NetIQ Sentinel 7.1

Guía de instalación y configuración

June 2013

Información legal

Tabla de contenido

Acerca de este libro y la biblioteca

La *Guía de instalación y configuración* ofrece una introducción a NetIQ Sentinel y explica cómo instalar y configurar Sentinel.

A quién va dirigida

Esta guía está dirigida a administradores y consultores de Sentinel.

Otra información de la biblioteca

La biblioteca ofrece los siguientes recursos informativos:

Guía de administración

Proporciona información sobre administración y las tareas necesarias para gestionar una implementación de Sentinel.

Guía del usuario

Proporciona información conceptual sobre Sentinel. En este libro se ofrece también una descripción general de las interfaces del usuario y una guía paso a paso para realizar muchas tareas.

Acerca de NetIQ Corporation

Somos una empresa mundial de software empresarial, centrada en resolver los tres principales desafíos de su entorno, a saber, cambios, complejidad y riesgo, y en cómo podemos ayudarle a controlarlos.

Nuestro punto de vista

La adaptación a los cambios y la gestión de la complejidad y los riesgos no son conceptos nuevos

De hecho, de todos los desafíos a los que se enfrenta, quizá sean estas las variables más destacadas que le deniegan el control necesario para poder medir, supervisar y gestionar de forma segura sus entornos físico, virtual y de cloud computing.

Activación de servicios esenciales para el negocio de forma más rápida y eficiente

Creemos que la única forma de hacer posible una prestación de servicios más puntual y económica es dotar a las organizaciones de TI del mayor control posible. La presión continua de los cambios y la complejidad seguirá aumentando a medida que las organizaciones sigan creciendo y las tecnologías necesarias para gestionarlas se hagan intrínsecamente más complejas.

Nuestra filosofía

Vender soluciones inteligentes, no solo software

Para poder ofrecer un control fiable, debemos entender primero los escenarios reales en los que —día a día— operan las organizaciones de TI como la suya. Esa es la única forma de desarrollar soluciones de TI prácticas e inteligentes que proporcionen resultados conmensurables con una eficacia demostrada. Y eso es mucho más satisfactorio que vender simplemente software.

Fomentar su éxito es nuestra pasión

Ayudarle a alcanzar el éxito es el objetivo primordial de nuestro trabajo. Desde la concepción al desarrollo, sabemos que usted necesita soluciones de TI que funcionen bien y se integren a la perfección con su inversión existente; necesita asistencia continua y formación posterior a la implementación; y, para variar, también necesita trabajar con alguien que le facilite las cosas. En definitiva, su éxito será también el nuestro.

Nuestras soluciones

- Control de identidad y acceso
- Gestión de acceso
- Gestión de la seguridad
- Gestión de sistemas y aplicaciones
- Gestión del trabajo
- Gestión de servicios

Cómo contactar con asistencia para ventas

Para cualquier pregunta sobre nuestros productos, precios y capacidades, póngase en contacto con su representante local. Si no puede contactar con su representante local, comuníquese con nuestro equipo de Asistencia para ventas.

Oficinas mundiales:	www.netiq.com/about_netiq/officelocations.asp
Estados Unidos y Canadá:	1-888-323-6768
Correo electrónico:	info@netiq.com
sitio Web de iFolder:	www.netiq.com

Cómo ponerse en contacto con el personal de asistencia técnica

Para obtener información sobre problemas con productos específicos, póngase en contacto con nuestro equipo de asistencia técnica.

Oficinas mundiales:	www.netiq.com/support/contactinfo.asp
Norteamérica y Sudamérica:	1-713-418-5555
Europa, Oriente Medio y África:	+353 (0) 91-782 677
Correo electrónico:	support@netiq.com
sitio Web de iFolder:	www.netiq.com/support

Cómo contactar con asistencia para documentación

Nuestro objetivo es proporcionar documentación que satisfaga sus necesidades. Si tiene sugerencias de mejoras, haga clic en **Add Comment** (Agregar comentario) en la parte de abajo de cualquier página de las versiones HTML de la documentación publicada en www.netiq.com/documentation. Si lo desea, también puede enviar un correo electrónico a Documentation-Feedback@netiq.com. Agradecemos sus comentarios y estamos deseando oír sus sugerencias.

Cómo contactar con la Comunidad de usuarios en línea

Qmunity, la comunidad de NetIQ en línea, es una red de colaboración que le pone en contacto con sus colegas y con otros expertos de NetIQ. Qmunity le ayuda a dominar los conocimientos que necesita para hacer realidad todo el potencial de su inversión en TI de la que depende, al proporcionarle información inmediata, enlaces útiles a recursos prácticos y acceso a los expertos de NetIQ. Para obtener más información, visite la página http://community.netiq.com.

Conocer Sentinel

En esta sección se proporciona una descripción detallada de Sentinel y cómo Sentinel ofrece a su organización una solución de gestión de eventos.

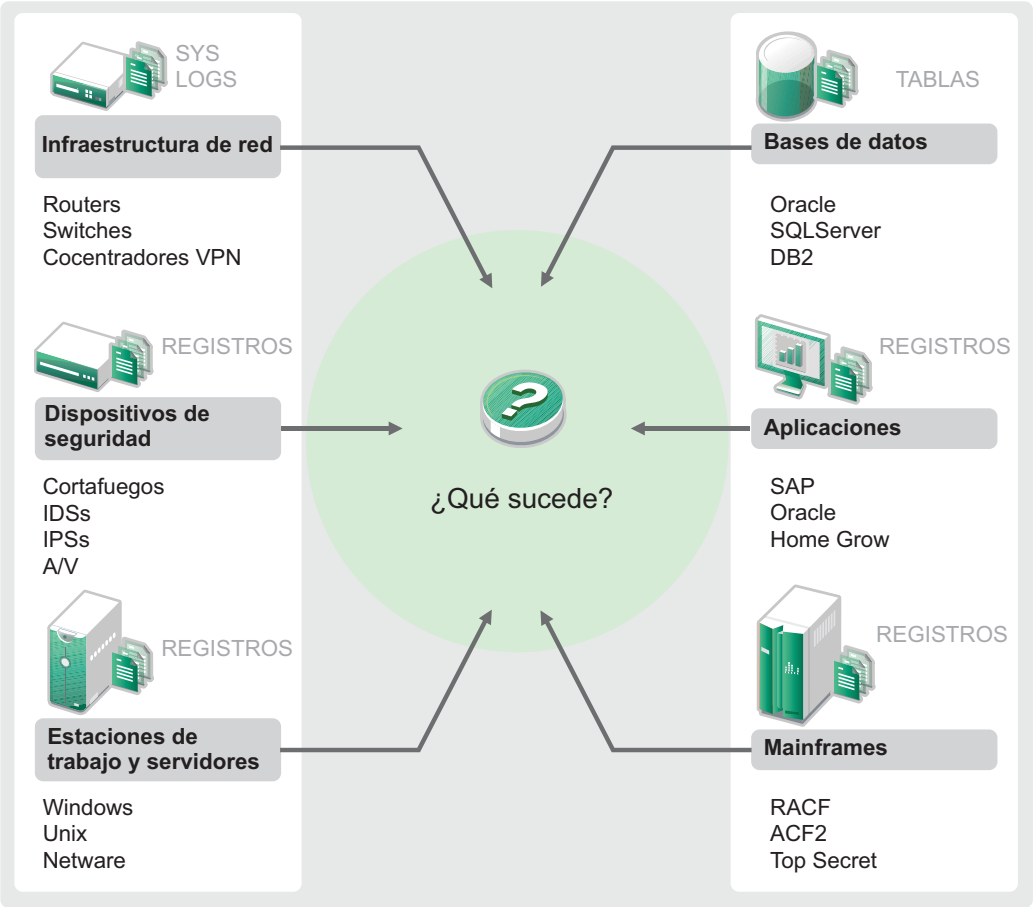
1 ¿Qué es Sentinel?

Sentinel es una solución de gestión de información de seguridad y eventos (SIEM) y de supervisión del cumplimiento. Sentinel supervisa automáticamente los entornos TI más complejos y ofrece la seguridad requerida para protegerlos.

1.1 Retos de proteger un entorno de TI

Asegurar su entorno TI es un reto debido a su complejidad. Existe una gran diversidad de aplicaciones, bases de datos, mainframes, estaciones de trabajo y servidores, y todos ellos mantienen registros de los eventos que se producen. Asimismo, cuenta con dispositivos de seguridad y dispositivos de infraestructura de red que a su vez contienen registros de lo que ocurre en su entorno de TI.

Figura 1-1 *Qué ocurre en su entorno.*



Los retos surgen por los siguientes hechos:

- Existen muchos dispositivos en su entorno de TI.
- Los registros tienen diferentes formatos.
- Los registros se almacenan en silos.
- La cantidad de información generada en los registros.
- No puede determinar quién hizo qué sin analizar manualmente todos los registros.

Para que la información sea útil, debe poder realizar las siguientes acciones:

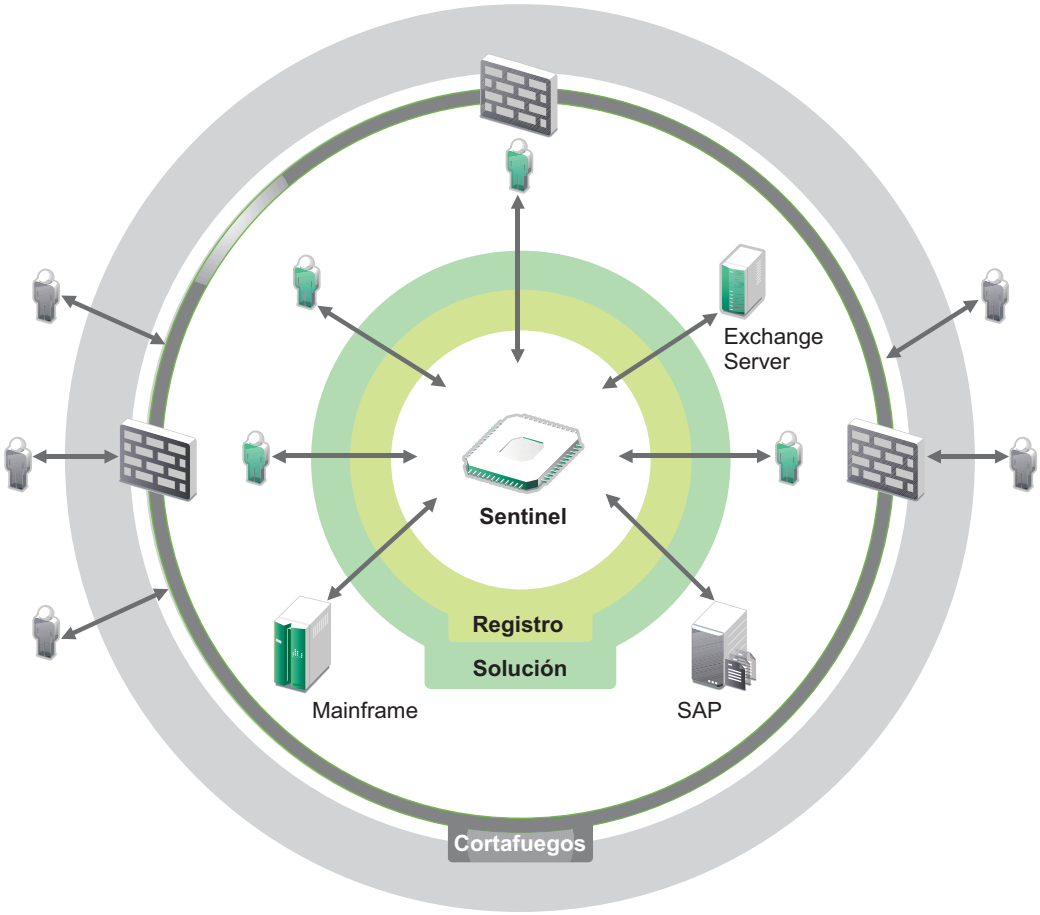
- Recopilar los datos.
- Consolidar los datos.
- Normalizar datos dispares en eventos que se puedan comparar fácilmente.
- Asignar eventos a regulaciones estándar.
- Analizar los datos.
- Comparar los eventos en múltiples sistemas para determinar si existen problemas de seguridad.
- Enviar notificaciones cuando los datos no se ajusten a las normas.
- Tomar medidas en las notificaciones para cumplir las directivas de empresa.
- Generar informes para demostrar el cumplimiento.

Tras conocer los retos que plantea la protección de su entorno de TI, necesita determinar cómo proteger la empresa para los usuarios, pero también frente a estos, sin tratarles como usuarios maliciosos ni imponerles cargas que les impidan ser productivos. Sentinel ofrece la solución.

1.2 La solución que ofrece Sentinel

Sentinel actúa como el sistema nervioso central para la seguridad de la empresa. Recoge datos de toda la infraestructura: aplicaciones, bases de datos, servidores, almacenamiento y dispositivos de seguridad. Analiza y establece correlaciones entre datos, y los convierte en datos procesables, ya sea de forma manual o automática.

Figura 1-2 *La solución que ofrece Sentinel*



El resultado es que usted conoce lo que sucede en su entorno de TI en un punto dado, y tiene la capacidad de enlazar las acciones realizadas sobre los recursos con las personas que realizan esas acciones. Esto le permite determinar la conducta del usuario y supervisar el control efectivamente. Independientemente de si la persona es interna o no, puede enlazar todas las acciones juntas de modo que las actividades no autorizadas estén claramente identificadas antes de que supongan un daño.

Sentinel realiza esto de un modo rentable del siguiente modo:

- Ofreciendo una solución única para tratar los controles TI en múltiples regulaciones. .
- Llenando el vacío de conocimiento entre lo que debería ocurrir y lo que está ocurriendo realmente en su entorno conectado en red.
- Demostrando a los auditores y reguladores que su organización documenta, supervisa e informa sobre los controles de seguridad.
- Ofreciendo programas de información y supervisión del cumplimiento listos para usar.
- Obteniendo la visibilidad y el control requeridos para evaluar continuamente el éxito de los programas de cumplimiento y seguridad de su organización.

Sentinel automatiza la recogida de registros, análisis y los procesos de generación de informes para asegurar que los controles TI son efectivos para apoyar los requisitos de detección de amenazas y auditoría. Sentinel proporciona funciones de supervisión automática de los eventos de seguridad, los eventos de conformidad y de los controles de TI, permitiendo tomar medidas inmediatas si se produce una vulneración de la seguridad o un evento no conforme. Sentinel también le permite reunir con facilidad información resumida sobre su entorno para que pueda comunicar su postura general en materia de seguridad a los principales interesados.

2 Cómo funciona Sentinel

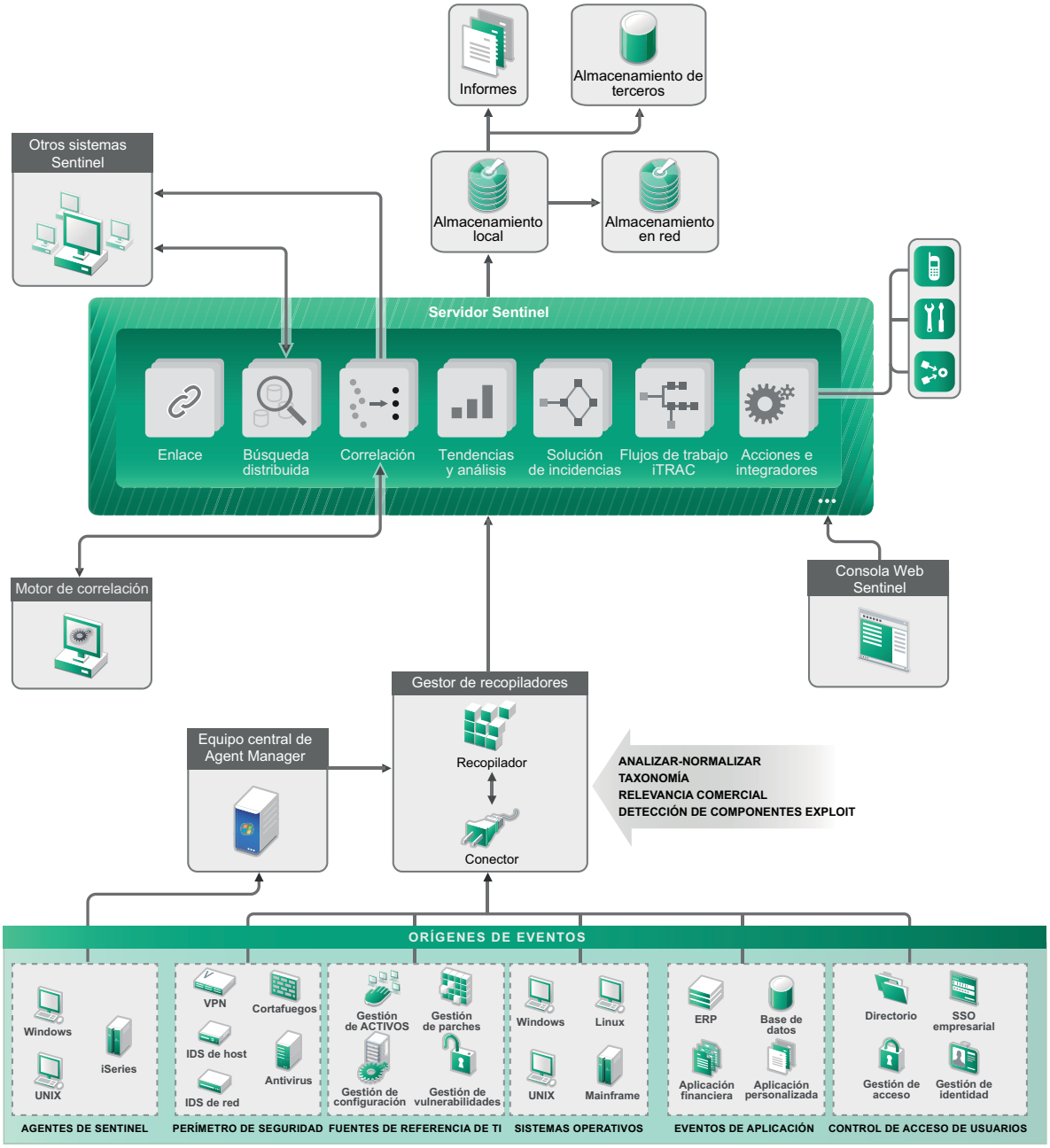
Sentinel gestiona de forma continua la información de seguridad y los eventos en todo el entorno de TI para ofrecer una solución de supervisión completa.

Sentinel hace lo siguiente:

- Reúne registros, eventos e información de seguridad de todos los orígenes de eventos diferentes en su entorno de TI.
- Normaliza los registros recopilados, eventos e información de seguridad en un formato común.
- Almacena eventos en un almacén de datos basado en archivos con directivas de retención de datos personalizables.
- Proporciona la posibilidad de vincular de forma jerárquica varios sistemas Sentinel, incluido Sentinel Log Manager.
- Le permite buscar eventos no solo en su servidor local de Sentinel, sino también en otros servidores de Sentinel distribuidos en el mundo.
- Realiza un análisis estático que le permite definir una línea de base y luego lo compara con lo que está ocurriendo para determinar si hay problemas no detectados.
- Correlaciona un conjunto de eventos similares o comparables en un período dado para determinar un patrón.
- Organiza eventos de incidentes para una gestión de la respuesta y seguimiento eficiente.
- Ofrece informes basados en eventos en tiempo real e históricos.

La siguiente figura muestra cómo funciona Sentinel:

Figura 2-1 *Arquitectura de Sentinel*



En las siguientes secciones se describen detalladamente los componentes de Sentinel:

- Sección 2.1, “Orígenes de eventos”, en la página 21
- Sección 2.2, “Evento de Sentinel”, en la página 21
- Sección 2.3, “Gestor de recopiladores”, en la página 23
- Sección 2.4, “Gestor de agentes”, en la página 23
- Sección 2.5, “Correlación”, en la página 24
- Sección 2.6, “Inteligencia de seguridad”, en la página 24
- Sección 2.7, “Solución de incidencias”, en la página 24

2.1 Orígenes de eventos

Sentinel reúne información de seguridad y eventos de muchos orígenes diferentes en su entorno TI. Estos orígenes se llaman orígenes de eventos. Los orígenes de eventos pueden ser diferentes elementos en su red.

Perímetro de seguridad: Dispositivos de seguridad que incluyen hardware y software utilizados para crear un perímetro de seguridad para su entorno, por ejemplo cortafuegos, IDS y VPN.

Sistemas operativos: Eventos de los diferentes sistemas operativos que operan en la red.

Orígenes de TI referenciales: El software utilizado para mantener y seguir activos, revisiones, configuración y vulnerabilidad.

Eventos de la aplicación: Los eventos generados de las aplicaciones instaladas en la red.

Control de acceso de usuarios: Los eventos generados de las aplicaciones o dispositivos que permiten a los usuarios acceder a los recursos de la compañía.

2.2 Evento de Sentinel

Sentinel recibe información de los dispositivos, normaliza esta información en una estructura denominada evento, clasifica el evento y lo envía para ser procesado. Al añadir la información de categoría (taxonomía) a los eventos, estos pueden compararse más fácilmente entre los sistemas que notifican los eventos de manera diferente. Por ejemplo, fallos de autenticación. Los eventos se procesan mediante visualización en tiempo real, el motor de correlación, consolas y el servidor backend.

Un evento está formado por más de 200 campos. Los campos de evento son de diferentes tipos y sirven para diferentes fines. Existen algunos campos predefinidos como gravedad, importancia, IP de destino y puerto de destino. Existen dos conjuntos de campos configurables: campos reservados para el uso interno de Sentinel para permitir la expansión futura y campos del cliente para extensiones de clientes.

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

2.2.1 Servicio de asignación

El servicio de asignación permite un mecanismo sofisticado para propagar los datos de relevancia empresarial en el sistema. Estos datos pueden enriquecer los eventos con información de referencia que proporcionará el contexto que permita a los analistas tomar mejores decisiones, redactar informes más útiles y crear reglas de correlación bien fundadas.

Puede enriquecer los datos de eventos utilizando asignaciones para añadir información adicional como el host y los datos de identidad a los eventos entrantes de los dispositivos de origen. Esta información adicional puede utilizarse para fines de correlación y generación de informes avanzados. El sistema admite varias asignaciones incorporadas además de asignaciones definidas por el usuario personalizadas.

Las asignaciones definidas en Sentinel se almacenan de dos formas diferentes:

- Las asignaciones incorporadas se almacenan en la base de datos, se actualizan utilizando APIs en código del recopilador y se exportan automáticamente al servicio de asignación.
- Las asignaciones personalizadas se almacenan en archivos CSV y se pueden actualizar en el sistema de archivos o a través de la interfaz del usuario de Configuración de los datos de la asignación, y luego los carga el Servicio de asignación.

En ambos casos, los archivos CSV se guardan en el servidor Sentinel central, pero los cambios en las asignaciones se distribuyen a cada gestor de recopiladores y se aplican a nivel local. Este procesamiento distribuido garantiza que la actividad de asignación no sobrecargue el servidor principal.

2.2.2 Asignaciones de emisión continua

El servicio de asignación emplea un modelo de actualización dinámico y reproduce las asignaciones de un punto a otro, evitando la creación de grandes asignaciones estáticas en la memoria dinámica. El valor de esta función de emisión es particularmente importante en un sistema en tiempo real esencial como Sentinel donde debe haber un movimiento seguro, predictivo y ágil de independencia de datos de alguna carga transitoria en el sistema.

2.2.3 Detección de explotaciones (Servicio de asignación)

Sentinel ofrece la capacidad de contrastar las firmas de datos de eventos con los datos del escáner de vulnerabilidad. Los usuarios son notificados automática e inmediatamente cuando un ataque intenta explotar un sistema vulnerable. Esto se realiza mediante:

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

El asesor proporciona una referencia cruzada entre firmas de datos de eventos y datos del escáner de vulnerabilidad. Los datos del asesor contienen información sobre vulnerabilidades y amenazas así como una normalización de las firmas de eventos y los módulos auxiliares (plug-in) de vulnerabilidad. Para más información sobre el asesor, visite "Cómo configurar el asesor" en la *Guía de administración de NetIQ Sentinel 7.1* .

2.3 Gestor de recopiladores

El gestor de recopiladores gestiona la recopilación de datos, supervisa los mensajes de estado del sistema y realiza un filtrado de eventos según sea necesario. Entre las principales funciones del gestor de recopiladores destacan:

- Transformar eventos.
- Añadir relevancia empresarial a los eventos a través del servicio de asignación.
- Realizar el filtrado global de los eventos.
- Enrutar eventos.
- Determinar los datos de tiempo real, vulnerabilidad, activos o de tiempo no real.
- Enviar mensajes de estado al servidor de Sentinel.

2.3.1 Recopiladores

Los recopiladores normalizan y recogen la información de los conectores. Los recopiladores están escritos en JavaScript y definen la lógica para las siguientes acciones:

- Recibir datos en bruto de los conectores.
- Analizar y normalizar los datos.
- Aplicar la lógica repetible a los datos.
- Traducir los datos específicos de dispositivos a los datos específicos de Sentinel.
- Dar formato a los eventos.
- Pasar los datos normalizados, analizados y formateados al gestor de recopiladores.
- Filtrado de eventos según el dispositivo.

2.3.2 Conectores

Los conectores ofrecen conexiones desde los orígenes de eventos al sistema Sentinel. Los conectores utilizan protocolos estándar del sector para obtener los eventos, como por ejemplo syslog, JDBC para leer tablas de la base de datos, WMI para leer los registros de eventos de Windows, etc. Los conectores proporcionan:

- Transporte de datos de eventos en bruto desde los orígenes de eventos al recopilador.
- Filtrado específico de conexión.
- Gestión de errores de conexión.

2.4 Gestor de agentes

Agent Manager ofrece recopilación de datos basada en host que complementa la recopilación de datos sin agentes permitiéndole:

- Acceder a registros que no están disponibles en la red.
- Operar en entornos de red con un estricto control.
- Mejorar la posición de seguridad al limitar la zona de ataque en servidores cruciales.
- Proporcionar una mayor fiabilidad en la recopilación de datos durante las interrupciones en la red.

Agent Manager le permite implementar agentes, gestionar su configuración y actuar como punto de recopilación de los eventos que fluyen hacia Sentinel. Para obtener más información sobre Agent Manager, consulte la documentación de Agent Manager.

2.5 Correlación

Un solo evento puede parecer insignificante, pero en combinación con otros eventos, puede advertir sobre un problema potencial. Sentinel le ayuda a establecer correlaciones entre estos eventos al usar las reglas que crea e implementa en el motor de correlación, y al tomar las medidas adecuadas para paliar los problemas.

La 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 más información, consulte "Correlating Event Data" (Datos de eventos de correlación) en la *NetIQ Sentinel 7.1 User Guide (Guía del usuario de NetIQ Sentinel 7.0.1)*.

Para supervisar eventos de acuerdo con las reglas de correlación, debe implementar las reglas en el motor de correlación. Cuando se produce un evento que satisface los criterios de una regla, el motor de correlación genera un evento de correlación que describe el patrón. Para obtener más información, consulte "Correlation Engine" (Motor de correlación) en la *NetIQ Sentinel 7.1 User Guide* (Guía del usuario de NetIQ Sentinel 7.1).

2.6 Inteligencia de seguridad

La función de correlación de Sentinel proporciona la capacidad de conocer patrones de actividad, ya sea por motivos de seguridad, conformidad o de otro tipo. La función de Inteligencia de seguridad busca actividad fuera de lo normal, que puede ser de tipo malicioso, pero que no coincide con ningún patrón conocido.

La característica de Inteligencia de seguridad en Sentinel se centra en el análisis estadístico de los datos de series temporales para permitir a los analistas identificar y analizar las desviaciones (anomalías) mediante un motor estadístico automatizado o mediante la representación visual de los datos estadísticos para la interpretación manual. Para más información, consulte "Analyzing Trends in Data" (Cómo analizar tendencias en datos) en la *NetIQ Sentinel 7.1 User Guide (Guía del usuario de NetIQ Sentinel 7.0.1)*.

2.7 Solución de incidencias

Sentinel proporciona un sistema de gestión automatizada de respuestas a incidencias que le permite documentar y formalizar el proceso de seguimiento, derivación y respuesta a incidencias y violaciones de directivas, y le proporciona una integración en dos sentidos con sistemas de mensajes sobre problemas. Sentinel le permite reaccionar rápidamente y solucionar incidencias de forma eficaz. Para más información, consulte "Configuring incidents" (Cómo configurar incidencias) en la *NetIQ Sentinel 7.1 User Guide (Guía del usuario de NetIQ Sentinel 7.1)*.

2.8 Flujos de trabajo de iTRAC

Los flujos de trabajo de iTrac están diseñados para ofrecer una solución sencilla y flexible para automatizar y seguir los procesos de respuesta a incidentes de una empresa. iTrac aprovecha el sistema de incidentes interno de Sentinel para seguir la seguridad o problemas de sistemas de la identificación (mediante las reglas de correlación o identificación manual) a la resolución.

Los flujos de trabajo pueden crearse utilizando pasos manuales o automatizados. Las características avanzadas como ramificación, escalada basada en el tiempo y variables locales son compatibles. La integración con guiones externos y plug-ins permite la interacción flexible con sistemas de terceros. La generación de informes completa permite a los administradores entender y afinar los procesos de respuesta a incidentes. Para más información, consulte "Configuring iTRAC Workflows" (Cómo configurar los flujos de trabajo iTRAC) en la *NetIQ Sentinel 7.1 User Guide (Guía del usuario de NetIQ Sentinel 7.0.1)*.

2.9 Acciones e integradores

Las acciones ejecutan en Sentinel algún tipo de acción de forma manual o automática, como por ejemplo enviar mensajes de correo electrónico. Las acciones pueden desencadenarse por medio de reglas de encaminamiento, al ejecutar manualmente una operación de evento o incidencia y también por medio de reglas de correlación. Sentinel proporciona una lista de acciones previamente configuradas. Puede usar las acciones por defecto y reconfigurarlas según sea necesario, o ben puede añadir nuevas acciones. Para obtener más información, consulte "Configuring Actions" (Configuración de acciones) en la *NetIQ Sentinel 7.1 Administration Guide* (Guía de administración de NetIQ Sentinel 7.1).

Una acción puede ejecutarse por sí misma o puede utilizar una instancia de integrador configurada desde un módulo auxiliar (plug-in) de integrador. Los módulos auxiliares (plug-in) amplían las características y la funcionalidad de las acciones de solución de Sentinel. Los integradores proporcionan la capacidad de conectarse a un sistema externo, como un servidor LDAP, SMTP o SOAP para ejecutar una acción. Para más información, consulte "Configuring Integrators" (Configuración de integradores) en la *NetIQ Sentinel 7.1 Administration Guide (Guía de administración de NetIQ Sentinel 7.1*.

2.10 Informes

Sentinel ofrece la capacidad para ejecutar informes sobre los datos reunidos. Sentinel se suministra con una variedad de informes personalizables. Algunos informes son flexibles, para permitir especificar las columnas que se mostrarán en los resultados.

Puede ejecutar o programar informes y enviarlos por correo electrónico en formato PDF. También puede ejecutar informes como búsquedas e interactuar con los resultados, como perfeccionar la búsqueda y también realizar una acción basada en los resultados. También puede ejecutar informes en los servidores Sentinel que se distribuyen en diferentes localizaciones geográficas. Para más información, consulte "Reporting" (Informe) en la *NetIQ Sentinel 7.1 User Guide (Guía de usuario de NetIQ Sentinel 7.0.1)*.

2.11 Análisis de eventos

Sentinel proporciona un potente conjunto de herramientas que le ayudan a buscar y analizar con facilidad datos de eventos fundamentales. El sistema se ajusta y optimiza para obtener una máxima eficiencia en cualquier tipo de análisis en particular, y se proporcionan métodos para hacer fácilmente la transición de un tipo de análisis a otro de una forma transparente.

La investigación de eventos en Sentinel a menudo comienza con las Vistas activas casi en tiempo real. Si bien se dispone de herramientas más avanzadas, Vistas activas muestra los flujos de eventos filtrados junto con diagramas de resumen que pueden servir para un análisis sencillo y somero de las tendencias de los eventos, los datos de eventos y para la identificación de eventos específicos. Con el tiempo, se construyen filtros mejorados para clases de datos específicos, como por ejemplo resultados de correlación. Puede usar Vistas activas como consola para mostrar una posición operativa y de seguridad general.

Luego puede usar la búsqueda interactiva para realizar un análisis más detallado de los eventos. Esto le permite buscar fácil y rápidamente datos relacionados con una consulta específica, como la actividad de un usuario en particular o en un sistema específico. Al hacer clic en los datos del evento o usar el panel de mejora de la izquierda, podrá enfocarse en eventos de interés específico.

Al analizar cientos de eventos, las funciones de generación de eventos de Sentinel proporcionan un control personalizado de la disposición de los eventos y pueden mostrar un mayor volumen de datos. Sentinel facilita esta transición aún más al permitirle transferir búsquedas interactivas incorporadas a la interfaz de búsqueda a una plantilla de generación de informe, que permite crear de manera inmediata un informe que muestra los mismos datos pero en un formato más adecuado para un mayor número de eventos.

Sentinel incluye muchas plantillas para este fin. Algunas plantillas están mejoradas para mostrar un tipo particular de información, como datos de autenticación o creación de usuarios, y otras plantillas son de uso general y permiten personalizar grupos y columnas en el informe de manera interactiva.

Con el tiempo, desarrollará filtros de uso común e informes que facilitan el flujo de trabajo. Sentinel admite plenamente el almacenamiento de esta información y su distribución a personas de su organización. Para obtener más información, consulte la *Guía del usuario de NetIQ Sentinel 7.1*.

2.12 Encaminamiento y almacenamiento de datos de Sentinel

Sentinel proporciona numerosas opciones para encaminar, almacenar y extraer los datos recopilados. Por defecto, Sentinel recibe dos cadenas de datos independientes pero similares de los gestores de recopiladores: los datos analizados y los datos en bruto del evento. Los datos en bruto se almacenan inmediatamente en particiones protegidas para proporcionar una cadena de evidencia segura. Los datos analizados del evento se encaminan de acuerdo con reglas definidas y se pueden filtrar, enviarse al almacenamiento, enviarse a herramientas de análisis en tiempo real y encaminarse a sistemas externos. Todos los datos de eventos que se envían a almacenamiento se hacen corresponder con directivas de retención definidas por el usuario, las cuales determinan la partición en la que se colocan los datos, y además definen la directiva de limpieza según la cual se retienen los datos y posteriormente se eliminan.

El almacenamiento de datos de Sentinel se basa en una arquitectura de tres niveles:

- **Almacenamiento en línea**
  - **Almacenamiento principal o local:** optimizado para escribir y recuperar datos de forma rápida. Los datos de eventos recopilados más recientemente (y los buscados con más frecuencia) se almacenan aquí.

- **Almacenamiento secundario o en red:** optimizado para reducir la utilización del espacio lo que facilita una recuperación rápida. Sentinel migra de forma automática las particiones de datos a un almacenamiento secundario.

Nota: El uso de un almacenamiento secundario es opcional. Las directivas de retención de datos, las búsquedas y los informes operan en las particiones de datos de eventos independientemente de si residen en el almacenamiento principal, secundario o en ambos.

- **Almacenamiento sin conexión o de reserva:**

  Una vez que las particiones estén cerradas, es posible realizar copias de seguridad de ellas en un almacenamiento sin conexión, como por ejemplo un sistema de almacenamiento masivo económico, Amazon Glacier, etc. Si fuera necesario, puede volver a importar temporalmente las particiones sin conexión para su análisis a posteriori a largo plazo.

También puede configurar Sentinel para extraer datos de eventos y resúmenes de datos de eventos a una base de datos externa mediante el uso de directivas de sincronización de datos. Para obtener más información, consulte "Configuring Data Storage" (Configuración de almacenamiento de datos) en la *NetIQ Sentinel 7.1 Administration Guide* (Guía de administración de NetIQ Sentinel 7.1).

II Planificación de su instalación de Sentinel

En esta sección se ofrece una guía sobre consideraciones de planificación antes de instalar Sentinel. Si desea instalar una configuración no contemplada en las secciones siguientes, o si tiene alguna pregunta, póngase en contacto con el servicio de Asistencia técnica de NetIQ.

3 Lista de verificación de implementación

Utilice la siguiente lista de verificación para llevar a cabo la planificación, instalación y configuración de Sentinel:

❒	Tareas	Consulte
❒	Revise la información sobre la arquitectura del producto para conocer los componentes de Sentinel.	Parte I, “Conocer Sentinel”, en la página 13.
❒	Revise la información sobre licencias de Sentinel a fin de determinar si necesita instalar la versión de prueba o la versión empresarial de Sentinel.	Capítulo 4, “Información sobre licencias”, en la página 33.
❒	Evalúe su entorno para determinar la configuración de hardware. Asegúrese de que los sistemas en los que instale Sentinel y sus componentes cumplan los requisitos especificados.	Capítulo 5, “Cumplimiento de los requisitos del sistema”, en la página 35.
❒	Por defecto, Sentinel se suministra con un gestor de recopiladores y un motor de correlación. Revise los eventos por segundo (EPS) del gestor de recopiladores y del motor de correlación para determinar si necesita instalar más gestores de recopiladores y motores de correlación a fin de mejorar el rendimiento y el equilibrio de carga.	Sección 9.1, “Ventajas de los gestores de recopiladores adicionales”, en la página 70 and Sección 9.2, “Ventajas de los motores de correlación adicionales”, en la página 70.
❒	Instale Sentinel.	Parte III, “Instalación de Sentinel”, en la página 67.
❒	Asegúrese de configurar la hora en el servidor Sentinel.	Capítulo 16, “Configuración de la hora”, en la página 105.
❒	Al instalar Sentinel, se instalan por defecto los módulos auxiliares (plug-ins) disponibles en el momento de editarse la versión de Sentinel. Configure los módulos auxiliares (plug-ins) predefinidos para la recopilación de datos y la generación de informes.	Capítulo 17, “Configuración de módulos auxiliares (plug-ins) genéricos”, en la página 109.
❒	Instale recopiladores y conectores adicionales en su entorno según sea necesario.	Capítulo 13, “Instalación de conectores y recopiladores adicionales”, en la página 97.
❒	Instale gestores de recopiladores y motores de correlación adicionales en su entorno según sea necesario.	Sección 11.6, “Instalación de gestores de recopiladores y motores de correlación adicionales”, en la página 80.

4 Información sobre licencias

Sentinel tiene varias licencias a su disposición. Por defecto, Sentinel se suministra con la licencia de prueba.

4.1 Licencia de prueba

La licencia por defecto de Sentinel le permite usar todas las funciones empresariales de Sentinel durante el período de evaluación de 90 días. Un sistema que ejecute la licencia de prueba muestra un indicador en la interfaz Web que indica que se está utilizando la clave de licencia temporal. También muestra el número de días que quedan para que caduque la funcionalidad e indica la forma de actualizar a una licencia completa.

Nota: La fecha de caducidad del sistema se basa en los datos más antiguos del sistema. Si restaura eventos antiguos en el sistema, se ajustará la fecha de caducidad en la forma correspondiente.

Después del período de prueba de 90 días, se inhabilitan la mayoría de funciones, aunque aún podrá acceder al sistema y actualizarlo para usar una clave de licencia empresarial.

Después de actualizar a una licencia empresarial, se restaura toda la funcionalidad. Para prevenir cualquier interrupción de la funcionalidad, debe actualizar el sistema a una licencia empresarial antes de la fecha de caducidad.

4.2 Licencias empresariales

Al adquirir Sentinel, recibe una clave de licencia a través del portal para clientes. Dependiendo de la licencia que adquiera, la clave de licencia habilita determinadas funciones, índices de recopilación de datos y orígenes de eventos. Puede haber condiciones adicionales de licencia que no aplique la clave de licencia, por lo que se recomienda leer detenidamente el acuerdo de licencia.

Para hacer cambios a la licencia, comuníquese con su gerente de cuentas. Para añadir una clave de licencia al sistema, consulte la *NetIQ Sentinel 7.1 Administration Guide* (Guía de administración de NetIQ Sentinel 7.1).

5 Cumplimiento de los requisitos del sistema

En este capítulo se proporciona información sobre los requisitos de hardware, sistema operativo y navegador para Sentinel.

5.1 Sistemas operativos y plataformas compatibles

NetIQ admite Sentinel en los sistemas operativos descritos en esta sección. NetIQ también admite Sentinel en sistemas con pequeñas actualizaciones a estos sistemas operativos, como por ejemplo parches de seguridad y correcciones (hotfixes). No obstante, NetIQ no permite ejecutar Sentinel en sistemas que tengan actualizaciones importantes de los siguientes sistemas operativos hasta que NetIQ haya probado y certificado dichas actualizaciones.

NetIQ admite el servidor Sentinel, el gestor de recopiladores y el motor de correlación en los siguientes sistemas operativos y plataformas:

Categoría	Requisito
Sistema operativo	Sentinel es compatible con los siguientes sistemas operativos: ◆ SUSE Linux Enterprise Server (SLES) 11 SP2 de 64 bits * ◆ Red Hat Enterprise Linux for Servers (RHEL) 6 de 64 bits * Sentinel no se admite en las instalaciones Open Enterprise Server de SLES. **Importante:** Para instalaciones tradicionales, asegúrese de que esté habilitado el protocolo de Internet versión 6 (IPv6) en su sistema operativo. Si IPv6 no está habilitado, algunos componentes fundamentales no funcionarán correctamente. Para instalaciones de dispositivo, IPv6 está habilitado por defecto.

Categoría	Requisito
Plataforma virtual	NetIQ proporciona dispositivos que instalan un servidor SLES 11 SP2 de 64 bits y Sentinel en las siguientes plataformas virtuales: ◆ VMWare ESX 4.0 y 5.0 ◆ Xen 4.0
Imágenes ISO en DVD	NetIQ proporciona un archivo de imagen ISO en DVD que instala SLES 11 SP2 de 64 bits y Sentinel en: ◆ Servidor Hyper-V 2008 R2 ◆ Hardware sin sistema operativo instalado
Sistema de archivos	**Instalaciones tradicionales:** ◆ **En sistemas SLES:** Sentinel admite los sistemas de archivos ext3 y XFS. ◆ **En sistemas RHEL:** Sentinel es compatible con los sistemas de archivos ext4 y XFS. **Instalaciones de dispositivos:** Sentinel utiliza 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 *SLES 11 SP2 Storage Administration Guide* (Guía de administración del almacenamiento de SLES 11 SP2).

5.2 Plataformas de bases de datos compatibles

Sentinel incluye un sistema de almacenamiento basado en archivos integrado y la base de datos PostgreSQL, que son todo lo necesario para ejecutar Sentinel. Sin embargo, si utiliza la función opcional de sincronización de datos para copiar datos a un almacén de datos, Sentinel admite el uso de PostgreSQL, Oracle versión 11g R2 o Microsoft SQL Server 2008 R2 como almacén de datos.

5.3 Navegadores compatibles

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

Nota: Para cargar correctamente las aplicaciones del cliente de Sentinel, debe tener instalado en su sistema el módulo Java Webstart.

Plataforma	Navegador
Windows 7	◆ Firefox versión 5 a versión 18 ◆ Internet Explorer 8, 9 y 10.* Para obtener más información sobre Internet Explorer 8, consulte “Requisitos previos para Internet Explorer” en la página 37.
SLES 11 SP2 y RHEL 6	◆ Firefox versión 5 a versión 18

5.3.1 Requisitos previos para Internet Explorer

Si el nivel de Seguridad de Internet se configura en Alto, aparece una página en blanco después de entrar en Sentinel y el navegador podría bloquear la ventana emergente de descarga de archivos. Para salvar este problema, deberá fijar primero el nivel de seguridad en Medio-alto y luego cambiar a nivel Personalizado de la siguiente manera:

1. Desplácese a *Herramientas* > *Opciones de Internet* > *pestaña Seguridad* y fije el nivel de seguridad en *Medio-alto*.
2. Asegúrese de que no esté seleccionada la opción *Herramientas* > *Vista de compatibilidad*.
3. Desplácese a *Herramientas* > *Opciones de Internet* > *pestaña Seguridad*> *Nivel personalizado*, luego desplácese a la sección *Descargas* y elija *Habilitar* en la opción *Pedir intervención del usuario automática para descargas de archivo*.

5.4 Información de tamaño del sistema

Una implementación de Sentinel puede variar en función de las necesidades del entorno, por lo que se recomienda consultar con Servicios de consultoría de NetIQ o con algún socio de NetIQ Sentinel antes de finalizar la arquitectura de Sentinel.

En esta sección se proporciona información sobre tamaño basada en las pruebas realizadas en NetIQ con el hardware disponible en el momento de la prueba. Es probable que otras configuraciones de hardware de mayor dimensión y potencia puedan manejar una carga mayor.

Las configuraciones "todo en uno" ponen toda la carga de procesamiento en el servidor Sentinel en lugar de distribuirla a los gestores de recopiladores y los motores de correlación remotos. Aunque la configuración integral o "todo en uno" puede funcionar muy bien en escenarios sencillos donde solo se utiliza un pequeño conjunto de funciones de forma limitada, no sucede igual cuando existe un gran número de funciones que se utilizan de manera más amplia. Por ejemplo, si utiliza más reglas de correlación que las predefinidas, se sobrecarga el sistema y ello puede dar lugar a que otras funciones del mismo servidor se resientan debido a un aumento de utilización de recursos del motor de correlación.

- Se requiere distribuir la carga a los gestores de recopiladores remotos cuando se utiliza más de un pequeño número de recopiladores.
- Se requiere distribuir la carga a los motores de correlación remotos cuando se utilizan más reglas de correlación que las predefinidas.
- Distribuir la carga es una buena idea cuando se prevé aumentar el número de funciones o intensificar su uso.

La capacidad de la CPU para llevar a cabo la función de hyperthreading ha demostrado tener un efecto muy positivo en la carga que puede manejar el sistema. Por lo tanto, a la hora de decidir qué tipo de CPU adquirir, asegúrese de tener en cuenta si se había habilitado la función de hyperthreading durante las pruebas de referencia a continuación y asegúrese de que la CPU elegida tenga capacidades de hyperthreading buenas u óptimas.

Categoría	Descripción	Demostración "todo en uno" no prevista para producción	"Todo en uno" mediana	Recopilación de datos basada en agentes mediana	"Todo en uno" grande	Recopilación de datos sin agentes distribuida grande	Muy grande
Capacidad de EPS conservados	La tasa de eventos por segundo procesada por los componentes en tiempo real y conservados en el almacenamiento por el sistema.	100 EPS	2500 EPS	2500 EPS	9000 EPS	11000 EPS	+11000 EPS
Capacidad de EPS operativos	La tasa total de eventos por segundo recibidos por el sistema de los orígenes de eventos. Incluye los datos abandonados por la función de filtrado inteligente del sistema antes de almacenarse y es el número utilizado para fines de cumplimiento de licencias basadas en EPS.	100 EPS	+2500 EPS	+2500 EPS	9000 EPS	16000 EPS	+16000 EPS
Hardware de servidor Sentinel							

Categoría	Descripción	Demostración "todo en uno" no prevista para producción	"Todo en uno" mediana	Recopilación de datos basada en agentes mediana	"Todo en uno" grande	Recopilación de datos sin agentes distribuida grande	Muy grande
CPU		CPU Intel Xeon E5420 a 2,50 GHz (4 núcleos CPU), sin hyper-threading	Dos CPU Intel Xeon E5450 a 3,00 GHz (4 núcleos por CPU; 8 núcleos en total), sin hyper-threading	Dos AMD Opteron 2431 a 2,40 GHz (6 núcleos por CPU; 12 núcleos en total)	Dos CPU Intel(R) Xeon(R) E5-2680 0 a 2,70 GHz (8 núcleos) (16 núcleos en total), con hyper-threading		Póngase en contacto con los servicios de NetIQ
Almacenamiento local	Datos almacenados en caché local para ofrecer un mejor rendimiento de búsqueda.	Unidad de 500 GB a 7200 RPM	5 SAS de 300 GB a 15000 RPM (Hardware RAID 0)	3 SAS de 146 GB a 10000 RPM (RAID 0, stripe size 128k)	5 TB, 8 SAS de 600 GB a 15 000 RPM (Hardware RAID 0, tamaño de franja 128k)		
Almacenamiento en red	Incluye una copia de los datos en el almacenamiento local.	No se utiliza	No se utiliza	No se utiliza	No se utiliza		
Memoria		4 GB	24 GB	16 GB	64 GB		
Hardware de gestor de recopiladores remoto n.º 1							
CPU		No corresponde (solo CM integrado local)				Dos CPU Intel(R) Xeon(R) E5-2680 0 a 2,70 GHz (8 núcleos) (16 núcleos en total), con hyper-threading	Póngase en contacto con los servicios de NetIQ

Categoría	Descripción	Demostración "todo en uno" no prevista para producción	"Todo en uno" mediana	Recopilación de datos basada en agentes mediana	"Todo en uno" grande	Recopilación de datos sin agentes distribuida grande	Muy grande
Almacenamiento						20 GB de espacio libre	Póngase en contacto con los servicios de NetIQ
Memoria						24 GB	
Hardware de gestor de recopiladores remoto n.º 2							
CPU		No corresponde (solo CM integrado local)				8 CPU Core Intel(R) Xeon(R) X5570 a 2,93 GHz (máquina virtual)	Póngase en contacto con los servicios de NetIQ
Almacenamiento						50 GB	
Memoria						8 GB	
Hardware de Agent Manager							
CPU		No corresponde (solo recopilación sin agentes)		Dos Intel Xeon 5140 a 2,33 GHz (2 núcleos por CPU; 4 núcleos en total)	No corresponde (solo recopilación sin agentes)		Póngase en contacto con los servicios de NetIQ
Almacenamiento				2 SAS de 300 GB a 10000 RPM (RAID 0, tamaño de franja 128k)			
Memoria				16 GB			
Hardware de motor de correlación remoto							

Categoría	Descripción	Demostración "todo en uno" no prevista para producción	"Todo en uno" mediana	Recopilación de datos basada en agentes mediana	"Todo en uno" grande	Recopilación de datos sin agentes distribuida grande	Muy grande
CPU		No corresponde (solo CE integrado local)					Póngase en contacto con los servicios de NetIQ
Almacenamiento							
Memoria							

Categoría	Descripción	Demostración "todo en uno" no prevista para producción	"Todo en uno" mediana	Recopilación de datos basada en agentes mediana	"Todo en uno" grande	Recopilación de datos sin agentes distribuida grande	Muy grande
Recopilación de datos							
Distribución de gestores de recopiladores (CM)	El número de orígenes de eventos y la carga de eventos por segundo asignada a cada gestor de recopiladores. El porcentaje filtrado indica cuántos eventos normalizados se filtraron inmediatamente después de la recopilación, sin almacenarse o trasladarse a motores de análisis. Tenga en cuenta que los datos del registro en bruto no normalizados en los que se basan los eventos normalizados no se ven afectados por el filtrado y siempre se almacenan. El gestor de recopiladores (CM) integrado local está ubicado en el equipo del servidor Sentinel.	**CM integrado local** Orígenes de eventos: 101 EPS: 100 Filtrados: 0%	**CM integrado local** Orígenes de eventos: 2500 EPS: 2500 Filtrados: 0%	**CM integrado local** Orígenes de eventos: 5000 EPS: 2500 Filtrados: 0%	**CM integrado local** Orígenes de eventos: 500 EPS: 9000 Filtrados: 0%	**CM integrado local** No se utiliza **CM remoto n.º 1** Orígenes de eventos: 110 EPS: 9500 Filtrados: 21% Datos en bruto inhabilitados **CM remoto n.º 2** Orígenes de eventos: 20 EPS: 6500 Filtrados: 54% Datos en bruto inhabilitados	Póngase en contacto con los servicios de NetIQ

Categoría	Descripción	Demostración "todo en uno" no prevista para producción	"Todo en uno" mediana	Recopilación de datos basada en agentes mediana	"Todo en uno" grande	Recopilación de datos sin agentes distribuida grande	Muy grande
Recopiladores utilizados		**IBM AIX 6.1r3** Orígenes: 100 EPS: 99 **NetIQ Universal Event 2011.1r1** Orígenes: 1 EPS: 1	Cada recopilador tenía su propio servidor syslog. **Oracle Solaris 6.1r3** Orígenes: 1000 EPS: 1000 **IBM AIX 6.1r3** Orígenes: 1000 EPS: 1000 **Sourcefire Snort 2011.1r1** Orígenes: 500 EPS:500	Recopilador de prueba personalizado (sin análisis) **Agent Manager Connector Server 1** Orígenes: 5000 EPS: 2500	Cada uno de los siguientes recopiladores tenía su propio servidor syslog, que analizaba el siguiente número de EPS: **Oracle Solaris 6.1r3** EPS: 2000 **Sourcefire Snort 2011.1r1** EPS: 1500 **NetIQ Universal Event 2011.1r1** EPS: 2000 **Juniper Netscreen Series 2011.1r1** EPS: 1500 **IBM AIX 6.1r3: 2000** EPS: 2000	Cada uno de los siguientes recopiladores tenía su propio servidor syslog, que analizaba el siguiente número de EPS: **Oracle Solaris 6.1r3** RCM n.º 1: 2000 RCM n.º 2: 2000 **Sourcefire Snort 2011.1r1** RCM n.º 1: 2000 RCM n.º 2: 2000 **NetIQ Universal Event 2011.1r1** RCM n.º 1: 2000 RCM n.º 2: 0 **Juniper Netscreen Series 2011.1r1** RCM n.º 1: 2000 RCM n.º 2: 1500	Póngase en contacto con los servicios de NetIQ

Categoría	Descripción	Demostración "todo en uno" no prevista para producción	"Todo en uno" mediana	Recopilación de datos basada en agentes mediana	"Todo en uno" grande	Recopilación de datos sin agentes distribuida grande	Muy grande
						IBM AIX 6.1r3 RCM n.º 1: 1500 RCM n.º 2: 0 **IBM iSeries 2011.1r3** RCM n.º 1: 0 RCM n.º 2: 2000	Póngase en contacto con los servicios de NetIQ
Total		Origen de eventos: 101 EPS: 100 Filtrados: 0%	Origen de eventos: 2500 EPS: 2500 Filtrados: 0%	Origen de eventos: 5000 EPS: 2500 Filtrados: 0%	Origen de eventos: 500 EPS: 9000 Filtrados: 0%	Origen de eventos: 130 EPS operativos: 16000 EPS conservados: 11000 Filtrados: 25%	
Almacenamiento de datos							

Categoría	Descripción	Demostración "todo en uno" no prevista para producción	"Todo en uno" mediana	Recopilación de datos basada en agentes mediana	"Todo en uno" grande	Recopilación de datos sin agentes distribuida grande	Muy grande
¿Hasta qué punto del pasado los usuarios buscarán datos con regularidad?	Cantidad de datos almacenados en caché local para mejorar el rendimiento de búsqueda.	7 días					Póngase en contacto con los servicios de NetIQ
¿Qué porcentaje de búsquedas corresponderá a datos anteriores al número de días de indicado arriba?	Afecta a la cantidad de operaciones de entrada/salida por segundo (IOPS) en el almacenamiento local o en red.	10%					
¿Hasta qué punto en el pasado se conservarán los datos?	Afecta a la cantidad de espacio en el disco que se necesita para conservar todos los datos. Si está habilitado el almacenamiento en red, esto afectará al tamaño de almacenamiento en red necesario. De lo contrario, afectará al tamaño del almacenamiento local necesario.	14 días					

Categoría	Descripción	Demostración "todo en uno" no prevista para producción	"Todo en uno" mediana	Recopilación de datos basada en agentes mediana	"Todo en uno" grande	Recopilación de datos sin agentes distribuida grande	Muy grande
¿Habrá un dispositivo de almacenamiento en red disponible y conectado?	Afecta a si todos los datos se almacenarán a nivel local o si hay disponible un almacenamiento en red para almacenar datos en línea de forma económica a largo plazo. Los datos del almacenamiento en red se conservan en línea.	No					Póngase en contacto con los servicios de NetIQ
¿Cuántos informes se optimizarán mediante resúmenes y otras directivas de sincronización de datos?	Afecta al número de directivas de sincronización de datos, lo que incide en el tamaño y el número de IOPS del almacenamiento local.	5 (predefinidas)			4 (predefinidas excepto el RDD de resumen de orígenes, que se demora)		
Actividad de usuarios							

Categoría	Descripción	Demostración "todo en uno" no prevista para producción	"Todo en uno" mediana	Recopilación de datos basada en agentes mediana	"Todo en uno" grande	Recopilación de datos sin agentes distribuida grande	Muy grande
¿Qué promedio de usuarios estarán activos al mismo tiempo?	Afecta al número de IOPS de almacenamiento local y en red y otros elementos.	1					Póngase en contacto con los servicios de NetIQ
¿Cuántas búsquedas, en promedio, realizará un usuario activo a la vez?	Afecta al número de IOPS de almacenamiento local y en red.	1 búsqueda o un informe (pero no ambos a la vez) 20000 eventos por informe, 100 millones de eventos por búsqueda		No se ha probado con carga de búsqueda o generación de informes	1 80 millones de eventos por búsqueda	1 20 millones de eventos por búsqueda	
¿Cuántos informes, en promedio, ejecutará un usuario activo a la vez?	Afecta al número de IOPS de almacenamiento local y en red.	1 búsqueda o un informe (pero no ambos a la vez) 20000 eventos por informe, 100 millones de eventos por búsqueda		No se ha probado con carga de búsqueda o generación de informes	1 1000 eventos por informe	1 60000 eventos por informe	
Análisis							
¿Qué porcentaje promedio de datos del evento es relevante con respecto a las reglas de correlación?	Cantidad de datos que procesará el motor de correlación.	100% (predefinidas) (3 correlaciones por segundo)		100% (predefinidas) (0 correlaciones por segundo)	0%	0% (algunos datos se reciben demasiado tarde para la correlación en tiempo real)	Póngase en contacto con los servicios de NetIQ

Categoría	Descripción	Demostración "todo en uno" no prevista para producción	"Todo en uno" mediana	Recopilación de datos basada en agentes mediana	"Todo en uno" grande	Recopilación de datos sin agentes distribuida grande	Muy grande
¿Cuántas reglas de correlación sencillas (solo filtros/ activadores) se utilizarán?	Afecta a la utilización de la CPU por el motor de correlación.	84 (predefinidas)			0		Póngase en contacto con los servicios de NetIQ
¿Cuántas reglas de correlación complejas se utilizarán?	Afecta a la utilización de la CPU y la memoria por el motor de correlación.	0 (predefinidas)					
Distribución del motor de correlación (CE)		CE integrado local (todas las reglas)					
¿En cuántos conjuntos de datos se realizará la detección de anomalías?	El número de consolas de Inteligencia de seguridad, que afecta a la CPU, el tamaño de almacenamiento local y la utilización de memoria.	1 (1% de flujo de eventos en cada una)		0			

Categoría	Descripción	Demostración "todo en uno" no prevista para producción	"Todo en uno" mediana	Recopilación de datos basada en agentes mediana	"Todo en uno" grande	Recopilación de datos sin agentes distribuida grande	Muy grande
Gran disponibilidad							
Notes	Funcionalidad destacada inhabilitada o advertencias cuando se excede la carga del sistema descrita anteriormente.				Datos en bruto inhabilitados No se utiliza correlación ni Inteligencia de seguridad Los informes de más de 30000 eventos producen inestabilidad	Datos en bruto inhabilitados No se utiliza la correlación ni Inteligencia de seguridad Los informes de más del número indicado de eventos producen inestabilidad El aumento de los EPS conservados producirá en última instancia inestabilidad en la configuración de este sistema	Póngase en contacto con los servicios de NetIQ

5.5 Planificación de particiones para el almacenamiento de datos

Al instalar Sentinel, debe montar la partición del disco de almacenamiento local en la misma ubicación en la que está instalado Sentinel, por defecto, el directorio `/var/opt/novell`.

Toda la estructura del directorio `/var/opt/novell/sentinel` debe residir en una misma partición de disco para garantizar que se realicen los cálculos de utilización de disco adecuados. De lo contrario, las funciones de gestión automática de datos podrían eliminar los datos de eventos de forma prematura. Para obtener más información sobre la estructura de directorios de Sentinel, consulte el Capítulo 15, "Estructura de directorios de Sentinel", en la página 101.

Una práctica óptima consiste en asegurarse de que este directorio de datos esté ubicado y almacenado en una partición de disco separada de la de los archivos ejecutables, de configuración y del sistema operativo. Las ventajas de almacenar los datos variables por separado son la mayor facilidad de realizar copias de seguridad y la recuperación más sencilla en caso de que se dañen los datos, y además fortalece el sistema en caso de que una partición se llene por completo. Además, mejora el rendimiento general de los sistemas donde los sistemas de archivos más pequeños son más eficientes. Para obtener más información, consulte "Disk partitioning" (Creación de particiones de disco).

5.5.1 Uso de particiones en instalaciones tradicionales

En instalaciones tradicionales, puede modificar la disposición de particiones de disco del sistema operativo antes de instalar Sentinel. El administrador debe crear y montar las particiones deseadas en los directorios adecuados, en función de la estructura de directorios detallada en la Sección 15, "Estructura de directorios de Sentinel", en la página 101. Al ejecutar el instalador, Sentinel se instala en los directorios creados previamente, lo que da lugar a una instalación que abarca varias particiones.

Nota:

- Puede usar la opción`--location` mientras ejecuta el instalador para especificar una ubicación de nivel superior diferente de los directorios por defecto para almacenar el archivo. El valor que asigne a la opción `--location` se antepone a las vías de los directorios. Por ejemplo, si especifica `--location=/foo`, el directorio de datos será `/foo/var/opt/novell/sentinel/data` y el directorio de configuración será `/foo/etc/opt/novell/sentinel/config`.
- No debe usar enlaces al sistema de archivos (por ejemplo, enlaces condicionales) para la opción `--location`.

5.5.2 Uso de particiones en una instalación de dispositivo

Al usar el formato de dispositivo DVD ISO, se pueden configurar las particiones del sistema de archivos del dispositivo durante la instalación. Por ejemplo, puede crear una partición separada para el punto de montaje `/var/opt/novell/sentinel` para poner todos los datos en una partición separada. Sin embargo, para otros formatos de dispositivo, puede configurar las particiones solamente después de la instalación. Puede añadir particiones y mover un directorio a la nueva partición utilizando la herramienta de configuración del sistema SuSE YaST. Para obtener más información sobre la creación de particiones después de la instalación, consulte la Sección 12.4.2, "Creación de particiones", en la página 92.

5.6 Requisitos del sistema para conectores y recopiladores

Cada conector y recopilador tiene sus propios requisitos del sistema y plataformas compatibles. Consulte la documentación del conector y del recopilador en la página Web de módulos auxiliares (plug-ins) de Sentinel (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

5.7 Entorno virtual

Sentinel se ha probado a fondo en servidores VMware ESX y la compatibilidad es total. Al configurar un entorno virtual, los equipos virtuales deben tener 2 o más CPU. Para obtener resultados de rendimiento comparables a los resultados obtenidos en las pruebas con equipos físicos en ESX o en otro entorno virtual, el entorno virtual debe contar con la misma capacidad de memoria, CPU, espacio en disco y opciones de E/S que las recomendaciones para equipos físicos.

Para obtener información sobre recomendaciones para equipos físicos, consulte la Capítulo 5, “Cumplimiento de los requisitos del sistema”, en la página 35.

6 Consideraciones de implementación para el uso de Sentinel en modo FIPS140-2

Sentinel puede configurarse de forma opcional para usar los Servicios de seguridad de la red de Mozilla (NSS), que es un proveedor de cifrado validado FIPS 140-2, para sus funciones internas de cifrado y de otro tipo. El objetivo de hacer esto es garantizar que Sentinel integre 'FIPS 140-2 en su interior' y que cumpla con las directivas y los estándares federales de adquisición de los Estados Unidos.

Habilitar el modo FIPS 140-2 en Sentinel facilita la comunicación entre el servidor Sentinel, los gestores de recopiladores remotos de Sentinel, los motores de correlación remotos de Sentinel, la interfaz de usuario web de Sentinel, el Centro de control de Sentinel y el servicio Asesor de Sentinel para usar cifrado validado FIPS 140-2.

6.1 Implementación de FIPS en Sentinel

Sentinel utiliza las bibliotecas NSS de Mozilla suministradas por el sistema operativo. Red Hat Enterprise Linux (RHEL) y SUSE Linux Enterprise Server (SLES) tienen conjuntos diferentes de paquetes NSS.

El módulo de cifrado NSS proporcionado por RHEL 6.2 está validado para FIPS 140-2. El módulo de cifrado NSS proporcionado por SLES 11 SP2 aún no ha sido validado oficialmente para FIPS 140-2, pero la validación del módulo SUSE para FIPS 140-2 está en curso. Una vez que esté disponible la validación, no prevé la necesidad de realizar cambios a Sentinel para integrar 'FIPS 140-2 en el interior' en la plataforma SUSE.

Para obtener más información acerca de la certificación FIPS 140-2 en RHEL 6.2, consulte los *Módulos de cifrado validados FIPS 140-1 y FIPS 140-2*.

6.1.1 Paquetes de NSS de RHEL

Sentinel requiere los siguientes paquetes NSS de 64 bits para admitir el modo FIPS 140-2:

- nspr-4.9-1.el6.x86_64
- nss-sysinit-3.13.3-6.el6.x86_64
- nss-util-3.13.3-2.el6.x86_64

- nss-softokn-freebl-3.12.9-11.el6.x86_64
- nss-softokn-3.12.9-11.el6.x86_64
- nss-3.13.3-6.el6.x86_64
- nss-tools-3.13.3-6.el6.x86_64

Si alguno de estos paquetes no está instalado, debe instalarlo antes de habilitar el modo FIPS 140-2 en Sentinel.

6.1.2 Paquetes NSS de SLES

Sentinel requiere los siguientes paquetes NSS de 64 bits para admitir el modo FIPS 140-2:

- libfreebl3-3.13.1-0.2.1
- mozilla-nspr-4.8.9-1.2.2.1
- mozilla-nss-3.13.1-0.2.1
- mozilla-nss-tools-3.13.1-0.2.1

Si alguno de estos paquetes no está instalado, debe instalarlo antes de habilitar el modo FIPS 140-2 en Sentinel.

6.2 Componentes habilitados para FIPS en Sentinel

Los siguientes componentes de Sentinel son compatibles con FIPS 140-2:

- Todos los componentes de la plataforma Sentinel se actualizan para admitir el modo FIPS 140-2.
- Los siguientes módulos auxiliares (plug-ins) de Sentinel que admiten cifrado se actualizan para admitir el modo FIPS 140-2:
  - Agent Manager Connector 2011.1r1 y versiones posteriores
  - Database (JDBC) Connector 2011.1r2 y versiones posteriores
  - File Connector 2011.1r1 y versiones posteriores - Solo si el tipo de origen de evento del archivo es local o NFS.
  - LDAP Integrator 2011.1r1 y versiones posteriores
  - Sentinel Link Connector 2011.1r3 y versiones posteriores
  - Sentinel Link Integrator 2011.1r2 y versiones posteriores
  - SMTP Integrator 2011.1r1 y versiones posteriores
  - Syslog Connector 2011.1r2 y versiones posteriores
  - Windows Event (WMI) Connector 2011.1r2 y versiones posteriores

  Para obtener más información sobre cómo configurar estos módulos auxiliares (plug-ins) de Sentinel para ejecutarse en modo FIPS 140-2, consulte "Configuración de módulos auxiliares (plug-ins) de Sentinel para la ejecución en modo FIPS 140-2" en la página 116.

Los siguientes conectores de Sentinel que admiten cifrado opcional no se habían actualizado aún para admitir el modo FIPS 140-2 en el momento de publicar este documento. Sin embargo, puede seguir recopilando eventos con estos conectores. Para obtener instrucciones sobre cómo usar estos conectores con Sentinel en el modo FIPS 140-2, consulte "Uso de conectores no habilitados para FIPS con Sentinel en el modo FIPS 140-2" en la página 121.

- Check Point (LEA) Connector 2011.1r2

- Cisco SDEE Connector 2011.1r1
- File Connector 2011.1r1 - Las funciones de CIFS y SCP incluyen cifrado y no funcionarán en el modo FIPS 140-2.
- NetIQ Audit Connector 2011.1r1
- SNMP Connector 2011.1r1

Los siguientes integradores de Sentinel que admiten SSL no se habían actualizado aún para admitir el modo FIPS 140-2 en la fecha de publicación de este documento. Sin embargo, puede seguir usando conexiones sin cifrar cuando se utilicen estos integradores con Sentinel en el modo FIPS 140-2.

- Remedy Integrator 2011.1r1 o versiones posteriores
- SOAP Integrator 2011.1r1 o versiones posteriores

Cualquier otro módulo auxiliar (plug-in) de Sentinel que no esté en la lista anterior no usa cifrado y no se ve afectado al habilitar el modo FIPS 140-2 en Sentinel. No es necesario realizar ningún otro paso para usarlos con Sentinel en modo FIPS 140-2.

Para obtener más información sobre los módulos auxiliares (plug-ins) de Sentinel, consulte el sitio web de módulos auxiliares de Sentinel. Si desea solicitar que uno de los módulos auxiliares (plug-ins) que aún no se ha actualizado esté disponible con compatibilidad para FIPS, envíe una solicitud mediante Bugzilla.

6.3 Lista de verificación de implementación

La tabla siguiente ofrece una descripción general de las tareas necesarias para configurar Sentinel para el funcionamiento en modo FIPS 140-2.

Tareas	Para obtener más información, consulte la…
Planifique la implementación.	Sección 6.4, “Entornos de instalación”, en la página 56.
Determine si necesita habilitar el modo FIPS 140-2 durante la instalación de Sentinel o si desea habilitarlo en el futuro. Para habilitar Sentinel en el modo FIPS 140-2 durante la instalación, deberá seleccionar el método de instalación Personalizado o Silencioso durante el proceso de instalación.	Sección 11.2.2, “Instalación personalizada”, en la página 75. Sección 11.3, “Instalación silenciosa”, en la página 77 Capítulo 18, “Habilitar el modo FIPS 140-2 en una instalación de Sentinel existente”, en la página 111
Configure los módulos auxiliares (plug-ins) de Sentinel para ejecutarse en modo FIPS 140-2.	Sección 19.5, “Configuración de módulos auxiliares (plug-ins) de Sentinel para la ejecución en modo FIPS 140-2”, en la página 116.
Importe certificados en el Almacén de claves de FIPS de Sentinel.	Sección 19.6, “Importación de certificados en la base de datos del almacén de claves de FIPS”, en la página 122

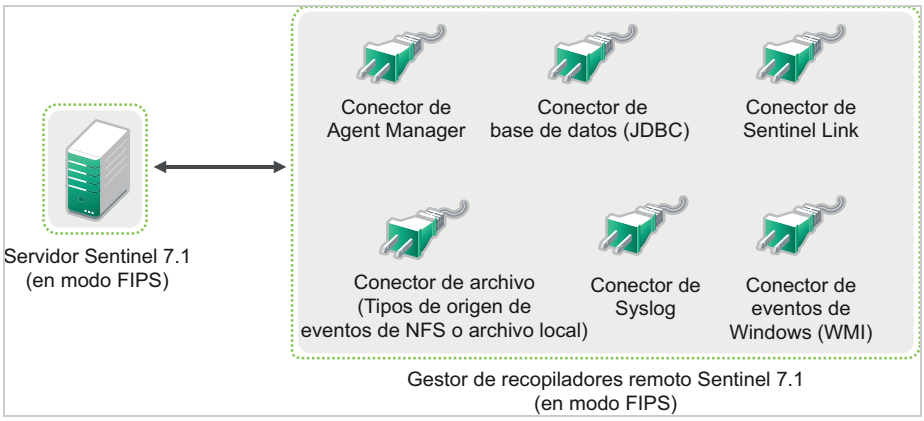
Nota: NetIQ recomienda encarecidamente realizar una copia de seguridad de sus sistemas Sentinel antes de iniciar la conversión al modo FIPS. Si por algún motivo es necesario revertir el servidor a un modo que no sea FIPS, el único método admitido para ello implica la restauración a partir de una copia de seguridad. Para obtener más información sobre cómo revertir a un modo diferente de FIPS, consulte “Reversión de Sentinel al modo diferente de FIPS” en la página 122.

6.4 Entornos de instalación

En esta sección se proporciona información sobre los diferentes escenarios de implementación de Sentinel en modo FIPS 140-2.

6.4.1 Escenario 1: Recopilación de datos en modo FIPS 140-2 completo

En este escenario, se realiza la recopilación de datos solamente a través de conectores compatibles con el modo FIPS 140-2. Se presupone que este entorno tiene un servidor Sentinel y que los datos se recopilan a través de un gestor de recopiladores remoto. Puede tener uno o varios gestores de recopiladores remotos.



Debe realizar el siguiente procedimiento únicamente si su entorno incluye recopilación de datos de orígenes de eventos que utilizan conectores compatibles con el modo FIPS 140-2.

1. Debe tener un servidor Sentinel 7.1 en modo FIPS 140-2.

   Nota: Si su servidor Sentinel (recién instalado o actualizado) no tiene habilitado el modo FIPS, debe habilitar FIPS en el servidor Sentinel. Para obtener más información, consulte la "Habilitar el servidor Sentinel para su ejecución en modo FIPS 140-2" en la página 111.

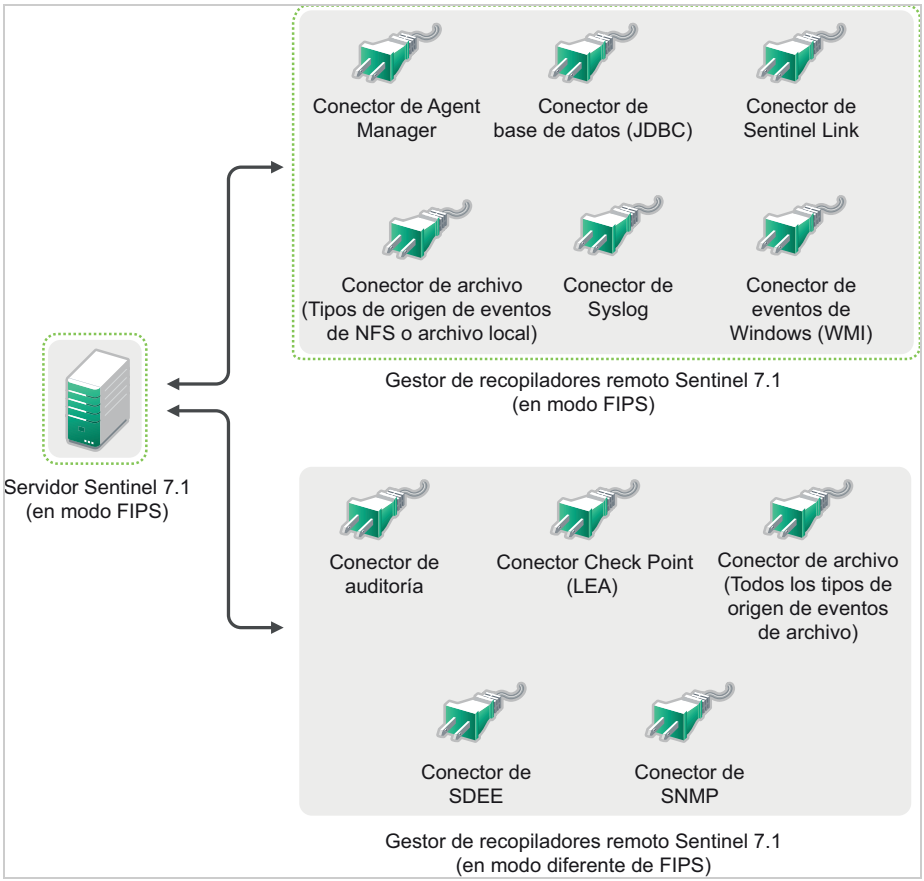
2. Debe tener un gestor de recopiladores remoto Sentinel 7.1 que se ejecute en modo FIPS 140-2.

   Nota: Si su gestor de recopiladores remoto (recién instalado o actualizado) no se ejecuta en el modo FIPS, debe habilitar FIPS en el gestor de recopiladores remoto. Para obtener más información, consulte la "Habilitar el modo FIPS 140-2 en gestores de recopiladores y motores de correlación remotos" en la página 111.

3. Asegúrese de que el servidor FIPS y los gestores de recopiladores remotos se comuniquen entre sí.
4. Convierta los motores de correlación remotos si los hay para que se ejecuten en modo FIPS. Para obtener más información, consulte la "Habilitar el modo FIPS 140-2 en gestores de recopiladores y motores de correlación remotos" en la página 111.
5. Configure los módulos auxiliares (plug-ins) de Sentinel para que se ejecuten en modo FIPS 140-2. Para obtener más información, consulte la "Configuración de módulos auxiliares (plug-ins) de Sentinel para la ejecución en modo FIPS 140-2" en la página 116.

6.4.2 Escenario 2: Recopilación de datos en modo FIPS 140-2 parcial

En este escenario, la recopilación de datos se realiza utilizando conectores compatibles con el modo FIPS 140-2 y conectores no compatibles con el modo FIPS 140-2. Se presupone que este entorno tiene un servidor Sentinel y que los datos se recopilan a través de un gestor de recopiladores remoto. Puede tener uno o varios gestores de recopiladores remotos.



Para manejar la recopilación de datos mediante conectores compatibles y otros no compatibles con el modo FIPS 140-2, se recomienda tener dos gestores de recopiladores remotos: uno que se ejecute en modo FIPS 140-2 para los conectores compatibles con FIPS y otro que se ejecute en modo diferente de FIPS (normal) para los conectores que no son compatibles con el modo FIPS 140-2.

Debe realizar el siguiente procedimiento si su entorno implica recopilar datos de orígenes de eventos que utilizan conectores compatibles con el modo FIPS 140-2 y conectores que aún no son compatibles con el modo FIPS 140-2.

1 Debe tener un servidor Sentinel 7.1 en el modo FIPS 140-2.

Nota: Si su servidor Sentinel (recién instalado o actualizado) no tiene habilitado el modo FIPS, debe habilitar FIPS en el servidor Sentinel. Para obtener más información, consulte la "Habilitar el servidor Sentinel para su ejecución en modo FIPS 140-2" en la página 111.

2 Asegúrese de que un gestor de recopiladores remoto se ejecute en modo FIPS 140-2 y otro gestor de recopiladores remoto se ejecute en modo diferente de FIPS.

   2a Si no tiene un gestor de recopiladores remoto con el modo FIPS 140-2 habilitado, debe habilitar el modo FIPS en el gestor de recopiladores remoto. Para obtener más información, consulte la "Habilitar el modo FIPS 140-2 en gestores de recopiladores y motores de correlación remotos" en la página 111.

   2b Actualice el certificado del servidor en el gestor de recopiladores remoto sin modo FIPS. Para obtener más información, consulte la "Actualización de certificados del servidor en gestores de recopiladores y motores de correlación remotos" en la página 115.

3 Asegúrese de que los dos gestores de recopiladores remotos se comuniquen con el servidor Sentinel habilitado para FIPS 140-2.

4 Convierta los motores de correlación remotos, si los hay, para ejecutarse en modo FIPS. Para obtener más información, consulte la "Habilitar el modo FIPS 140-2 en gestores de recopiladores y motores de correlación remotos" en la página 111.

5 Configure los módulos auxiliares (plug-ins) de Sentinel para que se ejecuten en modo FIPS 140-2. Para obtener más información, consulte la "Configuración de módulos auxiliares (plug-ins) de Sentinel para la ejecución en modo FIPS 140-2" en la página 116.

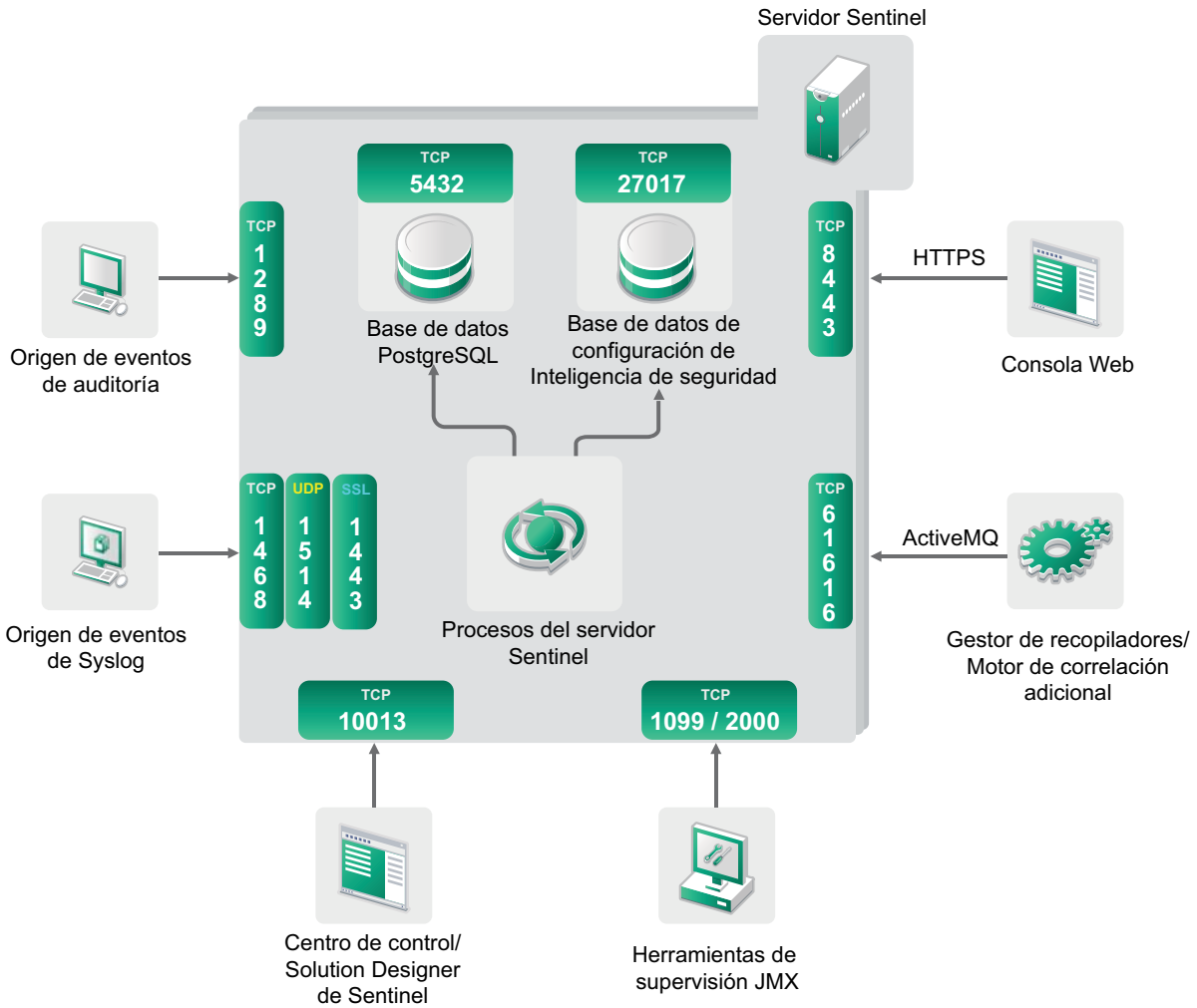
   5a Implemente conectores compatibles con el modo FIPS 140-2 en el gestor de recopiladores remoto que se ejecuta en modo FIPS.

   5b Implemente los conectores que no son compatibles con el modo FIPS 140-2 en el gestor de recopiladores remoto que no tiene habilitado el modo FIPS.

7 Puertos utilizados

Sentinel utiliza diferentes puertos para la comunicación externa con otros componentes. Para la instalación del dispositivo, los puertos se abren en el cortafuegos por defecto. No obstante, para la instalación tradicional, es necesario configurar el sistema operativo en el que va a instalar Sentinel para poder abrir los puertos en el cortafuegos. La figura a continuación ilustra los puertos utilizados en Sentinel:

Figura 7-1 *Puertos utilizados en Sentinel*



7.1 Puertos del servidor Sentinel

El servidor Sentinel utiliza los siguientes puertos para las comunicaciones internas y externas.

7.1.1 Puertos locales

Sentinel utiliza los siguientes puertos para la comunicación interna con la base de datos y demás procesos internos:

Puertos	Descripción
TCP 27017	Se utiliza para la base de datos de configuración Inteligencia de seguridad.
TCP 28017	Se utiliza para la interfaz Web de la base de datos Inteligencia de seguridad.
TCP 32000	Se utiliza para la comunicación interna entre el proceso empaquetador (wrapper) y el proceso del servidor.

7.1.2 Puertos de red

Para que Sentinel funcione correctamente, asegúrese de que estén abiertos en el cortafuegos los siguientes puertos:

Puertos	Dirección	Necesario/ Opcional	Descripción
TCP 5432	Entrante	Opcional. Por defecto, este puerto solo escucha la interfaz de retrobucle.	Se utiliza para la base de datos PostgreSQL. No es necesario abrir este puerto por defecto. No obstante, debe abrir este puerto cuando elabore informes utilizando el SDK de Sentinel. Para obtener más información, consulte el SDK de módulos auxiliares (plug-in) de Sentinel.
TCP 1099 y 2000	Entrante	Opcional	Los utilizan conjuntamente las herramientas de supervisión para conectar con el proceso del servidor Sentinel utilizando las Extensiones de gestión de Java (JMX).
TCP 1289	Entrante	Opcional	Se utiliza para las conexiones de Audit.
UDP 1514	Entrante	Opcional	Se utiliza para los mensajes de syslog.
TCP 8443	Entrante	Requerido	Se utiliza para la comunicación de HTTPS.
TCP 1443	Entrante	Opcional	Se utiliza para los mensajes de syslog con SSL cifrado.
TCP 61616	Entrante	Opcional	Se utiliza para las conexiones entrantes de gestores de recopiladores y motores de correlación.
TCP 10013	Entrante	Requerido	Utilizados por el Centro de control de Sentinel y Solution Designer.
TCP 1468	Entrante	Opcional	Se utiliza para los mensajes de syslog.
TCP 10014	Entrante	Opcional	Lo utilizan los gestores de recopiladores remotos con el fin de conectar con el servidor a través de un proxy de SSL. Sin embargo, esto es poco común. Por defecto, los gestores de recopiladores remotos utilizan el puerto SSL 61616 para conectar con el servidor.

Puertos	Dirección	Necesario/ Opcional	Descripción
TCP 443	Saliente	Opcional	Si se utiliza el Asesor, el puerto inicia una conexión con el servicio del Asesor a través de Internet a la dirección URL de actualizaciones del Asesor (https://secure-www.novell.com/sentinel/download/advisor/).
TCP 8443	Saliente	Opcional	Si se utiliza una búsqueda distribuida, el puerto inicia una conexión con otros sistemas Sentinel para llevar a cabo la búsqueda distribuida.
TCP 389 o 636	Saliente	Opcional	Si se utiliza la autenticación LDAP, el puerto inicia una conexión con el servidor LDAP.
TCP/UDP 111 y TCP/UDP 2049	Saliente	Opcional	Si está configurado el almacenamiento en red para usar NFS.
TCP 137, 138, 139, 445	Saliente	Opcional	Si está configurado el almacenamiento en red para usar CIFS.
TCP JDBC (dependiente de la base de datos)	Saliente	Opcional	Si se utiliza sincronización de datos, el puerto inicia una conexión con la base de datos de destino mediante JDBC. El puerto utilizado depende de la base de datos de destino.
TCP 25	Saliente	Opcional	Inicia una conexión con el servidor de correo.
TCP 1290	Saliente	Opcional	Cuando Sentinel reenvía eventos a otro sistema Sentinel, este puerto inicia una conexión de Sentinel Link a ese sistema.
UDP 162	Saliente	Opcional	Cuando Sentinel reenvía eventos al sistema que recibe mensajes de alerta de SNMP, el puerto envía un paquete al receptor.
UDP 514 o TCP 1468	Saliente	Opcional	Este puerto se utiliza cuando Sentinel reenvía eventos al sistema que recibe mensajes de Syslog. Si el puerto es UDP, envía un paquete al receptor. Si el puerto es TCP, inicia una conexión con el receptor.

7.1.3 Puertos específicos del dispositivo del servidor Sentinel

Además de los puertos anteriores, están abiertos los siguientes puertos para el dispositivo.

Puertos	Dirección	Necesario/ Opcional	Descripción
TCP 22	Entrante	Requerido	Se utiliza para el acceso mediante secure shell al dispositivo Sentinel
TCP 54984	Entrante	Requerido	Lo utiliza la consola de gestión del dispositivo de Sentinel (WebYaST). También lo utiliza el dispositivo Sentinel para el servicio de actualización.
TCP 289	Entrante	Opcional	Se reenvía a 1289 para las conexiones de Audit.
UDP 443	Entrante	Opcional	Se remite a 8443 para la comunicación HTTPS.
UDP 514	Entrante	Opcional	Se reenvía a 1514 para los mensajes de syslog.

Puertos	Dirección	Necesario/ Opcional	Descripción
TCP 1290	Entrante	Opcional	Puerto de Sentinel Link al que se permite conectar a través del cortafuegos de SuSE.
UDP y TCP 40000 - 41000	Entrante	Opcional	Puertos que pueden utilizarse al configurar los servidores de recopilación de datos, como syslog. Sentinel no escucha estos puertos por defecto.
TCP 443 o 80	Saliente	Requerido	Inicia una conexión al repositorio de actualización del software del dispositivo de NetIQ en Internet o a un servicio de Subscription Management Tool de su red.
TCP 80	Saliente	Opcional	Inicia una conexión a Subscription Management Tool.

7.2 Puertos del gestor de recopiladores

El gestor de recopiladores utiliza los siguientes puertos para comunicarse con otros componentes.

7.2.1 Puertos de red

Para que el gestor de recopiladores de Sentinel funcione correctamente, asegúrese de que estén abiertos en el cortafuegos los siguientes puertos:

Puertos	Dirección	Necesario/ Opcional	Descripción
TCP 1289	Entrante	Opcional	Se utiliza para las conexiones de Audit.
UDP 1514	Entrante	Opcional	Se utiliza para los mensajes de syslog.
TCP 1443	Entrante	Opcional	Se utiliza para los mensajes de syslog con SSL cifrado.
TCP 1468	Entrante	Opcional	Se utiliza para los mensajes de syslog.
TCP 1099 y 2000	Entrante	Opcional	Los utilizan conjuntamente las herramientas de supervisión para conectar con el proceso del servidor Sentinel utilizando las Extensiones de gestión de Java (JMX).
TCP 61616	Saliente	Requerido	Inicia una conexión con el servidor Sentinel.

7.2.2 Puertos específicos del dispositivo del gestor de recopiladores

Además de los puertos anteriores, los siguientes puertos están abiertos para el dispositivo del gestor de recopiladores de Sentinel.

Puertos	Dirección	Necesario/ Opcional	Descripción
TCP 22	Entrante	Requerido	Se utiliza para el acceso mediante secure shell al dispositivo Sentinel

Puertos	Dirección	Necesario/ Opcional	Descripción
TCP 54984	Entrante	Requerido	Lo utiliza la consola de gestión del dispositivo de Sentinel (WebYaST). También lo utiliza el dispositivo Sentinel para el servicio de actualización.
TCP 289	Entrante	Opcional	Se reenvía a 1289 para las conexiones de Audit.
UDP 514	Entrante	Opcional	Se reenvía a 1514 para los mensajes de syslog.
TCP 1290	Entrante	Opcional	Este es el puerto de Sentinel Link al que se permite conectar a través del cortafuegos de SuSE.
UDP y TCP 40000 - 41000	Entrante	Opcional	Puertos que pueden utilizarse al configurar los servidores de recopilación de datos, como syslog. Sentinel no escucha estos puertos por defecto.
TCP 443	Saliente	Requerido	Inicia una conexión al repositorio de actualización del software del dispositivo de NetIQ en Internet o a un servicio de Subscription Management Tool de su red.
TCP 80	Saliente	Opcional	Inicia una conexión a Subscription Management Tool.

7.3 Puertos del motor de correlación

El motor de correlación utiliza los siguientes puertos para comunicarse con otros componentes.

7.3.1 Puertos de red

Para que el motor de correlación de Sentinel funcione correctamente, asegúrese de que los siguientes puertos estén abiertos en el cortafuegos:

Puertos	Dirección	Necesario/ Opcional	Descripción
TCP 1099 y 2000	Entrante	Opcional	Los utilizan conjuntamente las herramientas de supervisión para conectar con el proceso del servidor Sentinel utilizando las Extensiones de gestión de Java (JMX).
TCP 61616	Saliente	Requerido	Inicia una conexión con el servidor Sentinel.

7.3.2 Puertos específicos del dispositivo del motor de correlación

Además de los puertos anteriores, los siguientes puertos están abiertos en el dispositivo del motor de correlación de Sentinel.

Puertos	Dirección	Necesario/ Opcional	Descripción
TCP 22	Entrante	Requerido	Se utiliza para el acceso mediante secure shell al dispositivo Sentinel

Puertos	Dirección	Necesario/ Opcional	Descripción
TCP 54984	Entrante	Requerido	Lo utiliza la consola de gestión del dispositivo de Sentinel (WebYaST). También lo utiliza el dispositivo Sentinel para el servicio de actualización.
TCP 443	Saliente	Requerido	Inicia una conexión al repositorio de actualización del software del dispositivo de NetIQ en Internet o a un servicio de Subscription Management Tool de su red.
TCP 80	Saliente	Opcional	Inicia una conexión a Subscription Management Tool.

8 Opciones de instalación

Puede realizar una instalación tradicional de Sentinel o instalar el dispositivo. En este capítulo se proporciona información sobre las dos opciones de instalación.

8.1 Instalación tradicional

La instalación tradicional instala Sentinel en un sistema operativo SUSE Linux Enterprise Server (SLES) 11 o Red Hat Enterprise Linux (RHEL) 6 existente, mediante el instalador de la aplicación. Puede instalar Sentinel de las formas siguientes:

- **Interactivo:** la instalación se lleva a cabo con datos que introduce el usuario. Durante la instalación, puede registrar las opciones de instalación (valores introducidos por el usuario o valores por defecto) en un archivo, que podrá utilizar posteriormente para una instalación en modo silencioso. Puede realizar una instalación estándar o personalizada.

Instalación estándar	Instalación personalizada
Utiliza los valores por defecto para la configuración. Sólo se requiere la intervención del usuario para introducir la contraseña.	Le indica que debe especificar valores de configuración. Puede seleccionar valores por defecto o especificar los valores necesarios.
Se instala con una clave de evaluación por defecto de 90 días.	Le permite realizar la instalación con una clave de licencia de 90 días o con una clave de licencia válida.
Permite especificar la contraseña del administrador y utiliza esta contraseña como contraseña por defecto tanto para el usuario dbauser como appuser.	Permite especificar la contraseña del administrador. Para dbauser y appuser, puede especificar una contraseña nueva o usar la contraseña del administrador.
Instala los puertos por defecto para todos los componentes.	Le permite especificar puertos para diferentes componentes.
Instala Sentinel en modo diferente de FIPS.	Permite instalar Sentinel en modo FIPS 140-2.
Autentica los usuarios con la base de datos interna.	Proporciona la opción de establecer autenticación LDAP para Sentinel además de autenticación de la base de datos. Al configurar Sentinel para la autenticación LDAP, los usuarios pueden entrar en el servidor utilizando sus credenciales de Novell eDirectory o de Microsoft Active Directory.

Para obtener más información sobre una instalación interactiva, consulte Sección 11.2, “Realización de una instalación interactiva”, en la página 74.

- **Silencio:** Si desea instalar varios servidores de Sentinel en su implantación, puede registrar las opciones de instalación durante la instalación estándar o personalizada en un archivo de configuración y luego usar el archivo para ejecutar una instalación sin supervisión. Para obtener más información acerca de una instalación en modo silencioso, consulte la Sección 11.3, "Instalación silenciosa", en la página 77.

8.2 Instalación del dispositivo

La instalación del dispositivo instala tanto el sistema operativo SLES 11 SP2 de 64 bits como Sentinel.

El dispositivo Sentinel está disponible en los formatos siguientes:

- Una imagen de dispositivo VMWare
- Una imagen de dispositivo Xen
- Una imagen de dispositivo hardware Live DVD que se distribuye directamente en un servidor de hardware

Para obtener más información sobre la instalación del dispositivo, consulte el Capítulo 12, "Instalación del dispositivo", en la página 83.

III Instalación de Sentinel

En esta sección se proporciona información sobre la instalación de Sentinel y componentes adicionales.

9 Descripción general de la instalación

La instalación de Sentinel instala los siguientes componentes en el servidor Sentinel:

- **Proceso del servidor Sentinel:** este es el primer componente de Sentinel. El proceso del servidor Sentinel maneja las peticiones de otros componentes de Sentinel y facilita la funcionalidad del sistema de forma transparente. El proceso del servidor Sentinel maneja las peticiones, por ejemplo de filtrado de datos, el procesamiento de consultas de búsqueda y la gestión de tareas administrativas que incluyen autenticación y autorización de usuarios.
- **Servidor Web:** Sentinel utiliza Jetty como servidor Web para permitir la conexión segura con la interfaz Web de Sentinel.
- **Base de datos de PostgreSQL:** Sentinel tiene una base de datos integrada que almacena la información de configuración de Sentinel, los datos de activos y vulnerabilidad, la información de identidad, el estado de incidencias y del flujo de trabajo, etc.
- **Base de datos MongoDB:** almacena los datos de Inteligencia de seguridad.
- **Gestor de recopiladores:** El gestor de recopiladores proporciona un punto de recopilación de datos flexible para Sentinel. El instalador de Sentinel instala un gestor de recopiladores por defecto durante la instalación.
- **Motor de correlación:** El motor de correlación procesa eventos del flujo de eventos en tiempo real para determinar si estos deberían activar alguna de las reglas de correlación.
- **Asesor:** El Asesor, con tecnología de Security Nexus, es un servicio de suscripción opcional que proporciona una correlación a nivel de dispositivo entre eventos en tiempo real, desde los sistemas de prevención y detección de intrusiones, y los resultados de la exploración de vulnerabilidades empresariales. Para más información sobre el asesor, visite "Cómo configurar el asesor" en la *Guía de administración de NetIQ Sentinel 7.1*.
- **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. Puede descargar módulos auxiliares (plug-ins) adicionales del sitio web de módulos auxiliares de Sentinel. Los módulos auxiliares (plug-ins) de Sentinel incluyen lo siguiente:
  - Recopiladores
  - Conectores
  - Reglas y acciones de correlación
  - Informes
  - Flujos de trabajo de iTRAC
  - Paquetes de soluciones

Sentinel dispone de una arquitectura muy ampliable y, en caso de que se espere un gran número de eventos, puede distribuir los componentes entre varios equipos para conseguir el mejor rendimiento del sistema. La ampliación independiente de componentes ofrece un rendimiento y una capacidad de ampliación rentables.

9.1 Ventajas de los gestores de recopiladores adicionales

Puede instalar gestores de recopiladores adicionales en ubicaciones adecuadas de su red. Estos gestores de recopiladores remotos ejecutan conectores y recopiladores y reenvían los datos obtenidos al servidor Sentinel para su almacenamiento y procesamiento. Para obtener información sobre la instalación de gestores de recopiladores adicionales, consulte Sección 11.6, “Instalación de gestores de recopiladores y motores de correlación adicionales”, en la página 80.

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 datos de eventos en un entorno distribuido, lo que incrementa 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.
- **Almacenamiento de archivos en el caché:** los gestores de recopiladores adicionales pueden 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.

Nota: No es posible instalar más de un gestor de recopiladores en un solo sistema. Puede instalar más gestores de recopiladores en sistemas remotos y conectarlos después al servidor Sentinel.

9.2 Ventajas de los motores de correlación adicionales

Puede distribuir múltiples motores de correlación, cada uno en su propio servidor, sin necesidad de replicar configuraciones ni añadir bases de datos. Para los entornos que tengan gran cantidad de reglas de correlación o un número extremadamente elevado de eventos, puede ser beneficioso instalar más de un motor de correlación y volver a implementar algunas reglas en el nuevo motor de correlación. Varios motores de correlación proporcionan la capacidad de ampliarse a medida que el sistema Sentinel incorpora orígenes de datos adicionales o aumenta el número de eventos. Para obtener información sobre la instalación de motores de correlación adicionales, consulte Sección 11.6, “Instalación de gestores de recopiladores y motores de correlación adicionales”, en la página 80.

Nota: No es posible instalar más de un motor de correlación en un solo sistema. Puede instalar motores de correlación adicionales en sistemas remotos y luego conectarlos al servidor Sentinel.

10 Lista de verificación de instalación

Asegúrese de haber realizado las siguientes tareas antes de iniciar la instalación:

- ❒ Verifique que el hardware y el software cumplen los requisitos del sistema enumerados en la Capítulo 5, "Cumplimiento de los requisitos del sistema", en la página 35.
- ❒ Si había una instalación previa de Sentinel, asegúrese de que no queden archivos ni ajustes del sistema de una instalación anterior. Para obtener más información, consulte la Apéndice C, "Desinstalación", en la página 159.
- ❒ Si piensa instalar la versión con licencia, obtenga su clave de licencia del Centro de atención al cliente de Novell.
- ❒ Asegúrese de que los puertos enumerados en la Capítulo 7, "Puertos utilizados", en la página 59 estén abiertos en el cortafuegos.
- ❒ Para que el instalador de Sentinel funcione adecuadamente, el sistema debe poder enviar el nombre de host o una dirección IP válida. Para hacerlo, añada el nombre de host al archivo `/etc/hosts` en la línea que contiene la dirección IP y luego introduzca `hostname -f` para asegurarse de que el nombre de host se muestre correctamente.
- ❒ Sincronice el tiempo utilizando el protocolo de tiempo de red (NTP).
- ❒ **En sistemas RHEL:** Para obtener un rendimiento óptimo, los ajustes de memoria deben definirse correctamente para la base de datos PostgreSQL. El parámetro SHMMAX debe ser mayor o igual que 1073741824.

  Para establecer el valor adecuado, añada la siguiente información al final del archivo `/etc/sysctl.conf`:

  ```
  # for Sentinel Postgresql
  kernel.shmmax=1073741824
  ```

- ❒ **Para instalaciones tradicionales:**
  - ❒ Asegúrese de que IPv6 esté habilitado en su sistema operativo. Si no lo está, algunos componentes fundamentales no funcionarán correctamente.
  - ❒ El sistema operativo del servidor Sentinel debe incluir al menos los componentes del Servidor base del servidor SLES o del servidor RHEL 6. Sentinel requiere las versiones de 64 bits de los siguientes RPM:
    - bash
    - bc
    - coreutils
    - gettext
    - glibc
    - grep
    - libgcc

- libstdc
- lsof
- net-tools
- openssl
- python-libs
- sed
- zlib

11 Instalación tradicional

En este capítulo se proporciona información sobre las diversas formas de instalar Sentinel.

11.1 Descripción de las opciones de instalación

`./install-sentinel --help` muestra las siguientes opciones:

Opciones	Valor	Descripción
--location	Directorio	Especifica un directorio diferente de root (/) para instalar Sentinel.
-m, --manifest	Nombre de archivo	Especifica un archivo de inventario del producto que se utilizará en lugar del archivo de inventario por defecto.
--no-configure		Especifica que no se debe configurar el producto después de la instalación.
-n, --no-start		Especifica que no se debe iniciar o reiniciar Sentinel después de la instalación o configuración.
-r, --recordunattended	Nombre de archivo	Especifica un archivo para registrar los parámetros que se pueden utilizar para una instalación sin supervisión.
-u, --unattended	Nombre de archivo	Utiliza parámetros del archivo especificado para instalar Sentinel en sistemas sin supervisión.
-h, --help		Muestra las opciones que se pueden utilizar al instalar Sentinel.
-l, --log-file	Nombre de archivo	Registra los mensajes del registro en un archivo.
--no-banner		Anula la visualización de un mensaje de banda.
-q, --quiet		Muestra menos mensajes.
-v, --verbose		Muestra todos los mensajes durante la instalación.

11.2 Realización de una instalación interactiva

En esta sección se proporciona información sobre la instalación estándar y personalizada.

- Sección 11.2.1, “Instalación estándar”, en la página 74
- Sección 11.2.2, “Instalación personalizada”, en la página 75

11.2.1 Instalación estándar

Siga los pasos indicados a continuación para llevar a cabo una instalación estándar:

1. Descargue el archivo de instalación de Sentinel de la página Web de descargas de Novell (http://download.novell.com/index.jsp):
   - **1a** En el campo *Product or Technology* (Producto o Tecnología), examine y seleccione *SIEM-Sentinel*.
   - **1b** Haga clic en *Buscar*.
   - **1c** Haga clic en el botón de la columna *Download* (Descargar) para obtener una versión de *Evaluación de Sentinel 7.1*.
   - **1d** Haga clic en *proceed to download* (continuar con la descarga), y luego especifique su nombre de usuario y contraseña.
   - **1e** Haga clic en *download* (descargar) para obtener la versión de instalación de su plataforma.
2. Especifique en la línea de comandos el siguiente comando para extraer el archivo de instalación.

   ```
   tar zxvf <install_filename>
   ```

   Reemplace <*nombre de archivo_instalación*> por el nombre real del archivo de instalación.
3. Acceda al directorio en el que ha extraído el instalador:

   ```
   cd <directory_name>
   ```
4. Especifique el siguiente comando para instalar Sentinel:

   ```
   ./install-sentinel
   ```

   O bien

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

   ```
   ./install-sentinel -r <response_filename>
   ```
5. Especifique el número del idioma que desea utilizar para la instalación y luego pulse Intro.

   El acuerdo de licencia de usuario final se muestra en el idioma seleccionado.
6. Pulse la barra espaciadora para leer todo el acuerdo de licencia.
7. Introduzca `yes` o `y` para aceptar la licencia y continuar con la instalación.

   La instalación puede tardar unos segundos en cargar los paquetes de instalación y solicitar el tipo de configuración.
8. Cuando se le indique, especifique `1` para continuar con la configuración 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.

9 Especifique la contraseña del usuario administrador `admin`.

10 Confirme la contraseña de nuevo.

Esta contraseña la utilizan los usuarios `admin`, `dbauser` y `appuser`.

La instalación de Sentinel finaliza y se inicia el servidor. Puede tardarse unos segundos en iniciar todos los servicios después de la instalación porque el sistema realiza una inicialización única. Espere a que termine la instalación antes de entrar en el servidor.

Para acceder a la interfaz Web de Sentinel, especifique la siguiente dirección URL en el navegador Web:

`https://<IP_Address_Sentinel_server>:8443.`

El valor <*dirección_IP_servidor_Sentinel*> es la dirección IP o el nombre de DNS del servidor Sentinel y 8443 es el puerto por defecto del servidor Sentinel.

11.2.2 Instalación personalizada

Si va a instalar Sentinel con una configuración personalizada, puede especificar la clave de licencia, cambiar la contraseña para diferentes usuarios y especificar valores para puertos diferentes que se utilizan para interactuar con los componentes internos.

1 Descargue el archivo de instalación de Sentinel de la página Web de descargas de Novell :

1a En el campo *Product or Technology* (Producto o Tecnología), examine y seleccione *SIEM-Sentinel*.

1b Haga clic en *Buscar*.

1c Haga clic en el botón de la columna *Download* (Descargar) para obtener una versión de *Evaluación de Sentinel 7.1*.

1d Haga clic en *proceed to download* (continuar con la descarga), y luego especifique su nombre de usuario y contraseña.

1e Haga clic en *download* (descargar) para obtener la versión de instalación de su plataforma.

2 Especifique en la línea de comandos el siguiente comando para extraer el archivo de instalación.

`tar zxvf <install_filename>`

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

3 Especifique el siguiente comando en la raíz del directorio extraído para instalar Sentinel:

`./install-sentinel`

O bien

Si desea utilizar esta configuración personalizada para instalar Sentinel en más de un sistema, puede registrar sus opciones de instalación en un archivo. Puede utilizar este archivo para una instalación de Sentinel sin supervisión en otros sistemas. Para registrar sus opciones de instalación, especifique el siguiente comando:

`./install-sentinel -r <response_filename>`

4 Especifique el número del idioma que desea utilizar para la instalación y luego pulse Intro.

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

5 Pulse la barra espaciadora para leer todo el acuerdo de licencia.

6 Introduzca `yes` o `y` para aceptar el acuerdo de licencia y continuar con la instalación.

La instalación puede tardar unos segundos en cargar los paquetes de instalación y solicitar el tipo de configuración.

7 Especifique `2` para realizar una configuración personalizada de Sentinel.

8 Introduzca `1` para usar la clave de licencia de evaluación por defecto de 90 días.

O bien

Introduzca `2` para especificar una clave de licencia adquirida para Sentinel.

9 Especifique la contraseña del usuario administrador `admin` y confirme de nuevo la contraseña.

10 Especifique la contraseña para el usuario de la base de datos `dbauser` y confirme de nuevo la contraseña.

La cuenta `dbauser` es la identidad utilizada por Sentinel para interactuar con la base de datos. La contraseña que introduzca aquí puede utilizarse para llevar a cabo tareas de mantenimiento de la base de datos, incluido el restablecimiento de la contraseña del administrador si se pierde o se olvida.

11 Especifique la contraseña para el usuario de la aplicación `appuser` y confirme de nuevo la contraseña.

12 Cambie las asignaciones de puertos de los servicios de Sentinel introduciendo el número deseado y luego especifique el nuevo número de puerto.

13 Después de cambiar los puertos, especifique 7 cuando haya terminado.

14 Introduzca `1` para autenticar a los usuarios utilizando únicamente la base de datos interna.

O bien

Si ha configurado un directorio LDAP en su dominio, introduzca `2` para autenticar a los usuarios mediante la autenticación de directorios LDAP.

El valor por defecto es `1`.

15 ***Si desea habilitar Sentinel en el modo FIPS 140-2***, pulse `s`.

15a Especifique una contraseña robusta para la base de datos del almacén de claves y confirme de nuevo la contraseña.

Nota: La contraseña debe tener como mínimo siete caracteres. La contraseña debe tener al menos tres de los siguientes tipos de caracteres: dígitos, letras minúsculas en formato ASCII, letras mayúsculas en formato ASCII, caracteres no alfanuméricos en formato ASCII y caracteres que no estén en formato ASCII.

Si el primer carácter es una letra mayúscula en ASCII o si el último carácter es un dígito, estos no se cuentan.

15b Si desea insertar certificados externos en la base de datos del almacén de claves a fin de establecer confianza, pulse `s` y especifique la vía para el archivo de certificado. De lo contrario, pulse `n`

15c Lleve a cabo la configuración del modo FIPS 140-2 realizando las tareas mencionadas en el Capítulo 19, “Funcionamiento de Sentinel en el modo FIPS 140-2”, en la página 113.

La instalación de Sentinel finaliza y se inicia el servidor. Puede tardarse unos segundos en iniciar todos los servicios después de la instalación porque el sistema realiza una inicialización única. Espere a que termine la instalación antes de entrar en el servidor.

Para acceder a la interfaz Web de Sentinel, especifique la siguiente dirección URL en el navegador Web:

`https://<IP_Address_Sentinel_server>:8443.`

El valor <*dirección_IP_servidor_Sentinel*> es la dirección IP o el nombre de DNS del servidor Sentinel y 8443 es el puerto por defecto del servidor Sentinel.

11.3 Instalación silenciosa

La instalación silenciosa o sin supervisión resulta útil si tiene que instalar más de un servidor Sentinel en su implantación. En tal caso, puede registrar los parámetros de instalación durante la instalación interactiva y luego ejecutar el archivo registrado en otros servidores. Puede registrar los parámetros de instalación mientras instala Sentinel con la configuración estándar o personalizada.

Para llevar a cabo una instalación silenciosa, asegúrese de haber registrado los parámetros de instalación en un archivo. Para obtener información sobre cómo crear el archivo de respuesta, consulte la Sección 11.2.1, "Instalación estándar", en la página 74 o bien la Sección 11.2.2, "Instalación personalizada", en la página 75.

Para habilitar Sentinel en modo FIPS 140-2, asegúrese de que el archivo de respuesta incluya los siguientes parámetros:

- ENABLE_FIPS_MODE
- NSS_DB_PASSWORD

Para realizar una instalación en modo silencioso, siga estos pasos:

1. Descargue los archivos de instalación de la página Web de descargas de Novell .
2. Entre como usuario `root` en el servidor en el que desea instalar Sentinel.
3. Especifique el siguiente comando para extraer los archivos de instalación del archivo tar:

   ```
   tar -zxvf <install_filename>
   ```

   Reemplace *<nombre de archivo_instalación>* por el nombre real del archivo de instalación.
4. Especifique el siguiente comando para instalar Sentinel en el modo silencioso:

   ```
   ./install-sentinel -u <response_file>
   ```

   La instalación continúa con los valores almacenados en el archivo de respuesta.
5. **Si elige habilitar el modo FIPS 140-2,** lleve a cabo la configuración del modo FIPS 140-2 realizando las tareas mencionadas en el Capítulo 19, "Funcionamiento de Sentinel en el modo FIPS 140-2", en la página 113.

La instalación de Sentinel finaliza y se inicia el servidor. Puede tardarse unos segundos en iniciar todos los servicios después de la instalación porque el sistema realiza una inicialización única. Espere a que termine la instalación antes de entrar en el servidor.

11.4 Instalación de Sentinel como usuario diferente de root

Si la directiva de su organización no le permite ejecutar la instalación completa de Sentinel como usuario `root`, puede realizar la instalación de Sentinel como un usuario diferente. En esta instalación, algunos pasos se realizan como usuario `root` y luego se continúa la instalación de Sentinel como otro usuario diferente creado por el usuario `root`. Por último, el usuario `root` finaliza la instalación.

1. Descargue los archivos de instalación de la página Web de descargas de Novell.
2. Especifique el siguiente comando en la línea de comandos para extraer los archivos de instalación del archivo tar:

   ```
   tar -zxvf <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 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. Si desea que el usuario diferente de root instale Sentinel en una ubicación diferente de la ubicación por defecto, especifique la opción --location junto con el comando. Por ejemplo:

```
./bin/root_install_prepare --location=/foo
```

El valor que utilice en la opción `--location foo` se antepone en las vías del directorio.

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 (Condicional) Para realizar una instalación interactiva:

7a Especifique el siguiente comando:

```
./install-sentinel
```

Para instalar Sentinel en una ubicación diferente de la ubicación por defecto, especifique la opción --location junto con el comando. Por ejemplo:.

```
./install-sentinel --location=/foo
```

7b Continúe con el Paso 9.

8 (Condicional) Para realizar una instalación silenciosa:

8a Especifique el siguiente comando:

```
./install-sentinel -u <response_file>
```

La instalación continúa con los valores almacenados en el archivo de respuesta.

8b Continúe con el Paso 12.

9 Especifique el número del idioma que desea usar para la instalación.

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

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

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

11 Se le indicará que especifique el modo de instalación.

- Si decide continuar con la configuración estándar, continúe con el Paso 8 al Paso 10 de la Sección 11.2.1, “Instalación estándar”, en la página 74.
- Si decide continuar con la configuración personalizada, continúe con el Paso 7 al Paso 14 de la Sección 11.2.2, “Instalación personalizada”, en la página 75.

12 Entre como usuario `root` y especifique el siguiente comando para finalizar la instalación:

```
./bin/root_install_finish
```

La instalación de Sentinel finaliza y se inicia el servidor. Puede tardarse unos segundos en iniciar todos los servicios después de la instalación porque el sistema realiza una inicialización única. Espere a que termine la instalación antes de entrar en el servidor.

Para acceder a la interfaz Web de Sentinel, especifique la siguiente dirección URL en el navegador Web:

`https://<IP_Address_Sentinel_server>:8443.`

El valor <*dirección_IP_servidor_Sentinel*> es la dirección IP o el nombre de DNS del servidor Sentinel y 8443 es el puerto por defecto del servidor Sentinel.

11.5 Modificación de la configuración después de la instalación

Después de instalar Sentinel, si desea introducir una clave de licencia válida, cambiar la contraseña o modificar cualquiera de los puertos asignados, puede ejecutar el guión `configure.sh` para modificarlos. El guión se encuentra en la carpeta `/opt/novell/sentinel/setup`.

1. Especifique el siguiente comando en la línea de comandos para ejecutar el guión `configure.sh`:

   ```
   ./configure.sh
   ```

2. Especifique `1` para llevar a cabo una configuración estándar o bien `2` para realizar una configuración personalizada de Sentinel.
3. Pulse la barra espaciadora para leer todo el acuerdo de licencia.
4. Introduzca `yes` o `y` para aceptar el acuerdo de licencia y continuar con la instalación.

   La instalación puede tardar varios segundos en cargar los paquetes de instalación.
5. Introduzca `1` para usar la clave de licencia de evaluación por defecto de 90 días.

   O bien

   Introduzca `2` para especificar una clave de licencia adquirida para Sentinel.
6. Decida si desea conservar la contraseña existente para el usuario administrador `admin`.
   - Si desea conservar la contraseña existente, introduzca `1` y luego continúe con el Paso 7.
   - Si desea cambiar la contraseña existente, introduzca `2`, especifique la nueva contraseña, confírmela y luego continúe con el Paso 7.
7. Decida si desea conservar la contraseña existente para el usuario de la base de datos `dbauser`.
   - Si desea conservar la contraseña existente, introduzca `1` y luego continúe con el Paso 8.
   - Si desea cambiar la contraseña existente, introduzca `2`, especifique la nueva contraseña, confírmela y luego continúe con el Paso 8.

   La cuenta `dbauser` es la identidad utilizada por Sentinel para interactuar con la base de datos. La contraseña que introduzca aquí puede utilizarse para llevar a cabo tareas de mantenimiento de la base de datos, incluido el restablecimiento de la contraseña del administrador si se pierde o se olvida.
8. Decida si desea conservar la contraseña existente para el usuario de la aplicación `appuser`.
   - Si desea conservar la contraseña existente, introduzca `1` y luego continúe con el Paso 9.
   - Si desea cambiar la contraseña existente, introduzca `2`, especifique la nueva contraseña, confírmela y luego continúe con el Paso 9.
9. Cambie las asignaciones de puertos de los servicios de Sentinel introduciendo el número deseado y luego especifique el nuevo número de puerto.
10. Después de cambiar los puertos, especifique 7 cuando haya terminado.
11. Introduzca `1` para autenticar a los usuarios utilizando únicamente la base de datos interna.

    O bien

Si ha configurado un directorio LDAP en su dominio, introduzca `2` para autenticar a los usuarios mediante la autenticación de directorios LDAP.

El valor por defecto es `1`.

11.6 Instalación de gestores de recopiladores y motores de correlación adicionales

Por defecto, Sentinel instala un gestor de recopiladores y un motor de correlación. Dependiendo del entorno, podría necesitar más gestores de recopiladores y motores de correlación. Para obtener información acerca de las ventajas de tener gestores de recopiladores y motores de correlación adicionales, consulte la Sección 9.1, "Ventajas de los gestores de recopiladores adicionales", en la página 70 y la Sección 9.2, "Ventajas de los motores de correlación adicionales", en la página 70.

Importante: Debe instalar el gestor de recopiladores o el motor de correlación adicional en sistemas independientes. El gestor de recopiladores remoto o el motor de correlación remoto no deben estar en el mismo sistema en el que se ha instalado el servidor Sentinel.

11.6.1 Lista de verificación de instalación

Asegúrese de que haya realizado las siguientes tareas antes de iniciar la instalación.

- ❒ Asegúrese de que cumple los requisitos mínimos de hardware y software. Para obtener más información, consulte Capítulo 5, "Cumplimiento de los requisitos del sistema", en la página 35.
- ❒ Sincronice el tiempo 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 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.

11.6.2 Instalación de gestores de recopiladores y motores de correlación adicionales

1. Lance la interfaz Web de Sentinel especificando la siguiente dirección URL en el navegador Web:

   `https://<IP_Address_Sentinel_server>:8443.`

   El valor <*dirección_IP_servidor_Sentinel*> es la dirección IP o el nombre de DNS del servidor Sentinel y 8443 es el puerto por defecto del servidor Sentinel.

   Inicie sesión con el nombre de usuario y la contraseña especificados durante la instalación del servidor Sentinel.
2. En la barra de herramientas, haga clic en *Descargas*.
3. En el encabezado Gestor de recopiladores, haga clic en *Descargar instalador*.
4. Haga clic en *Guardar archivo* para guardar el instalador en la ubicación deseada.

5 Especifique el siguiente comando para extraer el archivo de instalación.

```
tar zxvf <install_filename>
```

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

6 Acceda al directorio en el que ha extraído el instalador.

7 Especifique el siguiente comando para instalar el gestor de recopiladores o el motor de correlación:

Para gestor de recopiladores:

```
./install-cm
```

Para motor de correlación:

```
./install-ce
```

El guion de instalación comprueba primero si hay memoria y espacio disponibles en el disco. Si hay menos de 1.5 GB de memoria disponible, el guión cierra la instalación de forma automática.

8 Especifique el número del idioma que desea usar para la instalación.

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

9 Pulse la barra espaciadora para leer todo el acuerdo de licencia.

10 Introduzca `yes` o `y` para aceptar el acuerdo de licencia y continuar con la instalación.

La instalación podría tardar unos segundos en solicitar el tipo de configuración.

11 Cuando se le indique, especifique 1 para continuar con la configuración estándar.

12 Introduzca el Nombre de host del servidor de comunicaciones por defecto o la Dirección IP del equipo en el que está instalado Sentinel.

13 Especifique el nombre de usuario y la contraseña para el gestor de recopiladores o el motor de correlación.

El nombre de usuario y la contraseña se almacenan en el archivo `/<install_dir>/etc/opt/novell/sentinel/config/activemqusers.properties` ubicado en el servidor de Sentinel.

14 Acepte el certificado de forma permanente cuando se le indique.

15 Introduzca `sí` o `s` para habilitar el modo FIPS 140-2 en Sentinel y continúe con la configuración de FIPS.

16 Siga con la instalación según las indicaciones hasta su finalización.

11.6.3 Adición de un usuario personalizado para el gestor de recopiladores o el motor de correlación

Sentinel recomienda que utilice los nombres de usuario por defecto para el gestor de recopiladores remoto y el motor de correlación remoto. No obstante, si tiene instalados varios gestores de recopiladores remotos y desea identificarlos por separado, puede crear nuevos usuarios:

1 Acceda al servidor como el usuario que tiene acceso a los archivos de instalación de Sentinel.

2 Abra el archivo `activemqgroups.properties`.

El archivo se encuentra en el directorio `/<install_dir>/etc/opt/novell/sentinel/config/`.

3 Añada los nuevos nombres de usuario separados por comas, de la siguiente manera:

Para el gestor de recopiladores, añada los nuevos usuarios en la sección cm. Por ejemplo:

```
cm=collectormanager,cmuser1,cmuser2,...
```

Para el motor de correlación, añada los nuevos usuarios en la sección admins. Por ejemplo:

```
admins=system,correlationengine,ceuser1,ceuser2,...
```

4. Guarde y cierre el archivo.
5. Abra el archivo `activemqusers.properties`.

   Este archivo se encuentra en el directorio `/<install_dir>/etc/opt/novell/sentinel/config/`.
6. Añada la contraseña del usuario que creó en el Paso 3.

   La contraseña puede ser cualquier cadena aleatoria. Por ejemplo:

   Para los usuarios del gestor de recopiladores:

   ```
   system=c7f34372ecd20d831cceb29e754e5ac9
   collectormanager=1c51ae56
   cmuser1=1b51de55
   cmuser2=1a51ce57
   ```

   Para los usuarios del motor de correlación:

   ```
   system=c7f34372ecd20d831cceb29e754e5ac9
   correlationengine=68790d7a
   ceuser1=69700c6d
   ceuser2=70701b5c
   ```
7. Guarde y cierre el archivo.
8. Reinicie el servidor Sentinel.

12 Instalación del dispositivo

El dispositivo Sentinel es un dispositivo de software listo para ejecutarse basado en SUSE Studio. El dispositivo combina un sistema operativo SUSE Linux Enterprise Server (SLES) 11 SP 2 reforzado y el servicio de actualización integrado del software de Sentinel para proporcionar una experiencia fácil y transparente al usuario, que permite a los clientes aprovechar su inversión actual. El dispositivo de software puede instalarse en hardware o en un entorno virtual.

12.1 Instalación del dispositivo VMware

En esta sección se proporciona información sobre la instalación de Sentinel, el gestor de recopiladores y el motor de correlación en un servidor ESX de VMware.

12.1.1 Instalación de Sentinel

Siga estos pasos para instalar Sentinel en un servidor ESX de VMware:

1. Descargue el archivo de instalación del dispositivo VMware del sitio Web de descargas de Novell.

   El archivo correcto del dispositivo VMware tiene `vmx` en el nombre del archivo. Por ejemplo, `sentinel_server_7.1.0.0.x86_64.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. Utilice el siguiente comando para extraer la imagen comprimida del dispositivo desde el equipo donde está instalado VM Converter:

   ```
   tar zxvf <install_file>
   ```

   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 de software de SUSE Linux Enterprise Server (SLES) 11 SP2.

11 Lea y acepte el acuerdo de licencia del usuario final de NetIQ Sentinel.

12 En la pantalla Nombre de host y Nombre de dominio, especifique los valores correspondientes y asegúrese de que esté seleccionada la opción *Assign Hostname to Loopback IP* (Asignar nombre de host a IP de retrobucle).

13 Haga clic en *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 *Use Following Configuration* (Usar la siguiente configuración) en la página Configuración de red II y luego haga clic en *Siguiente*.
- Para cambiar los ajustes de conexión de red, seleccione *Change* (Cambiar), realice los cambios necesarios y haga clic en *Siguiente*.

Se guardan los ajustes de conexiones de red.

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

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` y luego haga clic en *Siguiente*.

La instalación comprueba si hay memoria y espacio disponible en el disco. Si la memoria disponible es inferior a 2.5 GB, la instalación no le permitirá continuar y el botón *Siguiente* aparece atenuado.

Si hay entre 2.5 GB y 6.7 GB de memoria disponible, la instalación muestra un mensaje que indica que hay menos memoria de la recomendada. Cuando aparezca este mensaje, haga clic en *Siguiente* para continuar con la instalación.

17 Defina la contraseña del administrador de Sentinel y haga clic en *Siguiente*.

Puede tardarse unos segundos en iniciar todos los servicios después de la instalación porque el sistema realiza una inicialización única. Espere a que termine la instalación antes de entrar en el servidor.

18 Anote la dirección IP del dispositivo que aparece en la consola.

19 Pase a la Sección 12.4, “Configuración del dispositivo posterior a la instalación”, en la página 92.

12.1.2 Instalación de gestores de recopiladores y motores de correlación adicionales

El procedimiento para instalar un gestor de recopiladores o un motor de correlación es el mismo, excepto que es necesario descargar el archivo adecuado del sitio Web de descargas de Novell.

1. Descargue el archivo de instalación del dispositivo VMware del sitio Web de descargas de Novell (http://download.novell.com/index.jsp).

   El archivo correcto del dispositivo VMware tiene `vmx` en el nombre del archivo. Por ejemplo, `sentinel_collector_manager_7.1.0.0.x86_64.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. Utilice el siguiente comando para extraer la imagen comprimida del dispositivo desde el equipo donde está instalado VM Converter:

   ```
   tar zxvf <install_file>
   ```

   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. Especifique el nombre de host/la dirección IP del servidor Sentinel al que debe conectarse el gestor de recopiladores.
9. Especifique el número de puerto del servidor de comunicaciones. El puerto del bus de mensajes por defecto es `61616`.
10. Especifique el nombre de usuario de JMS, que representa el nombre de usuario del gestor de recopiladores o del motor de correlación. El nombre de usuario por defecto es collectormanager para el gestor de recopiladores y correlationengine para el motor de correlación.
11. Especifique la contraseña del usuario de JMS.

    El nombre de usuario y la contraseña se almacenan en el archivo `/<install_dir>/etc/opt/novell/sentinel/config/activemqusers.properties`, ubicado en el servidor Sentinel.
12. (Opcional) Para verificar la contraseña, consulte la siguiente línea en `activemqusers.properties`.

    Para el gestor de recopiladores:

    ```
    collectormanager=<password>
    ```

    En este ejemplo, `collectormanager` es el nombre de usuario y el valor correspondiente es la contraseña.

    Para el motor de correlación:

    ```
    correlationengine=<password>
    ```

    En este ejemplo, `correlationengine` es el nombre de usuario y el valor correspondiente es la contraseña.
13. Haga clic en *Siguiente*.
14. Acepte el certificado.

15 Haga clic en *Siguiente* para completar la instalación.

Cuando haya finalizado la instalación, el instalador mostrará un mensaje que indica que el dispositivo es el gestor de recopiladores o el motor de correlación de Sentinel, en función de lo que haya elegido instalar, además de la dirección IP. Además, muestra la dirección IP de la interfaz del usuario del servidor Sentinel.

12.1.3 Instalación de VMware Tools

Para que Sentinel funcione de forma eficaz en el servidor VMware, debe instalar VMware Tools. VMware Tools es un conjunto de utilidades que mejora el rendimiento del sistema operativo del equipo virtual. Además, mejora la gestión del equipo virtual. Para obtener más información sobre la instalación de VMware Tools, consulte VMware Tools for Linux Guests (https://www.vmware.com/support/ws55/doc/ws_newguest_tools_linux.html#wp1127177) (VMware Tools para sistemas Linux invitados).

Para obtener más información sobre la documentación de VMware, consulte el Manual del usuario de la estación de trabajo (http://www.vmware.com/pdf/ws71_manual.pdf)..

12.2 Instalación del dispositivo Xen

En esta sección se proporciona información sobre la instalación de Sentinel, el gestor de recopiladores y un motor de correlación en una imagen de dispositivo Xen.

- Sección 12.2.1, “Instalación de Sentinel”, en la página 86
- Sección 12.2.2, “Instalación de gestores de recopiladores y motores de correlación adicionales”, en la página 88

12.2.1 Instalación de Sentinel

Siga los pasos indicados a continuación para instalar Sentinel en una imagen de dispositivo Xen:

1 Descargue el archivo de instalación del dispositivo virtual Xen del sitio Web de descargas de Novell (http://download.novell.com/index.jsp) en `/var/lib/xen/images`.

El archivo correcto del dispositivo virtual Xen incluye `xen` en el nombre de archivo. Por ejemplo, `Sentinel_7.1.0.0.x86_64.xen.tar.gz`.

2 Especifique el siguiente comando para desempaquetar el archivo:

```
tar -zxvf <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:

- *<nombre_archivo>*`.raw`
- *<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`.
- Especifique el ajuste de puente para la configuración de red. Por ejemplo, `"bridge=br0"` o `"bridge=xenbr0"`.
- Especifique los valores para `name` y `memory`.

Por ejemplo:

```
# -*- mode: python; -*-
name="Sentinel_7.1.0.0.x86_64"
memory=4096
```

- Comente la siguiente línea:

  ```
  vfb=["type=vnc,vncunused=1,vnclisten=0.0.0.0"]
  ```

- Añada la siguiente línea:

  ```
  extra = "console=hvc0 xencons=tty"
  ```

El archivo `xenconfig` actualizado debe ser el siguiente:

```
# -*- mode: python; -*-
name=install_file_name
memory=4096
disk=["tap:aio:/var/lib/xen/images/install_directory/install_filename]
vif=[ "bridge=br0" ]
#vfb=["type=vnc,vncunused=1,vnclisten=0.0.0.0"]
extra = "console=hvc0 xencons=tty"
```

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

```
xm create <file_name>.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 que se genera.

Por ejemplo, si ha configurado `name="Sentinel_7.1.0.0.x86_64"`en el archivo `.xenconfig`, entonces la máquina virtual aparece con ese nombre.

8 Para iniciar la instalación, especifique el siguiente comando:

```
xm console <vm name>
```

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_7.1.0.0.x86_64
```

La instalación comprueba primero si hay memoria y espacio disponible en el disco. Si hay menos de 2.5 GB de memoria disponible, la instalación se cancela de forma automática. Si hay entre 2.5 GB y 6.7 GB de memoria disponible, la instalación muestra un mensaje que indica que hay menos memoria de la recomendada. Escriba `y` si desea continuar con la instalación o `n` si no es así.

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 SUSE Linux Enterprise Server (SLES) 11 SP2.

12 Lea y acepte el acuerdo de licencia del usuario final de NetIQ Sentinel.

13 En la pantalla Nombre de host y Nombre de dominio, especifique los valores correspondientes y asegúrese de que esté seleccionada la opción *Assign Hostname to Loopback IP* (Asignar nombre de host a IP de retrobucle).

14 Seleccione *Siguiente*. Se guardará la información configurada de 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 *Change* (Cambiar) y luego realice los cambios necesarios.

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

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

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
```

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

19 Defina la contraseña del administrador de Sentinel y luego haga clic en *Siguiente*.

La instalación de Sentinel continúa y finaliza. Puede tardarse unos minutos en iniciar todos los servicios después de la instalación, porque el sistema lleva a cabo una inicialización única. Espere a que termine la instalación antes de entrar en el servidor.

Anote la dirección IP del dispositivo que aparece en la consola.

20 Pase a la Sección 12.4, “Configuración del dispositivo posterior a la instalación”, en la página 92.

12.2.2 Instalación de gestores de recopiladores y motores de correlación adicionales

El procedimiento para instalar un gestor de recopiladores o un motor de correlación es el mismo, excepto que es necesario descargar el archivo adecuado del sitio Web de descargas de Novell.

1 Realice el Paso 1 al Paso 14 de la Sección 12.2.1, “Instalación de Sentinel”, en la página 86.

2 En la pantalla Configuración de red II, seleccione *Cambiar* y especifique la dirección IP de la máquina virtual en la que desea instalar el gestor de recopiladores o el motor de correlación adicional.

3 Especifique la máscara de subred de la dirección IP especificada.

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

5 Establezca la fecha y la hora y luego seleccione *Siguiente*.

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
```

6 Defina la contraseña `root` de SUSE Enterprise Server, y luego seleccione *Siguiente*.

7 Especifique el nombre de host/la dirección IP del servidor Sentinel al que debe conectarse el gestor de recopiladores o el motor de correlación.

8 Especifique el número de puerto del servidor de comunicaciones. El puerto del bus de mensajes por defecto es `61616`.

9 Especifique el nombre de usuario de JMS, que representa el nombre de usuario del gestor de recopiladores o del motor de correlación.

10 Especifique la contraseña del usuario de JMS.

El nombre de usuario y la contraseña se almacenan en el archivo/`<install_dir>`/etc/opt/novell/sentinel/config/activemqusers.properties ubicado en el servidor de Sentinel.

11 (Opcional) Para verificar la contraseña, consulte la siguiente línea del archivo `activemqusers.properties`:

Para el gestor de recopiladores:

```
collectormanager=<password>
```

En este ejemplo, `collectormanager` es el nombre de usuario y el valor correspondiente es la contraseña.

Para el motor de correlación:

```
correlationengine=<password>
```

En este ejemplo, `correlationengine` es el nombre de usuario y el valor correspondiente es la contraseña.

12 Seleccione *Siguiente* para finalizar la instalación.

Cuando la instalación haya terminado, muestra un mensaje que indica que este dispositivo es el gestor de recopiladores o el motor de correlación de Sentinel, en función de lo que eligió instalar, junto con la dirección IP.

12.3 Instalación del dispositivo ISO

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

Importante: La instalación en hardware utilizando la imagen ISO en disco (desde cero e Hyper-V) requiere una memoria mínima de 4,5 GB para poder finalizar la instalación.

- Sección 12.3.1, “Instalación de Sentinel”, en la página 89
- Sección 12.3.2, “Instalación de gestores de recopiladores y motores de correlación adicionales”, en la página 91

12.3.1 Instalación de Sentinel

Siga los pasos indicados a continuación para instalar el dispositivo Sentinel en el hardware:

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.

La instalación comprueba primero si hay memoria y espacio disponible en el disco. Si hay menos de 2.5 GB de memoria disponible, la instalación se cancela de forma automática. Si hay entre 2.5 GB y 6.7 GB de memoria disponible, la instalación muestra un mensaje que indica que hay menos memoria de la recomendada. Escriba `y` si desea continuar con la instalación o `n` si no es así.

4. Seleccione el idioma deseado y luego, haga clic en *Siguiente*.
5. Seleccione la disposición del teclado y haga clic en *Siguiente*.
6. Lea y acepte el acuerdo de licencia del software de SUSE Enterprise Server.
7. Lea y acepte el acuerdo de licencia del usuario final de NetIQ Sentinel.
8. Seleccione *Siguiente*.
9. En la pantalla Nombre de host y Nombre de dominio, especifique los valores correspondientes y asegúrese de que esté seleccionada la opción *Assign Hostname to Loopback IP* (Asignar nombre de host a IP de retrobucle).
10. Seleccione *Siguiente*. Se guarda la configuración del nombre de host.
11. 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 página de Network Configuration II (Configuración de red II).
    - Para cambiar los ajustes de conexión de red, seleccione *Change* (Cambiar) y luego realice los cambios necesarios.
12. Seleccione *Siguiente*. Se guardan los ajustes de conexiones de red.
13. Establezca la fecha y la hora y luego haga clic en *Siguiente*.

    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
    ```
14. Defina la contraseña `root` y luego haga clic en *Siguiente*.
15. Defina la contraseña del administrador de Sentinel y luego haga clic en *Siguiente*.
16. 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 la contraseña definida en el Paso 14.
17. Detenga el servidor Sentinel:

    ```
    service sentinel stop
    ```
18. Introduzca el siguiente comando para restablecer la interfaz del usuario para crear una pantalla nueva en YaST:

    ```
    reset
    ```
19. Para instalar el dispositivo en el servidor físico, asegúrese de que haya seleccionado la casilla de verificación *Install Sentinel appliance to hard drive (for Live DVD image only)* (Instalar dispositivo de Sentinel en el disco duro [solo para la imagen de Live DVD]).

    Esta casilla de verificación está seleccionada por defecto. Si desactiva esta casilla de verificación, el dispositivo no se instala en el servidor físico y solo se ejecutará en modo LIVE DVD.

Pueden tardarse unos minutos en iniciar todos los servicios después de la instalación porque el sistema realiza una inicialización única. Espere a que termine la instalación antes de entrar en el servidor.

20 Anote la dirección IP del dispositivo que aparece en la consola.

21 Pase a la Sección 12.4, "Configuración del dispositivo posterior a la instalación", en la página 92.

12.3.2 Instalación de gestores de recopiladores y motores de correlación adicionales

El procedimiento para instalar un gestor de recopiladores o un motor de correlación es el mismo, excepto que es necesario descargar el archivo adecuado del sitio web de descargas de Novell.

1 Realice el Paso 1 al Paso 14 de la Sección 12.3.1, "Instalación de Sentinel", en la página 89.

2 Especifique el nombre de host/la dirección IP del servidor Sentinel al que debe conectarse el gestor de recopiladores.

3 Especifique el número de puerto del servidor de comunicaciones. El puerto del bus de mensajes por defecto es `61616`.

4 Especifique el nombre de usuario de JMS, que representa el nombre de usuario del gestor de recopiladores o del motor de correlación.

5 Especifique la contraseña del usuario de JMS.

6 Haga clic en *Siguiente*.

El nombre de usuario y la contraseña se almacenan en el archivo `/<install_dir>/etc/opt/novell/sentinel/config/activemqusers.properties` ubicado en el servidor de Sentinel.

7 Para verificar la contraseña, consulte la siguiente línea en el archivo `activemqusers.properties`:

Para el gestor de recopiladores:

```
collectormanager=<password>
```

En este ejemplo, `collectormanager` es el nombre de usuario y el valor correspondiente es la contraseña.

Para el motor de correlación:

```
correlationengine=<password>
```

En este ejemplo, `correlationengine` es el nombre de usuario y el valor correspondiente es la contraseña.

8 Para instalar el dispositivo en el servidor físico, asegúrese de que haya seleccionado la casilla de verificación *Install Sentinel appliance to hard drive (for Live DVD image only)* (Instalar el dispositivo Sentinel en el disco duro [solo para la imagen de Live DVD])

Esta casilla de verificación está seleccionada por defecto. Si desactiva esta casilla de verificación, el dispositivo no se instalará en el servidor físico y solo se ejecutará en modo Live DVD.

9 Acepte el certificado cuando se le indique.

10 Introduzca `sí` o `s` para habilitar el modo FIPS 140-2 en Sentinel y continúe con la configuración FIPS.

11 Continúe con la instalación según se le indique hasta finalizarla.

Una vez finalizada la instalación, muestra un mensaje para indicar que el dispositivo es el gestor de recopiladores o el motor de correlación de Sentinel, en función de lo que eligió instalar, junto con la dirección IP. Además, muestra la dirección IP de la interfaz del usuario del servidor Sentinel.

12.4 Configuración del dispositivo posterior a la instalación

Después de instalar Sentinel, es necesario realizar una configuración adicional para que el dispositivo funcione correctamente.

12.4.1 Configuración de WebYaST

La interfaz del usuario del dispositivo Sentinel está equipada con WebYaST, que es una consola remota basada en la Web para controlar los dispositivos basados en SUSE Linux Enterprise. Puede acceder, configurar y supervisar los dispositivos de Sentinel 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 (Guía del usuario de WebYaST)* (http://www.novell.com/documentation/webyast/).

1 Entre en el dispositivo de Sentinel.
2 Haga clic en *Appliance* (Dispositivo).
3 Configure el servidor de Sentinel para recibir actualizaciones tal como se describió en Sección 12.4.3, "Registro para recibir actualizaciones", en la página 93.
4 Haga clic en *Siguiente* para finalizar la instalación inicial.

12.4.2 Creación de particiones

Puede añadir particiones en el dispositivo y mover un directorio a la nueva partición mediante la herramienta YaST.

Utilice el siguiente procedimiento para crear una partición nueva y mover archivos de datos de su directorio a la partición recién creada:

1 Acceda a Sentinel como usuario `root`.
2 Ejecute el siguiente comando para detener Sentinel en el dispositivo:

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

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

```
su -novell
```

4 Mueva el contenido del directorio en `/var/opt/novell/sentinel/` a una ubicación temporal.
5 Cambie al usuario `root`.
6 Introduzca el siguiente comando para acceder al Centro de control de YaST2:

```
yast
```

7 Seleccione *System* > *Partitioner* (Sistema > Creador de particiones).

8 Lea la advertencia y seleccione *Yes* (Sí) para añadir la nueva partición no utilizada.

9 Monte la nueva partición en `/var/opt/novell/sentinel`.

10 Especifique el siguiente comando para cambiar al usuario `novell`:

```
su -novell
```

11 Mueva el contenido del directorio de datos de la ubicación temporal (donde se guardó en el Paso 4) de nuevo a `/var/opt/novell/sentinel/` en la nueva partición.

12 Ejecute el siguiente comando para reiniciar el dispositivo Sentinel:

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

12.4.3 Registro para recibir actualizaciones

Debe registrar el dispositivo Sentinel con el canal de actualización de dispositivos para poder recibir actualizaciones de parches. Para registrar el dispositivo, primero debe obtener el código de registro de dispositivo o la clave de activación del dispositivo en el Centro de atención al cliente de Novell.

Siga estos pasos para registrar el dispositivo para las actualizaciones:

1 Entre en el dispositivo de Sentinel.

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

3 Haga clic en *Registration* (Registro).

4 Especifique la ID del correo electrónico en la que desea recibir actualizaciones y luego especifique el nombre del sistema y el código de registro del dispositivo.

5 Haga clic en *Guardar*.

12.4.4 Configuración del dispositivo con SMT

En entornos protegidos en los que el dispositivo debe ejecutarse sin acceso directo a Internet, puede configurar el dispositivo con la herramienta SMT (Subscription Management Tool), que le permite actualizar el dispositivo a la versión más reciente de Sentinel a medida que se vayan lanzando. SMT es un sistema apoderado de paquetes integrado en Centro de servicios al cliente de Novell que proporciona funciones clave de dicho centro.

- "Requisitos previos" en la página 93
- "Configuración del dispositivo" en la página 94
- "Actualización del dispositivo" en la página 94

Requisitos previos

- Obtenga las credenciales del Centro de servicios al cliente de Novell para Sentinel para obtener actualizaciones de Novell. Para obtener información sobre la forma de obtener credenciales, comuníquese con Asistencia de Novell.
- Asegúrese de que SLES 11 SP2 esté instalada con los siguientes paquetes en el equipo donde desea instalar la herramienta SMT:
  - htmldoc
  - perl-DBIx-Transaction
  - perl-File-Basename-Object

- perl-DBIx-Migration-Director
- perl-MIME-Lite
- perl-Text-ASCIITable
- yum-metadata-parser
- createrepo
- perl-DBI
- apache2-prefork
- libapr1
- perl-Data-ShowTable
- perl-Net-Daemon
- perl-Tie-IxHash
- fltk
- libapr-util1
- perl-PIRPC
- apache2-mod_perl
- apache2-utils
- apache2
- perl-DBD-mysql

- Instale SMT y configure el servidor de SMT. Para obtener más información, consulte las siguientes secciones de la documentación de SMT:
  - Instalación de SMT
  - Configuración del servidor de SMT
  - Duplicación de los repositorios de instalación y actualizaciones con SMT
- Instale la utilidad `wget` en el equipo del dispositivo.

Configuración del dispositivo

Para obtener información sobre la configuración del dispositivo con SMT, consulte la documentación Subscription Management Tool (SMT) for SUSE Linux Enterprise 11 (Herramienta de gestión de suscripciones (SMT) para SUSE Linux Enterprise 11).

Para habilitar los repositorios del dispositivo, ejecute el siguiente comando:

```
smt-repos -e Sentinel-Server-7.0-Updates sle-11-x86_64

smt-repos -e Sentinel-Collector-Manager-7.0-Updates sle-11-x86_64

smt-repos -e Sentinel-Correlation-Engine-7.0-Updates sle-11-x86_64
```

Actualización del dispositivo

Para obtener información sobre cómo actualizar el dispositivo, consulte la Sección 21.3, “Actualización de la aplicación con SMT”, en la página 130.

12.5 Inicio y detención del servidor mediante WebYaST

Puede iniciar y detener el servidor de Sentinel utilizando la interfaz basada en la Web de la siguiente manera:

1. Entre en el dispositivo de Sentinel.
2. Haga clic en *Appliance* (Dispositivo) para lanzar WebYaST.
3. Haga clic en *System Services* (Servicios del sistema).
4. Para detener el servidor de Sentinel, haga clic en *detener*.
5. Para iniciar el servidor de Sentinel, haga clic en *iniciar*.

13 Instalación de conectores y recopiladores adicionales

Por defecto, todos los recopiladores y conectores distribuidos están instalados en Sentinel. Si desea instalar un nuevo recopilador o conector publicado después del lanzamiento de Sentinel, utilice la información de las siguientes secciones.

13.1 Instalación de un recopilador

Siga los pasos indicados a continuación para instalar un recopilador:

1. Descargue el recopilador deseado de la página Web de módulos auxiliares (plug-ins) de Sentinel.
2. Acceda a la interfaz Web de Sentinel en la dirección https://<*dirección IP*>:8443, donde 8443 es el puerto por defecto del servidor Sentinel.
3. Haga clic en *aplicaciones* en la barra de herramientas y luego haga clic en *Aplicaciones*.
4. Haga clic en *Lanzar el Centro de control* para lanzar el Centro de control de Sentinel.
5. En la barra de herramientas, haga clic en *Gestión de orígenes de eventos* > *Vista activa* y luego haga clic en *Herramientas* > *Importar módulo auxiliar (plug-in)*.
6. Busque y seleccione el archivo de recopilador que descargó en el Paso 1, y luego haga clic en *Siguiente*.
7. Siga las indicaciones restantes y luego haga clic en *Finalizar*.

Para configurar el recopilador, consulte la documentación específica del recopilador en la página Web de módulos auxiliares (plug-ins) de Sentinel.

13.2 Instalación de un conector

Siga los pasos indicados a continuación para instalar un conector:

1. Descargue el conector deseado de la página Web de módulos auxiliares (plug-ins) de Sentinel.
2. Acceda a la interfaz Web de Sentinel en la dirección https://<*dirección IP*>:8443, donde 8443 es el puerto por defecto del servidor Sentinel.
3. Haga clic en *aplicación* en la barra de herramientas y luego haga clic en *Aplicaciones*.
4. Haga clic en *Lanzar el Centro de control* para lanzar el Centro de control de Sentinel.
5. En la barra de herramientas, seleccione *Gestión de orígenes de eventos* > *Vista activa* y luego haga clic en *Herramientas* > *Importar módulo auxiliar (plug-in)*.

6 Busque y seleccione el archivo de conector que descargó en el Paso 1, y luego haga clic en *Siguiente*.

7 Siga las indicaciones restantes y luego haga clic en *Finalizar*.

Para configurar el conector, consulte la documentación específica del conector en la página Web de módulos auxiliares (plug-ins) de Sentinel.

14 Verificación de la instalación

Puede determinar si la instalación se realizó correctamente mediante los siguientes pasos:

- Verificación de la versión de Sentinel:

  ```
  /etc/init.d/sentinel version
  ```

- Verifique si los servicios de Sentinel funcionan y están activos:

  ```
  /etc/init.d/sentinel status
  ```

- Verifique si los servicios Web funcionan y están activos:

  ```
  netstat -an |grep 'LISTEN' |grep <HTTPS_port_number>
  ```

  El número de puerto por defecto es 8443.

- Acceso a la interfaz web de Sentinel:

  1. Lance un navegador Web compatible.
  2. Especifique la dirección URL de la interfaz Web de Sentinel:

     ```
     https://<IP_Address/DNS_Sentinel_server:8443>
     ```

     IP_Address/DNS_Sentinel_server es la dirección IP o el nombre DNS del servidor Sentinel y 8443 es el puerto por defecto del servidor Sentinel.
  3. Entre a una sesión con el nombre y la contraseña del administrador especificados durante la instalación. El nombre de usuario por defecto es admin.

15 Estructura de directorios de Sentinel

Por defecto, los directorios de Sentinel se encuentran en las siguientes ubicaciones:

- Los archivos de datos se encuentran en los directorios `/var/opt/novell/sentinel/data` y `/var/opt/novell/sentinel/3rdparty`.
- Los archivos ejecutables y las bibliotecas se encuentran en los siguientes directorios:
  - `/opt/novell/sentinel/bin`
  - `/opt/novell/sentinel/setup`
  - `/opt/novell/sentinel/3rdparty`
- Los archivos de registro se encuentran en el directorio `/var/opt/novell/sentinel/log`
- Los archivos de configuración se encuentran en el siguiente directorio `/etc/opt/novell/sentinel`
- El archivo de ID de proceso (PID) se encuentra en el directorio`/var/run/sentinel/server.pid`.

  Mediante el PID, los administradores pueden identificar el proceso padre del servidor Sentinel y supervisar o terminar el proceso.

IV Configuración de Sentinel

En esta sección se proporciona información sobre la configuración de Sentinel y sobre los módulos auxiliares (plug-ins) genéricos de Sentinel.

16 Configuración de la hora

La hora de un evento es crucial para su procesamiento en Sentinel. Es importante para la generación de informes y para fines de auditoría, además de para el procesamiento en tiempo real. En esta sección se proporciona información para comprender el tiempo en Sentinel, cómo configurar la hora y cómo manejar las zonas horarias.

16.1 Comprender el tiempo en Sentinel

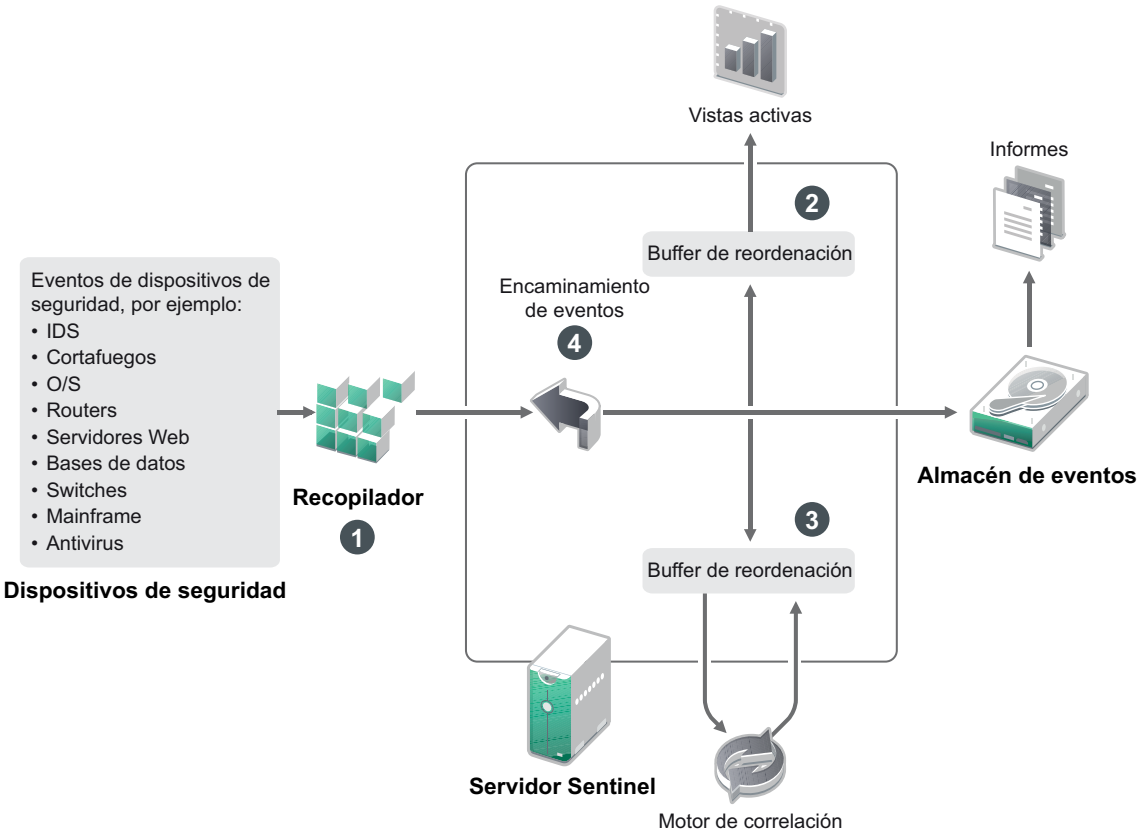
Sentinel es un sistema distribuido compuesto por varios procesos distribuidos a través de la red. Además, puede haber algún retraso introducido por el origen de evento. Para adaptarlo, los procesos de Sentinel reordenan los eventos en un flujo ordenado por tiempo antes de procesarlos.

Cada eventos tiene tres campos de tiempo:

- **Tiempo del evento:** este tiempo u hora del evento lo utilizan todos los motores analíticos, las búsquedas, los informes, etc.
- **Hora de proceso de Sentinel:** la hora a la que Sentinel recopiló los datos del dispositivo, que se obtiene de la hora del sistema del gestor de recopiladores.
- **Hora del evento del observador:** se trata de la marca horaria que el dispositivo pone en los datos. Los datos podrían no incluir siempre una marca horaria fiable y puede ser bastante diferente de la hora de proceso de Sentinel. Por ejemplo, cuando el dispositivo proporciona los datos por lotes.

En la siguiente ilustración se explica cómo Sentinel lleva a cabo esta operación:

Figura 16-1 *Hora de Sentinel*



1. Por defecto, la hora del evento se define en la hora de proceso de Sentinel. Lo ideal, sin embargo, es que la hora del evento coincida con la hora del evento del observador, si está disponible y es de confianza. Lo mejor es configurar la recopilación de datos en **Hora del origen de eventos predeterminado** si está disponible la hora del dispositivo, es exacta y es analizada correctamente por el recopilador. El recopilador define la hora del evento para que coincida con la hora del evento del observador.
2. Los eventos que tienen una hora de evento dentro de un intervalo de 5 minutos con respecto a la hora del servidor (anterior o posterior) se procesan normalmente en Vistas activas. Los eventos que tienen una hora del evento más de 5 minutos posterior no se muestran en las Vistas activas, pero se ingresan en el almacén de eventos. Los eventos que tienen una hora del evento más de 5 minutos posterior y menos de 24 horas anterior siguen mostrándose en los diagramas, pero no se muestran en los datos de eventos de dicho diagrama. Es necesaria una operación en profundidad para recuperar esos eventos del almacén de eventos.
3. Los eventos se clasifican en intervalos de 30 segundos para que el motor de correlación pueda profesarlos en orden cronológico. En el caso de que la hora del evento sea más de 30 segundos anterior a la hora del servidor, el motor de correlación no procesará los eventos.
4. Si la hora del evento es más de 5 minutos anterior a la hora del sistema del gestor de recopiladores, Sentinel encamina directamente los eventos al almacén de eventos, omitiendo los sistemas en tiempo real como Correlación, Vistas activas e Inteligencia de seguridad.

16.2 Configuración de la hora en Sentinel

El motor de correlación procesa flujos de eventos ordenados por tiempo y detecta patrones dentro de los eventos, además de patrones temporales en el flujo. Sin embargo, el dispositivo que generó el evento podría no incluir la hora en sus mensajes de registro. Para configurar la hora para que funcione correctamente con Sentinel, tiene dos opciones:

- Configure NTP en el gestor de recopiladores y deseleccione *Hora del origen de eventos predeterminado* en el origen de eventos del Gestor de orígenes de eventos. Sentinel utiliza el gestor de recopiladores como origen de la hora de los eventos.
- Seleccione *Hora del origen de eventos predeterminado* en el origen de evento del Gestor de orígenes de eventos. Sentinel utiliza la hora del mensaje de registro como la hora correcta.

Para cambiar este ajuste en el origen de evento:

1. Entre en Gestión de orígenes de eventos.

   Para obtener más información, consulte "Accessing Event Source Management" (Cómo acceder a Gestión de orígenes de eventos) en la *NetIQ Sentinel 7.1 Administration Guide* (Guía de administración de NetIQ Sentinel 7.1).
2. Haga clic con el botón derecho del ratón en el origen de evento cuya hora desea cambiar y luego seleccione *Editar*.
3. Seleccione o deseleccione *Origen de eventos predeterminado* en la parte de abajo de la pestaña *General*.
4. Haga clic en *Aceptar* para guardar el cambio.

16.3 Cómo manejar las zonas horarias

El manejo de las zonas horarias puede llegar a ser muy complejo en un entorno distribuido. Por ejemplo, podría tener un origen de evento en una zona horaria, el gestor de recopiladores en otra zona, el servidor Sentinel posterior en otra y el cliente podría visualizar los datos en otra zona horaria. Si además se añade el componente del horario de verano y los numerosos orígenes de eventos que no informan de la zona horaria en la que están definidos (por ejemplo, los orígenes de syslog), son numerosos los problemas a tener en cuenta. Sentinel es flexible para que pueda representar adecuadamente la hora a la que los eventos ocurren realmente, y comparar esos eventos con eventos de otros orígenes de la misma zona horaria o zonas horarias diferentes.

En general, tres escenarios diferentes representan la forma en que los orígenes de eventos informan de las marcas horarias:

- El origen de evento informa de la hora en UTC. Por ejemplo, todos los eventos del Registro de eventos de Windows siempre se informan en UTC.
- El origen de evento se informa en la hora local, pero siempre incluye la zona horaria en la marca horaria. Por ejemplo, cualquier origen de evento que siga el formato RFC3339 para la estructuración de marcas horarias incluye la zona horaria como diferencia horaria; otros orígenes informan IDs de zona horaria en formato largo, como América/Nueva York, o en formato corto como EST, lo cual puede presentar problemas debido a conflictos y resoluciones inadecuadas.
- El origen de evento informa de la hora local, pero no indica la zona horaria. Desgraciadamente, el formato syslog tan común sigue este modelo.

Para el primer escenario, siempre es posible calcular la hora UTC absoluta a la que se produjo un evento (suponiendo que se está utilizando un protocolo de sincronización horaria), de manera que se puede comparar fácilmente la hora del evento con cualquier otro origen de evento en el mundo. Sin

embargo, no es posible determinar automáticamente la hora local a la que ocurrió el evento. Por este motivo, Sentinel permite a los clientes definir manualmente la zona horaria de un origen de evento editando el nodo Origen de evento en el Gestor de orígenes de eventos y especificando la zona horaria adecuada. Esta información no afecta al cálculo de la hora del evento del dispositivo (DeviceEventTime) o la hora del evento (EventTime), pero se coloca en el campo de zona horaria de observador (ObserverTZ), y se utiliza para calcular varios campos de zona horaria del observador (ObserverTZ), como hora de la zona horaria del observador (ObserverTZHour). Estos campos siempre se expresan en la hora local.

En el segundo escenario, si se utilizan las IDs de zona horaria de formato largo o diferencias horarias, es posible convertir al formato UTC para obtener la hora UTC canónica absoluta (guardada en DeviceEventTime), pero también se pueden calcular los campos ObserverTZ de hora local. Si se utiliza la ID de zona horaria de formato corto, existe la posibilidad de que surjan conflictos.

El tercer escenario requiere que el administrador defina manualmente la zona horaria del origen del evento para todos los orígenes afectados de manera que Sentinel pueda calcular correctamente la hora UTC. Si la zona horaria no se especifica correctamente editando el nodo de Origen de eventos en el Gestor de orígenes de eventos, entonces puede que DeviceEventTime (y probablemente EventTime) sea incorrecto; además, el campo ObserverTZ y sus campos asociados podrían ser incorrectos.

En general, el recopilador de un tipo determinado de origen de evento (por ejemplo, Microsoft Windows) sabe cómo un origen de evento presenta las marcas horarias y se ajusta en la forma adecuada. Siempre es una buena directiva definir manualmente la zona horaria para todos los nodos de orígenes de eventos en el gestor de orígenes de eventos, a menos que el origen del evento informe la hora local y siempre incluya la zona horaria en su marca horaria.

El procesamiento de la presentación de la marca horaria en el origen del evento tiene lugar en el recopilador y en el gestor de recopiladores. Los campos DeviceEventTime y EventTime se almacenan como UTC, y los campos de ObserverTZ se almacenan como cadenas definidas en la hora local del origen de evento. Esta información se envía desde el gestor de recopiladores al servidor Sentinel y se guarda en el almacén de eventos. La zona horaria en la que se encuentran el gestor de recopiladores y el servidor Sentinel no debería afectar a este proceso ni a los datos almacenados. Sin embargo, cuando un cliente visualiza el evento en un navegador Web, la hora UTC del evento se convierte a la zona local en función del navegador Web, de manera que todos los eventos se presentan a los clientes en la zona horaria local. Si los usuarios desean ver la hora local del origen, pueden examinar los campos ObserverTZ para obtener más detalles.

17 Configuración de módulos auxiliares (plug-ins) genéricos

Por defecto, Sentinel se suministra con varios módulos auxiliares (plug-ins). En este capítulo se proporciona información sobre cómo configurar los módulos auxiliares (plug-ins) genéricos.

17.1 Configuración de paquetes de soluciones

Sentinel se suministra con un variado contenido predefinido que resulta útil y que puede usar de inmediato para satisfacer muchas de las necesidades de análisis. Gran parte de este contenido viene de los paquetes Sentinel Core Solution Pack y del paquete de soluciones para la serie ISO 27000. Para obtener más información, consulte “Using Solution Packs” (Uso de paquetes de soluciones) en la *NetIQ Sentinel 7.1 Administration Guide* (Guía de administración de NetIQ Sentinel 7.1).

Los paquetes de soluciones permiten clasificar y agrupar el contenido en "controles" o conjuntos de directivas que se consideran como una unidad. Los controles de los Paquetes de soluciones vienen preinstalados para proporcionarle este contenido predefinido, pero tiene que implementarlos formalmente o probarlos mediante la consola Web de Sentinel.

Si se desea contar con un cierto grado de rigor para ayudar a mostrar que la implementación de Sentinel funciona según el diseño, puede usar el proceso de certificación formal incorporado a los Paquetes de soluciones. Este proceso de certificación implementa y prueba los controles del Paquete de soluciones de la misma forma que se implementarían y probarían los controles de cualquier otro paquete de soluciones. Dentro de este proceso, el implementador y el responsable de la prueba certificarán que han finalizado su trabajo; estas certificaciones luego formarán parte de un seguimiento de auditoría que se puede examinar a fin de demostrar que cualquier control dado se implementó adecuadamente.

Puede realizar este proceso de certificación mediante Solution Manager. Para obtener más información sobre cómo implementar y probar los controles, consulte “Installing and Managing Solution Packs” (Instalación y gestión de paquetes de soluciones) de la *NetIQ Sentinel 7.1 Administration Guide* (Guía de administración de NetIQ Sentinel 7.1).

17.2 Configuración de recopiladores, conectores, integradores y acciones

Para obtener información acerca de la configuración de módulos auxiliares (plug-ins) predefinidos, consulte la documentación específica al respecto disponible en el sitio Web de módulos auxiliares (plug-ins) de Sentinel.

18 Habilitar el modo FIPS 140-2 en una instalación de Sentinel existente

En este capítulo se proporciona información sobre cómo habilitar el modo FIPS 140-2 en una instalación de Sentinel existente.

Nota: En estas instrucciones se presupone que Sentinel está instalado en el directorio `/opt/novell/sentinel`. Los comandos deben ejecutarse como usuario `novell`.

18.1 Habilitar el servidor Sentinel para su ejecución en modo FIPS 140-2

Para habilitar el servidor Sentinel para ejecutarse en modo FIPS 140-2:

1. Entre en el servidor Sentinel.
2. Cambie al usuario `novell` (`su novell`).
3. Examine el directorio bin de Sentinel.
4. Ejecute el guión `convert_to_fips.sh` y siga las instrucciones en pantalla.
5. Lleve a cabo la configuración del modo FIPS 140-2 realizando las tareas mencionadas en el Capítulo 19, "Funcionamiento de Sentinel en el modo FIPS 140-2", en la página 113.

18.2 Habilitar el modo FIPS 140-2 en gestores de recopiladores y motores de correlación remotos

Debe habilitar el modo FIPS 140-2 en el gestor de recopiladores y el motor de correlación remotos si desea usar las comunicaciones aptas para FIPS con el servidor Sentinel que se ejecuta en modo FIPS 140-2.

Para habilitar un gestor de recopiladores o un motor de correlación remoto para ejecutarse en modo FIPS 140-2:

1. Acceda al sistema de gestor de recopiladores o motor de correlación remoto.
2. Cambie al usuario `novell` (`su novell`).
3. Busque el directorio bin. La ubicación por defecto es `/opt/novell/sentinel/bin`.

4 Ejecute el guión `convert_to_fips.sh` y siga las instrucciones en pantalla.

5 Lleve a cabo la configuración del modo FIPS 140-2 realizando las tareas mencionadas en el Capítulo 19, “Funcionamiento de Sentinel en el modo FIPS 140-2”, en la página 113.

19 Funcionamiento de Sentinel en el modo FIPS 140-2

En este capítulo se proporciona información sobre la configuración y el funcionamiento de Sentinel en modo FIPS 140-2.

19.1 Configuración del servicio Asesor en modo FIPS 140-2

El servicio Asesor utiliza una conexión HTTPS segura para descargar su contenido desde el servidor del Asesor. El certificado utilizado por el servidor para la comunicación segura debe añadirse a la base de datos del almacén de claves de FIPS de Sentinel.

Para verificar el registro correcto en la base de datos de Gestión de recursos:

1. Descargue el certificado desde el servidor del Asesor y guarde el archivo como `advisor.cer`.
2. Importe el certificado del servidor del Asesor al almacén de claves de FIPS de Sentinel.

   Para obtener más información sobre la importación del certificado, consulte “Importación de certificados en la base de datos del almacén de claves de FIPS” en la página 122.

19.2 Configuración de búsqueda distribuida en modo FIPS 140-2

En esta sección se proporciona información sobre cómo configurar búsquedas distribuidas en el modo FIPS 140-2.

Escenario 1: tanto los servidores Sentinel de origen como de destino están en modo FIPS 140-2

Para permitir búsquedas distribuidas en varios servidores Sentinel que se ejecutan en modo FIPS 140-2, es necesario añadir los certificados utilizados para las comunicaciones seguras al almacén de claves FIPS.

1. Entre en el equipo de origen de búsqueda distribuida.
2. Busque el directorio del certificado:

   ```
   cd <sentinel_install_directory>/config
   ```

3. Copie el certificado de origen (`sentinel.cer`) a una ubicación temporal en el equipo de destino.
4. Importe el certificado de origen al almacén de claves de FIPS de Sentinel de destino.

   Para obtener más información sobre la importación del certificado, consulte "Importación de certificados en la base de datos del almacén de claves de FIPS" en la página 122.
5. Entre en el equipo de destino de búsqueda distribuida.
6. Busque el directorio del certificado:

   ```
   cd /etc/opt/novell/sentinel/config
   ```

7. Copie el certificado de destino (`sentinel.cer`) a una ubicación temporal del equipo de origen.
8. Importe el certificado del sistema de destino en el almacén de claves de FIPS de Sentinel.
9. Reinicie los servicios Sentinel tanto en el equipo de origen como en el de destino.

Escenario 2: el servidor Sentinel de origen no está en modo FIPS y el servidor Sentinel de destino está en modo FIPS 140-2.

Debe convertir el almacén de claves del servidor Web del equipo de origen al formato del certificado y luego exportar el certificado al equipo de destino.

1. Entre en el equipo de origen de búsqueda distribuida.
2. Cree el almacén de claves del servidor Web en el formato del certificado (`.cer`):

   ```
   <sentinel_install_directory>/jre/bin/keytool -export -alias webserver -
   keystore <sentinel_install_directory>/config/.webserverkeystore.jks -storepass
   password -file <certificate_name.cer>
   ```

3. Copie el certificado del origen de la búsqueda distribuida (`Sentinel.cer`) a una ubicación temporal del equipo de destino de búsqueda distribuida.
4. Entre en el equipo de destino de búsqueda distribuida.
5. Importe el certificado de origen al almacén de claves de FIPS de Sentinel de destino.

   Para obtener más información sobre la importación del certificado, consulte "Importación de certificados en la base de datos del almacén de claves de FIPS" en la página 122.
6. Reinicie los servicios de Sentinel en el equipo de destino.

Escenario 3: el servidor Sentinel de origen está en el modo FIPS y el servidor Sentinel de destino está en modo diferente de FIPS.

1. Entre en el equipo de destino de búsqueda distribuida.
2. Cree el almacén de claves del servidor Web en formato del certificado (.cer):

   ```
   <sentinel_install_directory>/jre/bin/keytool -export -alias webserver -
   keystore <sentinel_install_directory>/config/.webserverkeystore.jks -storepass
   password -file <certificate_name.cer>
   ```

3. Copie el certificado a una ubicación temporal del equipo de origen de búsqueda distribuida.
4. Importe el certificado de destino al almacén de claves de FIPS de Sentinel de origen.

Para obtener más información sobre la importación del certificado, consulte "Importación de certificados en la base de datos del almacén de claves de FIPS" en la página 122.

5 Reinicie los servicios de Sentinel en el equipo de origen.

19.3 Configuración de autenticación de LDAP en el modo FIPS 140-2

Para configurar la autenticación de LDAP para los servidores Sentinel que se ejecutan en modo FIPS 140-2:

1 Obtenga el certificado del servidor LDAP del administrador de LDAP, o bien utilice un comando. Por ejemplo,

```
openssl s_client -connect <LDAP server IP>:636
```

y después copie el texto recibido (entre las líneas BEGIN y END, excluyendo ambas) a un archivo.

2 Importe el certificado del servidor LDAP al almacén de claves de FIPS de Sentinel.

Para obtener más información sobre la importación del certificado, consulte "Importación de certificados en la base de datos del almacén de claves de FIPS" en la página 122.

3 Entre en una sesión en la consola Web de Sentinel como usuario con la función de administrador y continúe con la configuración de autenticación de LDAP.

Para más información, consulte *Configuring LDAP Authentication* (Cómo configurar la autenticación LDAP) en la *NetIQ Sentinel 7.1 Administration Guide (Guía de administración de NetIQ Sentinel 7.1.*

Nota: También puede configurar la autenticación LDAP para un servidor Sentinel que se ejecute en modo FIPS 140-2 ejecutando el guión `ldap_auth_config.sh` en el directorio `/opt/novell/sentinel/setup`.

19.4 Actualización de certificados del servidor en gestores de recopiladores y motores de correlación remotos

Para configurar los gestores de recopiladores remotos y los motores de correlación remotos existentes de manera que se comuniquen con un servidor Sentinel que se ejecuta en modo FIPS 140-2, puede bien convertir el sistema remoto en modo FIPS 140-2 o bien actualizar el certificado del servidor Sentinel para el sistema remoto y dejar el gestor de recopiladores o el motor de correlación en el modo diferente de FIPS. Los gestores de recopiladores remotos en modo FIPS podrían no funcionar con orígenes de eventos que no sean compatibles con FIPS o que requieran uno de los conectores de Sentinel que aún no se hayan habilitado para FIPS.

Si no tiene previsto habilitar el modo FIPS 140-2 en el gestor de recopiladores o el motor de correlación remoto, debe copiar el certificado del servidor Sentinel más actualizado al sistema remoto, de manera que el gestor de recopiladores o el motor de correlación puedan comunicarse con el servidor Sentinel.

Para actualizar el certificado del servidor Sentinel en el gestor de recopiladores o el motor de correlación remoto:

1 Entre en el equipo del gestor de recopiladores o del motor de correlación remoto.

2 Cambie al usuario `novell` (`su novell`).

3 Busque el directorio bin. La ubicación por defecto es `/opt/novell/sentinel/bin`.

4 Ejecute el guión `updateServerCert.sh` y siga las instrucciones en pantalla.

19.5 Configuración de módulos auxiliares (plug-ins) de Sentinel para la ejecución en modo FIPS 140-2

En esta sección se proporciona información sobre la configuración de varios módulos auxiliares (plug-in) de Sentinel en modo FIPS 140-2.

Nota: Estas instrucciones presuponen que Sentinel está instalado en el directorio `/opt/novell/sentinel`. Los comandos deben ejecutarse como usuario`novell`.

19.5.1 Conector de Agent Manager

Siga el procedimiento a continuación solamente si ha seleccionado la opción *Cifrado (HTTPS)* al configurar los ajustes de red del Servidor de orígenes de eventos de Agent Manager.

Para configurar el conector de Agent Manager para su ejecución en modo FIPS 140-2:

1 Añada o edite el servidor de orígenes de eventos de Agent Manager. Siga por las pantallas de configuración hasta que se muestre la ventana de Seguridad. Para obtener más información, consulte la *Agent Manager Connector Guide* (Guía de conectores de Agent Manager).

2 Seleccione una de las opciones del campo *Tipo de autenticación del cliente*. El tipo de autenticación del cliente determina qué grado de control ejerce el servidor de orígenes de eventos de SSL Agent Manager al verificar la identidad de los orígenes de eventos de Agent Manager que están tratando de enviar datos.

- **Abrir:** Permite todas las conexiones SSL procedentes de agentes de Agent Manager. No realiza ninguna validación o autenticación del certificado del cliente.
- **Estricto:** Confirma que el certificado sea del tipo X.509 válido y comprueba además que el certificado del cliente sea de confianza para el servidor de orígenes de eventos. Los nuevos orígenes se deberán añadir de forma explícita a Sentinel (esto evita que orígenes ficticios envíen datos no autorizados).

Para la opción *Estricto*, debe importar el certificado de cada cliente de Agent Manager nuevo al almacén de claves de FIPS de Sentinel. Cuando Sentinel se ejecuta en modo FIPS 140-2, no es posible importar el certificado de cliente utilizando la interfaz de Gestión de orígenes de eventos (ESM).

Para obtener más información sobre la importación del certificado, consulte "Importación de certificados en la base de datos del almacén de claves de FIPS" en la página 122.

Nota: En el modo FIPS 140-2, el servidor de orígenes de eventos de Agent Manager utiliza el par de claves del servidor Sentinel; no se requiere importar el par de claves del servidor.

---

3 Si está habilitada la autenticación del servidor en los agentes, estos deben configurarse además para confiar en el servidor Sentinel o en el certificado del gestor de recopiladores remoto, dependiendo de donde esté implementado el conector.

Ubicación del certificado del servidor Sentinel: `/etc/opt/novell/sentinel/config/sentinel.cer`

Ubicación del certificado del gestor de recopiladores remoto: `/etc/opt/novell/sentinel/config/rcm.cer`

Nota: Al utilizar certificados personalizados con firma digital de una autoridad certificadora (CA), el agente de Agent Manager debe confiar en el archivo de certificado correspondiente.

19.5.2 Conector de base de datos (JDBC)

Siga el procedimiento a continuación solamente si ha seleccionado la opción *SSL* al configurar la conexión de base de datos.

Para configurar el conector de la base de datos para su ejecución en el modo FIPS 140-2:

1 Antes de configurar el conector, descargue el certificado del servidor de la base de datos y guárdelo como archivo `database.cert` en el directorio`/etc/opt/novell/sentinel/config` del servidor Sentinel.

Para obtener más información, consulte la documentación respectiva de la base de datos.

2 Importe el certificado al almacén de claves de FIPS de Sentinel.

Para obtener más información sobre la importación del certificado, consulte "Importación de certificados en la base de datos del almacén de claves de FIPS" en la página 122.

3 Continúe con la configuración del conector.

19.5.3 Conector de Sentinel Link

Siga el procedimiento a continuación solamente si ha seleccionado la opción *Cifrado (HTTPS)* al configurar los ajustes de red del servidor de orígenes de eventos de Sentinel Link.

Para configurar el conector de Sentinel Link para su ejecución en modo FIPS 140-2:

1 Añada o edite el servidor de orígenes de eventos de Sentinel Link. Siga por las pantallas de configuración hasta que se muestre la ventana de Seguridad. Para obtener más información, consulte la *Sentinel Link Connector Guide* (Guía de conectores de Sentinel Link).

2 Seleccione una de las opciones del campo *Tipo de autenticación del cliente*. El tipo de autenticación del cliente determina qué grado de control ejerce el servidor de orígenes de eventos de SSL Sentinel Link al verificar la identidad de los orígenes de eventos de Sentinel Link (integradores de Sentinel Link) que están tratando de enviar datos.

- **Abrir:** Permite las conexiones SSL procedentes de los clientes (integradores de Sentinel Link). No lleva a cabo ninguna validación ni autenticación de certificados de integrador.
- **Estricto:** Comprueba que el certificado del integrador sea del tipo X.509 válido y además comprueba que el certificado del integrador sea de confianza para el servidor de orígenes de eventos. Para obtener más información, consulte la documentación respectiva de la base de datos.

  Para la opción *Estricto*:

  - Si el integrador de Sentinel Link está en modo FIPS 140-2, debe copiar el archivo `/etc/opt/novell/sentinel/config/sentinel.cer` del equipo Sentinel remitente al equipo Sentinel destinatario. Importe este certificado al almacén de claves de FIPS del Sentinel destinatario.

    Nota: Al usar certificados personalizados con firma digital de una autoridad certificadora (CA), debe importar el archivo de certificado personalizado adecuado.

  - Si el integrador de Sentinel Link no está en modo FIPS, debe importar el certificado del integrados al almacén de claves de FIPS de Sentinel destinatario.

    Nota: Si el remitente es Sentinel Log Manager (en modo diferentes de FIPS) y el destinatario es Sentinel en modo FIPS 140-2, el certificado de servidor que se debe importar en el remitente es el archivo `/etc/opt/novell/sentinel/config/sentinel.cer` del equipo Sentinel destinatario.

  Cuando Sentinel se ejecuta en modo FIPS 140-2, no es posible importar el certificado de cliente utilizando la interfaz de Gestión de orígenes de eventos (ESM). Para obtener más información sobre la importación del certificado, consulte "Importación de certificados en la base de datos del almacén de claves de FIPS" en la página 122.

Nota: En el modo FIPS 140-2, el servidor de orígenes de eventos de Sentinel Link utiliza el par de claves del servidor Sentinel. No se requiere importar el par de claves del servidor.

19.5.4 Conector syslog

Siga el procedimiento a continuación solamente si ha seleccionado el protocolo *SSL* al configurar los ajustes de red del servidor de orígenes de eventos de Syslog.

Para configurar el conector Syslog para su ejecución en el modo FIPS 140-2:

1 Añada o edite el servidor de orígenes de eventos de Syslog. Continúe por las pantallas de configuración hasta que se muestre la ventana Conectividad. Para obtener más información, consulte la *Syslog Connector Guide* (Guía de conectores de Syslog).

2 Haga clic en *Ajustes*.

3 Seleccione una de las opciones del campo *Tipo de autenticación del cliente*. El tipo de autenticación del cliente determina qué grado de control ejerce el servidor de orígenes de eventos SSL de Syslog al verificar la identidad de los orígenes de eventos de Syslog que están tratando de enviar datos.

- **Abrir:** Permite las conexiones SSL procedentes de los clientes (orígenes de eventos). No realiza ninguna validación ni autenticación de certificados de cliente.

- **Estricto:** Confirma que el certificado sea del tipo X.509 válido y comprueba además que el certificado del cliente sea de confianza para el servidor de orígenes de eventos. Será necesario añadir nuevos orígenes de forma explícita a Sentinel (esto impide que orígenes ficticios envíen datos a Sentinel).

  Para la opción *Estricto*, debe importar el certificado del cliente syslog al almacén de claves de FIPS de Sentinel.

  Cuando Sentinel se ejecuta en modo FIPS 140-2, no es posible importar el certificado de cliente utilizando la interfaz de Gestión de orígenes de eventos (ESM).

  Para obtener más información sobre la importación del certificado, consulte "Importación de certificados en la base de datos del almacén de claves de FIPS" en la página 122.

Nota: En el modo FIPS 140-2, el servidor de orígenes de eventos de Syslog utiliza el par de claves del servidor Sentinel. No se requiere importar el par de claves del servidor.

---

4 Si está habilitada la autenticación del servidor en el cliente syslog, el cliente debe confiar en el certificado del servidor Sentinel o en el certificado del gestor de recopiladores remoto, dependiendo de donde esté implementado el conector.

El archivo de certificado del servidor Sentinel se encuentra en `/etc/opt/novell/sentinel/config/sentinel.cer`.

El archivo de certificado del gestor de recopiladores remoto se encuentra en `/etc/opt/novell/sentinel/config/rcm.cer`.

Nota: Al utilizar certificados personalizados con firma digital de una autoridad certificadora (CA), el cliente debe confiar en el archivo de certificado adecuado.

19.5.5 Conector de eventos Windows (WMI)

Para configurar el conector de eventos de Windows (WMI) para su ejecución en modo FIPS 140-2:

1 Añada o edite el conector de eventos de Windows. Siga por las pantallas de configuración hasta que se muestre la ventana de Seguridad. Para obtener más información, consulte la *Windows Event (WMI) Connector Guide* (Guía de conectores de eventos de Windows (WMI)).

2 Haga clic en *Ajustes*.

3 Seleccione una de las opciones del campo *Tipo de autenticación del cliente*. El tipo de autenticación del cliente determina qué grado de control ejerce el conector de eventos de Windows al verificar la identidad de los servicios de recopilación de eventos de Windows (WECS) del cliente que están tratando de enviar datos.

- **Abrir:** permite todas las conexiones SSL procedentes de WECS del cliente. No realiza ninguna validación o autenticación del certificado del cliente.
- **Estricto:** Comprueba que el certificado sea del tipo X.509 válido y comprueba además que el certificado de WECS del cliente esté firmado por una CA. Los nuevos orígenes deberán añadirse de forma explícita (esto impide que orígenes ficticios envíen datos a Sentinel).

  Para la opción *Estricto*, debe importar el certificado de WECS del cliente al almacén de claves de FIPS de Sentinel. Cuando Sentinel se ejecuta en modo FIPS 140-2, no es posible importar el certificado de cliente utilizando la interfaz de Gestión de orígenes de eventos (ESM).

  Para obtener más información sobre la importación del certificado, consulte "Importación de certificados en la base de datos del almacén de claves de FIPS" en la página 122.

Nota: En el modo FIPS 140-2, el servidor de orígenes de eventos de Windows utiliza el par de claves del servidor Sentinel. No se requiere importar el par de claves del servidor.

4 Si está habilitada la autenticación del servidor en el cliente Windows, el cliente debe confiar en el certificado del servidor Sentinel o en el certificado del gestor de recopiladores remoto, dependiendo de donde esté implementado el conector.

El archivo de certificado del servidor Sentinel se encuentra en `/etc/opt/novell/sentinel/config/sentinel.cer`.

El archivo de certificado del gestor de recopiladores remoto se encuentra en `/etc/opt/novell/sentinel/config/rcm.cer`.

Nota: Al utilizar certificados personalizados con firma digital de una autoridad certificadora (CA), el cliente debe confiar en el archivo de certificado adecuado.

5 Si desea sincronizar automáticamente los orígenes de eventos o completar la lista de orígenes de eventos mediante una conexión a un Active Directory, debe importar el certificado del servidor Active Directory al almacén de claves de FIPS de Sentinel.

Para obtener más información sobre la importación del certificado, consulte "Importación de certificados en la base de datos del almacén de claves de FIPS" en la página 122.

19.5.6 Integrador de Sentinel Link

Siga el procedimiento a continuación solamente si ha seleccionado la opción *Cifrado (HTTPS)* al configurar los ajustes de red del integrador de Sentinel Link.

Para configurar el integrador de Sentinel Link para su ejecución en el modo FIPS 140-2:

1 Cuando el integrador de Sentinel Link se encuentre en el modo FIPS 140-2, es obligatoria la autenticación del servidor. Antes de configurar la instancia del integrador, importe el certificado del servidor de Sentinel Link al almacén de claves de FIPS de Sentinel:

- **Si el conector de Sentinel Link está en el modo FIPS 140-2**:

  Si el conector se implementa en el servidor Sentinel, debe copiar el archivo`/etc/opt/novell/sentinel/config/sentinel.cer` desde el equipo Sentinel destinatario al equipo Sentinel remitente.

  Si el conector se implementa en un gestor de recopiladores remoto, debe copiar el archivo `/etc/opt/novell/sentinel/config/rcm.cer` desde el equipo de gestor de recopiladores remoto destinatario al equipo Sentinel destinatario.

  Importe este certificado al almacén de claves de FIPS de Sentinel.

  Nota: Al utilizar certificados personalizados con firma digital de una autoridad certificadora (CA), debe importar el archivo de certificado personalizado adecuado.

- Si el conector de Sentinel Link no está en modo FIPS:

  Importe el certificado del servidor de Sentinel Link personalizado al almacén de claves de FIPS de Sentinel remitente.

  Nota: Cuando el integrador de Sentinel Link está en el modo FIPS 140-2 y el conector de Sentinel Link está en modo diferente de FIPS, utilice el par de claves de servidor personalizado en el conector. No instale el par de claves del servidor interno.

para obtener más información sobre la importación del certificado, consulte la "Importación de certificados en la base de datos del almacén de claves de FIPS" en la página 122.

2 Continúe con la configuración de la instancia del integrador.

Nota: En el modo FIPS 140-2, el integrador de Sentinel Link utiliza el par de claves del servidor Sentinel. No se requiere importar el par de claves del integrador.

19.5.7 Integrador de LDAP

Para configurar el integrador de LDAP para que se ejecute en modo FIPS 140-2:

1 Antes de configurar la instancia del integrador, descargue el certificado del servidor LDAP y guárdelo como archivo `ldap.cert` en el directorio `/etc/opt/novell/sentinel/config` del servidor Sentinel.

Por ejemplo, utilice:

```
openssl s_client -connect <LDAP server IP>:636
```

y después copie el texto enviado (entre las líneas BEGIN y END, excluyéndolas) a un archivo.

2 Importe el certificado al almacén de claves de FIPS de Sentinel.

Para obtener más información sobre la importación del certificado, consulte "Importación de certificados en la base de datos del almacén de claves de FIPS" en la página 122.

3 Continúe con la configuración de la instancia del integrador.

19.5.8 Integrador de SMTP

El integrador de SMTP admite FIPS 140-2 a partir de la versión 2011.1r2 y versiones posteriores. No se requieren cambios de configuración.

19.5.9 Uso de conectores no habilitados para FIPS con Sentinel en el modo FIPS 140-2

En esta sección se proporciona información sobre cómo usar conectores no habilitados para FIPS con un servidor Sentinel en el modo FIPS 140-2. Se recomienda este planteamiento si tiene orígenes que no son compatibles con FIPS o si desea recopilar eventos de los conectores no compatibles con FIPS en su entorno.

Para usar conectores que no están en modo FIPS con Sentinel en el modo FIPS 140-2:

1 Instale un gestor de recopiladores remoto en el modo diferente de FIPS para conectar con el servidor Sentinel en el modo FIPS 140-2.

Para obtener más información, consulte la Sección 11.6, "Instalación de gestores de recopiladores y motores de correlación adicionales", en la página 80.

2 Implemente los conectores sin FIPS específicamente en el gestor de recopiladores remoto que no está en modo FIPS.

Nota: Estos son algunos de los problemas conocidos que surgen cuando conectores que no admiten FIPS como el conector de auditoría y el conector de archivos se implementan en un gestor de recopiladores remoto que no admite FIPS conectado a un servidor Sentinel 7.1 en el modo FIPS 140-2. Para obtener más información sobre estos problemas conocidos, consulte "NetIQ Sentinel 7.0.1 Readme" (Archivo Léame de NetIQ Sentinel 7.1).

19.6 Importación de certificados en la base de datos del almacén de claves de FIPS

Debe insertar los certificados en la base de datos del almacén de claves de FIPS para establecer comunicaciones seguras (SSL) desde los componentes propietarios de dichos certificados a Sentinel. No es posible cargar certificados utilizando la interfaz del usuario de Sentinel en la forma habitual cuando está habilitado el modo FIPS 140-2 en Sentinel. Debe importar manualmente el certificado a la base de datos del almacén de claves de FIPS.

Para los orígenes de eventos que utilizan conectores implementados en un gestor de recopiladores remoto, debe importar los certificados a la base de datos del almacén de claves de FIPS del gestor de recopiladores remoto en lugar de al servidor central de Sentinel.

Para importar certificados a la base de datos del almacén de claves de FIPS:

1. Copie el archivo de certificado a cualquier ubicación temporal del servidor Sentinel o del gestor de recopiladores remoto.
2. Busque el directorio bin de Sentinel. La ubicación por defecto es `/opt/novell/sentinel/bin`.
3. Ejecute el siguiente comando para importar el certificado a la base de datos del almacén de claves de FIPS y luego siga las instrucciones en pantalla.

   ```
   ./convert_to_fips.sh -i <certificate file path>
   ```

4. Introduzca `sí` o `s` cuando se le indique reiniciar el servidor Sentinel o el gestor de recopiladores remoto.

19.7 Reversión de Sentinel al modo diferente de FIPS

En esta sección se proporciona información sobre cómo revertir Sentinel y sus componentes al modo diferente de FIPS.

- Sección 19.7.1, “Reversión del servidor Sentinel al modo diferente de FIPS”, en la página 122
- Sección 19.7.2, “Reversión de gestores de recopiladores o motores de correlación remotos al modo diferente de FIPS”, en la página 123

19.7.1 Reversión del servidor Sentinel al modo diferente de FIPS

Puede revertir un servidor Sentinel que se ejecuta en modo FIPS 140-2 al modo diferente de FIPS solamente si ha realizado una copia de seguridad del servidor Sentinel antes de convertirlo para ejecutarse en modo FIPS 140-2.

Nota: Cuando revierte un servidor Sentinel al modo diferente de FIPS, perderá los eventos, datos de incidencia y cambios de configuración que haya realizado al servidor Sentinel después de convertirlo para ejecutarse en modo diferente de FIPS 140-2. El sistema Sentinel se restaurará al último punto de restauración en el modo diferente de FIPS. Debe realizar una copia de seguridad del sistema actual antes de revertirlo al modo diferente a FIPS para su uso en el futuro.

Para revertir el servidor Sentinel al modo diferente de FIPS:

1. Entre al servidor de Sentinel como usuario `root`.
2. Cambie al usuario `novell`.
3. Busque el directorio bin de Sentinel. La ubicación por defecto es `/opt/novell/sentinel/bin`.

4 Ejecute el siguiente comando para revertir el servidor Sentinel al modo diferente de FIPS y siga las instrucciones en pantalla:

```
./backup_util.sh -f <backup_file_name.tar.gz> -m 'restore'
```

Por ejemplo, si `non-fips201301241911359034887.tar.gz` es el archivo de copia de seguridad, ejecute el siguiente comando:

```
./backup_util.sh -f non-fips201301241911359034887.tar.gz -m 'restore'
```

5 Reinicie el servidor Sentinel.

19.7.2 Reversión de gestores de recopiladores o motores de correlación remotos al modo diferente de FIPS

Puede revertir los gestores de recopiladores o motores de correlación remotos al modo diferente de FIPS.

Para revertir gestores de recopiladores remotos o un motor de correlación remoto al modo diferente de FIPS:

1 Entre en el sistema del gestor de recopiladores remoto o del motor de correlación remoto.

2 Cambie al usuario `novell` (`su novell`).

3 Busque el directorio bin. La ubicación por defecto es `/opt/novell/sentinel/bin`.

4 Ejecute el guión `revert_to_nonfips.sh` y siga las instrucciones en pantalla.

5 Reinicie el gestor de recopiladores remoto o el motor de correlación remoto.

V Actualización de Sentinel

En esta sección se proporciona información sobre la actualización de Sentinel y otros componentes.

20 Actualización del servidor Sentinel

Importante: Sentinel 7.1 y versiones posteriores requieren que IPv6 esté habilitado en el sistema operativo. Asegúrese de que IPv6 esté habilitado en el sistema operativo antes de actualizar su sistema a Sentinel 7.1 o una versión posterior. Si IPv6 no está habilitado, algunos componentes fundamentales no funcionarán correctamente.

Siga los pasos indicados a continuación para actualizar el servidor Sentinel:

1. Realice una copia de seguridad de su configuración y, a continuación, cree una exportación de ESM.

   Para obtener más información sobre cómo realizar una copia de seguridad de los datos, consulte"Copia de seguridad y restauración de datos" en la *NetIQ Sentinel 7.1 Administration Guide (Guía de administración de NetIQ Sentinel 7.1)*.
2. Descargue el programa de instalación más reciente del sitio de descargas de Novell.
3. Entre como usuario `root` en el servidor en el que desea actualizar Sentinel.
4. 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.
5. Vaya al directorio donde extrajo el archivo de instalación.
6. Especifique el siguiente comando para actualizar Sentinel:

   ```
   ./install-sentinel
   ```
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 el acuerdo de 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. Para continuar con la actualización, pulse s.

   La instalación comienza instalando todos los paquetes RPM. Esta instalación puede tardar unos segundos en finalizar.
10. Borre la memoria caché del navegador Web para ver la versión más reciente de Sentinel.
11. (Condicional) Para actualizar los sistemas de gestor de recopiladores y los sistemas de motor de correlación, consulte el Capítulo 22, "Actualización del gestor de recopiladores o del motor de correlación", en la página 133.

21 Actualización del dispositivo Sentinel

Los procedimientos de este capítulo le guiarán en la actualización del dispositivo Sentinel así como de los dispositivos de gestor de recopiladores y de motor de correlación.

21.1 Actualización de Sentinel 7.0.2 y dispositivos de versiones posteriores

1. Entre en el dispositivo Sentinel como usuario con funciones de administrador.
2. **Si desea actualizar el dispositivo Sentinel**, haga clic en *Dispositivo* para lanzar WebYaST.
3. **Si desea actualizar un dispositivo de gestor de recopiladores o de motor de correlación**, especifique la dirección URL del equipo del gestor de recopiladores o del motor de correlación utilizando el puerto 54984 para lanzar WebYaST.
4. Realice una copia de seguridad de su configuración y, a continuación, cree una exportación de ESM.

   Para obtener más información sobre cómo realizar una copia de seguridad de los datos, consulte“Copia de seguridad y restauración de datos” en la *NetIQ Sentinel 7.1 Administration Guide (Guía de administración de NetIQ Sentinel 7.1)*.
5. (Condicional) Si aún no ha registrado el dispositivo para actualizaciones automáticas, hágalo ahora.

   Para obtener más información, consulte la Sección 12.4.3, “Registro para recibir actualizaciones”, en la página 93.

   Si el dispositivo no está registrado, Sentinel muestra una advertencia en amarillo que indica que el dispositivo no está registrado.
6. Para comprobar si existen actualizaciones, haga clic en *Updates* (Actualizaciones).

   Se muestran las actualizaciones disponibles.
7. Seleccione y aplique las actualizaciones.

   Las actualizaciones pueden tardar unos minutos en finalizar. Una vez finalizada de forma satisfactoria la actualización, se mostrará la página de acceso de WebYaST.

   Antes de actualizar la aplicación, WebYaST detiene el servicio de Sentinel automáticamente. Cuando finalice la actualización, debe reiniciar este servicio manualmente.
8. Reinicie el servicio Sentinel utilizando la interfaz basada en la Web.

Para obtener más información, consulte la Sección 12.5, “Inicio y detención del servidor mediante WebYaST”, en la página 95.

9 Borre la memoria caché del navegador Web para ver la versión más reciente de Sentinel.

21.2 Actualización de dispositivos Sentinel 7.0 y 7.0.1

La actualización de dispositivos Sentinel 7.0 y 7.0.1 falla en WebYaST porque el nombre del proveedor del parche ha cambiado de Novell a NetIQ. Es necesario actualizar el dispositivo mediante el parche zypper.

Para actualizar el dispositivo utilizando el parche zypper:

1 Realice una copia de seguridad de su configuración y luego cree una exportación de ESM. Para obtener más información, consulte “Backing Up and Restoring Data (Copia de seguridad y restauración de datos)” en la*NetIQ Sentinel 7.1 Administration Guide (Guía de administración de NetIQ Sentinel 7.1)*.

2 Entre a la consola de la aplicación como usuario `root`.

3 Ejecute el comando siguiente:

```
/usr/bin/zypper patch
```

4 Introduzca `1` para aceptar el cambio de Novell a NetIQ.

5 Pulse `S` para continuar.

6 Pulse `sí` para aceptar el acuerdo de licencia.

7 Reinicie la aplicación Sentinel.

8 Borre la memoria caché del navegador web para ver la versión más reciente de Sentinel.

21.3 Actualización de la aplicación con SMT

En entornos protegidos en los que el dispositivo debe ejecutarse sin acceso directo a Internet, debe configurar el dispositivo con la herramienta SMT (Subscription Management Tool), que le permite actualizar el dispositivo a las versiones más recientes disponibles.

1 Asegúrese de que la aplicación está configurada con SMT.

Para obtener más información, consulte Sección 12.4.4, “Configuración del dispositivo con SMT”, en la página 93.

2 Entre a la consola de la aplicación como usuario `root`.

3 Actualice el repositorio para la actualización:

```
zypper ref -s
```

4 Compruebe si la aplicación está habilitada para la actualización:

```
zypper lr
```

5 (Opcional) Compruebe las actualizaciones disponibles para la aplicación:

```
zypper lu
```

6 (Opcional) Compruebe los paquetes que incluyen las actualizaciones disponibles para la aplicación:

```
zypper lp -r SMT-http_<smt_server_fqdn>:<package_name>
```

7 Actualice la aplicación:

```
zypper up -t patch -r SMT-http_<smt_server_fqdn>:<package_name>
```

8 Reinicie el dispositivo.

```
rcsentinel restart
```

22 Actualización del gestor de recopiladores o del motor de correlación

Siga los pasos a continuación para actualizar el gestor de recopiladores o el motor de correlación:

1. Realice una copia de seguridad de su configuración y cree una exportación de ESM.

   Para obtener más información, consulte "Backing Up and Restoring Data (Copia de seguridad y restauración de datos)" en la*NetIQ Sentinel 7.1 Administration Guide (Guía de administración de NetIQ Sentinel 7.1)*.
2. Entre en la interfaz basada en la Web de Sentinel como usuario con funciones de administrador.
3. Seleccione *Descargas*.
4. Haga clic en *Descargar instalador* de la sección Instalador de gestor de recopiladores.

   Se muestra una ventana con opciones para abrir o guardar el archivo del instalador en el equipo local.
5. Guarde el archivo.
6. Copie el archivo en una ubicación temporal.
7. Extraiga el contenido del archivo.
8. Ejecute el guión siguiente:

   Para gestor de recopiladores:

   ```
   ./install-cm
   ```

   Para motor de correlación:

   ```
   ./install-ce
   ```
9. Siga las instrucciones que aparecen en pantalla para finalizar el procedimiento de instalación.
10. Borre la memoria caché del navegador web para ver la versión más reciente de Sentinel.

23 Actualización de módulos auxiliares (plug-in) de Sentinel

Las instalaciones de actualizaciones de Sentinel no actualizan los módulos auxiliares (plug-ins) a menos que uno de los módulos auxiliares no sea compatible con la versión más reciente de Sentinel.

Los módulos auxiliares (plug-in) nuevos y actualizados de Sentinel se cargan con frecuencia en el sitio Web de módulos auxiliares de Sentinel . Para obtener las correcciones de defectos, documentación y mejoras más recientes de un módulo auxiliar (plug-in), descargue e instale la versión más reciente de dicho módulo auxiliar. Para obtener más información sobre cómo instalar un módulo auxiliar (plug-in), consulte la documentación específica del módulo auxiliar en cuestión.

VI Apéndices

A Configuración de Sentinel para alta disponibilidad

Muchos clientes pretenden instalar Sentinel en entornos de alta disponibilidad con el objetivo de garantizar la recopilación de eventos empresariales cruciales de la forma más sistemática posible. Muchos requisitos de seguridad y cumplimiento dependen de la recopilación de datos completos para demostrar el cumplimiento de dichos requisitos; la pérdida de algunos eventos podría impedir la detección de una amenaza o infracción y poner a la organización en un riesgo inaceptable. Se han realizado pruebas en NetIQ que certifican que puede utilizarse en un entorno de alta disponibilidad y que es compatible con arquitecturas de recuperación tras fallos.

En este apéndice se describe cómo instalar el producto en modo de alta disponibilidad Activo-Pasivo, que permite a Sentinel realizar un failover a un nodo de clúster redundante en caso de producirse un fallo del hardware o software. No cubre las configuraciones Activa-Pasiva y no garantiza ningún objetivo de tiempo de actividad en particular. NetIQ Consulting (servicios de consultoría) y los socios de NetIQ pueden ayudarle a implementar las funciones de alta disponibilidad y recuperación tras fallos de Sentinel.

Nota: NetIQ admite la configuración de Alta disponibilidad solamente en Sentinel en instalaciones "todo en uno". No admite directamente instalaciones distribuidas de gestores de recopiladores o motores de correlación.

A.1 Conceptos

Alta disponibilidad se refiere a una metodología de diseño destinada a mantener la disponibilidad de un sistema para su utilización en la máxima medida posible. La intención es reducir al mínimo las causas de tiempo de inactividad, como por ejemplo fallos del sistema y mantenimiento y minimizar el tiempo que se tarda en detectar y recuperarse de los eventos que producen tiempo de inactividad cada vez que ocurran. En la práctica, se hace necesario contar con un medio automatizado para detectar y recuperarse rápidamente los eventos que causan tiempo de inactividad a medida que se deben obtener niveles más altos de disponibilidad.

A.1.1 Sistemas externos

Sentinel es una aplicación compleja multinivel que depende de y proporciona una amplia variedad de servicios. Por otro lado, se integra con varios sistemas de terceros externos para la recopilación de datos, uso compartido de datos y resolución de incidencias. La mayoría de soluciones de alta disponibilidad permiten a los encargados de implementarlas declarar dependencias entre los servicios que deben estar altamente disponibles y servicios dependientes, pero esto solo se aplica a los servicios que se ejecutan en el propio clúster. Los sistemas externos a Sentinel como los orígenes de eventos deben configurarse por separado para tener la disponibilidad que requiere la organización, y también deben configurarse para manejar correctamente situaciones en las que Sentinel no está disponible durante un cierto período de tiempo, como por ejemplo cuando se produce un evento de failover. Si los derechos de acceso están muy restringidos, por ejemplo si se utilizan sesiones autenticadas para enviar/recibir datos entre un sistema tercero y Sentinel, entonces el sistema tercero debe configurarse para aceptar las sesiones procedentes de cualquier nodo del clúster o para iniciar sesión en cualquier nodo del clúster (para este fin, Sentinel debe configurarse con una IP virtual). NetIQ no puede garantizar ningún nivel de alta disponibilidad en particular entre nuestro producto y sistemas terceros que no están bajo nuestro control.

A.1.2 Almacenamiento compartido

Todos los clústeres de alta disponibilidad requieren alguna forma de almacenamiento compartido que permita mover rápidamente los datos de aplicaciones de un nodo de clúster a otro en caso de fallo del nodo de origen. El almacenamiento en sí debería tener una alta disponibilidad; eso se consigue por lo general mediante la tecnología de Red de área de almacenamiento (SAN) conectada a los nodos del clúster mediante una red de Canal de fibra. Otros sistemas utilizan Almacenamiento con interconexión a la red (NAS), iSCSI u otras tecnologías que permiten el montaje remoto de almacenamiento compartido. El requisito fundamental del almacenamiento compartido es que el clúster pueda mover de forma transparente el almacenamiento desde un nodo de clúster que ha fallado a un nuevo nodo de clúster.

Nota: Para iSCSI, debe usar la unidad de transferencia de mensajes (MTU) más grande que sea compatible con su hardware. Las MTU de mayor tamaño optimizan el rendimiento del almacenamiento. Sentinel podría tener problemas si la latencia o el ancho de banda para almacenamiento son inferiores al valor recomendado.

Existen dos planteamientos básicos que puede usar Sentinel para el almacenamiento compartido. El primero localiza todos los componentes: binarios de aplicaciones, configuración y datos de eventos, en el almacenamiento compartido. Al producirse el failover, el almacenamiento se desmonta del nodo principal y se mueve al nodo de reserva, el cual carga toda la aplicación y la configuración desde el almacenamiento compartido. El segundo planteamiento almacena los datos de eventos en el almacenamiento compartido, pero los binarios de la aplicación y la configuración residen en cada nodo del clúster. Al producirse el failover, solo los datos de eventos se mueven al nodo de reserva.

Cada uno de estos planteamientos tiene ventajas y desventajas, pero el segundo permite a la instalación de Sentinel utilizar vías de instalación estándar compatibles con FHS, permite la verificación de paquetes RPM y también la aplicación de parches en caliente y la reconfiguración con el fin de reducir al mínimo el tiempo de inactividad.

Esta solución le guiará en un ejemplo del proceso de instalación en un clúster que utiliza almacenamiento compartido iSCSI y localiza los binarios de la aplicación/la configuración en cada nodo del clúster.

A.1.3 Supervisión de servicios

Un componente clave de cualquier entorno de alta disponibilidad es una forma sistemática y fiable de supervisar los recursos que deben tener una alta disponibilidad, junto con cualquier recurso del que dependen. EL SLE HAE utiliza un componente denominado Resource Agent para llevar a cabo esta supervisión: el trabajo de Resource Agent consiste en proporcionar el estado de cada recurso, y además (cuando se le pida) iniciar o detener dicho recurso.

Los Resource Agents deben proporcionar un estado fiable de los recursos supervisados para prevenir cualquier tiempo de inactividad innecesario. Los falsos positivos (cuando se considera que un recurso ha fallado, pero de hecho se recupera por sí solo) pueden provocar una migración del servicio (y el tiempo de inactividad asociado) cuando en realidad no es necesario y los falsos negativos (cuando el Resource Agent informa que un recurso está funcionando correctamente cuando de hecho no lo está) pueden impedir el uso adecuado del servicio. Por otro lado, la supervisión externa de un servicio puede ser bastante difícil; un puerto de servicio Web podría responder a un ping sencillo, por ejemplo, pero podría no ofrecer datos correctos cuando se envía una consulta real. En muchos casos, la funcionalidad de autocomprobación debe integrarse en el propio servicio para proporcionar una medida verdaderamente exacta.

Esta solución proporciona un OCF Resource Agent básico para Sentinel capaz de supervisar y detectar un fallo importante de hardware, del sistema operativo o del sistema Sentinel. En este momento las capacidades de supervisión externas de Sentinel se basan en la investigación de puertos IP y existe cierta posibilidad de que se produzcan lecturas de falsos positivos y negativos. Tenemos previsto mejorar en el futuro tanto Sentinel como Resource Agent con el fin de mejorar la exactitud de este componente.

A.1.4 Fencing

Dentro de un clúster de alta disponibilidad (HA), se supervisan de forma constante los servicios cruciales y se reinician automáticamente en otros nodos en caso de fallo. Esta automatización puede presentar problemas, no obstante, si ocurre algún problema de comunicación con el nodo principal; aunque el servicio que se ejecuta en dicho nodo parece estar inactivo, de hecho sigue ejecutándose y escribiendo datos en el almacenamiento compartido. En ese caso, comenzar un nuevo conjunto de servicios en un nodo de reserva podría dañar fácilmente los datos.

Los clústeres utilizan una variedad de técnicas denominadas de forma colectiva "fencing" que impiden que esto suceda, incluidas SBD (Split Brain Detection) y STONITH (Shoot The Other Node In The Head). El objetivo principal es prevenir que se dañen los datos en el almacenamiento compartido.

A.2 Compatibilidad

NetIQ admite esta solución basada en las características del clúster definidas y en el comportamiento previsto, según se define en el documento y según se ha comprobado en nuestros laboratorios. Otras configuraciones de clúster solo serán compatibles si los problemas observados en su entorno se pueden reproducir en nuestros entornos de prueba, lo cual eliminaría las diferencias locales de implementación como causa del problema.

A.3 Requisitos del sistema

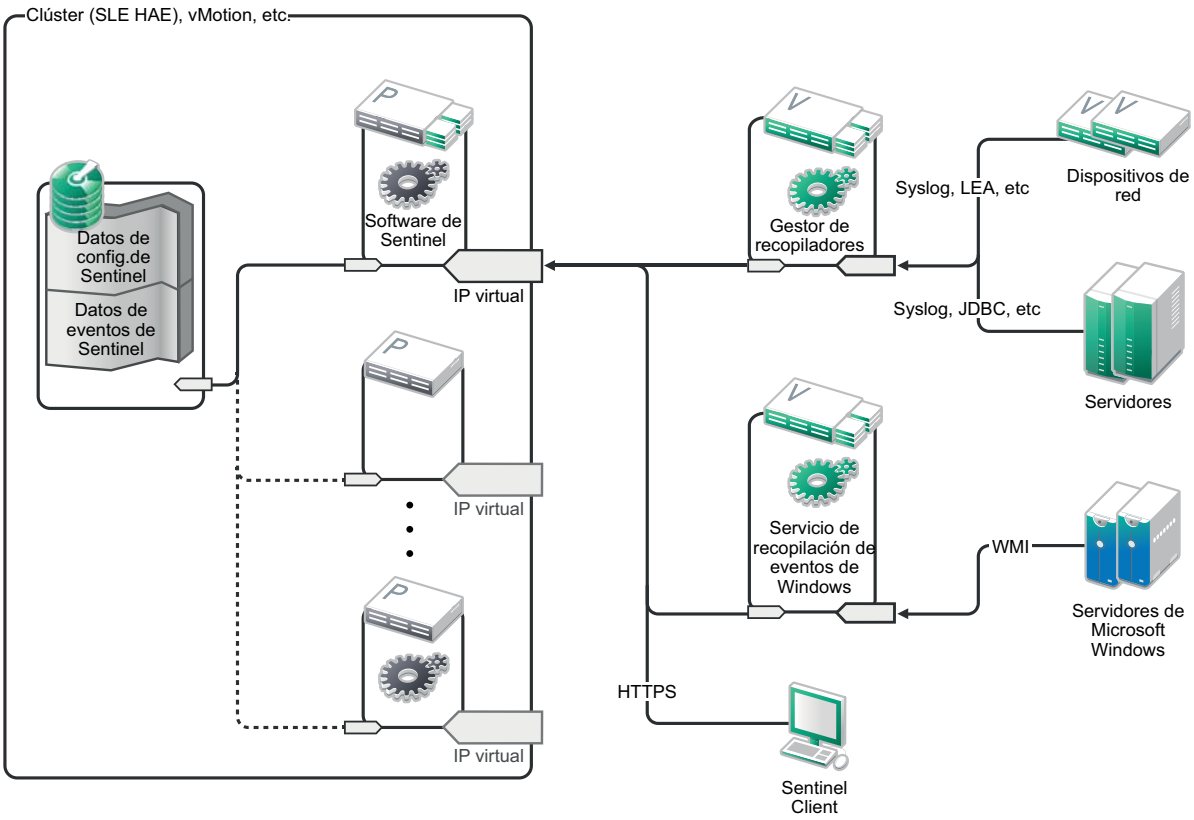
Al asignar recursos de clúster para ofrecer compatibilidad con una instalación de alta disponibilidad, tenga en cuenta los siguientes requisitos:

- Cada nodo de clúster que alberga servicios de Sentinel debe cumplir los requisitos especificados en el Capítulo 5, “Cumplimiento de los requisitos del sistema”, en la página 35.
- Asegúrese de que haya espacio de almacenamiento compartido suficiente para los datos y la aplicación Sentinel.
- Una dirección IP virtual para los servicios que se pueda migrar de un nodo a otro al producirse el failover.
- El instalador de Sentinel (archivo TAR) con licencia válida.
- La extensión SUSE Linux High Availability Extension (imagen de ISO) con licencia válida.
- Un dispositivo de almacenamiento compartido que cumpla las características de rendimiento y tamaño tal como se documentó en el Capítulo 5, “Cumplimiento de los requisitos del sistema”, en la página 35. La solución de ejemplo utilizará una SUSE Linux VM estándar con destinos iSCSI como almacenamiento compartido.
- Un mínimo de dos nodos de clúster que cumplan los requisitos de recursos para ejecutar Sentinel en el entorno del cliente. La solución de ejemplo utilizará dos SUSE Linux VM.
- Un método de comunicación de los nodos del clúster con el almacenamiento compartido, como FibreChannel para una SAN. La solución de ejemplo utilizará una dirección IP dedicada para conectar con el destino iSCSI.
- Una dirección IP que se pueda migrar desde un nodo del clúster a otro para que sirva como dirección IP externa de Sentinel.
- Al menos una dirección IP por nodo del clúster para las comunicaciones internas del clúster. La solución de ejemplo utilizará una dirección IP de unidifusión simple pero se prefiere multidifusión para los entornos de producción.

A.4 Instalación y configuración

En esta sección se proporcionan los pasos de instalación y configuración de Sentinel en un entorno de alta disponibilidad. Cada paso describe el planteamiento general y luego se refiere a una configuración de demostración que detalla una solución de clúster de ejemplo. Puede usar otras opciones o tecnología diferentes de las enumeradas en este documento, en función de las limitaciones descritas en la Sección A.2, “Compatibilidad”, en la página 141.

El siguiente diagrama representa una arquitectura de alta disponibilidad (HA) activa-pasiva:



A.4.1 Config inicial

Configure el hardware del equipo, el hardware de red, el hardware de almacenamiento, los sistemas operativos, las cuentas de usuario y demás recursos básicos del sistema de acuerdo con los requisitos documentados para los requisitos locales del cliente y de Sentinel. Pruebe los sistemas para garantizar su funcionamiento y estabilidad adecuados.

- Como práctica óptima, todos los nodos de clúster deben estar sincronizados en el tiempo; utilice NTP o una tecnología similar para este fin.
- El clúster requerirá una resolución de nombre de host fiable. Como práctica óptima, quizá sea una buena idea introducir todos los nombres de host de clúster internos en el archivo `/etc/hosts` para garantizar la continuidad del clúster en caso de fallo del DNS. Si algún nodo de clúster no puede resolver otros nodos ***por nombre***, la configuración descrita en este apartado fallará.
- Las características de CPU, RAM y espacio en el disco para cada nodo del clúster deben cumplir los requisitos del sistema definidos en el Capítulo 5, “Cumplimiento de los requisitos del sistema”, en la página 35 en base al número de eventos esperado.

- Las características de espacio en el disco y E/S para los nodos de almacenamiento deben cumplir los requisitos del sistema definidos en el Capítulo 5, “Cumplimiento de los requisitos del sistema”, en la página 35 en función del número de eventos esperado y de las directivas de retención de datos del almacenamiento local y/o en red.
- Si desea configurar cortafuegos en el sistema operativo para limitar el acceso a Sentinel y al clúster, consulte el Capítulo 7, “Puertos utilizados”, en la página 59 para obtener detalles sobre qué puertos deben estar disponibles dependiendo de la configuración local y de los orígenes que enviarán los datos de eventos.

La solución de ejemplo utilizará la siguiente configuración:

- Dos VM de nodo de clúster SUSE Linux 11 SP2
  - La instalación del SO no necesita instalar X Windows, pero puede hacerlo si se desea la configuración de la interfaz gráfica del usuario. Los guiones de arranque pueden definirse para iniciarse sin X (runlevel 3), que puede iniciarse solamente cuando sea necesario.
  - Los nodos tendrán dos NICS: una para acceso externo y otra para comunicaciones iSCSI.
  - Configure las NIC externas con direcciones IP que permitan el acceso remoto a través de SSH o similar. Para este ejemplo, utilizaremos 172.16.0.1 (node01) y 172.16.0.2 (node02).
  - Cada nodo debe tener suficiente espacio de disco para el sistema operativo, binarios de Sentinel y datos de configuración, software del clúster, espacio temporal, etc. Consulte los requisitos del sistema de SUSE Linux y SLE HAE, y los requisitos de la aplicación Sentinel.
- Una SUSE Linux 11 SP2 VM configurada con destinos iSCSI Targets para almacenamiento compartido
  - La instalación del SO no necesita instalar X Windows, pero puede hacerlo si se desea la configuración de la interfaz gráfica del usuario. Los guiones de arranque pueden definirse para comenzar sin X (runlevel 3), que puede iniciarse solamente cuando sea necesario.
  - Los nodos tendrán dos NICS: una para acceso externo y otra para comunicaciones iSCSI.
  - Configure las NIC externas con una dirección IP que permita el acceso remoto a través de SSH o similar. Para este ejemplo, utilizaremos 172.16.0.3 (storage03).
  - El sistema debería tener espacio suficiente para el sistema operativo, espacio temporal, un gran volumen para almacenamiento compartido para albergar datos de Sentinel, y una pequeña cantidad de espacio para una partición SBD. Consulte los requisitos del sistema SUSE Linux y los requisitos de almacenamiento de datos de eventos de Sentinel. Para la solución de ejemplo pondremos todos los datos (local, red, SBD) en un solo disco, pero para las implementaciones de producción, esto podría asignarse a diferentes nodos.

Nota: En un clúster de producción, puede usar IPs internas, no encaminables en tarjetas NIC independientes (posiblemente un par de ellas, para ofrecer redundancia) para las comunicaciones internas del clúster.

A.4.2 Configuración de almacenamiento compartido

Configure su almacenamiento compartido y asegúrese de que pueda montarlo en cada nodo del clúster. Si utiliza FibreChannel y una SAN, esto puede requerir conexiones físicas y otra configuración. El almacenamiento compartido se utilizará para albergar bases de datos y datos de eventos de Sentinel, por lo que su tamaño debe ser acorde con el entorno del cliente en función del número de eventos esperado y de las directivas de retención de datos.

Una implementación típica podría usar una SAN rápida conectada a través de FibreChannel a todos los nodos del clúster, con una matriz RAID para almacenar datos de eventos locales. Se podría utilizar una NAS independiente o un nodo iSCSI para el almacenamiento de red más lento. Siempre

que el nodo del clúster pueda montar el almacenamiento local como dispositivo de bloques normal, podrá ser utilizado por la solución. El almacenamiento en red también puede montarse como dispositivo de bloques, o bien podría ser un NFS o volumen CIFS.

Nota: Debe configurar su almacenamiento compartido y probar el montaje en cada nodo del clúster, pero el montaje real del almacenamiento lo manejará la configuración del clúster.

Para la solución de ejemplo, utilizaremos destinos iSCSI albergados por una SUSE Linux VM:

La solución de ejemplo utilizará destinos iSCSI configurados en una SUSE Linux VM. La VM es `storage03` tal como se indica en Config inicial. Los dispositivos iSCSI se pueden crear utilizando cualquier archivo o dispositivo de bloque, pero para simplificar, aquí utilizaremos un archivo creado con este propósito.

Conecte con `storage03` e inicie una sesión de consola. Utilice el comando `dd` para crear un archivo en blanco de cualquier tamaño para el almacenamiento local de Sentinel:

```
dd if=/dev/zero of=/localdata count=10240000 bs=1024
```

En ese caso, creamos un archivo de 10 GB lleno de ceros (copiado de `/dev/zero pseudo-device`). Consulte la información o la página manual de `dd` para conocer los detalles de las opciones de línea de comandos. Por ejemplo, para crear "discos" de diferente tamaño. El destino iSCSI trata este archivo como si fuera un disco; por supuesto que puede usar un disco real si lo prefiere.

Repita este procedimiento para crear un archivo para almacenamiento en red:

```
dd if=/dev/zero of=/networkdata count=10240000 bs=1024
```

Para este ejemplo utilizamos dos archivos ("discos") del mismo tamaño y características de rendimiento. Para una implementación de producción, podría poner el almacenamiento local en una red SAN rápida y el almacenamiento en red en un iSCSI, NFS o volumen CIFS más lentos.

Configure estos archivos como destinos iSCSI:

1. Ejecute YaST desde la línea de comandos (o bien utilice la interfaz gráfica del usuario, si lo prefiere): `/sbin/yast`
2. Seleccione **Dispositivos de red** > **Configuración de red**.
3. Asegúrese de que esté seleccionada la pestaña **Descripción general**.
4. Seleccione la NIC secundaria en la lista que aparece y luego desplácese hacia delante para Editar y pulse `Intro`.
5. En la pestaña **Dirección**, asigne la dirección IP estática 10.0.0.3. Esta será la IP de comunicaciones SCSI internas.
6. Haga clic en **Siguiente** y después en **Aceptar**.
7. En la pantalla principal, seleccione **Servicios de red** > **Destino iSCSI**.
8. Cuando se le indique, instale el software necesario (`iscsitarget RPM`) del soporte SUSE Linux 11 SP2.
9. Haga clic en **Servicio**, seleccione la opción**When Booting** (En el arranque) para asegurarse de que el servicio se inicia al arrancar el sistema operativo.
10. Haga clic en **Global** y después seleccione **No Authentication** (Sin autenticación) porque el OCF Resource Agent actual para iSCSI no es compatible con autenticación.
11. Haga clic en **Destinos** y luego en **Añadir** para añadir un nuevo destino.

    El destino iSCSI generará automáticamente una ID y después presentará una lista vacía de LUN (unidades) que están disponibles.

12 Haga clic en **Añadir** para añadir un nuevo LUN.

13 Deje el número LUN 0, y después busque en el cuadro de diálogo **Vía** (en Type=fileio) y seleccione el archivo `/localdata` que ha creado. Si tiene un disco dedicad para almacenamiento, especifique un dispositivo de bloque, como por ejemplo `/dev/sdc`.

14 Repita los pasos 12 y 13, y añada esta vez LUN 1 y `/networkdata` .

15 Deje las demás opciones en sus valores por defecto. Haga clic en **Aceptar** y, a continuación, en **Siguiente**.

16 Haga clic de nuevo en **Siguiente** para seleccionar las opciones de autenticación por defecto, y luego en **Finalizar** para salir de la configuración. Pulse para Aceptar si se le pide reiniciar iSCSI.

17 Salga de YaST.

El procedimiento anterior expone dos destinos iSCSI del servidor en la dirección IP 10.0.0.3. En cada nodo del clúster, asegúrese de que pueda montar el dispositivo de almacenamiento compartido de datos locales. También debe formatear los dispositivos (una vez):

1 Conéctese a uno de los nodos del clúster (node01) e inicie YaST.

2 Seleccione **Dispositivos de red** > **Configuración de red**.

3 Asegúrese de que esté seleccionada la pestaña **Descripción general**.

4 Seleccione la NIC secundaria en la lista que aparece y luego desplácese hacia delante para Editar y pulse `Intro`.

5 Haga clic en **Dirección**, asigne la dirección IP estática 10.0.0.1. Esta será la IP de comunicaciones internas de iSCSI.

6 Seleccione **Siguiente** y después **Aceptar**.

7 Haga clic en **Network Services** (Servicios de red) > **iSCSI Initiator** (Iniciador de iSCSI).

8 Si se le solicita, instale el software necesario (open-iscsi RPM) desde el soporte SUSE Linux 11 SP2.

9 Haga clic en **Service** (Servicio), seleccione **When Booting** (Al arrancar) para asegurarse de que el servicio iSCSI se inicia durante el arranque.

10 Haga clic en **Discovered Targets** (Destinos descubiertos) y seleccione **Discovery** (Descubrimiento).

11 Especifique la dirección IP de iSCSI (10.0.0.3), seleccione **No Authentication** (Sin autenticación) y luego haga clic en **Siguiente**.

12 Seleccione el destino iSCSI descubierto con la dirección IP 10.0.0.3 y después seleccione**Log In** (Entrar).

13 Cambie a automático en el cuadro desplegable **Startup** (Inicio) y seleccione **No Authentication** (Sin autenticación) y luego haga clic en**Siguiente**.

14 Cambie a la pestaña **Connected Targets** (Destinos conectados) para garantizar que se establezca la conexión con el destino.

15 Salga de la configuración. Esta acción debería haber montado los destinos iSCSI como dispositivos de bloque en el nodo del clúster.

16 En el menú principal YaST, seleccione **System** (Sistema) > **Partitioner** (Particionador).

17 En la Vista del sistema, deberá ver nuevos discos duros (por ejemplo `/dev/sdb` y `/dev/sdc`) en la lista; tendrá IET-VIRTUAL-DISK como tipo. Desplácese hacia el primero de la lista (que debería ser el almacenamiento local), selecciónelo y pulse `Intro`.

18 Seleccione **Add**(Añadir) para añadir una nueva partición al disco vacío. Dé formato al disco como partición ext3 principal, pero no lo monte. Asegúrese de que esté seleccionada la opción Do not mount partition (No montar partición).

19 Seleccione **Siguiente** y luego **Finalizar** después de revisar los cambios que se realizarán. Dando por supuesto que se crea una sola partición grande en este LUN iSCSI compartido, al final se debe tener `/dev/sdb1` o un disco formateado similar (denominado `/dev/<SHARED1>` a continuación).

20 Regrese al particionador y repita el proceso de creación de particiones/formato (pasos 16-19) para `/dev/sdc` o sea cual sea el dispositivo de bloque que corresponda con el almacenamiento en red. Esto debe dar lugar a una partición `/dev/sdc1` o disco formateado similar (denominado `/dev/<NETWORK1>` a continuación).

21 Salga de YaST.

22 Por último, cree un punto de montaje y pruebe el montaje de la partición local de la siguiente manera (el nombre exacto del dispositivo dependerá de la implementación específica):

```
# mkdir /var/opt/novell
# mount /dev/<SHARED1> /var/opt/novell
```

23 Debe poder crear archivos en la nueva partición y verlos siempre que esté montada.

Para desmontar:

```
# umount /var/opt/novell
```

Repita los pasos 1-15 del procedimiento anterior y asegúrese de que cada nodo de clúster pueda montar el almacenamiento compartido local. Sin embargo, reemplace la IP del nodo del paso 5, por una IP diferente (p. ej., node02 > 10.0.0.2).

A.4.3 Instalación de Sentinel

Hay dos opciones para instalar Sentinel: instalar cada uno de los componentes de Sentinel en el almacenamiento compartido (usando la opción de ubicación para redirigir la instalación de Sentinel a donde sea que se haya montado el almacenamiento compartido) o poner solo los datos variables de la aplicación en el almacenamiento compartido.

En esta solución de ejemplo, seguiremos el segundo planteamiento e instalaremos Sentinel en cada nodo que pueda albergarlo. La primera vez que se instala Sentinel, realizaremos una instalación completa que incluye binarios de la aplicación, configuración y todos los almacenes de datos. Las instalaciones posteriores en los demás nodos del clúster solo instalarán la aplicación y darán por supuesto que los datos reales de Sentinel estarán disponibles dentro de cierto tiempo (p. ej., una vez que se monte el almacenamiento compartido).

Solución de ejemplo:

En esta solución de ejemplo, instalaremos Sentinel en cada nodo del clúster, almacenando solo los datos variables de la aplicación en el almacenamiento compartido. Esto conserva los binarios de la aplicación y la configuración en ubicaciones estándar, nos permite verificar los RPM y además nos permite aplicar parches en caliente en determinados escenarios.

Instalación del primer nodo

1 Conéctese a uno de los nodos de clúster (node01) y abra la ventana de la consola.

2 Descargue el instalador de Sentinel (un archivo tar.gz) y guárdelo en `/tmp` en el nodo de clúster.

3 Ejecute los comandos siguientes:

```
mount /dev/<SHARED1> /var/opt/novell

cd /tmp

tar -xvzf sentinel_server*.tar.gz
```

```
cd sentinel_server*

./install-sentinel --record-unattended=/tmp/install.props
```

1. Ejecute la instalación estándar, configurando el producto como corresponda. El instalador instalará los binarios, la configuración, las bases de datos y configurará los nombres de usuario/contraseñas y los puertos de red.
2. Inicie Sentinel y pruebe las funciones básicas. Puede usar la dirección IP de nodo de clúster externa estándar para acceder al producto.
3. Apague Sentinel y desmonte el almacenamiento compartido:

   ```
   rcsentinel stop

   umount /var/opt/novell
   ```

   Este paso eliminará los guiones de inicio automático de manera que el clúster pueda gestionar el producto.

   ```
   cd /

   insserv -r sentinel
   ```

Instalación de nodos posteriores

Repita la instalación en otros nodos:

El instalador inicial de Sentinel crea una cuenta de usuario para su uso por parte del producto, que utiliza la siguiente ID de usuario disponible en el momento de la instalación. Las instalaciones posteriores en modo sin supervisión tratarán de usar la misma ID para la creación de la cuenta, pero existe la posibilidad de que surjan conflictos (si los nodos del clúster no son idénticos en el momento de la instalación). Se recomienda encarecidamente realizar una de las siguientes acciones:

- Sincronizar la base de datos de la cuenta en todos los nodos del clúster (manualmente a través de LDAP o similar), asegurándose de que se produzca la sincronización antes de realizar instalaciones posteriores. En ese caso, el instalador detectará la presencia de la cuenta de usuario y utilizará la existente.
- Observe el resultado de las instalaciones posteriores sin supervisión: se emitirá una advertencia si no fue posible crear la cuenta de usuario con la misma ID de usuario.

1. Conéctese a cada nodo del clúster adicional (node02) y abra una ventana de consola.
2. Realice lo siguiente:

   ```
   cd /tmp

   scp root@node01:/tmp/sentinel_server*.tar.gz

   scp root@node01:/tmp/install.props

   tar -xvzf sentinel_server*.tar.gz

   ./install-sentinel --no-start --cluster-node --unattended=/tmp/install.props

   cd /

   insserv -r sentinel
   ```

Al finalizar el proceso, Sentinel deberá estar instalado en todos los nodos, pero es probable que no funcione correctamente en ninguno de ellos salvo el primero hasta que varias claves estén sincronizadas, lo que sucederá cuando se configuren los recursos del clúster.

A.4.4 Instalación del clúster

Instale el software del clúster en cada nodo y registre cada nodo del clúster con el gestor de clústeres. Los procedimientos para realizarlo variarán en función de la implementación del clúster, pero al final del proceso cada nodo del clúster deberá aparecer en la consola de gestión de clústeres.

Para nuestra solución de ejemplo, configuraremos la extensión SUSE Linux High Availability Extension y la superpondremos con los agentes de recursos específicos de Sentinel:

Si no utiliza el OCF Resource Agent para supervisar Sentinel, es probable que desarrolle una solución de supervisión similar para el entorno de clúster local. El OCF Resource Agent para Sentinel es un guión shell sencillo que ejecuta una variedad de comprobaciones para verificar si Sentinel es funcional. Si desea desarrollar el suyo propio, debe examinar el Resource Agent existente para ver ejemplos (el Resource Agent está almacenado en `sentinel-ha.rpm` en el paquete de descarga de Sentinel).

Existen muchas formas diferentes de configurar el clúster SLE HAE, pero seleccionaremos opciones que simplifican enormemente la configuración. El primer paso consiste en instalar el software central de SLE HAE; el proceso se explica detalladamente en la Documentación de SLE HAE. Para obtener información sobre la instalación de productos complementarios de SLES, consulte la Guía de implementación.

Debe instalar el SLE HAE en todos los nodos del clúster, node01 y node02 en nuestro ejemplo. El producto complementario instalará el software de comunicaciones y gestión de clústeres central, además de cualquier Resource Agent que se utilice para supervisar los recursos del clúster.

Una vez instalado el software del clúster, deberá instalarse un RPM adicional para proporcionar Resource Agents de clúster adicionales específicos de Sentinel. El RPM puede encontrarse en `novell-Sentinel-ha-7.1*.rpm` incluido en la descarga normal de Sentinel, que desempaquetó para instalar el producto.

En cada nodo del clúster, copie el `novell-Sentinel-ha-7.1*.rpm` en el directorio `/tmp` y luego:

```
cd /tmp
rpm -i novell-Sentinel-ha-7.1*.rpm
```

A.4.5 Configuración del clúster

Debe configurar el software del clúster para registrar cada nodo del clúster como miembro del clúster. Aparte de esta configuración, también puede configurar los recursos de fencing y STONITH para garantizar la coherencia del clúster.

En nuestra solución de ejemplo, básicamente usamos la configuración más sencilla sin redundancia adicional u otras funciones avanzadas. Además utilizamos dirección de unidifusión (en lugar de la dirección de multidifusión preferida) porque requiere menos interacción con los administradores de red y es suficiente para fines de prueba. Además configuramos un recurso simple de fencing basado en SBD.

Solución de ejemplo:

La solución de ejemplo utilizará direcciones IP privadas para las comunicaciones internas del clúster y utilizará unidifusión para minimizar la necesidad de solicitar direcciones de multidifusión de un administrador de red. La solución utilizará además un destino iSCSI configurado en la misma SUSE Linux VM que alberga el almacenamiento compartido que servirá como dispositivo SBD para fines de fencing. Igual que antes, se pueden crear dispositivos iSCSI utilizando cualquier archivo o dispositivo de bloque, pero para simplificar aquí usaremos un archivo creado para este fin.

Los siguientes pasos de configuración son muy similares a los de la configuración de almacenamiento compartido:

Configuración de SBD

Conéctese a `storage03` e inicie una sesión de la consola. Use el comando **dd** para crear un archivo en blanco de cualquier tamaño:

```
dd if=/dev/zero of=/sbd count=1024 bs=1024
```

En este caso, creamos un archivo de 1 MB lleno de ceros (copiado de`/dev/zero` pseudo-device).

Configure el archivo como destino iSCSI:

1. Ejecute YaST desde la línea de comandos (o utilice la interfaz gráfica del usuario, si lo prefiere): `/sbin/yast`
2. Seleccione **Servicios de red** > **Destino iSCSI**.
3. Haga clic en **Destinos** y seleccione el destino existente.
4. Seleccione**Editar**. La interfaz del usuario presentará una lista de LUN (unidades) que están disponibles.
5. Seleccione **Añadir** para añadir un LUN nuevo.
6. Deje el número LUN 2. Busque en el cuadro de diálogo **Vía** y seleccione el archivo `/sbd` que ha creado.
7. Deje las demás opciones en sus valores por defecto y luego seleccione **Aceptar** y después **Siguiente**; a continuación haga clic de nuevo en **Siguiente** para seleccionar las opciones de autenticación por defecto.
8. Haga clic en **Finalizar** para salir de la configuración. Si es necesario, reinicie los servicios. Salga de YaST.

Nota: Los pasos siguientes requieren que cada nodo del clúster sea capaz de resolver el nombre de host de todos los demás nodos del clúster (el servicio de sincronización de archivos csync2 fallará si no es el caso). Si no se configura el DNS o no está disponible, añade entradas para cada host en el archivo`/etc/hosts` que enumera cada IP junto con su nombre de host (tal como lo indica el comando de nombre de host).

Este procedimiento debe exponer un destino iSCSI para el dispositivo SBD en el servidor en la dirección IP 10.0.0.3 (storage03).

Configuración de nodos

Conéctese a un nodo del clúster (node01) y abra una consola:

1. Ejecute YaST.
2. Abra **Network Services** (Servicios de red) > **iSCSI Initiator** (Iniciador de iSCSI).
3. Seleccione **Connected Targets** (Destinos conectados) y luego el destino iSCSI que configuró anteriormente.
4. Seleccione la opción **Log Out** (Salir) para salir del destino.
5. Cambie a la pestaña **Discovered Targets** (Destinos descubiertos) y seleccione el **Destino** y vuelva a entrar para actualizar la lista de dispositivos (deje la opción de inicio automático con la opción Sin autenticación).
6. Seleccione **Aceptar** para salir de la herramienta del Iniciador de iSCSI.
7. Abra**System** (Sistema) > **Partitioner** (Particionador) e identifique el dispositivo SBD como el 1MB IET-VIRTUAL-DISK. Aparecerá como **/dev/sdd** o similar; observe cuál.

8. Salga de YaST.
9. Ejecute el comando `ls -l /dev/disk/by-id/` y observe la ID del dispositivo que está vinculada al nombre del dispositivo identificado anteriormente.
10. Ejecute el comando `sleha-init`.
11. Cuando se le pregunte a qué dirección de red desea vincularlo, especifique la IP de NIC externa (172.16.0.1).
12. Acepte la dirección de multidifusión y el puerto por defecto. Más tarde sobrescribiremos estos valores.
13. Introduzca 's' para habilitar SBD y luego especifique `/dev/disk/by-id/<device id>`, donde`<device id>` es la ID que identificó anteriormente (puede usar el tabulador para completar automáticamente la vía).
14. Complete el asistente y asegúrese de que no se generen errores.
15. Inicie YaST.
16. Seleccione **High Availability** (Alta disponibilidad) > **Cluster** (Clúster) (o simplemente Clúster en algunos sistemas).
17. En el cuadro de la izquierda, asegúrese de que se haya seleccionado **Communication Channels** (Canales de comunicación).
18. Desplácese hasta la línea superior de configuración y cambie la selección de udp a udpu (esto inhabilita multidifusión y selecciona unidifusión).
19. Seleccione la opción para **Add a Member Address** (Añadir una dirección de miembro) y especifique este nodo (172.16.0.1), luego repita y añada el otro o los otros nodos del clúster: 172.16.0.2.
20. Seleccione **Finalizar** para completar la instalación.
21. Salga de YaST.
22. Ejecute el comando `/etc/rc.d/openais` para reiniciar los servicios de clúster con el nuevo protocolo de sincronización.

Conéctese a cada nodo de clúster adicional (node02) y abra una consola:

1. Ejecute el comando siguiente: `sleha-join`
2. Introduzca la dirección IP del primer nodo del clúster.

En algunas circunstancias las comunicaciones del clúster no se inician correctamente. Si el clúster no se inicia (el servicio `openais` fallará al iniciarse):

- Copia manualmente `corosync.conf` de node1 a node02, o ejecute `csync2 -x -v` en el nodo 1, o bien configure manualmente el clúster en node02 a través de YaST.
- Ejecute `/etc/rc.d/openais start` en node02

En algunos casos, el guión de instalación fallará porque el servicio `xinetd` no añade correctamente el nuevo servicio `csync2`. Este servicio es necesario para que el otro nodo pueda sincronizar los archivos de configuración del clúster hasta este nodo. Si ve errores como `csync2 run failed`, podría tener este problema. Para solucionar este problema, ejecute: `kill -HUP ``cat /var/run/xinetd.init.pid` y luego vuelva a ejecutar el guión `sleha-join`.

En este punto debería poder ejecutar crm_mon en cada nodo del clúster y observar que el clúster se ejecuta correctamente. Alternativamente, puede usar 'hawk', la consola Web; las credenciales de entrada por defecto son 'hacluster / linux'.

Existen dos parámetros adicionales con los que debemos jugar para este ejemplo; si estos se van a aplicar a un clúster de producción del cliente dependerá de su configuración:

1. Defina la opción global del clúster `no-quorum-policy` en `ignore`. Esto se hace porque solo tenemos un clúster de dos nodos, por lo que cualquier fallo en un nodo rompería el quórum e inhabilitaría todo el clúster: `crm configure property no-quorum-policy=ignore`

   Nota: Si el clúster tiene más de dos nodos, no defina esta opción.

2. Defina la opción global del clúster `default-resource-stickiness to 1`. Esto alentará al administrador de recursos a dejar los recursos en ejecución en su lugar en vez de cambiarlos de sitio: `crm configure property default-resource-stickiness=1`.

A.4.6 Configuración de recursos

Tal como se mencionó en Instalación de clúster, esta solución proporciona un OCF Resource Agent para supervisar los servicios centrales en SLE HAE, y puede crear alternativas si lo desea. El software también depende de otros recursos varios, para los que se proporcionan Resource Agents por defecto con SLE HAE. Si no utiliza SLE HAE, deberá supervisar estos recursos adicionales utilizando otra tecnología:

- Un recurso de sistema de archivos correspondiente al almacenamiento compartido que utiliza el software.
- Un recurso de dirección IP que se corresponde con la IP virtual por la que se accederá a los servicios.
- El software de base de datos Postgres que utiliza el software para almacenar la configuración y los metadatos de eventos.

Existen recursos adicionales, como MongoDB que se utiliza para Inteligencia de seguridad y el bus de mensajes ActiveMQ; al menos por el momento estos se supervisan dentro de los servicios centrales.

Solución de ejemplo

La solución de ejemplo utiliza versiones simples de los recursos necesarios, como por ejemplo Filesystem Resource Agent. Puede elegir recursos de clúster más sofisticados como cLVM (una versión de volumen lógico del sistema de archivos) si es necesario.

La solución de ejemplo proporciona un guión `crm` para ayudar en la configuración del clúster. El guión envía variables de configuración relevantes desde el archivo de configuración sin supervisión generado dentro de la instalación de Sentinel. Si no generó el archivo de configuración, o si desea cambiar la configuración de los recursos, puede editar el guión según corresponda.

Conéctese al nodo original en el que instaló Sentinel (debe ser el nodo en el que ejecutó la instalación completa de Sentinel) y realice lo siguiente (<SHARED1> es el volumen compartido que creó anteriormente):

```
mount /dev/<SHARED1> /var/opt/novell

cd /usr/lib/ocf/resource.d/novell

./install-resources.sh
```

Podrían surgir problemas con los nuevos recursos que aparecen en el clúster; ejecute `/etc/rc.d/openais restart` en node02 si experimenta este problema.

El guión `install-resources.sh` le pedirá algunos valores, principalmente la IP virtual que desea que utilicen las personas para acceder a Sentinel y el nombre del dispositivo del almacenamiento compartido, y luego se crearán automáticamente los recursos de clúster necesarios. Tenga en cuenta que el guión requiere que el volumen compartido ya esté montado y también requiere que esté presente el archivo de instalación sin supervisión que se creó durante la instalación de Sentinel (`/tmp/install.props`). No es necesario que ejecute este guión en ningún nodo instalado salvo el primero; todos los archivos de configuración relevantes se sincronizarán automáticamente en los otros nodos.

Si el entorno del cliente varía con respecto a esta solución de ejemplo, puede editar el archivo `resources.cli` (en el mismo directorio) y modificar las definiciones primitivas desde aquí. Por ejemplo, la solución de ejemplo utiliza el recurso de Sistema de archivos; quizá desee usar un recurso cLVM más atento al clúster.

Después de ejecutar el guión shell, puede emitir un comando de estado de crm y el resultado debería ser similar a:

```
crm status
```

```
Last updated: Thu Jul 26 16:34:34 2012
Last change: Thu Jul 26 16:28:52 2012 by hacluster via crmd on node01
Stack: openais
Current DC: node01 - partition with quorum
Version: 1.1.6-b988976485d15cb702c9307df55512d323831a5e
2 Nodes configured, 2 expected votes
5 Resources configured.
```

```
Online: [ node01, node02 ]
stonith-sbd    (stonith:external/sbd):    Started node01
 Resource Group: sentinelgrp
     sentinelip    (ocf::heartbeat:IPaddr2):    Started node01
     sentinelfs    (ocf::heartbeat:Filesystem):    Started node01
     sentineldb    (ocf::novell:pgsql):    Started node01
     sentinelserver    (ocf::novell:sentinel):    Started node01
```

En este punto, los recursos relevantes de Sentinel deben configurarse en el clúster. Puede examinar cómo se configuran y agrupan en la herramienta de gestión del clúster, por ejemplo ejecutando el estado de crm.

A.4.7 Configuración del almacenamiento en red

Como paso final de este proceso, configure el almacenamiento en red de manera que Sentinel puede migrar las particiones de eventos a un almacenamiento menos costoso. Esto es opcional y de hecho el almacenamiento en red no tiene que tener una alta disponibilidad de la misma forma que el resto del sistema; se puede usar cualquier directorio (montado desde una SAN o no), un NFS o volumen CIFS.

Haga clic en**Almacenamiento** en la barra de menú superior y luego seleccione **Configuración**, y a continuación seleccione los botones circulares de Almacenamiento de red no configurado para configurar esta opción.

Solución de ejemplo

La solución de ejemplo usará un destino iSCSI simple como ubicación de almacenamiento compartido en red, con prácticamente la misma configuración que el almacenamiento local. En implementaciones de producción, es probable que se utilicen tecnologías de almacenamiento diferentes.

Utilice el siguiente procedimiento para configurar el almacenamiento en red para su uso en Sentinel:

Nota: Puesto que utilizaremos un destino iSCSI para esta solución de ejemplo, el destino se montará como directorio para su uso como almacenamiento en red. Por lo tanto, necesitaremos configurar el montaje como recurso de sistema de archivos de forma parecida a como se configuró el sistema de archivos de almacenamiento local. Esto no se configuró automáticamente dentro del guión de instalación de recursos, ya que existen otras variaciones posibles; realizaremos la configuración manualmente.

1. Revise los pasos anteriores para determinar qué partición se creó para su uso como almacenamiento en red (`/dev/<NETWORK1>`, o algo parecido a `/dev/sdc1`). Si es necesario, cree un directorio vacío en el que se pueda montar la partición (por ejemplo `/var/opt/netdata`).
2. Configure el sistema de archivos de red como recurso de clúster; utilice la interfaz gráfica del usuario o ejecute el comendo:

   ```
   crm configure primitive sentinelnetfs ocf:heartbeat:Filesystem params device="/
   dev/<NETWORK1>" directory="<PATH>" fstype="ext3" op monitor interval=60s
   ```

   donde `/dev/<NETWORK1>` es la partición que se creó en la sección Configuración de almacenamiento compartido anterior, y <PATH> es cualquier directorio local en el que se puede montar.
3. Añada el nuevo recurso al grupo de recursos gestionados:

   ```
   crm resource stop sentinelgrp
   crm configure delete sentinelgrp
   crm configure group sentinelgrp sentinelip sentinelfs sentinelnetfs sentineldb
   sentinelserver
   crm resource start sentinelgrp
   ```
4. Puede conectarse al nodo que alberga actualmente los recursos (utilice estado de crm status o Hawk) y asegúrese de que el almacenamiento en red esté montado correctamente (utilice el comando mount).
5. Entre en la interfaz Web de Sentinel.
6. Seleccione **Almacenamiento** y después **Configuración**, y a continuación seleccione la **SAN (montada localmente**) en Almacenamiento de red no configurado.
7. Introduzca la vía en la que se ha montado el almacenamiento de red, por ejemplo `/var/opt/netdata`.

La solución de ejemplo utiliza versiones simples de los recursos necesarios, como por ejemplo el Filesystem Resource Agent simple; los clientes pueden elegir usar recursos de clúster más sofisticados como cLVM (una versión de volumen lógico del sistema de archivos) si lo desean.

A.5 Recuperación de datos y copias de seguridad

El clúster de failover de alta disponibilidad descrito en este documento proporciona un nivel de redundancia para que, si un servicio falla en un nodo del clúster, se producirá automáticamente el failover y la recuperación en otro nodo del clúster. Cuando sucede un evento de este tipo, es importante devolver el nodo fallido al estado operativo de manera que se pueda restaurar la redundancia de sistema y protegerlo en caso de otro fallo. En esta sección se describe la restauración del nodo fallido en una variedad de condiciones de fallo.

- Sección A.5.1, “Copia de seguridad”, en la página 155
- Sección A.5.2, “Recuperación”, en la página 155

A.5.1 Copia de seguridad

Si bien el clúster de failover de alta disponibilidad descrito en este documento proporciona un nivel de redundancia, sigue siendo importante realizar una copia de seguridad tradicional de la configuración y los datos, que haría muy fácil la recuperación en caso de pérdida o daño de los mismos. En la sección "Backing Up and Restoring Data" (Copia de seguridad y recuperación de datos) de *NetIQ Sentinel 7.1 Administration Guide* (Guía de administración de NetIQ Sentinel 7.1) se describe cómo usar las herramientas integradas en Sentinel para crear una copia de seguridad. Estas herramientas deben usarse en el nodo activo del clúster porque el nodo pasivo del clúster no tendrá el acceso necesario al dispositivo de almacenamiento compartido. Sería posible usar en su lugar otras herramientas comerciales de copia de seguridad disponibles que podrían tener requisitos diferentes sobre en qué nodo se pueden usar.

A.5.2 Recuperación

- "Fallo temporal" en la página 155
- "Daño del nodo" en la página 155
- "Configuración de datos del clúster" en la página 155

Fallo temporal

Si se trató de un fallo temporal y no parece que haya daños en la aplicación o el software del sistema operativo y la configuración, entonces será posible devolver el nodo al estado operativo eliminando simplemente el fallo temporal, por ejemplo reiniciando el nodo. Puede utilizarse la interfaz del usuario de gestión del clúster para recuperar la configuración inicial del servicio en ejecución al nodo del clúster original, si así lo desea.

Daño del nodo

Si el fallo dio lugar a daños en la aplicación o el software del sistema operativo o en la configuración presente en el sistema de almacenamiento del nodo, será necesario reinstalar el software. La repetición de los pasos de adición de un nodo al clúster descrita anteriormente en este documento devolverá el nodo a un estado operativo. Puede utilizarse la interfaz del usuario de gestión del clúster para recuperar la configuración inicial del servicio en ejecución al nodo del clúster original, si así lo desea.

Configuración de datos del clúster

Si se producen daños en los datos del dispositivo de almacenamiento compartido de forma que no es posible recuperar este dispositivo, los daños producidos afectarían a todo el clúster de manera que no se podrá recuperar automáticamente al usar el clúster de failover de alta disponibilidad descrito en este documento. La sección "Backing Up and Restoring Data" (Copia de seguridad y restauración de datos) de *NetIQ Sentinel 7.1 Administration Guide* (Guía de administración de NetIQ Sentinel 7.1) describe cómo usar las herramientas integradas de Sentinel para restaurarlo a partir de una copia de seguridad. Estas herramientas deben usarse en el nodo activo del clúster porque el nodo pasivo del clúster no tendrá el acceso necesario al dispositivo de almacenamiento compartido. Sería posible usar en su lugar otras herramientas comerciales de copia de seguridad y restauración disponibles que podrían tener requisitos diferentes sobre en qué nodo se pueden usar.

B Resolución de problemas en la instalación

En esta sección se enumeran los problemas que podrían ocurrir durante la instalación y las medidas para solucionar dichos problemas.

B.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 en el dispositivo.

Para solucionar este problema, configure adecuadamente los ajustes de red. Para verificar la configuración, utilice el comando `ipconfig` para devolver la dirección IP válida y utilice el comando `hostname -f` para devolver el nombre de host válido.

B.2 El UUID no se crea para gestores de recopiladores con imagen o motores de correlación.

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

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

1. Suprima el archivo `host.id` o `sentinel.id` ubicado en la carpeta `/var/opt/novell/sentinel_/data`.
2. Reinicie el gestor de recopiladores.

   El gestor de recopiladores genera de forma automática el UUID.

C Desinstalación

En este apéndice se proporciona información sobre la desinstalación de Sentinel y otras tareas posteriores a la desinstalación.

C.1 Lista de verificación de desinstalación

Utilice la siguiente lista de verificación para desinstalar Sentinel:

- ❒ Desinstale el servidor Sentinel.
- ❒ Desinstale el gestor de recopiladores y el motor de correlación, si los hay.
- ❒ Lleve a cabo las tareas posteriores a la desinstalación para finalizar la desinstalación de Sentinel.

C.2 Desinstalación de Sentinel

Hay disponible un guión de desinstalación que le ayudará a eliminar una instalación de Sentinel. Antes de ejecutar una nueva instalación, debe ejecutar todos los pasos siguientes para asegurarse de que no quedan archivos ni ajustes del sistema procedentes de una instalación anterior.

Advertencia: Estas instrucciones implican la modificación de valores de configuración y archivos del sistema operativo. Si no está familiarizado con la modificación de estos valores de configuración y archivos del sistema, póngase en contacto con el administrador del sistema.

C.2.1 Desinstalación del servidor de Sentinel

Siga los pasos indicados a continuación para desinstalar el servidor Sentinel:

1. Entre en Sentinel como usuario `root`.

   Nota: No es posible desinstalar el servidor Sentinel como usuario diferente de root si la instalación la llevó a cabo el usuario `root`. Sin embargo, un usuario diferente de root puede desinstalar el servidor Sentinel si la instalación fue realizada por un usuario diferente de root.

2. Acceda al siguiente directorio:

   ```
   /opt/novell/sentinel/setup/
   ```

3. Ejecute el comando siguiente:

   ```
   ./uninstall-sentinel
   ```

4 Cuando se le indique que vuelva a confirmar que desea continuar con la desinstalación, pulse s.

El guión detiene primero el servicio y luego lo elimina por completo.

C.2.2 Desinstalación del gestor de recopiladores o del motor de correlación

Siga los pasos indicados a continuación para desinstalar el gestor de recopiladores y el motor de correlación:

1 Entre a la sesión como usuario `root`.

Nota: No es posible desinstalar un gestor de recopiladores remoto o un motor de correlación remoto como usuario diferente de root, si la instalación se realizó como usuario `root`. Sin embargo, un usuario diferente de root puede realizar la desinstalación, si la instalación la llevó a cabo un usuario diferente de root.

2 Vaya a la siguiente ubicación:

```
/opt/novell/sentinel/setup
```

3 Ejecute el comando siguiente:

```
./uninstall-sentinel
```

El guión muestra una advertencia que indica que el gestor de recopiladores o el motor de correlación y todos los datos asociados se eliminarán por completo.

4 Introduzca s para eliminar el gestor de recopiladores o el motor de correlación.

El guión detiene primero el servicio y luego lo elimina por completo. No obstante, aún podría visualizarse el icono del gestor de recopiladores y del motor de correlación en el estado inactivo en la interfaz Web.

5 Lleve a cabo los siguientes pasos adicionales para suprimir manualmente el gestor de recopiladores y el motor de correlación en la interfaz Web:

Gestor de recopiladores:

1. Acceda a *Gestión de orígenes de eventos* > *Vista activa*.
2. Haga clic con el botón derecho en el gestor de recopiladores que desee suprimir y, a continuación, haga clic en *Suprimir*.

Motor de correlación:

1. Acceda a la interfaz Web de Sentinel como administrador.
2. Amplíe *Correlación* y luego seleccione el motor de correlación que desea suprimir.
3. Haga clic en el botón *Suprimir* (icono de papelera).

C.3 Tareas posteriores a la desinstalación

La desinstalación del servidor Sentinel no supone la eliminación del usuario administrador de Sentinel del sistema operativo. Necesitará eliminarlo manualmente.

Después de desinstalar Sentinel, se conservan algunos ajustes del sistema. Es necesario eliminar estos ajustes antes de llevar a cabo una nueva instalación de Sentinel, en particular si se encuentran errores en la desinstalación de Sentinel.

Para eliminar manualmente los ajustes del sistema de Sentinel:

1. Entre a la sesión como usuario `root`.
2. Asegúrese de que todos los procesos de Sentinel están detenidos.
3. Elimine el contenido de `/opt/novell/sentinel` (o la carpeta en la que haya instalado el software de Sentinel).
4. Asegúrese de que nadie haya iniciado una sesión como usuario del sistema operativo del administrador de Sentinel (novell por defecto); a continuación, elimine el usuario, el directorio personal y el grupo.

   ```
   userdel -r novell
   ```

   ```
   groupdel novell
   ```
5. Reinicie el sistema operativo.