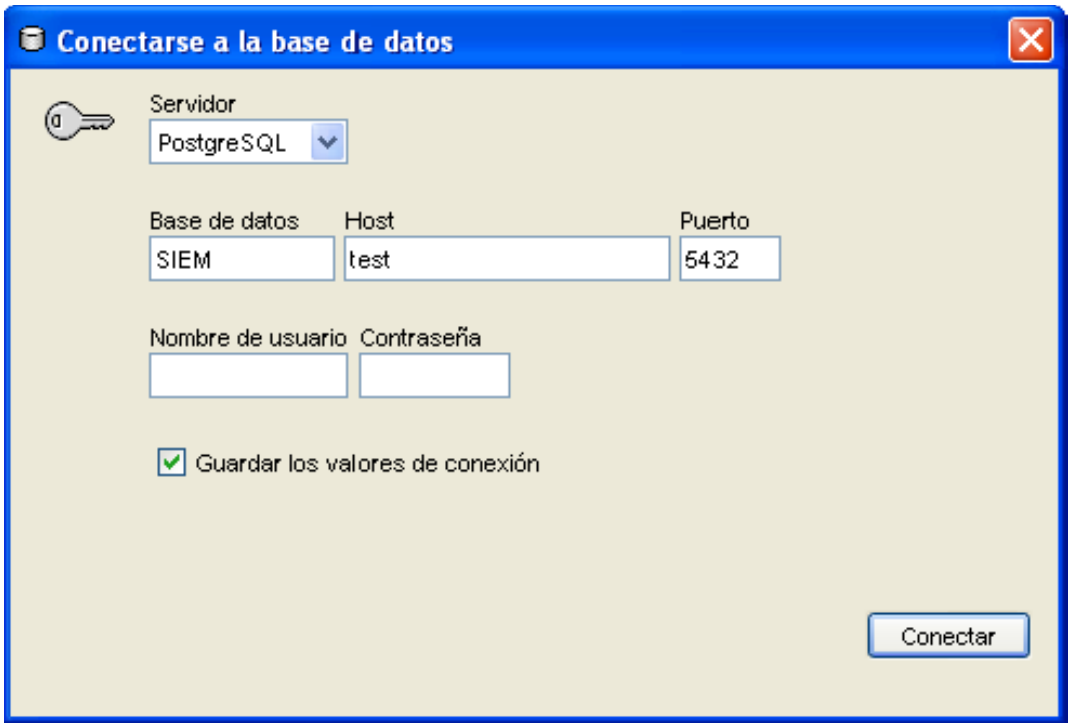
40 Haga clic en la pestaña *Active Views* y compruebe si se ha generado el evento correlacionado.



41 Cierre el Centro de control de Sentinel.

42 En la página Aplicaciones, haga clic en *Lanzar el Gestor de datos de Sentinel.*

43 Entre en el gestor de datos de Sentinel con el usuario administrativo de Sentinel especificado durante la instalación (admin por defecto).



44 Haga clic en cada una de las pestañas para comprobar que puede acceder a él.

45 Cierre el gestor de datos de Sentinel.

Si pudo llevar a cabo todos los pasos anteriores sin ningún problema, significa que ha terminado la verificación básica de la instalación del sistema de Sentinel.

6.2 Limpieza tras la prueba

Tras haber terminado la verificación del sistema, debería eliminar los objetos que se han creado para las pruebas.

1 Entre en el sistema utilizando el usuario administrativo de Sentinel especificado durante la instalación (admin por defecto).

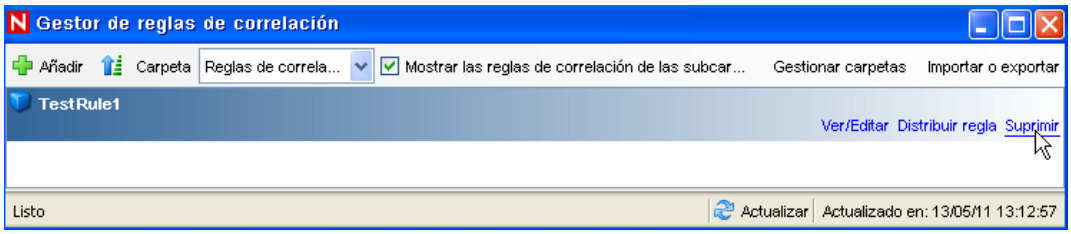
2 Seleccione la pestaña *Correlación.*

3 Abra el Gestor de motores de correlación.

4 Haga clic con el botón derecho en *ReglaPrueba1* en el Gestor de motores de correlación y seleccione *Anular.*

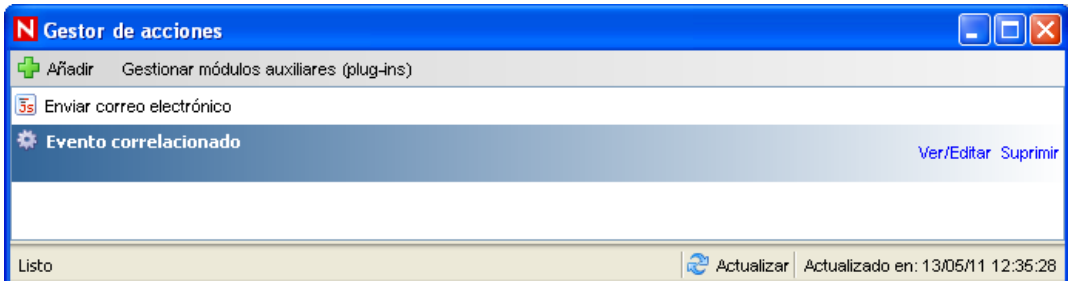
5 Abra el Gestor de reglas de correlación.

6 Seleccione *ReglaPrueba1* y haga clic en *Suprimir.*



7 Seleccione *Herramientas* > *Gestor de acciones* para mostrar la ventana Gestor de acciones.

8 Seleccione la acción *Evento correlacionado*, haga clic en *Suprimir* y, a continuación, en *Sí* para confirmar la supresión.



9 Abra el menú *Gestión de orígenes de eventos* y seleccione la *Vista activa.*

10 En la jerarquía gráfica del origen de eventos, haga clic con el botón derecho en *Recopilador general* y seleccione *Detener.*

11 Cierre la ventana Gestión de orígenes de eventos.

12 Haga clic en la pestaña *Incidencias.*

13 Abra el Gestor de vistas de incidencias.

14 Seleccione *IncidenciaPrueba1*, haga clic con el botón derecho y seleccione *Suprimir.*

6.3 Uso de datos reales

Para comenzar con datos reales, debe importar y configurar los recopiladores que sean adecuados para su entorno, configurar sus propias reglas, generar flujos de tareas ITRAC, etc. Para obtener más información, consulte la *Sentinel Rapid Deployment User Guide* (Guía del usuario de Sentinel Rapid Deployment). Los paquetes de soluciones de Sentinel le ayudarán a comenzar rápidamente. Consulte la página de contenido de Sentinel (http://support.novell.com/products/sentinel/sentinel61.html) para obtener más información.

Desinstalación de Sentinel Rapid Deployment 7

7.1 Desinstalación del servidor de Sentinel Rapid Deployment

1. Entre como usuario `root`.
2. Diríjase al directorio `setup`.

   `cd <install_directory>/setup`
3. Ejecute el guion `uninstall.sh` para desinstalar el servidor de Sentinel Rapid Deployment:

   `./uninstall.sh`

   El guion mostrará un mensaje que indica que Sentinel Rapid Deployment se eliminará por completo.
4. Indique si desea conservar o eliminar el usuario al desinstalar el servidor de Sentinel Rapid Deployment. Pulse `y` (sí) para eliminar el usuario o `n` para conservarlo.
5. Indique si desea conservar o eliminar el grupo al desinstalar el servidor de Sentinel Rapid Deployment. Pulse `y` (sí) para eliminar el grupo o `n` para conservarlo.
6. Indique `y` (sí) para desinstalar o `n` para salir de la desinstalación.

7.2 Desinstalación del gestor de recopiladores remotos y aplicaciones cliente de Sentinel

7.2.1 Linux

1. Entre a la sesión como usuario `Root`.
2. (Condicional) Si va a desinstalar el gestor de recopiladores, detenga los servicios de Sentinel Rapid Deployment:

   `<install_directory>/bin/sentinel.sh stop`
3. Vaya a la siguiente ubicación:

   `<install_directory>/_uninst`
4. Lleve a cabo una de estas acciones:

Modo	Comando
GUI	`./uninstall.bin` Continúe con el Paso 5 en la página 84.
Consola	`./uninstall.bin -console` Continúe con las instrucciones en pantalla.

5 Seleccione un idioma y haga clic en *Aceptar*.

6 En el Asistente UninstallShield de Sentinel, haga clic en *Siguiente*.

7 Seleccione los componentes que desea desinstalar y haga clic en *Siguiente*.

8 Asegúrese de que se han detenido todas las aplicaciones Sentinel en ejecución y haga clic en *Siguiente*.

Se muestra un resumen de las funciones seleccionadas para la desinstalación.

9 Haga clic en *Desinstalar*.

10 Haga clic en *Finalizar*.

7.2.2 Windows

1 Entre como un usuario administrador.

2 (Condicional) Si va a desinstalar el gestor de recopiladores, detenga los servicios de Sentinel Rapid Deployment:

`<install_directory>\bin\sentinel.bat stop`

3 Realice cualquiera de las siguientes acciones:

- Seleccione *Inicio* > *Todos los programas* > *Sentinel* > *Desinstalar Sentinel*.
- Seleccione *Inicio* > *Ejecutar*, introduzca `<directorio_instalación>\_uninst` y, a continuación, haga doble clic en `uninstall.exe`.

4 Seleccione un idioma y haga clic en *Aceptar*.

Se muestra el Asistente UninstallShield de Sentinel Rapid Deployment.

5 Haga clic en *Siguiente*.

6 Seleccione los componentes que desea desinstalar y haga clic en *Siguiente*.

7 Asegúrese de que se han detenido todas las aplicaciones Sentinel en ejecución y haga clic en *Siguiente*.

Se muestra un resumen de las funciones seleccionadas para la desinstalación.

8 Haga clic en *Desinstalar*.

9 Seleccione Reiniciar el sistema y haga clic en *Finalizar*.

7.2.3 Procedimientos posteriores a la desinstalación

Tras desinstalar las aplicaciones, permanecen determinados valores de configuración del sistema que se pueden eliminar de forma manual. Dichos valores de configuración se deben eliminar antes de realizar cualquier instalación nueva de Sentinel, especialmente si se produjeron errores durante la desinstalación de Sentinel.

Nota: en Linux, si se desinstalan el gestor de recopiladores o las aplicaciones del cliente el usuario administrador de Sentinel no se elimina del sistema operativo. Si desea eliminarlo, necesitará hacerlo manualmente.

- "Linux" en la página 85
- "Windows" en la página 85

Linux

1. Entre a la sesión como usuario `root`.
2. Elimine el contenido del `<directorio_instalación>` donde está instalado el software de Sentinel.
3. Elimine los archivos siguientes en el directorio `/etc/init.d`, si existen:

   `sentinel`

   Esto se aplica sólo si se ha instalado el gestor de recopiladores.
4. Asegúrese de que nadie ha iniciado una sesión como usuario administrador de Sentinel (esecadm por defecto); a continuación, elimine el usuario, el directorio personal y el grupo esec:
   - Ejecute `userdel -r esecadm`
   - Ejecute `groupdel esec`
5. Elimine el directorio `/root/InstallShield`.
6. Elimine la sección de InstallShield de `/etc/profile`.
7. Reinicie el equipo.

Windows

1. Suprima la carpeta `%CommonProgramFiles%\InstallShield\Universal` y todo su contenido.
2. Suprima la carpeta `<directorio_instalación>` (por defecto: `C:\Archivos de programa\Novell\Sentinel6`).
3. Haga clic con el botón derecho en *Mi PC* > *Propiedades* > *pestaña Opciones avanzadas.*
4. Haga clic en el botón *Variables de entorno*.
5. Si existen, suprima las siguientes variables:
   - ESEC_HOME
   - ESEC_VERSION
   - ESEC_JAVA_HOME

- ESEC_CONF_FILE
- WORKBENCH_HOME

6. Elimine las entradas de la variable de entorno PATH que indiquen una instalación de Sentinel.
7. Suprima todos los accesos directos de Sentinel del escritorio.
8. Suprima la carpeta de accesos directos *Inicio* > *Programas* > *Sentinel* del menú *Inicio*.
9. Reinicie el equipo.

Actualización del nombre de host de Sentinel Rapid Deployment

A

A.1 Servidor

En el servidor de Sentinel, los cambios en el nombre de host se actualizan automáticamente durante el tiempo de ejecución o durante la instalación. Si el servidor no funciona correctamente después de la actualización de un nombre de host, debe comprobar manualmente lo siguiente:

- Todos los archivos `jnlp` y el archivo `configuration.xml` se actualizan cuando se reinicia Sentinel.
- Se ha actualizado el nombre de host de la tabla de la base de datos `sentinel_host`.
- Ninguna de las referencias al bucle local (localhost o 127.0.0.1) en el archivo `<directorio_instalación>/config/configuration.xml` se ve afectada.

A.2 Aplicaciones cliente

Para las aplicaciones cliente, debe cambiar manualmente el nombre de host del servidor o la dirección IP en las ubicaciones siguientes para apuntar al servidor correcto:

- `<directorio_instalación>/config/configuration.xml`.

  El Centro de control de Sentinel y Solution Designer utilizan esta información.
- La URL de ayuda proporcionada en el archivo `<directorio_instalación>/config/SentinelPreferences.properties`.
- Ejecute el siguiente comando para actualizar el nombre de host en el archivo `sdm.connect`:

  ```
  sdm -action saveConnection -server <postgresql> -host <hostIpaddress/
  hostName> -port <portnum> -database <databaseName/SID> [-driverProps
  <propertiesFile] {-user <dbUser> -password <dbPass> | -winAuth} -
  connectFile <filenameToSaveConnection>
  ```

Sugerencias para la resolución de problemas

B

En esta sección obtendrá una lista de sugerencias para la solución de problemas que le pueden ayudar a determinar algunos de los problemas de instalación de Sentinel Rapid Deployment.

B.1 La autenticación de la base de datos falla al introducir credenciales no válidas

Causa común: la autenticación de la base de datos falla si se introduce un nombre de host o una dirección IP del servidor LDAP no válidos al configurar el servidor de Sentinel Rapid Deployment para la autenticación LDAP.

Acción: asegúrese de introducir un nombre de host o una dirección IP válidos para el servidor LDAP.

B.2 La interfaz Web de Sentinel no puede iniciarse

Causa común: ha instalado Sentinel Rapid Deployment en un equipo donde se está ejecutando un proceso de Identity Audit o la desinstalación es incompleta.

Acción: Sentinel Rapid Deployment y Novell Identity Audit no se pueden instalar en el mismo equipo. Antes de instalar Sentinel Rapid Deployment en el equipo en que está instalado Identity Audit, asegúrese de desinstalar por completo Identity Audit.

Si los procesos de Identity Audit no se han detenido completamente, la desinstalación de Identity Audit no se podrá completar correctamente. En este caso, hay posibilidades de conflictos al instalar Sentinel Rapid Deployment o al iniciar sus aplicaciones.

1. Ejecute el siguiente comando para cerrar los servicios de Identity Audit:

   ```
   /etc/init.d/identity_audit stop
   ```

2. Ejecute el siguiente comando para asegurarse de que Identity Audit ha dejado de funcionar:

   ```
   ps -ef | grep novell
   ```

3. Detenga manualmente todos los procesos restantes si fuera necesario.

   ```
   kill -9 pid
   ```

4 Desinstale Identity Audit con los permisos de `root` necesarios.

Para obtener más información, consulte la Guía de Identity Audit (http://www.novell.com/documentation/identityaudit/identityaudit10guide/data/).

B.3 El gestor de recopiladores remoto ha producido una excepción en Windows 2008 cuando UAC está habilitado

Problema: entre como cualquier usuario que pertenezca al grupo de administradores y ejecute el comando `setup.bat` en un indicador de terminal para instalar el gestor de recopiladores. Reinicie el sistema o inicie manualmente los servicios del gestor de recopiladores; a continuación, entre con las mismas credenciales de usuario. Las excepciones se registran en el archivo `collector_manager0.0.log` que afecta a las siguientes funciones del gestor de recopiladores:

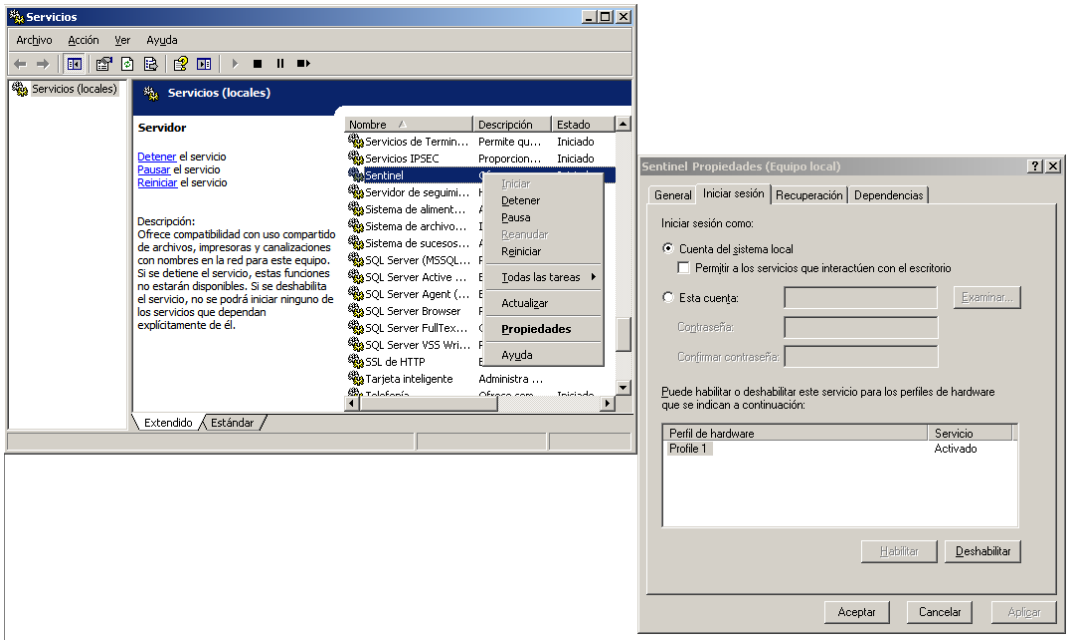
- Las asignaciones no se están inicializando.
- No puede elegir ningún archivo de orígenes de eventos en el sistema de archivos del equipo del gestor de recopiladores (Win2008) utilizando el Conector de archivos.

Causa común: ha instalado el gestor de recopiladores en Windows 2008 SP1 standard edition 64 bits. Por defecto, el equipo tiene el control de acceso de usuarios (UAC) definido como *Habilitado.*

Acción: cambie el propietario de *inicio de sesión* a los servicios de Sentinel Rapid Deployment al usuario actual. Por defecto el propietario de *inicio de sesión* está establecido en la *cuenta local del sistema*. Para cambiar la opción por defecto:

1 Ejecute `services.msc` para abrir la ventana *Servicios*.

2 Haga clic con el botón derecho y, a continuación, seleccione *Propiedades*.



3 En la ventana de propiedades de Sentinel, seleccione la pestaña *Iniciar sesión,*

4 Seleccione *Esta cuenta* y proporcione las credenciales del usuario actual que ha utilizado para instalar el gestor de recopiladores.

B.4 No se crean los UUID en los gestores de recopiladores con imágenes creadas

Si crea una imagen de un servidor del gestor de recopiladores (por ejemplo, mediante ZENworks Imaging) y restaura las imágenes en otros equipos, Sentinel Rapid Deployment no identifica de forma exclusiva las nuevas instancias del gestor de recopiladores. Esto ocurre debido a que hay UUID duplicados.

Debe generar el UUID siguiendo estos pasos en los sistemas del gestor de recopiladores recién instalados:

1 Suprima el archivo `host.id` o `sentinel.id` situado en la carpeta `<directorio_instalación>/data`.

2 Reinicie el gestor de recopiladores.

El gestor de recopiladores genera de forma automática el UUID.

Prácticas recomendadas de mantenimiento de la base de datos PostgreSQL

C

Es posible ajustar con precisión la base de datos para mejorar el rendimiento del servidor de la base de datos. Los límites mencionados en esta sección son recomendaciones aproximadas, no son estrictos. Sin embargo, en sistemas muy dinámicos es recomendable instalar en un buffer y dejar espacio para la expansión.

C.1 Modificación de los parámetros de configuración de la memoria

Para ajustar al detalle el servidor de la base de datos PostgreSQL, modifique los siguientes parámetros de configuración de la memoria en el archivo `<directorio_instalación>/3rd party/postgresql/data/postgresql.conf`:

- **shared_buffers:** permite determinar cuánta memoria dedica PostgreSQL a almacenar datos en caché. Para conseguir un mejor rendimiento, puede definir este parámetro a un cuarto de la capacidad de RAM disponible.
- **effective_cache_size:** permite determinar cuánta memoria hay disponible para el caché de disco en el sistema operativo y en la base de datos. Se puede calcular el tamaño de este parámetro teniendo en cuenta cuánta memoria usan el sistema operativo y otras aplicaciones. Puede asignar la mitad de la memoria total del sistema disponible a este parámetro.
- **work_mem:** permite determinar la cantidad de memoria usada por las operaciones de clasificación internas y las tablas hash antes de cambiar a los archivos de discos temporales. El valor se especifica en kilobytes. El valor por defecto es de 1.024 kilobytes (1 MB).

  En el caso de las consultas complejas, puede haber varias operaciones de clasificación o hash ejecutándose en paralelo. Cada operación usa tanta memoria como se especifique en el valor de work_mem antes de empezar a colocar datos en los archivos de discos temporales. Si va a programar más informes en el sistema Sentinel Rapid Deployment, defina este valor entre 500 MB y 1 GB.
- **maintenance_work_mem:** permite determinar la cantidad máxima de memoria que se debe usar en las operaciones de mantenimiento de la base de datos, como VACUUM (Vaciar), CREATE INDEX (Crear índice) o ALTER TABLE ADD FOREIGN KEY (Alterar clave foránea para añadir tabla). El valor se especifica en kilobytes. El valor por defecto es de 16.384 kilobytes (16 MB).

  Si se asignan valores mayores, el rendimiento del vaciado y la restauración de volcados de la base de datos podría mejorar. No cambie este parámetro, ya que el valor por defecto es suficiente para las operaciones de Sentinel Rapid Deployment.

C.2 Reducción del impacto de E/S de las operaciones de vacío y análisis

Es posible mejorar el rendimiento de la base de datos PostgreSQL de varias formas.

- Los dos parámetros siguientes toman el control de las operaciones de vacío automáticas y, por defecto, se comentan durante la instalación del servidor de Sentinel Rapid Deployment y debe eliminar el comentario y definir los valores.
  - **vacuum_cost_delay:** determina el periodo de tiempo que el proceso permanecerá inactivo cuando se supere el límite de coste. Por ejemplo, puede definir el valor en 100.
  - **vacuum_cost_limit:** determina el coste acumulado que provocará que el proceso de vacío pase a un estado inactivo. Por ejemplo, puede definir el valor en 10.000.

    Si define el valor de estos parámetros a un valor distinto a cero, se reducirá el impacto de E/S de los comandos de vacío y análisis en la actividad normal de la base de datos. El rendimiento podría verse afectado de forma casi imperceptible al ejecutar los informes, ya que el vacío tarda más que anteriormente.
- Por defecto, el proceso `autovacuum` (vaciado automático) está definido como verdadero y se ejecuta de forma periódica para recuperar espacio en el disco y actualizar las estadísticas de planificador. Cuando aumenta el tamaño de la base de datos, el proceso `autovacuum` no puede mantener todos los objetos de la base de datos. En ese caso, si el rendimiento se ralentiza, ejecute el guion `AnalyzePartitions` como tarea cron. Esta tarea cron debe definirla el usuario propietario de los procesos de Sentinel Rapid Deployment.

  Por ejemplo:

  ```
  30 11 * * * $ESEC_HOME/bin/AnalyzePartitions.sh
  ```

  Dónde:
  - `30` es el tiempo en minutos.
  - `11` es el tiempo en horas.
  - `ESEC_HOME` es la vía absoluta de la base de datos.

  En este ejemplo, el guion se ejecuta a las 11:30.
- Procure evitar que la programación del archivado coincida con la de la creación de informes. Si programa ambos procesos juntos, la creación de informes pasa a un estado de espera debido a unos errores de PostgreSQL y empieza a procesar los datos después de que se complete el archivado del trabajo. Este cambio afecta al rendimiento de la base de datos.