Guía de instalación

Novell®
Sentinel Log Manager

1.1

July 08, 2010

www.novell.com

Información legal

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

Documentación en línea: para acceder a la documentación en línea 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

Esta guía presenta una descripción general de Novell Sentinel Log Manager y de su instalación.

Audiencia

Esta guía está destinada a los administradores y usuarios finales de Novell Sentinel Log Manager.

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 de la parte inferior de cada página de la documentación en línea, o bien visite el sitio Web de comentarios sobre la documentación de Novell (http://www.novell.com/documentation/feedback.html) e introduzca allí sus comentarios.

Documentación adicional

Para obtener más información sobre cómo crear sus propios módulos auxiliares (plug-in) (por ejemplo, JasperReports), vaya a la página Web de Sentinel SDK (http://developer.novell.com/wiki/index.php/Develop_to_Sentinel). El entorno de creación de los módulos auxiliares (plug-in) de informes de Sentinel Log Manager es idéntico al que se ha documentado para Novell Sentinel.

Para obtener más información sobre la documentación de Sentinel, consulte el sitio Web de documentación de Sentinel (http://www.novell.com/documentation/sentinel61/index.html).

Para obtener más información sobre cómo configurar Sentinel Log Manager, consulte *Sentinel Log Manager 1.1 Administration Guide* (Guía de administración de Sentinel Log Manager 1.1).

Comunicar 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 revisiones (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)
- Foro de asistencia de la comunidad de Sentinel (http://forums.novell.com/novell-product-support-forums/sentinel/)

Introducción

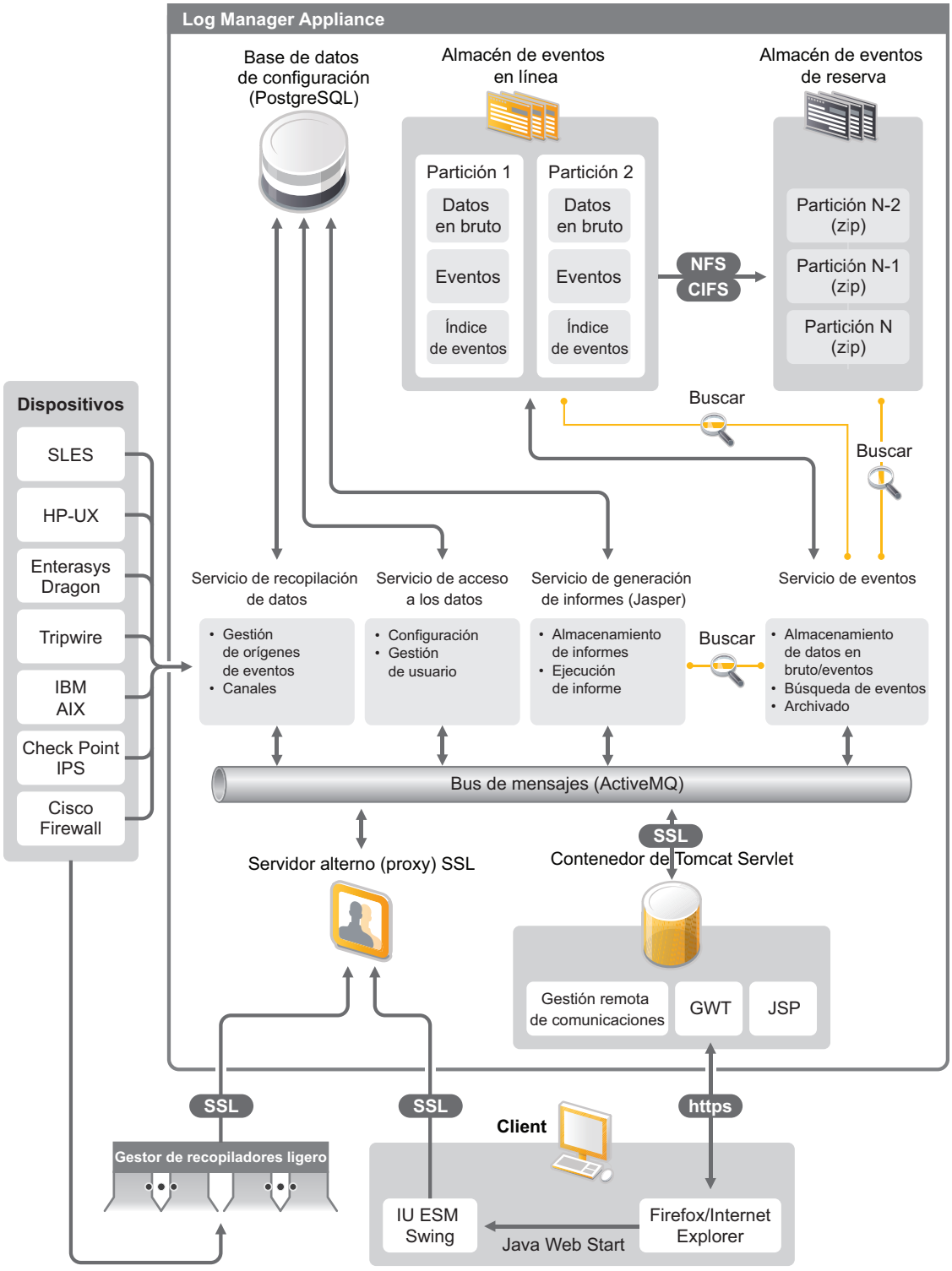
1

Novell Sentinel Log Manager recopila y gestiona datos de una amplia gama de dispositivos y aplicaciones, como orígenes de eventos de sistemas de detección de intrusos, cortafuegos, sistemas operativos, routers, servidores Web, bases de datos, conmutadores, mainframes y antivirus. Novell Sentinel Log Manager ofrece procesamiento de eventos de gran velocidad, retención de datos a largo plazo, retención de datos basada en directivas, adición de datos regionales y sencillas funciones de búsqueda y creación de informes para una variedad de aplicaciones y dispositivos.

1.1 Descripción general del producto

Novell Sentinel Log Manager 1.1 ofrece a las organizaciones una solución de gestión de registros flexible y escalable. Novell Sentinel Log Manager es una solución de gestión de registros que soluciona los desafíos básicos de la gestión y recopilación de registros y además ofrece una completa solución enfocada en reducir el coste y la complejidad del control del riesgo y simplificar los requisitos de conformidad.

Figura 1-1 *Arquitectura Novell Sentinel Log Manager*



Novell Sentinel Log Manager tiene las siguientes funciones:

- Las funciones de búsqueda distribuida permiten a los clientes buscar eventos recopilados no sólo en el servidor local de Sentinel Log Manager sino también en uno o varios servidores de Sentinel Log Manager desde una consola centralizada.
- Informes de conformidad previamente creados para simplificar la tarea de generar informes de conformidad para auditoría o análisis forenses.
- Al utilizar tecnología de almacenamiento no patentada, los clientes pueden aprovechar su infraestructura existente para gestionar los costes.
- Interfaz del usuario basada en navegador que admite la recopilación, almacenamiento, generación de informes y búsqueda de datos de registro para simplificar considerablemente las tareas de supervisión y gestión.
- Controles eficientes y granulares y personalización para administradores de TI a través de nuevas funciones de permisos de usuarios y grupos que proporcionan una mayor transparencia a las actividades de la infraestructura de TI.

Esta sección incluye la siguiente información:

1.1.1 Orígenes de eventos

Novell Sentinel Log Manager recopila datos de orígenes de eventos que generan registros en syslog, el registro de eventos de Windows, archivos, bases de datos, SNMP, Novell Audit (auditoría de Novell), Security Device Event Exchange (SDEE), Check Point Open Platforms for Security (OPSEC) y otros protocolos y mecanismos de almacenamiento.

Sentinel Log Manager admite todos los orígenes de eventos si existen recopiladores adecuados para analizar los datos de dichos orígenes de eventos. Novell Sentinel Log Manager proporciona recopiladores para numerosos orígenes de eventos. El Recopilador de eventos genérico recopila y procesa los datos de orígenes de eventos no reconocidos que tienen conectores adecuados.

Puede configurar los orígenes de eventos para la recopilación de datos mediante la interfaz Gestión de orígenes de eventos.

Para ver una lista completa de orígenes de eventos admitidos, consulte la Sección 2.6, “Orígenes de eventos admitidos”, en la página 22.

1.1.2 Gestión de orígenes de eventos

La interfaz Gestión de orígenes de eventos le permite importar y configurar los conectores y recopiladores de Sentinel 6.0 y 6.1.

Puede realizar las siguientes tareas a través de la vista activa de la ventana de Gestión de orígenes de eventos:

- Agregar o editar conexiones a orígenes de eventos utilizando los asistentes de configuración.
- Ver en tiempo real el estado de las conexiones a orígenes de eventos.
- Importar o exportar la configuración de orígenes de eventos hacia o desde la Vista activa.
- Ver y configurar conectores y recopiladores que están instalados con Sentinel.
- Importar o exportar conectores y recopiladores desde o hacia un repositorio centralizado.
- Supervisar el flujo de datos a través de los recopiladores y conectores configurados.
- Ver la información de los datos en bruto.
- Diseñar, configurar y crear los componentes de la jerarquía de orígenes de eventos y ejecutar las acciones requeridas utilizando estos componentes.

Para obtener más información, consulte la sección Gestión de orígenes de eventos en la *Guía del usuario de Sentinel* (http://www.novell.com/documentation/sentinel61/#admin).

1.1.3 Recopilación de datos

Novell Sentinel Log Manager recopila datos de los orígenes de eventos configurados con la ayuda de conectores y recopiladores.

Los recopiladores son guiones que analizan los datos de una variedad de orígenes de eventos en una estructura de eventos normalizada de Sentinel, o en algunos casos recopilan otras modalidades de datos de fuentes de datos externas. Cada recopilador se debe distribuir con un conector compatible. Los conectores facilitan la conectividad entre los recopiladores de Sentinel Log Manager y los orígenes de datos o eventos.

Novell Sentinel Log Manager proporciona una interfaz mejorada del usuario basada en la Web para syslog y Novell Audit que permite recopilar fácilmente registros de diversos orígenes de eventos.

Novell Sentinel Log Manager recopila datos por medio una variedad de métodos de conexión:

- El conector de syslog acepta y configura de forma automática los orígenes de datos de syslog que envían datos a través del Protocolo de datagrama del usuario (UDP), el Protocolo de control de transmisión (TCP) o el Sistema de capas de transporte (TLS) seguro.
- El conector de auditoría acepta y configura de forma automática los orígenes de datos de Novell habilitados para auditoría.
- El conector de archivo lee los archivos de registro.
- El conector de SNMP recibe los mensajes de alerta SNMP.
- El conector JDBC lee tablas de la base de datos.
- El conector WMS accede a los registros de eventos de Windows en los escritorios y los servidores.
- El conector SDEE se conecta a los dispositivos que admiten el protocolo SDEE, como por ejemplo los dispositivos de Cisco.
- El conector de Log Export API (LEA) de Check Point facilita la integración entre los recopiladores de Sentinel y los servidores de cortafuegos Check Point.

- El conector de Sentinel Link acepta datos de otros servidores de Novell Sentinel Log Manager.
- El conector de procesos acepta datos de procesos creados de forma personalizada que producen registros de eventos.

También puede adquirir una licencia adicional para descargar conectores para SAP y sistemas operativos mainframe.

Para obtener la licencia, llame al 1-800-529-3400 o póngase en contacto con Asistencia técnica de Novell (http://support.novell.com).

Para obtener más información sobre cómo configurar los conectores, consulte la documentación sobre los conectores en el sitio Web de contenido de Sentinel (http://support.novell.com/products/sentinel/sentinel61.html).

Para obtener más información sobre la configuración de recopilación de datos, consulte la sección "Configuración de recopilación de datos" de *Sentinel Log Manager 1.1 Administration Guide* (Guía de administración de Sentinel Log Manager).

Nota: Siempre debe descargar e importar la versión más reciente de los recopiladores y los conectores. Los recopiladores y conectores actualizados se publican con regularidad en el sitio Web de contenido de Sentinel 6.1 (http://support.novell.com/products/sentinel/sentinel61.html). Las actualizaciones de los conectores y recopiladores incluyen soluciones, asistencia para eventos adicionales y mejoras de rendimiento.

1.1.4 Gestor de recopiladores

El gestor de recopiladores proporciona un punto de recopilación de datos flexible para Sentinel Log Manager. Novell Sentinel Log Manager instala un gestor de recopiladores por defecto durante la instalación. No obstante, puede instalar gestores de recopiladores de manera remota en ubicaciones adecuadas dentro de la red. Estos gestores de recopiladores ejecutan conectores y recopiladores y distribuyen los datos recopilados a Novell Sentinel Log Manager para su almacenamiento y recopilación.

Para obtener información sobre la instalación de gestores de recopiladores adicionales, consulte "Instalación de gestores de recopiladores adicionales" en la página 52.

1.1.5 Almacenamiento de datos

Los datos fluyen entre los componentes de recopilación de datos y los componentes de almacenamiento de datos. Estos componentes utilizan un sistema de indexado y almacenamiento de datos basado en archivos que mantiene los datos de registro de los dispositivos recopilados, y una base de datos PostgreSQL que mantiene los datos de configuración de Novell Sentinel Log Manager.

Los datos se almacenan en un formato comprimido en el sistema de archivos del servidor y luego se almacenan en una ubicación configurada para su almacenamiento a largo plazo. Los datos se pueden almacenar a nivel local o en un recurso SMB montado a distancia (CIFS) o en un recurso compartido NFS. Los archivos de datos se suprimen de las ubicaciones de almacenamiento locales y de red en función del programa configurado en la directiva de retención de datos.

Puede configurar las directivas de retención de datos para suprimir datos de la ubicación de almacenamiento si se ha excedido el tiempo límite de retención de datos para determinados datos o si el espacio disponible disminuye por debajo de un valor especificado de espacio en el disco.

Para obtener más información sobre la configuración del almacenamiento de datos, consulte "Configuración de almacenamiento de datos" en *Sentinel Log Manager 1.1 Administration Guide* (Guía de administración de Sentinel Log Manager 1.1).

1.1.6 Búsqueda y generación de informes

Los componentes de búsqueda y generación de informes le ayudan a buscar y generar informes sobre los datos del registro de eventos en los sistemas de indexado y de almacenamiento tanto locales como de red. Los datos de eventos almacenados se pueden buscar de forma genérica o en campos de eventos específicos como el nombre de usuario de origen. Estos resultados de búsqueda se pueden delimitar o filtrar aún más y guardarlos en una plantilla de informes para su uso en el futuro.

Sentinel Log Manager incluye informes previamente instalados. También puede cargar informes adicionales. Puede ejecutar informes según un programa o siempre que sea necesario.

Para obtener información sobre una lista de informes por defecto, consulte "Generación de informes" en *Sentinel Log Manager 1.1 Administration Guide* (Guía de administración de Sentinel Log Manager 1.1).

Para obtener más información sobre la búsqueda de eventos y la generación de informes, consulte "Búsqueda" y "Generación de informes" en *Sentinel Log Manager 1.1 Administration Guide* (Guía de administración de Sentinel Log Manager 1.1).

1.1.7 Sentinel Link

Sentinel Link se puede utilizar para remitir datos de eventos desde un servidor Sentinel Log Manager a otro. Con un conjunto jerárquico de gestores Sentinel Log Manager, se pueden conservar registros completos en diversas ubicaciones regionales, mientras que los eventos más importantes se remiten a un único Sentinel Log Manager para realización de informes y búsquedas centralizadas.

Además, Sentinel Link puede remitir eventos importantes a Novell Sentinel, un sistema de gestión de eventos de información de seguridad (SIEM) completo, para correlación avanzada, solución de incidentes e inyección de información de contexto de gran valor como, por ejemplo, la importancia del servidor o información de identidad desde un sistema de gestión de identidades.

1.1.8 Interfaz de usuario basada en Web

Novell Sentinel Log Manager incluye una interfaz de usuario basada en la Web para configurar y usar el gestor de registros. La funcionalidad de la interfaz del usuario la facilita un servidor Web y una interfaz gráfica del usuario basada en Java Web Start. Todas las interfaces del usuario se comunican con el servidor por medio de una conexión cifrada.

Puede usar la interfaz Web de Novell Sentinel Log Manager para realizar las tareas siguientes:

- Buscar eventos
- Guardar los criterios de búsqueda como una plantilla de informe
- Ver y gestionar informes

- Lanzar la interfaz Gestión de orígenes de eventos para configurar la recopilación de datos para los orígenes de eventos que no sean syslog o las aplicaciones de Novell (sólo administradores)
- Configurar la remisión de datos (sólo administradores)
- Descargar el instalador del Gestor de recopiladores Sentinel para una instalación remota (sólo administradores)
- Ver la actividad de los orígenes de eventos (sólo administradores)
- Configurar la recopilación de datos para los orígenes de datos de syslog y Novell (sólo administradores)
- Configurar el almacenamiento de datos y ver la actividad de la base de datos (sólo administradores)
- Configurar el archivado de datos (sólo administradores)
- Configurar acciones asociadas para enviar los datos de evento coincidentes a los canales de salida (sólo para los administradores).
- Gestionar cuentas y permisos de usuarios (sólo administradores)

1.2 Descripción general de la instalación

Novell Sentinel Log Manager se puede instalar como dispositivo o en un sistema operativo SUSE Linux Enterprise Server (SLES) 11 existente. Cuando se instala Sentinel Log Manager como dispositivo, el servidor del Gestor de registros se instala en un sistema operativo SLES 11.

Novell Sentinel Log Manager instala los siguientes componentes por defecto:

- Servidor de Sentinel Log Manager
- Servidor de comunicaciones
- Servidor Web e interfaz del usuario basada en la Web
- Servidor de realización de informes
- Gestor de recopiladores

Algunos de estos componentes requieren una configuración adicional.

Novell Sentinel Log Manager instala por defecto un gestor de recopiladores. Si desea tener más gestores de recopiladores, puede instalarlos por separado en equipos remotos. Para obtener más información, consulte la Capítulo 7, “Instalación de gestores de recopiladores adicionales”, en la página 51.

Requisitos del sistema

2

En las siguientes secciones se describen los requisitos de hardware, sistema operativo, navegador, conectores admitidos y compatibilidad de orígenes de eventos para Novell Sentinel Log Manager.

2.1 Requisitos del hardware

2.1.1 Servidor de Sentinel Log Manager

Novell Sentinel Log Manager se admite en procesadores AMD Opteron e Intel Xeon de 64 bits, pero no se admite en procesadores Itanium.

Nota: Estos requisitos se aplican para un tamaño de evento medio de 300 bytes.

Se recomiendan los siguientes requisitos de hardware para un sistema de producción que albergue 90 días de datos en línea:

Tabla 2-1 *Requisitos de hardware de Sentinel Log Manager*

Requisitos	Sentinel Log Manager (500 EPS)	Sentinel Log Manager (2500 EPS)	Sentinel Log Manager (7500 EPS)
Compresión	Hasta 10:1	Hasta 10:1	Hasta 10:1
Orígenes de eventos máximos	Hasta 1000	Hasta 1000	Hasta 2000
Número de eventos máximo	500	2500	7500

Requisitos	Sentinel Log Manager (500 EPS)	Sentinel Log Manager (2500 EPS)	Sentinel Log Manager (7500 EPS)
CPU	Una CPU Intel Xeon E5450 3 GHz (4 núcleos) O bien Dos CPU Intel Xeon L5240 3 GHz (2 núcleos) (4 núcleos en total)	Una CPU Intel Xeon E5450 3 GHz (4 núcleos) O bien Dos CPU Intel Xeon L5240 3 GHz (2 núcleos) (4 núcleos en total)	Dos CPU Intel Xeon X5470 3,33 GHz (4 núcleos) CPUs (8 núcleos en total)
Memoria de acceso aleatorio (RAM)	4 GB	4 GB	8 GB
Almacenamiento	2 unidades de 7,2 k RPM de 500 GB (RAID basada en hardware con caché de 256 MB, RAID 1)	2 unidades de 7,2 k RPM de 1 TB (RAID basada en hardware con caché de 256 MB, RAID 1)	6 unidades del 15 k RPM de 450 GB (RAID basada en hardware con caché de 512 MB, RAID 10)

Nota:

- Un equipo puede incluir más de un origen de eventos. Por ejemplo, un servidor de Windows puede incluir dos orígenes de eventos de Sentinel porque se desea recopilar datos del sistema operativo Windows y también de la base de datos de SQL Server alojado en dicho equipo
- Debe configurar la ubicación de almacenamiento de red en un área de red de almacenamiento (SAN) externa de múltiples unidades o en un almacenamiento con interconexión a la red (NAS).
- El volumen de estado regular recomendado es del 80% del número máximo de EPS con licencia. Novell recomienda añadir más instancias de Sentinel Log Manager si se alcanza este límite.

Nota: Los límites para el máximo de orígenes de eventos no son límites estrictos sino recomendaciones basadas en las pruebas de rendimiento realizadas por Novell y dan por supuesto una velocidad media de eventos por segundo baja por origen de evento (menos de 3 EPS). Una velocidad de EPS más alta da lugar a orígenes de eventos máximos sostenibles más bajos. Puede usar la ecuación (orígenes de eventos máximos) x (media de EPS por origen de eventos) = número máximo de eventos para obtener los límites aproximados para la velocidad media de EPS específica o para el número de orígenes de eventos, siempre que el número máximo de orígenes de eventos no supere el límite indicado anteriormente.

2.1.2 Servidor del gestor de recopiladores

- ❑ Un procesador Intel Xeon L5240 de 3 GHz (CPU de 2 núcleos)
- ❑ 256 MB de RAM
- ❑ 10 GB de espacio libre en el disco duro.

2.1.3 Estimación de requisitos de almacenamiento de datos

Sentinel Log Manager se utiliza para retener datos en bruto durante un largo período de tiempo con el fin de cumplir los requisitos legales y de otro tipo. Sentinel Log Manager utiliza compresión para ayudarle a utilizar el espacio de almacenamiento local o de red de forma eficaz. Sin embargo, los requisitos de almacenamiento podrían aumentar de forma significativa transcurrido un largo período de tiempo.

Para superar los problemas de limitación de costes de los grandes sistemas de almacenamiento, puede usar sistemas de almacenamiento de datos económicos para almacenar los datos a largo plazo. Los sistemas de almacenamiento basados en cinta representan la solución más común y rentable. No obstante, las cintas no permiten el acceso aleatorio a los datos almacenados, que resulta necesario para realizar búsquedas rápidas. Por ello, resulta recomendable un planteamiento híbrido para el almacenamiento de datos a largo plazo, en el que los datos que se han de buscar están disponibles en un sistema de almacenamiento de acceso aleatorio y los datos que queremos conservar, y no buscar, se guardan en un medio alternativo y económico, como una cinta. Para obtener instrucciones sobre cómo aplicar este enfoque híbrido, consulte "Uso de almacenamiento de acceso secuencial para el almacenamiento de datos a largo plazo" en *Sentinel Log Manager 1.1 Administration Guide* (Guía de administración de Sentinel Log Manager 1.1).

Para determinar la cantidad de espacio de almacenamiento de acceso aleatorio necesario para Sentinel Log Manager, haga primero una estimación del número de días de datos que necesita buscar con regularidad o sobre los que necesita ejecutar informes. Debe tener suficiente espacio en el disco duro ya sea a nivel local en el equipo de Sentinel Log Manager o a distancia en el protocolo Server Message Block (SMB) o el protocolo CIFS, el sistema de archivos de red (NFS) o en una SAN para que Sentinel Log Manager los utilice con fines de archivado de datos.

Debe tener el siguiente espacio adicional en el disco duro aparte de los requisitos mínimos:

- Para acomodar las velocidades de datos superiores a las esperadas.
- Para copiar datos desde la cinta y de nuevo a Sentinel Log Manager para realizar búsquedas y generar informes sobre los datos históricos.

Utilice las siguientes fórmulas para estimar la cantidad de espacio necesario para almacenar datos:

- **Tamaño de almacenamiento de datos de eventos:** {número de días} x {eventos por segundo} x {tamaño medio del evento en bytes} x 0,000012 = GB de almacenamiento necesario

  Los tamaños de evento típicos tienen de 300 a 1000 bytes.
- **Tamaño de almacenamiento de datos en bruto:** {número de días} x {eventos por segundo} x {tamaño medio de los datos en bruto en bytes} x 0,000012 = GB de almacenamiento necesario

  El tamaño medio típico de datos en bruto para los mensajes de syslog es de 200 bytes.
- **Tamaño total de almacenamiento:** ({tamaño medio del evento en bytes} + {tamaño medio de los datos en bruto en bytes}) x {número de días} x {eventos por segundo} x 0,000012 = Total de GB de almacenamiento necesarios

---

Nota: Estas cifras son sólo estimaciones y dependen del tamaño de los datos del evento además del tamaño de los datos comprimidos.

Las fórmulas anteriores calculan el espacio de almacenamiento mínimo necesario para comprimir por completo los datos en el sistema de almacenamiento externo. Cuando se llena el almacenamiento local, Sentinel Log Manager comprime y mueve los datos desde un sistema local (parcialmente comprimido) a un sistema de almacenamiento externo (totalmente comprimido). Por lo tanto, estimar los requisitos de espacio de almacenamiento externo se convierte en una tarea fundamental para la retención de datos. Para mejorar el rendimiento de las búsquedas y generación de informes de los datos recientes, puede aumentar el espacio de almacenamiento local más allá de los requisitos de hardware de Sentinel Log Manager, aunque esto no es necesario.

Puede usar las fórmulas anteriores para determinar cuánto espacio de almacenamiento se requiere para un sistema de almacenamiento de datos a largo plazo, como por ejemplo una cinta.

2.1.4 Entorno virtual

Sentinel Log Manager se ha probado a fondo en servidores VMware ESX y la compatibilidad es total. Los resultados de rendimiento en un entorno virtual pueden compararse a los resultados obtenidos en las pruebas realizadas en un equipo físico, pero el entorno virtual debe proporcionar la misma memoria, CPU, espacio en el disco y E/S que las recomendaciones para el equipo físico.

2.2 Sistemas operativos compatibles

En esta sección se proporciona información sobre los sistemas operativos compatibles con el servidor de Sentinel Log Manager y el gestor de recopiladores remoto:

- Sección 2.2.1, “Sentinel Log Manager”, en la página 20
- Sección 2.2.2, “Gestor de recopiladores”, en la página 20

2.2.1 Sentinel Log Manager

Esta sección es pertinente únicamente si va a instalar Sentinel Log Manager en un sistema operativo existente.

- ❑ SUSE Linux Enterprise Server 11 de 64 bits.
- ❑ Un sistema de archivos de alto rendimiento.

Nota: Todas las pruebas de Novell se realizan con el sistema de archivos ext3.

2.2.2 Gestor de recopiladores

Puede instalar gestores de recopiladores adicionales en los siguientes sistemas operativos:

- “Linux” en la página 20
- “Windows” en la página 21

Linux

- ❑ SUSE Linux Enterprise Server 10 SP2 (32 y 64 bits)
- ❑ SUSE Linux Enterprise Server 11 (32 y 64 bits)

Windows

- ❑ Windows Server 2003 (32 y 64 bits)
- ❑ Windows Server 2003 SP2 (32 bits y 64 bits)
- ❑ Windows Server 2008 (64 bits)

2.3 Navegadores compatibles

La interfaz de Sentinel Log Manager está optimizada para una visualización a una resolución de 1280 x 1024 o superior en los siguientes navegadores:

- Sección 2.3.1, “Linux”, en la página 21
- Sección 2.3.2, “Windows”, en la página 21

2.3.1 Linux

- ❑ Mozilla Firefox 3.6

2.3.2 Windows

- ❑ Mozilla Firefox 3 (funcionamiento óptimo en 3.6)
- ❑ Microsoft Internet Explorer 8 (funcionamiento óptimo en 8.0)

Requisitos previos para Internet Explorer 8

- Si se establece el Nivel de seguridad de Internet en Alto, sólo aparecerá una página en blanco después de entrar en Novell Sentinel Log Manager. Para salvar este problema, vaya a *Herramientas > Opciones de Internet> pestaña Seguridad> Sitios de confianza*. Haga clic en el botón *Sitio* y añada el sitio Web de Sentinel Log Manager a la lista de sitios de confianza.
- Asegúrese de que no esté seleccionada la opción *Herramientas > Vista de compatibilidad*.
- Si no está habilitada la opción para *Preguntar automáticamente para descargas de archivos*, puede que el cuadro emergente de descarga de archivos esté bloqueado por el navegador. Para salvar este problema, vaya a *Herramientas >Opciones de Internet> pestaña Seguridad> Nivel personalizado* y luego desplácese hacia abajo a la sección de descarga y seleccione *Habilitar* para habilitar la opción *Preguntar automáticamente para descargas de archivos*.

2.4 Entorno virtual admitido

- ❑ VMware ESX/ESXi 3.5/4.0 o superior
- ❑ VMPlayer 3 (sólo demostración)
- ❑ Xen 3.1.1

2.5 Conectores admitidos

Sentinel Log Manager admite todos los conectores que son admitidos por Sentinel y Sentinel RD.

- ❑ Conector de auditoría
- ❑ Conector de proceso Check Point LEA

- Conector de base de datos
- Conector de generador de base de datos
- Conector de archivos
- Conector de procesos
- Conector syslog
- Conector de SNMP
- Conector de SDEE
- Conector de Sentinel Link
- Conector de WMS
- Conector de mainframe
- Conector de SAP

Nota: Los conectores de mainframe y SAP requieren una licencia aparte.

2.6 Orígenes de eventos admitidos

Sentinel Log Manager admite una amplia gama de dispositivos y aplicaciones, como orígenes de eventos de sistemas de detección de intrusos, cortafuegos, sistemas operativos, routers, servidores Web, bases de datos, conmutadores, mainframes y antivirus. Los datos de estos orígenes de eventos se analizan y normalizan en diversos grados dependiendo de si los datos se procesan mediante el recopilador de eventos genérico que pone toda la carga del evento en un campo común, o mediante un recopilador específico para los dispositivos que analiza los datos en campos individuales.

Sentinel Log Manager admite los siguientes orígenes de eventos:

- Cisco Firewall (6 y 7)
- Cisco Switch Catalyst serie 6500 (CatOS 8.7)
- Cisco Switch Catalyst serie 6500 (IOS 12.2SX)
- Cisco Switch Catalyst serie 5000 (CatOS 4.x)
- Cisco Switch Catalyst serie 4900 (IOS 12.2SG)
- Cisco Switch Catalyst serie 4500 (IOS 12.2SG)
- Cisco Switch Catalyst serie 4000 (CatOS 4.x)
- Cisco Switch Catalyst serie 3750 (IOS 12.2SE)
- Cisco Switch Catalyst serie 3650 (IOS 12.2SE)
- Cisco Switch Catalyst serie 3550 (IOS 12.2SE)
- Cisco Switch Catalyst serie 2970 (IOS 12.2SE)
- Cisco Switch Catalyst serie 2960 (IOS 12.2SE)
- Cisco VPN 3000 (4.1.5, 4.1.7 y 4.7.2)
- Extreme Networks Summit X650 (con ExtremeXOS 12.2.2 y anteriores)
- Extreme Networks Summit X450a (con ExtremeXOS 12.2.2 y anteriores)
- Extreme Networks Summit X450e (con ExtremeXOS 12.2.2 y anteriores)
- Extreme Networks Summit X350 (con ExtremeXOS 12.2.2 y anteriores)

- Extreme Networks Summit X250e (con ExtremeXOS 12.2.2 y anteriores)
- Extreme Networks Summit X150 (con ExtremeXOS 12.2.2 y anteriores)
- Enterasys Dragon (7.1 y 7.2)
- Recopilador de eventos genérico
- HP HP-UX (11iv1 y 11iv2)
- IBM AIX (5.2, 5.3 y 6.1)
- Juniper Netscreen serie 5
- McAfee Firewall Enterprise
- McAfee Network Security Platform (2.1, 3.x y 4.1)
- McAfee VirusScan Enterprise (8.0i, 8.5i y 8.7i)
- McAfee ePolicy Orchestrator (3.6 y 4.0)
- McAfee AV Via ePolicy Orchestrator 8.5
- Microsoft Active Directory (2000, 2003 y 2008)
- Microsoft SQL Server (2005 y 2008)
- Nortel VPN (1750, 2700, 2750 y 5000)
- Novell Access Manager 3.1
- Gestor de identidades 3.6.1 de Novell
- Novell Netware 6.5
- Servicios NMAS (autenticación modular) de Novell 3.3
- Novell Open Enterprise Server 2.0.2
- Novell Privileged User Manager 2.2.1
- Novell Sentinel Link 1
- Servidor de Novell SUSE Linux Enterprise
- Novell eDirectory 8.8.3 con el parche de utilidades de eDirectory que se encuentra en el Sitio Web de asistencia de Novell (http://download.novell.com/Download?buildid=RH_B5b3M6EQ~).
- Novell iManager 2.7
- Red Hat Enterprise Linux
- Sourcefire Snort (2.4.5, 2.6.1, 2.8.3.2 y 2.8.4)
- Snare for Windows Intersect Alliance (3.1.4 y 1.1.1)
- Sun Microsystems Solaris 10
- Symantec AntiVirus Corporate Edition (9 y 10)
- TippingPoint Security Management System (2.1 y 3.0)
- Websense Web Security 7.0
- Websense Web Filter 7.0

Nota: Para habilitar la recopilación de datos de orígenes de eventos de Novell iManager y Novell Netware 6.5, añada una instancia de recopilador y un conector hijo (conector de auditoría) en la interfaz de Gestión de orígenes de eventos para cada uno de los orígenes de eventos. Cuando haya terminado, estos orígenes de eventos aparecerán en la consola Web de Sentinel Log Manager en la pestaña de *Auditar servidores*.

Es posible obtener recopiladores que admiten otros orígenes de eventos en el sitio Web de contenido de Sentinel 6.1 (http://support.novell.com/products/sentinel/sentinel61.html) o se pueden crear mediante los módulos auxiliares (plug-in) de SDK disponibles en el sitio Web de SDK de módulos auxiliares (plug-in) de Sentinel (http://developer.novell.com/wiki/index.php?title=Develop_to_Sentinel).

Instalación en un sistema SLES 11 existente

3

En esta sección se describe el procedimiento para instalar Sentinel Log Manager en un sistema SUSE Linux Enterprise Server (SLES) 11 existente utilizando el instalador de la aplicación. Puede instalar el servidor de Sentinel Log Manager de varias formas: el procedimiento de instalación estándar, el procedimiento de instalación personalizada o el procedimiento de instalación silenciosa, en el que la instalación de desarrolla sin intervención del usuario y utiliza los valores por defecto. También puede instalar Sentinel Log Manager como usuario diferente de root.

Si elige el método de instalación personalizada, tendrá la opción de instalar el producto con una clave de licencia y además seleccionar una opción de autenticación. Puede configurar la autenticación LDAP para Sentinel Log Manager además de la autenticación de la base de datos. Al configurar Sentinel Log Manager para la autenticación LDAP, los usuarios pueden entrar en el servidor utilizando sus credenciales de Novell eDirectory o de Microsoft Active Directory.

Si desea instalar varios servidores de Sentinel Log Manager en su implantación, puede registrar las opciones de instalación en un archivo de configuración y luego usar el archivo para ejecutar una instalación sin supervisión. Consulte Sección 3.4, “Instalación silenciosa”, en la página 29 para obtener más información.

Antes de continuar con la instalación, asegúrese de que se cumplen los requisitos mínimos especificados en Capítulo 2, “Requisitos del sistema”, en la página 17.

3.1 Antes de empezar

- ❑ Asegúrese de que el hardware y el software cumplen los requisitos mínimos mencionados en el Capítulo 2, “Requisitos del sistema”, en la página 17.
- ❑ Configure el sistema operativo de manera que el comando `hostname -f` devuelva un nombre de host válido.
- ❑ Obtenga su clave de licencia delCentro de atención al cliente de Novell (https://secure-www.novell.com/center/ICSLogin/?%22https://secure-www.novell.com/center/regadmin/jsps/home_app.jsp%22), para instalar la versión con licencia.
- ❑ Sincronice el tiempo utilizando el protocolo de tiempo de red (NTP).
- ❑ Instale los siguientes comandos del sistema operativo:
  - `mount`
  - `umount`
  - `id`

- `df`
- `du`
- `sudo`

❑ Asegúrese de que los siguientes puertos estén abiertos en el cortafuegos:

TCP 8080, TCP 8443, TCP 61616, TCP 10013, TCP 1289, TCP 1468, TCP 1443 y UDP 1514

3.2 Instalación estándar

El procedimiento de instalación estándar instala Sentinel Log Manager con todas las opciones por defecto y una licencia de evaluación de 90 días.

1. Descargue y copie los archivos de instalación desde el sitio de descargas de Novell.
2. Entre como usuario `root` en el servidor en el que desea instalar Sentinel Log Manager.
3. Especifique el siguiente comando para extraer los archivos de instalación del archivo tar:

   `tar xfz <install_filename>`

   Reemplace <*nombre de archivo_instalación*> por el nombre real del archivo de instalación.
4. Especifique el siguiente comando para ejecutar el guión `install-slm` para instalar Sentinel Log Manager:

   `./install-slm`

   Si desea instalar Sentinel Log Manager en más de un sistema, puede registrar sus opciones de instalación en un archivo. Puede usar este archivo para instalar Sentinel Log Manager en otros sistemas sin supervisión. Para registrar sus opciones de instalación, especifique el siguiente comando:

   `./install-slm -r responseFile`
5. Para continuar con el idioma deseado, elija el número especificado junto al idioma.

   El acuerdo de licencia de usuario final se muestra en el idioma seleccionado.
6. Lea el acuerdo de licencia del usuario final e introduzca `sí` o `s` para aceptar el acuerdo y continuar con la instalación.

   La instalación comienza instalando todos los paquetes RPM. Esta instalación podría tardar varios segundos en finalizar.

   La instalación crea un grupo`novell` y un usuario `novell`, si aún no existen.
7. Cuando se le indique, especifique la opción para continuar con la instalación estándar.

   La instalación continúa con la clave de licencia de evaluación de 90 días incluida en el instalador. Esta clave de licencia activa todo el conjunto de funciones del producto durante un período de prueba de 90 días. En cualquier momento durante el período de prueba o después, puede sustituir la licencia de evaluación por una clave de licencia que haya adquirido.
8. Especifique la contraseña del usuario administrador.
9. Confirme la contraseña del usuario administrador.

   El instalador selecciona el método para *autenticar sólo en la base de datos*y continúa con la instalación.

   La instalación de Sentinel Log Manager finaliza y se inicia el servidor. Podría tardarse entre 5 y 10 minutos en iniciarse todos los servicios después de la instalación a medida que el sistema realiza una inicialización puntual. Espere este tiempo antes de entrar en el servidor.

10 Para entrar en el servidor de Sentinel Log Manager, utilice la dirección URL especificada en la instalación. La dirección URL se parece a `https://10.0.0.1:8443/novelllogmanager`.

   Para obtener más información sobre la forma de entrar en el servidor, consulte el Capítulo 5, "Acceso a la interfaz Web", en la página 43.

11 Para configurar orígenes de eventos para enviar datos a Sentinel Log Manager, consulte "Configuración de recopilación de datos" en*Sentinel Log Manager 1.1 Administration Guide* (Guía de administración de Sentinel Log Manager 1.1).

3.3 Instalación personalizada

Si elige el método de instalación personalizada, tendrá la opción de instalar el producto con una clave de licencia y además seleccionar una opción de autenticación. Puede configurar la autenticación LDAP para Sentinel Log Manager además de la autenticación de la base de datos. Al configurar Sentinel Log Manager para autenticación LDAP, los usuarios pueden entrar en el servidor utilizando sus credenciales del directorio LDAP.

Si no configura Sentinel Log Manager para autenticación LDAP durante el proceso de instalación, podrá configurar la autenticación después de la instalación, si es necesario. Para configurar la autenticación LDAP después de la instalación, consulte "Autenticación LDAP" en *Sentinel Log Manager 1.1 Administration Guide* (Guía de administración de Sentinel Log Manager 1.1).

1 Descargue e instale los archivos de instalación del sitio de descargas de Novell.

2 Entre como usuario `root` en el servidor en el que desea instalar Sentinel Log Manager.

3 Especifique el siguiente comando para extraer los archivos de instalación del archivo tar:

   `tar xfz <install_filename>`

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

4 Especifique el siguiente comando para ejecutar el guión`install-slm` para instalar Sentinel Log Manager:

   `./install-slm`

5 Para continuar con el idioma deseado, elige el número especificado junto al idioma.

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

6 Lea el acuerdo de licencia e introduzca `sí` o `s` para aceptar la licencia y continuar con la instalación.

   La instalación comienza instalando todos los paquetes RPM. La instalación puede tardar algunos segundos en finalizar.

   La instalación crea un grupo `novell` y un usuario `novell`, si aún no existen.

7 Cuando se le indique, especifique la opción para continuar con la instalación personalizada.

8 Cuando se le indique especificar la opción de clave de licencia, introduzca `2`para especificar la clave de licencia para el producto adquirido.

9 Especifique la clave de licencia y luego pulse Intro.

   Para obtener más información sobre claves de licencia, consulte "Gestión de claves de licencia" en *Sentinel Log Manager 1.1 Administration Guide* (Guía de administración de Sentinel Log Manager 1.1).

10 Especifique la contraseña del usuario administrador.

11 Confirme la contraseña del usuario administrador.

12 Especifique la contraseña para el administrador de bases de datos (dbauser).

13 Confirme la contraseña para el administrador de bases de datos (dbauser).

14 Puede configurar cualquier número de puerto válido dentro del rango especificado para los siguientes servicios:

- Servidor Web
- Servicio de mensajes Java
- Servicio de proxy de cliente
- Servicio de base de datos
- Gateway interno de agente

Si desea continuar con los puertos por defecto, introduzca la opción 6 para continuar con la instalación personalizada.

15 Especifique la opción para autenticar usuarios a través de un directorio LDAP externo.

16 Especifique la dirección IP o el nombre de host del 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 Log Manager.

17 Seleccione uno de los siguientes tipos de conexión LDAP:

- **Conexión LDAP SSL/TSL:** establece una conexión segura entre el navegador y el servidor para la autenticación. Introduzca 1 para especificar esta opción.
- **Conexión LDAP no cifrada:** establece una conexión no cifrada. Introduzca 2 para especificar esta opción.

18 Especifique el número de puerto del servidor LDAP. El puerto SSL por defecto es 636 y el puerto no SSL por defecto es 389.

19 (Condicional) Si selecciona la conexión LDAP SSL/TSL, especifique si el certificado del servidor LDAP está firmado por una autoridad de certificación conocida.

20 (Condicional) Si especificó `n`, especifique el nombre de archivo del certificado de servidor LDAP.

21 Seleccione si desea realizar búsquedas anónimas en el directorio LDAP:

- **Realizar búsquedas anónimas en el directorio LDAP:** el servidor de Sentinel Log Manager realiza una *búsqueda anónima* en el directorio LDAP basándose en el nombre de usuario especificado para recoger el nombre completo de usuario de LDAP correspondiente (DN). Introduzca 1 para especificar este método.
- **No realizar búsquedas anónimas en el directorio LDAP:** introduzca 2 para especificar esta opción.

22 (Condicional) Si seleccionó búsqueda anónima, especifique el atributo de búsqueda y vaya al Paso 25.

23 (Condicional) Si no seleccionó búsqueda anónima en el Paso 21, especifique si va a usar Microsoft Active Directory.

Para Active Directory, el atributo `userPrincipalName` cuyo valor aparece en la forma `nombredeusuario@nombrededominio` se puede usar opcionalmente para autenticar al usuario antes de buscar el objeto de usuario LDAP, sin necesidad de introducir el DN de usuario.

24 (Condicional) Si desea usar el enfoque anterior para Active Directory, especifique el nombre de dominio.

25 Especifique el DN base.

26 Pulse en s para especificar que las opciones facilitadas son correctas, o pulse n para cambiar la configuración.

27 Para entrar en el servidor de Sentinel Log Manager, utilice la dirección URL especificada en la instalación. La dirección URL se parece a `https://10.0.0.1:8443/novelllogmanager`.

Para obtener más información sobre cómo entrar en el servidor, consulte el Capítulo 5, "Acceso a la interfaz Web", en la página 43.

3.4 Instalación silenciosa

La instalación silenciosa o sin supervisión de Sentinel Log Manager resulta útil si desea instalar más de un servidor de Sentinel Log Manager en su implantación. En tal caso, puede registrar los parámetros de instalación durante la primera instalación y luego ejecutar el archivo registrado en todos los demás servidores.

1 Descargue y copie los archivos de instalación del sitio de descargas de Novell.

2 Entre como usuario `root` en el servidor en el que desea instalar Sentinel Log Manager.

3 Especifique el siguiente comando para extraer los archivos de instalación del archivo tar.

```
tar xfz <install_filename>
```

Reemplace <*nombre de archivo_instalación*> con el nombre de archivo de instalación.

4 Especifique el siguiente comando para ejecutar el guión `install-slm` para instalar Sentinel Log Manager en modo silencioso:

```
./install-slm -u responseFile
```

Para obtener más información sobre cómo crear el archivo de respuestas, consulte la Sección 3.2, "Instalación estándar", en la página 26. La instalación continúa con los valores almacenados en el archivo de respuestas.

5 Para entrar en el servidor de Sentinel Log Manager, utilice la dirección URL especificada en la instalación. La dirección URL se parece a `https://10.0.0.1:8443/novelllogmanager`.

Para obtener más información sobre cómo entrar en el servidor, consulte el Capítulo 5, "Acceso a la interfaz Web", en la página 43.

6 Para configurar orígenes de eventos para enviar datos a Sentinel Log Manager, consulte "Configuración de recopilación de datos" en "Sentinel Log Manager 1.1 Administration Guide" (Guía de administración de Sentinel Log Manager 1.1).

3.5 Instalación no root

Si la directiva de su organización no permite ejecutar la instalación completa de Sentinel Log Manager como usuario `root`, es posible ejecutar la mayoría de los pasos de instalación como otro usuario.

1 Descargue y copie los archivos de instalación del sitio de descargas de Novell.

2 Especifique el siguiente comando para extraer los archivos de instalación del archivo tar:

```
tar xfz <install_filename>
```

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

3 Entre como usuario `root` al servidor donde desea instalar Sentinel Log Manager as como usuario `root`.

4 Especifique el siguiente comando:

```
./bin/root_install_prepare
```

Se muestra una lista de comandos que se van a ejecutar con privilegios de usuario root.

Además se crea un grupo `novell` y un usuario `novell`, si aún no existen.

5. Acepte la lista de comandos.

   Se ejecutan los comandos visualizados.

6. Especifique el siguiente comendo para cambiar al nuevo usuario de `novell` diferente de root recién creado: `novell`:

   ```
   su novell
   ```

7. Especifique el siguiente comando:

   ```
   ./install-slm
   ```

8. Para continuar con el idioma deseado, seleccione el número especificado junto al idioma.

   Se muestra el acuerdo de licencia del usuario final en el idioma seleccionado.

9. Lea el acuerdo de licencia del usuario final e introduzca`sí` o `s` para aceptar la licencia y continuar con la instalación.

   La instalación comienza instalando todos los paquetes RPM. La instalación puede tardar algunos segundos en finalizar.

10. Se le indicará que especifique el modo de instalación.

    - Si selecciona continuar con una instalación estándar, siga los pasos 8 a 11 de Sección 3.2, “Instalación estándar”, en la página 26.
    - Si eligió continuar con la instalación personalizada, siga los pasos 8 a 23 de Sección 3.3, “Instalación personalizada”, en la página 27.

    La instalación de Sentinel Log Manager finaliza y se inicia el servidor.

11. Especifique el siguiente comando para cambiar al usuario`root`:

    ```
    su root
    ```

12. Especifique el siguiente comando para finalizar la instalación:

    ```
    ./bin/root_install_finish
    ```

13. Para entrar en el servidor de Sentinel Log Manager, utilice la dirección URL especificada en la producción de instalación. La dirección URL se parece a `https://10.0.0.1:8443/novelllogmanager`.

    Para obtener más información sobre cómo entrar en el servidor, consulte el Capítulo 5, “Acceso a la interfaz Web”, en la página 43.

Instalación del dispositivo

4

Novell Sentinel Log Manager es un dispositivo de software listo para ejecutarse, basado en SUSE Studio que combina un sistema operativo SUSE Linux Enterprise Server (SLES) 11 reforzado con un servicio de actualización integrado en el software de Novell Sentinel Log Manager para ofrecer una experiencia al usuario fácil y fluida además de permitir a los clientes aprovechar su inversión existente. El dispositivo de software puede instalarse en hardware o en un entorno virtual.

4.1 Antes de empezar

- Asegúrese de que se cumplen los requisitos de hardware. Para obtener más información, consulte la Sección 2.1, “Requisitos del hardware”, en la página 17.
- Obtenga su clave de licencia del Centro de atención al cliente de Novell (http://www.novell.com/center) para instalar la versión con licencia.
- Obtenga el código de registro del Centro de atención al cliente de Novell (http://www.novell.com/center) para registrarse para obtener actualizaciones de software.
- Sincronice la hora utilizando el protocolo de tiempo de red (NTP).
- (Condicional) Si tiene previsto usar VMware, asegúrese de que tiene VMware Converter para cargar simultáneamente la imagen al servidor VMware ESX y convertirla a un formato que pueda ejecutarse en el servidor ESX.

4.2 Puertos utilizados

Observe que el dispositivo Novell Sentinel Log Manager utiliza los siguientes puertos para la comunicación, y algunos de ellos están abiertos en el cortafuegos:

4.2.1 Puertos abiertos en el cortafuegos

Tabla 4-1 *Puertos de red utilizados por Sentinel Log Manager*

Puertos	Descripción
TCP 1289	Se utiliza para las conexiones de Novell Audit.
TCP 289	Se reenvía a 1289 para las conexiones de Novell Audit.
TCP 22	Se utiliza para el acceso mediante secure shell al dispositivo Sentinel Log Manager.
UDP 1514	Se utiliza para los mensajes de syslog.
UDP 514	Se reenvía a 1514 para los mensajes de syslog.
TCP 8080	Se utiliza para la comunicación con HTTP. También lo utiliza el dispositivo de Sentinel Log Manager Appliance para el servicio de actualización.
TCP 80	Se redirecciona a 8080 para el servidor Web de Sentinel Log Manager para la comunicación con HTTP. También lo utiliza el dispositivo de Sentinel Log Manager para el servicio de actualización.
TCP 8443	Se utiliza para la comunicación de HTTPS. También lo utiliza el dispositivo Sentinel Log Manager para el servicio de actualización.
TCP 1443	Se utiliza para los mensajes de syslog con SSL cifrado.
TCP 443	Se reenvía a 8443 para el servidor Web de Sentinel Log Manager para la comunicación de HTTPS. También lo utiliza el dispositivo de Sentinel Log Manager Appliance para el servicio de actualización.
TCP 61616	Se utiliza para la comunicación entre los gestores de recopiladores y el servidor.
TCP 10013	Lo utiliza el proxy SSL de la interfaz del usuario de Gestión de orígenes de eventos.
TCP 54984	Lo utiliza la consola de gestión del dispositivo de Sentinel Log Manager (WebYaST).
TCP 1468	Se utiliza para los mensajes de syslog.

4.2.2 Puertos utilizados a nivel local

Tabla 4-2 *Puertos utilizados para la comunicación a nivel local*

Puertos	Descripción
TCP 61617	Se utiliza para la comunicación local entre el servidor Web y el servidor.

Puertos	Descripción
TCP 5556	Se utiliza en la interfaz de retrobucle para la comunicación interna con el servidor de_gateway_interno y el gateway_interno. Se utiliza para la comunicación entre el motor de agente y el gestor de recopiladores.
TCP 5432	Se utiliza para la base de datos PostgreSQL. No es necesario abrir este puerto por defecto. No obstante, si crea informes utilizando Sentinel SDK, entonces deberá abrir este puerto. Para obtener más información, consulte el sitio Web de SDK de módulos auxiliares (plug-in) de Sentinel (http://developer.novell.com/wiki/index.php?title=Develop_to_Sentinel).
Dos puertos TCP adicionales seleccionados aleatoriamente	Se utilizan para la comunicación interna entre el motor de agentes y el gestor de recopiladores.
TCP 8005	Se utiliza para la comunicación interna con los procesos Tomcat.
TCP 32000	Se utiliza para la comunicación interna entre el motor de agentes y el gestor de recopiladores.

4.3 Instalación del dispositivo VMware

Para ejecutar la imagen del dispositivo desde el servidor VMware ESX, importe e instale la imagen del dispositivo en el servidor.

1. Descargue el archivo de instalación del dispositivo VMware.

   El archivo correcto del dispositivo VMware tiene `vmx` en el nombre del archivo. Por ejemplo, `Sentinel_Log_Manager_1.1.0.0_64_VMX.x86_64-0.777.0.vmx.tar.gz`
2. Establezca un almacén de datos de ESX en el que se pueda instalar la imagen del dispositivo.
3. Entre como usuario Administrador en el servidor en el que desea instalar el dispositivo.
4. Especifique el siguiente comando para extraer la imagen comprimida del dispositivo desde el equipo donde está instalado VM Converter:

   `tar zxvf <archivo_instalación>`

   Reemplace <*archivo_instalación*> por el nombre real del archivo.
5. Para importar la imagen de VMware al servidor ESX, utilice el VMware Converter y siga las instrucciones en pantalla del asistente de instalación.
6. Entre en el equipo del servidor ESX.
7. Seleccione la imagen de VMware importada del dispositivo y haga clic en el icono de *encendido*.
8. Seleccione el idioma deseado y luego, haga clic en *Siguiente*.
9. Seleccione la disposición del teclado y haga clic en *Siguiente*.
10. Lea y acepte el acuerdo de licencia del software de Novell SUSE Enterprise Server.
11. Lea y acepte el acuerdo de licencia del usuario final de Novell Sentinel Log Manager.

12 En la pantalla Nombre de host y Nombre de dominio, especifique los valores correspondientes. Asegúrese de que ha seleccionado la opción *Write hostname to /etc/hosts* (Escribir nombre de host en /etc/hosts).

13 Seleccione *Siguiente*. Se guardará la información configurada de nombre de host.

14 Realice una de las siguientes acciones:

- Para usar los ajustes de conexión de red actuales, seleccione la opción *Use the following configuration* (Usar la siguiente configuración) en la pantalla de *Network Configuration II* (Configuración de red II).
- Para cambiar los ajustes de conexión de red, seleccione la opción para *Cambiar*.

15 Establezca la fecha y la hora y haga clic en *Siguiente*, seguido de la opción para *Finalizar*.

Nota: Para cambiar la configuración de NTP después de la instalación utilice YaST en la línea de comandos del dispositivo. Puede usar WebYast para cambiar la fecha y la hora, pero no la configuración de NTP.

Si la hora parece no estar sincronizada inmediatamente después de la instalación, ejecute el siguiente comando para reiniciar NTP:

```
rcntp restart
```

---

16 Defina la contraseña `root` de Novell SUSE Enterprise Server, y luego haga clic en *Siguiente*.

17 Defina la contraseña `root` y luego haga clic en *Siguiente*.

18 Defina la contraseña de administrador de Sentinel Log Manager y la contraseña dbauser y luego haga clic en *Siguiente*.

19 Seleccione *Siguiente*. Se guardan los ajustes de conexiones de red.

La instalación continúa y finaliza. Anote la dirección IP del dispositivo que aparece en la consola.

20 Pase a la Sección 4.6, “Configuración posterior a la instalación de la aplicación”, en la página 37.

4.4 Instalación del dispositivo Xen

1 Descargue y copie el archivo de instalación del dispositivo virtual Xen a `/var/lib/xen/images`.

El nombre de archivo correcto del dispositivo virtual Xen contiene `xen`. Por ejemplo, `Sentinel_Log_Manager_1.1.0.0_64_Xen.x86_64-0.777.0.xen.tar.gz`

2 Especifique el siguiente comando para desempaquetar el archivo:

```
tar -xvzf <install_file>
```

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

3 Cambie al nuevo directorio de instalación. El directorio tiene los siguientes archivos:

- archivo de imagen <*nombre_archivo*>`.raw`
- archivo <*nombre_archivo*>`.xenconfig`

4 Abra el archivo <*nombre_archivo*>`.xenconfig` utilizando el editor de texto.

5 Modifique el archivo de la siguiente manera:

Especifique la vía completa al archivo `.raw` en el ajuste `disk` (disco).

Especifique el ajuste de puente para la configuración de red. Por ejemplo, `"bridge=br0"` o `"bridge=xenbr0"`.

Especifique los valores para `name` (nombre) y `memory` (memoria).

Por ejemplo:

```
# -*- mode: python; -*-
name="Sentinel_Log_Manager_1.1.0.0_64"
memory=4096
disk=[ "tap:aio:/var/lib/xen/images/Sentinel_Log_Manager_1.1.0.0_64_Xen-
0.777.0/Sentinel_Log_Manager_1.1.0.0_64_Xen.x86_64-0.777.0.raw,xvda,w" ]
vif=[ "bridge=br0" ]
```

6 Después de modificar el archivo *<nombredearchivo>*`.xenconfig`, especifique el siguiente comando para crear la máquina virtual:

```
xm create <nombre_archivo>.xenconfig
```

7 (Opcional) Para verificar si se ha creado la máquina virtual, especifique el siguiente comando:

xm list

La máquina virtual aparece en la lista.

Por ejemplo, si ha configurado `name="Sentinel_Log_Manager_1.1.0.0_64"`en el archivo `.xenconfig`, entonces la máquina virtual aparece con ese nombre.

8 Para iniciar la instalación, especifique el siguiente comando:

```
xm console <nombre vm>
```

Reemplace <*nombre_vm*> por el nombre especificado en el ajuste de nombre en el archivo `.xenconfig`, que también es el valor devuelto en el paso 7. Por ejemplo:

```
xm console Sentinel_Log_Manager_1.1.0.0_64
```

9 Seleccione el idioma deseado y luego haga clic en *Siguiente*.

10 Seleccione la disposición del teclado y haga clic en*Siguiente*.

11 Lea y acepte el acuerdo de licencia de software de Novell SUSE Enterprise Server.

12 Lea y acepte el acuerdo de licencia del usuario final de Novell Sentinel Log Manager.

13 En la pantalla Nombre de host y Nombre de dominio, especifique los valores correspondientes. Asegúrese de que esté seleccionada la opción *Write hostname to /etc/hosts* (Escribir nombre de host en /etc/hosts).

14 Seleccione *Siguiente*. Se guardará la configuración del nombre de host.

15 Realice una de las siguientes acciones:

- Para usar los ajustes de conexión de red actuales, seleccione la opción *Use the following configuration* (Usar la siguiente configuración) de la pantalla de *Network Configuration II* (Configuración de red II).
- Para cambiar los ajustes de conexión de red, seleccione la opción para *Cambiar*.

16 Seleccione la fecha y la hora y haga clic en *Siguiente*, y luego en *Finalizar*

Nota: Para cambiar la configuración de NTP después de la instalación, utilice YaST desde la línea de comandos del dispositivo. Puede usar WebYast para cambiar la fecha y la hora, pero no la configuración de NTP.

Si la hora parece no estar sincronizada inmediatamente después de la instalación, ejecute el siguiente comando para reiniciar NTP:

```
rcntp restart
```

17 Defina la contraseña `root` de Novell SUSE Enterprise Server y luego haga clic en *Siguiente*.

18 Defina la contraseña de administrador de Sentinel Log Manager y la contraseña de dbauser, y luego haga clic en *Siguiente*.

La instalación continúa y finaliza. Anote la dirección IP del dispositivo que se muestra en la consola.

19 Pase a la Sección 4.6, “Configuración posterior a la instalación de la aplicación”, en la página 37.

4.5 Instalación del dispositivo en hardware

Antes de instalar el dispositivo en el hardware, asegúrese de que la imagen de disco ISO del dispositivo se ha descargado desde el sitio de asistencia, y que se ha desempaquetado y está disponible en un DVD.

1 Arranque el equipo físico de la unidad de DVD con el DVD.

2 Siga las instrucciones en pantalla del asistente de instalación.

3 Ejecute la imagen del dispositivo en el DVD seleccionando la entrada superior del menú de arranque.

4 Lea y acepte el acuerdo de licencia del software de Novell SUSE Enterprise Server.

5 Lea y acepte el acuerdo de licencia del usuario final de Novell Sentinel Log Manager.

6 Seleccione *Siguiente*.

7 En la pantalla Nombre de host y Nombre de dominio, especifique los valores correspondientes.

Asegúrese de que está seleccionada la opción *Write hostname to /etc/hosts* (Escribir el nombre de host en /etc/hosts).

8 Seleccione *Siguiente*. Se guarda la configuración del nombre de host.

9 Realice una de las siguientes acciones:

- Para usar los ajustes de conexión de red actuales, seleccione la opción *Use the following configuration* (Usar la siguiente configuración) en la pantalla Network Configuration II (Configuración de red II).
- Para cambiar los ajustes de conexión de red, seleccione la opción para *Cambiar*.

10 Seleccione *Siguiente*. Se guardarán los ajustes de conexión de red.

11 Establezca la fecha y la hora y luego haga clic en *Siguiente*.

Nota: Para cambiar la configuración de NTP después de la instalación, utilice YaST desde la línea de comandos del dispositivo. Puede usar WebYast para cambiar la fecha y la hora, pero no la configuración de NTP.

Si la hora parece no estar sincronizada inmediatamente después de la instalación, ejecute el siguiente comando para reiniciar NTP:

```
rcntp restart
```

12 Defina la contraseña `root` y luego haga clic en *Siguiente*.

13 Defina la contraseña de administrador de Sentinel Log Manager y la contraseña de dbauser, y luego haga clic en *Siguiente*.

14 Introduzca el nombre de usuario y la contraseña en la consola para entrar en el dispositivo.

   El valor por defecto del nombre de usuario es`root` y la contraseña es `password`.

15 Para instalar el dispositivo en el servidor físico, ejecute el siguiente comando:

```
/sbin/yast2 live-installer
```

   La instalación continúa y finaliza. Anote la dirección IP del dispositivo que se muestra en la consola.

16 Pase a la Sección 4.6, “Configuración posterior a la instalación de la aplicación”, en la página 37.

4.6 Configuración posterior a la instalación de la aplicación

Para entrar en la consola Web del dispositivo e inicializar el software:

1 Abra un navegador Web y entre en https://*<dirección IP>*:*8443*. Se mostrará la página Web de Sentinel Log Manager.

   Se muestra la dirección IP del dispositivo en la consola del dispositivo después de que finalice la instalación y se reinicie el servidor.

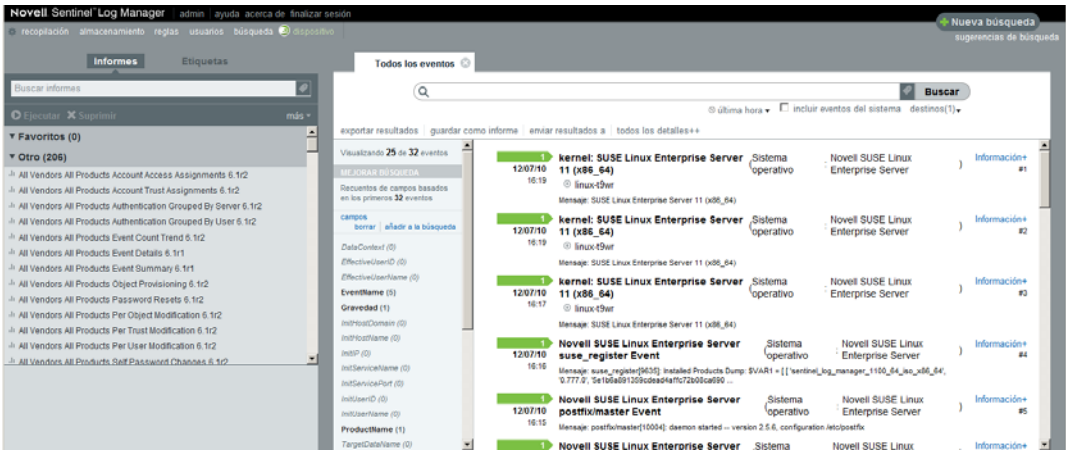
2 Puede configurar el dispositivo Sentinel Log Manager para el almacenamiento y la recopilación de datos. Para obtener más información sobre la configuración del dispositivo, consulte *Sentinel Log Manager 1.1 Administration Guide* (Guía de administración de Sentinel Log Manager 1.1).

3 Para registrarse para recibir actualizaciones, consulte la Sección 4.8, “Registro para recibir actualizaciones”, en la página 40.

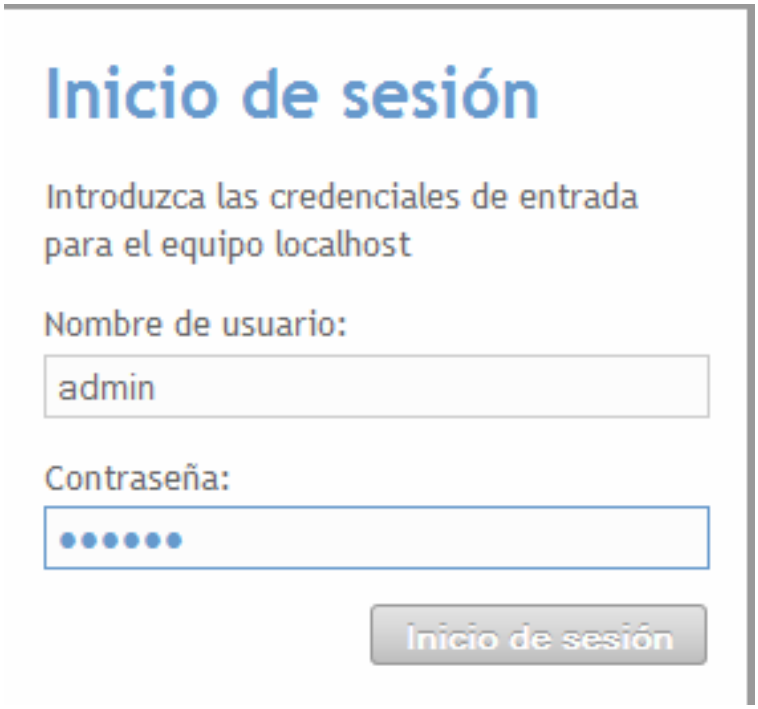
4.7 Configuración de WebYaST

La interfaz del usuario del dispositivo Novell Sentinel Log Manager está equipada con WebYaST. WebYaST es una consola remota basada en la Web para el control de dispositivos basada en SUSE Linux Enterprise. Puede acceder, configurar y supervisar los dispositivos de Sentinel Log Manager mediante WebYaST. El siguiente procedimiento describe brevemente los pasos necesarios para configurar WebYaST. Para obtener más información acerca de la configuración detallada, consulte WebYaST User Guide (http://www.novell.com/documentation/webyast/) (Guía del usuario de WebYaST).

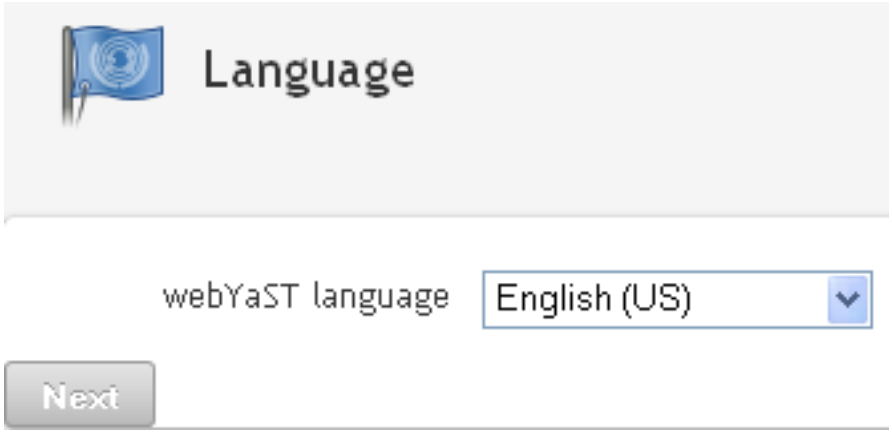
1 Entre en el dispositivo de Sentinel Log Manager.



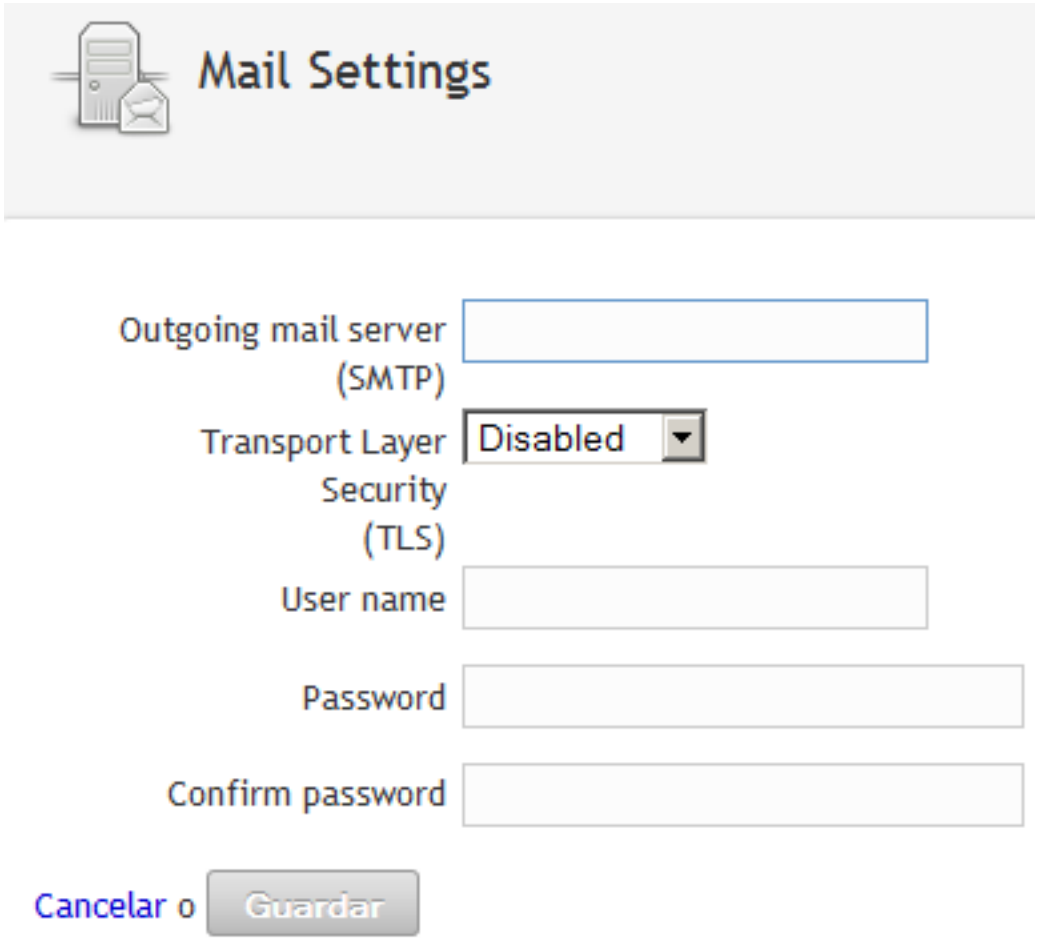
2 Haga clic en *Appliance* (Dispositivo).



3 Especifique las credenciales del sistema y luego haga clic en *Login* (Entrar).



4 Elija el idioma deseado y luego haga clic en*Siguiente*.



5 Especifique los detalles para configurar el servidor de correo y luego haga clic para *Guardar*. Aparecerá la página de registro.

6 Configure el servidor de Sentinel Log Manager para recibir actualizaciones tal como se describió en Sección 4.8, “Registro para recibir actualizaciones”, en la página 40.

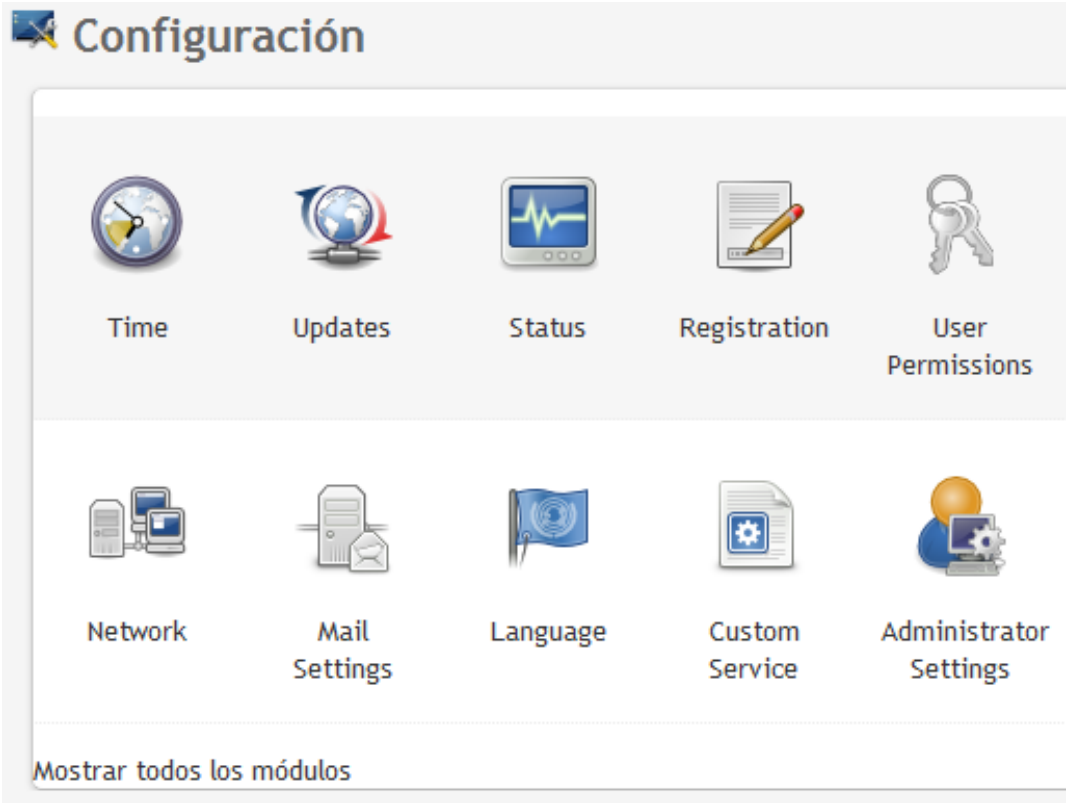
7 Haga clic en *Siguiente* para finalizar la instalación inicial.

4.8 Registro para recibir actualizaciones

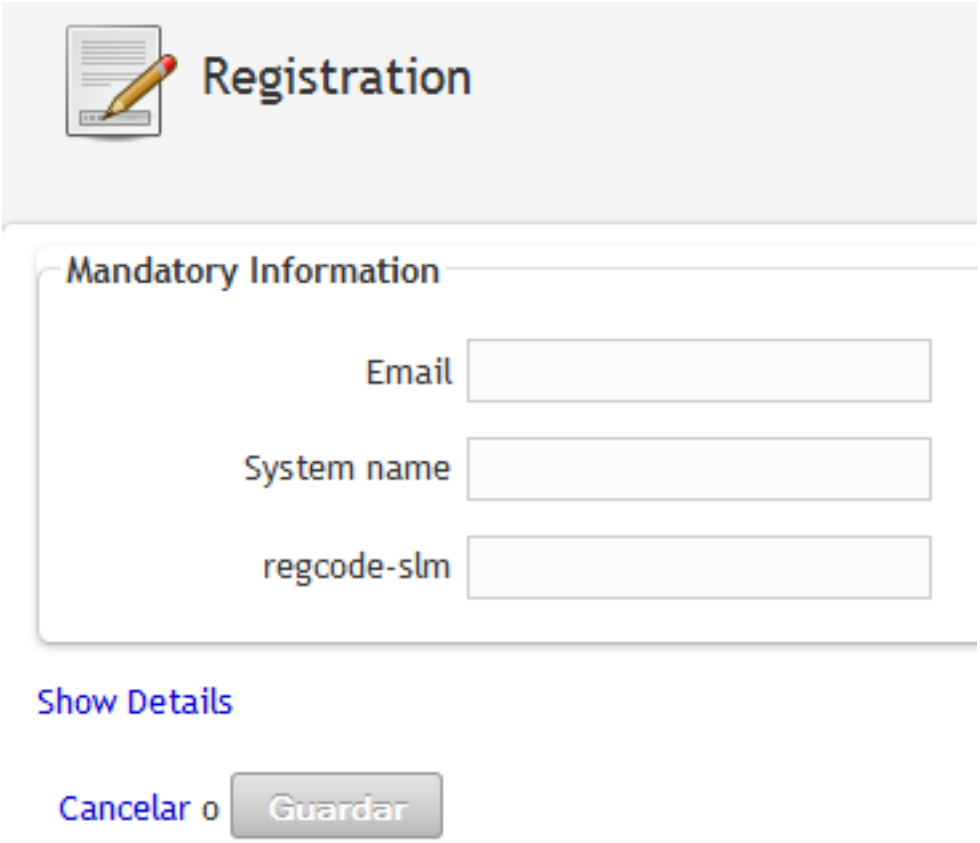
1 Entre en el dispositivo de Sentinel Log Manager.

Se mostrará la interfaz del usuario en la Web de Sentinel Log Manager.

2 Haga clic en *Appliance* (Dispositivo) para lanzar WebYaST.



3 Haga clic en *Registration* (Registro).

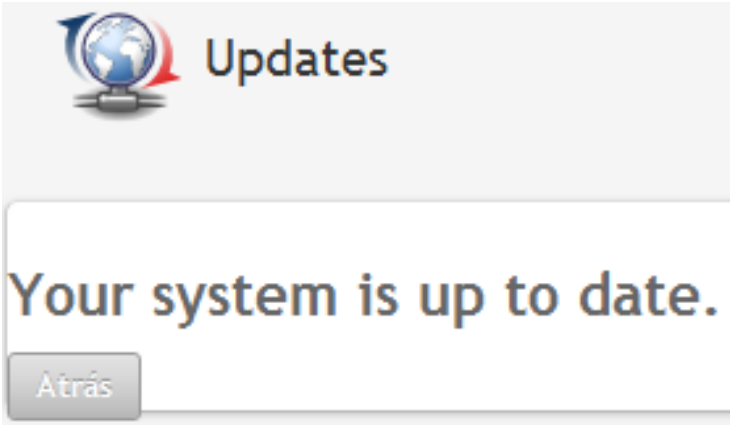


4 Especifique el código de registro del dispositivo.

5 Haga clic en *Guardar*.

6 Para comprobar si existen actualizaciones, haga clic en *Update* (Actualizar).

La página resultante indica si existen actualizaciones.



Acceso a la interfaz Web

5

El usuario administrador creado durante la instalación puede entrar en la interfaz Web para configurar y utilizar Sentinel Log Manager:

1. Abra un navegador Web compatible. Para obtener más información, consulte Sección 2.3, “Navegadores compatibles”, en la página 21.
2. Especifique la dirección URL de la página de Novell Sentinel Log Manager (por ejemplo, `https://10.0.0.1:8443/novelllogmanager`) y luego pulse Intro.
3. (Condicional) La primera vez que entre en Sentinel Log Manager, se le pedirá que acepte un certificado. Al aceptar el certificado se muestra la página de inicio de sesión de Sentinel Log Manager.

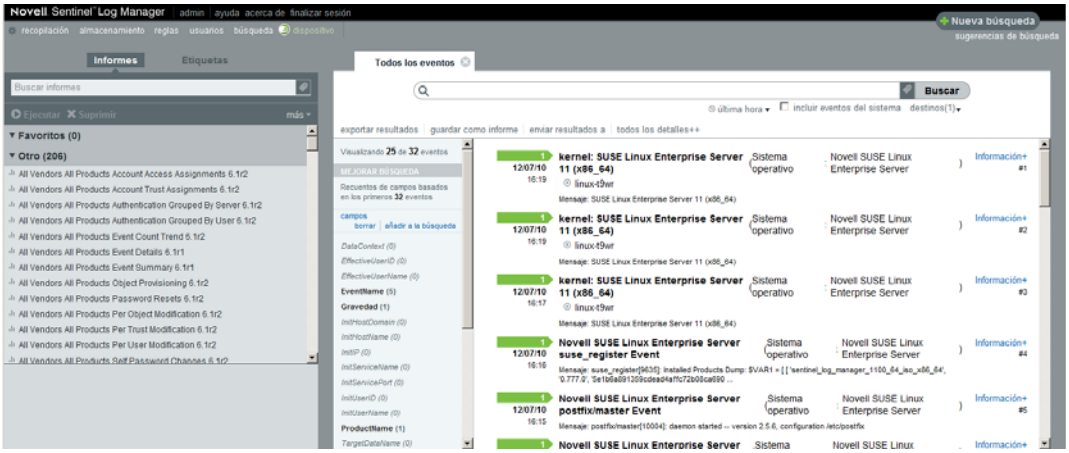
4 Especifique el nombre de usuario y la contraseña del administrador de Sentinel Log Manager.

5 Elija el idioma para la interfaz de Sentinel Log Manager.

La interfaz del usuario de Sentinel Log Manager está disponible en inglés, portugués, francés, italiano, alemán, español, japonés, chino tradicional y chino simplificado.

6 Haga clic en *Entrar*.

Se muestra la interfaz basada en la Web de Novell Sentinel Log Manager.



Actualización de Sentinel Log Manager

6

Puede actualizar Novell Sentinel Log Manager de la versión 1.0.0.4 o superior a Sentinel Log Manager 1.1 mediante el guión de actualización.

6.1 Actualización de 1.0 a 1.1

1. Si su versión del servidor de Sentinel Log Manager es anterior a la versión 1.0.0.4., primero deberá actualizar a la versión 1.0.0.4 o superior.
2. Descargue y copie los archivos de instalación del sitio de descargas de Novell.
3. Entre como usuario `root` en el servidor en el que desea instalar Sentinel Log Manager.
4. Especifique el siguiente comando para detener el servidor de Sentinel Log Manager:

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

   Por ejemplo, `/opt/novell/sentinel_log_mgr_1.0_x86-64/bin/server.sh stop`
5. Especifique el siguiente comando para extraer los archivos de instalación del archivo tar:

   `tar xfz <install_filename>`

   Reemplace <*nombre de archivo_instalación*> por el nombre real del archivo de instalación.
6. Especifique el siguiente comando para ejecutar el guión `install-slm` para actualizar Sentinel Log Manager:

   `./install-slm`
7. Para continuar con el idioma deseado, seleccione el número especificado junto al idioma.

   El acuerdo de licencia de usuario final se muestra en el idioma seleccionado.
8. Lea la licencia del usuario final e introduzca `sí` o `s`, para aceptar la licencia y continuar con la instalación.
9. El guión de instalación detecta que ya existe una versión del producto más antigua y le indica que debe especificar si desea actualizar el producto. Si pulsa n, la instalación se cancela. Para continuar con la actualización, pulse s.

   La instalación comienza instalando todos los paquetes RPM. Esta instalación puede tardar unos segundos en finalizar.

   La instalación existente de Sentinel Log Manager 1.0 permanece intacta, con las siguientes excepciones:

   - Si el directorio de datos de 1.0 (Por ejemplo, `/opt/novell/sentinel_log_manager_1.0_x86-64/data`) y el directorio de datos de 1.1 (Por ejemplo, `/var/opt/novell/sentinel_log_mgr/data`) se encuentran en el mismo sistema de archivos, entonces los subdirectorios `<1.0>/data/eventuate` y `<1.0>/data/rawdata` se transfieren a la ubicación de 1.1 porque los directorios de datos de

eventos y datos en bruto suelen ser muy grandes. Si los directorios de datos de 1.0 y 1.1 se encuentran en sistemas de archivos diferentes, entonces los subdirectorios de datos de eventos y datos en bruto se copian a la ubicación de 1.1, y los archivos de 1.0 permanecen intactos.

- Si el directorio de datos de 1.0 (Por ejemplo, `/opt/novell/sentinel_log_mgr_1.0_x86-64`) se encuentra en un sistema de archivos montado independiente y no hay espacio suficiente en el sistema de archivos que contiene el directorio de datos de 1.1 (`/var/opt/novell/sentinel_log_mgr/data`) entonces puede dejar que el instalador vuelva a montar el sistema de archivos de la ubicación de 1.0 a la ubicación de 1.1. También se actualiza una entrada de `/etc/fstab`. Si decide no permitir que el instalador vuelva a montar el sistema de archivos existente, la actualización se cerrará. Entonces podrá crear espacio suficiente en el sistema de archivos para el directorio de datos de 1.1.

10 Cuando la instalación de Sentinel Log Manager 1.1 finalice correctamente y el servidor esté operativo, entonces debe especificar el siguiente comando para eliminar manualmente el directorio de Sentinel Log Manager 1.0:

`rm -rf /opt/novell/slm_1.0_install_directory`

Por ejemplo:

`rm -rf /opt/novell/sentinel_log_mgr_1.0_x86-64`

Al eliminar el directorio de instalación se suprime de forma permanente la instalación de Sentinel Log Manager 1.0.

6.2 Actualización del gestor de recopiladores

1 Entre en Sentinel Log Manager como administrador.

2 Seleccione *recopilación* > *Avanzado*.

3 Haga clic en el enlace*Descargar instalador*. en la sección Instalador de actualización del gestor de recopiladores.

Se muestra una ventana con opciones para abrir o guardar el archivo `scm_upgrade_installer.zip` en el equipo local. Guarde el archivo.

4 Copie el archivo en una ubicación temporal.

5 Extraiga el contenido del archivo `.zip`.

6 Como propietario de la instalación del gestor de recopiladores, ejecute uno de los siguientes archivos de actualización dependiendo de su sistema operativo:

- Para actualizar el gestor de recopiladores de Windows, ejecute `service_pack.bat`.
- Para actualizar el gestor de recopiladores de Linux, ejecute `service_pack.sh`.

7 Siga las instrucciones que aparecen en pantalla para finalizar la instalación.

8 Reinicie el equipo.

6.3 Migración del dispositivo 1.0 a 1.1

Si ha instalado Sentinel Log Manager 1.0 y desea migrar a Sentinel Log Manager Appliance 1.1, siga los pasos a continuación para migrar los datos y la configuración

1. (Condicional) Si la versión de Sentinel Log Manager es anterior a 1.0 hotfix 4, actualícela a Sentinel Log Manager 1.0 hotfix 5, que representa el último hotfix disponible. Descargue el hotfix del sitio de descargas de parches de Novell (http://download.novell.com/protected/Summary.jsp?buildid=VgZ3aerzjYc~).

   Nota: Debe ser un usuario registrado para poder descargar parches. Si no se ha registrado, haga clic para registrarse y crear una cuenta de usuario en el sitio de descarga de parches.

2. Actualice a Sentinel Log Manager 1.1. Para obtener más información, consulte la Sección 6.1, “Actualización de 1.0 a 1.1”, en la página 47.

3. Especifique el siguiente comando para cambiar el usuario `novell`:

   ```
   su -novell
   ```

4. Especifique el siguiente comando para cambiar al directorio `/bin`:

   ```
   cd /opt/novell/sentinel_log_mgr/bin
   ```

5. Especifique el siguiente comando para realizar una copia de seguridad completa de los datos y la configuración de Sentinel Log Manager 1.1.

   ```
   ./backup_util.sh -m backup -c -e -l -r -s -w -f $APP_HOME/data/
   <backupfilename>
   ```

   Reemplace <*nombrearchivodecopiadeseguridad*> por un nombre de archivo para almacenar los datos de copia de seguridad.

   Para obtener más información sobre cómo realizar una copia de seguridad de los datos, consulte“Copia de seguridad y restauración de datos”.

6. Instale Sentinel Log Manager Appliance 1.1 en un equipo separado. Para obtener más información, consulte el Capítulo 4, “Instalación del dispositivo”, en la página 31.

7. Copie el archivo que contiene los datos guardados de copia de seguridad en el dispositivo Sentinel Log Manager 1.1 recién instalado.

8. Especifique el siguiente comando:

   ```
   chown novell:novell <backfupfilename>
   ```

9. Especifique el siguiente comando para cambiar al directorio `/bin`:

   ```
   cd /opt/novell/sentinel_log_mgr/bin
   ```

10. Especifique el siguiente comando para restaurar por completo los datos copiados en archivo de seguridad de la aplicación Sentinel Log Manager 1.1:

    ```
    ./backup_util.sh -m restore -f $APP_HOME/data/<backupfilename>
    ```

    Para obtener más información, consulte “Copia de seguridad y restauración de datos”.

Instalación de gestores de recopiladores adicionales

7

Los gestores de recopiladores gestionan toda la recopilación y análisis de datos de Novell Sentinel Log Manager. El proceso de instalación de Sentinel Log Manager instala un gestor de recopiladores por defecto en el servidor de Sentinel Log Manager. No obstante, puede instalar varios gestores de recopiladores en una configuración distribuida.

7.1 Antes de empezar

- Asegúrese de que el hardware y el software cumplen los requisitos mínimos mencionados en el Capítulo 2, “Requisitos del sistema”, en la página 17.
- Sincronice la hora utilizando el protocolo de tiempo de red (NTP).
- Un gestor de recopiladores requiere conectividad de red con el puerto de bus de mensajes (61616) en el servidor Sentinel Log Manager. Antes de instalar el gestor de recopiladores, asegúrese de que todos los ajustes del cortafuegos y de red puedan comunicarse a través de este puerto.

7.2 Ventajas de los gestores de recopiladores adicionales

La instalación de más de un gestor de recopiladores en una red distribuida aporta varias ventajas:

- **Mejora del rendimiento del sistema:** los gestores de recopiladores adicionales pueden analizar y procesar los datos de eventos en un entorno distribuido, incrementando de esta manera el rendimiento del sistema.
- **Mayor seguridad de los datos y menores requisitos de ancho de banda de la red:** si los gestores de recopiladores se encuentran ubicados conjuntamente con los orígenes de eventos, entonces puede aplicarse el filtrado, el cifrado y la compresión de datos en el origen.
- **Capacidad de recopilar datos de otros sistemas operativos:** por ejemplo, puede instalar un gestor de recopiladores en Microsoft Windows para habilitar la recopilación de datos a través del protocolo WMI.
- **Almacenamiento de archivos en el caché:** al habilitar el almacenamiento de archivos en el caché, el gestor de recopiladores remoto puede almacenar en el caché grandes cantidades de datos mientras que el servidor está ocupado temporalmente archivando eventos o procesando un aumento del número de eventos. Esta función es una ventaja para los protocolos, como syslog, que no admiten el almacenamiento en caché de forma original.

7.3 Instalación de gestores de recopiladores adicionales

1. Entre en Sentinel Log Manager como administrador.
2. Seleccione *recopilación* > *Avanzado*.
3. Haga clic en el enlace *Descargar instalador* en la sección del instalador del Gestor de recopiladores.

   Se muestra una ventana con opciones para abrir o guardar el archivo `scm_installer.zip` en el equipo local. Guarde el archivo.
4. Copie y extraiga el archivo a la ubicación donde desea instalar el gestor de recopiladores.
5. Ejecute uno de los siguientes archivos de instalación dependiendo del sistema operativo:
   - Para instalar el gestor de recopiladores en un sistema Windows, ejecute `setup.bat`.
   - Para instalar el gestor de recopiladores en un sistema Linux, ejecute `setup.sh`.
6. Seleccione un idioma y haga clic en *Aceptar*.

   Se muestra el asistente de instalación.
7. Haga clic en Aceptar.
8. Lea y acepte el acuerdo de licencia y luego haga clic en *Siguiente*.
9. Puede continuar con el directorio de instalación por defecto o examinar y seleccionar el directorio y luego hacer clic en *Siguiente*.
10. Deje el puerto de bus de mensajes por defecto (61616) sin modificar y especifique el nombre de host del servidor de comunicaciones; luego haga clic en *Siguiente*.
11. Haga clic en *Siguiente* para continuar con la Configuración automática de memoria (256 Megabytes).

    Se muestra un resumen de la instalación.
12. Haga clic en *Instalar*.
13. Especifique el nombre de usuario y la contraseña del gestor de recopiladores.

    Nota: El nombre de usuario y la contraseña se almacenan en el archivo`/etc/opt/novell/sentinel_log_mgr/config/activemqusers.properties` ubicado en el servidor de Sentinel Log Manager.

    ---
14. Acepte el certificado de forma permanente cuando se le indique.
15. Haga clic en *Finalizar* para terminar la instalación de
16. Reinicie el equipo.

Desinstalación de Sentinel Log Manager

8

En esta sección se analizan los procedimientos para desinstalar el servidor de Novell Sentinel Log Manager y el Gestor de recopiladores.

8.1 Desinstalación del dispositivo

Si desea retener los datos del Gestor de registros, entonces deberá hacer una copia de seguridad de los datos antes de desinstalar el dispositivo, de manera que pueda restaurar los datos más tarde. Para obtener más información, consulte “Copia de seguridad y restauración de datos” en *Sentinel Log Manager 1.1 Administration Guide* (Guía de administración de Sentinel Log Manager 1.1).

Si no necesita retener ningún dato, utilice los siguientes procedimientos para desinstalar el dispositivo:

- **Dispositivo VMware ESX:** si la máquina virtual está dedicada a Novell Sentinel Log Manager y si no necesita retener ningún dato, suprima la máquina virtual para desinstalar el dispositivo virtual del gestor de registros.
- **Dispositivo Xen:** si la máquina virtual Xen está dedicada a Novell Sentinel Log Manager y si no necesita retener ningún dato, suprima la máquina virtual para desinstalar el dispositivo virtual del gestor de registros.
- **Dispositivo de hardware:** si el sistema está dedicado a Novell Sentinel Log Manager y si no necesita retener ningún dato, reformatee el disco duro para desinstalar el gestor de registros en un equipo físico.

8.2 Desinstalación de un sistema SLES 11 existente

1. Entre en Sentinel Log Manager como usuario `root`.
2. Para ejecutar el guión de desinstalación, ejecute el siguiente comando:

   ```
   /opt/novell/sentinel_log_mgr/setup/uninstall-slm
   ```
3. Cuando se le indique que vuelva a confirmar que desea continuar con la desinstalación, pulse s.

   El servidor de Sentinel Log Manager se detiene primero y después se desinstala.

8.3 Desinstalación del gestor de recopiladores

En esta sección se describen los procedimientos necesarios para desinstalar el gestor de recopiladores instalado en equipos Windows o Linux.

8.3.1 Desinstalación del gestor de recopiladores en Linux

1. Entre a la sesión como usuario `Root`.
2. En el equipo donde está instalado el gestor de recopiladores, desplácese a la siguiente ubicación:

   ```
   $ESEC_HOME/_unist
   ```
3. Ejecute el comando siguiente:

   ```
   ./uninstall.bin
   ```
4. Seleccione un idioma y haga clic en *Aceptar*.
5. Haga clic en *Siguiente* en el asistente de instalación.
6. Seleccione las funciones que desea desinstalar y luego haga clic en *Siguiente*.
7. Detenga todas las aplicaciones de Sentinel Log Manager que estén en ejecución, y luego haga clic en *Siguiente*.
8. Haga clic en *Desinstalar*.
9. Haga clic en *Finalizar*.
10. Seleccione *Reiniciar el sistema y haga* clic en *Finalizar*.

8.3.2 Desinstalación del gestor de recopiladores en Windows

1. Entre como administrador.
2. Detenga el servidor de Sentinel Log Manager.
3. Seleccione Inicio > Ejecutar.
4. Especifique lo siguiente:

   ```
   %Esec_home%\_uninst
   ```
5. Haga doble clic en `uninstall.exe` para ejecutarlo.
6. Seleccione un idioma y haga clic en *Aceptar*.

   Se muestra el asistente de instalación.
7. Haga clic en Siguiente.
8. Seleccione las funciones que desea desinstalar y luego haga clic en *Siguiente*.
9. Detenga todas las aplicaciones de Sentinel Log Manager que estén en ejecución y luego haga clic en *Siguiente*.
10. Haga clic en *Desinstalar*.
11. Haga clic en *Finalizar*.
12. Seleccione *Reiniciar el sistema* y haga clic en *Finalizar*.

8.3.3 Limpieza manual de directorios

Linux

1. Entre en el equipo donde desinstaló en gestor de recopiladores como usuario `root`.
2. Detenga todos los procesos de Sentinel Log Manager.
3. Elimine el contenido de `/opt/novell/sentinel6`

Windows

1. Entre en el equipo donde desinstaló el gestor de recopiladores como administrador.
2. Suprima la carpeta `%CommonProgramFiles%\InstallShield\Universal` y todo su contenido.
3. Suprima la carpeta `%ESEC_HOME%` . La carpeta es por defecto `C:\Program Files\Novell\Sentinel6`.

Solución de problemas de instalación

A

En estas secciones se enumeran los problemas que podrían ocurrir durante la instalación y el procedimiento para solucionar dichos problemas.

A.1 La instalación falló debido a una configuración de red incorrecta

Durante el primer arranque, si el instalador detecta que los ajustes de red son incorrectos, se muestra un mensaje de error. Si la red no está disponible, falla la instalación de Sentinel Log Manager en el dispositivo.

Para solucionar este problema, configure adecuadamente los ajustes de red. Al verificar la configuración, el comando `ifconfig` debe devolver una dirección IP válida y el comando `hostname -f` debe devolver un nombre de host válido.

A.2 Problemas para configurar VMware Player 3 en SLES 11

Quizá aparezca el siguiente error al intentar configurar la red con VMware Player 3 en SLES 11:

```
Jan 12 14:57:34.761: vmx| VNET: MACVNetPortOpenDevice: Ethernet0: can't open
vmnet device (No such device or address)
Jan 12 14:57:34.761: vmx| VNET: MACVNetPort_Connect: Ethernet0: can't open
data fd
Jan 12 14:57:34.761: vmx| Msg_Post: Error
Jan 12 14:57:34.761: vmx| [msg.vnet.connectvnet] Could not connect Ethernet0
to virtual network "/dev/vmnet0". More information can be found in the
vmware.log file.
Jan 12 14:57:34.761: vmx|[msg.device.badconnect] Failed to connect virtual
device Ethernet0.
Jan 12 14:57:34.761: vmx| --
```

Este error indica que puede que otra máquina virtual haya abierto el archivo VMX. Para solucionar este problema, debe actualizar la dirección MAC del archivo VMX de la siguiente manera:

1. Abra el archivo VMX en un editor de texto.
2. Copie la dirección MAC del campo `ethernet0.generatedAddress`.
3. Abra el archivo `/etc/udev/rules.d/70-persistent-net.rules` del sistema operativo invitado.

4 Comente la línea original, y luego escriba una línea `SUBSYSTEM` de la siguiente manera:

```
SUBSYSTEM=="net", DRIVERS=="?*", ATTRS{address}==<MAC address>,
NAME="eth0"
```

5 Reemplace <*dirección MAC*> por la dirección MAC que copió en el paso 2Paso 2.

6 Guarde y cierre el archivo.

7 Abra la máquina virtual en VMware Player.

A.3 Actualización del gestor de registros instalado como usuario no root que no es el usuario de Novell

El procedimiento de actualización falla si intenta actualizar el servidor Novell Sentinel Log Manager 1.0 instalado como usuario diferente de root que no es `novell`. Este problema ocurre debido a la naturaleza de los permisos de archivos definidos durante la instalación de Sentinel Log Manager 1.0.

Para actualizar el servidor Sentinel Log Manager 1.0 instalado como usuario diferente de root que no es `novell`, haga lo siguiente:

1 Cree el usuario `novell`.

2 Cambie la propiedad de la instalación de Sentinel Log Manager 1.0 a`novell:novell`.

```
chown -R novell:novell /opt/novell/<install_directory>
```

Cambie <*directorio_instalación*> al nombre del directorio de instalación. Por ejemplo,

```
chown -R novell:novell /opt/novell/sentinel_log_mgr_1.0_x86-64
```

3 Cambie la entrada ESEC_USER en`config/esecuser.properties` a `novell`.

4 Entre como usuario `root`, y luego actualice a Sentinel Log Manager 1.1. Para obtener más información sobre cómo actualizar, consulte la Sección 6.1, “Actualización de 1.0 a 1.1”, en la página 47.

Terminología de Sentinel

En esta sección se describe la terminología utilizada en este documento.

Recopiladores
Utilidad que analiza los datos y ofrece un flujo de eventos más rico 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.

Conectores
Utilidad que utiliza métodos estándar del sector para conectar con los orígenes de datos para obtener datos en bruto.

Retención de datos
Directiva que define el período durante el cual permanecen los eventos antes de que se supriman del servidor de Sentinel Log Manager.

Origen de eventos
El aplicador o sistema que registra el evento.

Gestión de orígenes de eventos
ESM. La interfaz que permite gestionar y supervisar las conexiones entre Sentinel y los orígenes de eventos utilizando los conectores y recopiladores de Sentinel.

Eventos por segundo
EPS. Valor que mide la rapidez con que la red genera datos desde sus aplicaciones y dispositivos de seguridad. También representa una frecuencia según la cual Sentinel Log Manager puede recopilar y almacenar datos de los dispositivos de seguridad.

Integrador
Módulos auxiliares (plug-in) que permiten a los sistemas de Sentinel conectarse con otros sistemas externos. Las acciones de JavaScript pueden usar integradores para interactuar con otros sistemas.

Datos en bruto
Eventos sin procesar que se reciben en el conector y se envían directamente al bus de mensajes de Sentinel Log Manager para después escribirse en el servidor de Sentinel Log Manager. Los datos en bruto varían de un conector a otro debido al formato de los datos almacenados en el dispositivo.