NetIQ® Sentinel™

Guía de instalación y configuración

Diciembre de 2015

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 implantación 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 a la implantación, 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 implantación; 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 ponerse en contacto con la 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 ponerse en contacto con la 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 ponerse en contacto 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 información detallada sobre Sentinel y cómo Sentinel ofrece a su organización una solución de gestión de eventos.

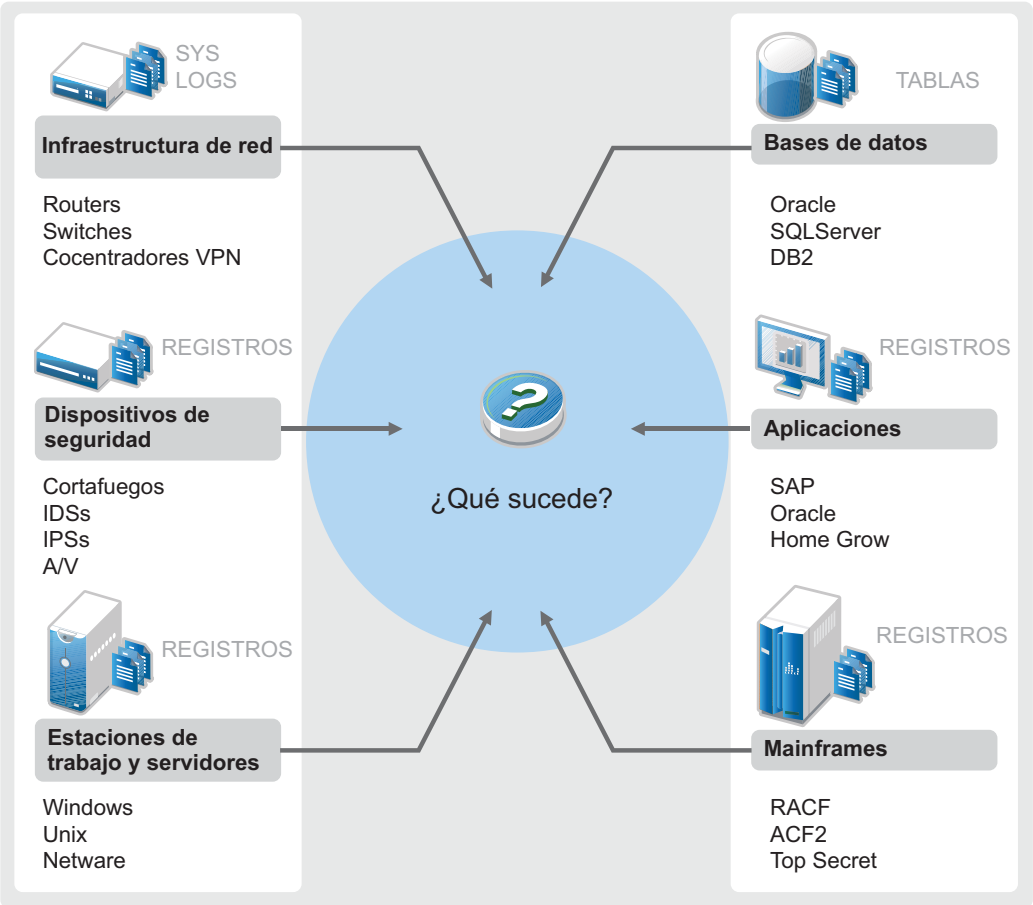
1 ¿Qué es Sentinel?

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

1.1 Retos de proteger un entorno de TI

La protección del entorno de TI es un desafío debido a su complejidad. Por lo general, los entornos de TI contienen muchas aplicaciones, bases de datos, mainframes, estaciones de trabajo y servidores, y todas estas entidades generan registros de eventos. Es posible que también tenga dispositivos de seguridad y dispositivos de infraestructura de red que generen registros de eventos en su entorno de TI.

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



Los desafíos surgen por los siguientes hechos:

- Existen muchos dispositivos en su entorno de TI.
- Los registros tienen diferentes formatos.
- Los registros se almacenan en distintas ubicaciones.
- En los archivos de registro se captura una gran cantidad de información.
- Resulta imposible determinar los activadores de eventos sin antes analizar manualmente los archivos de registro.

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

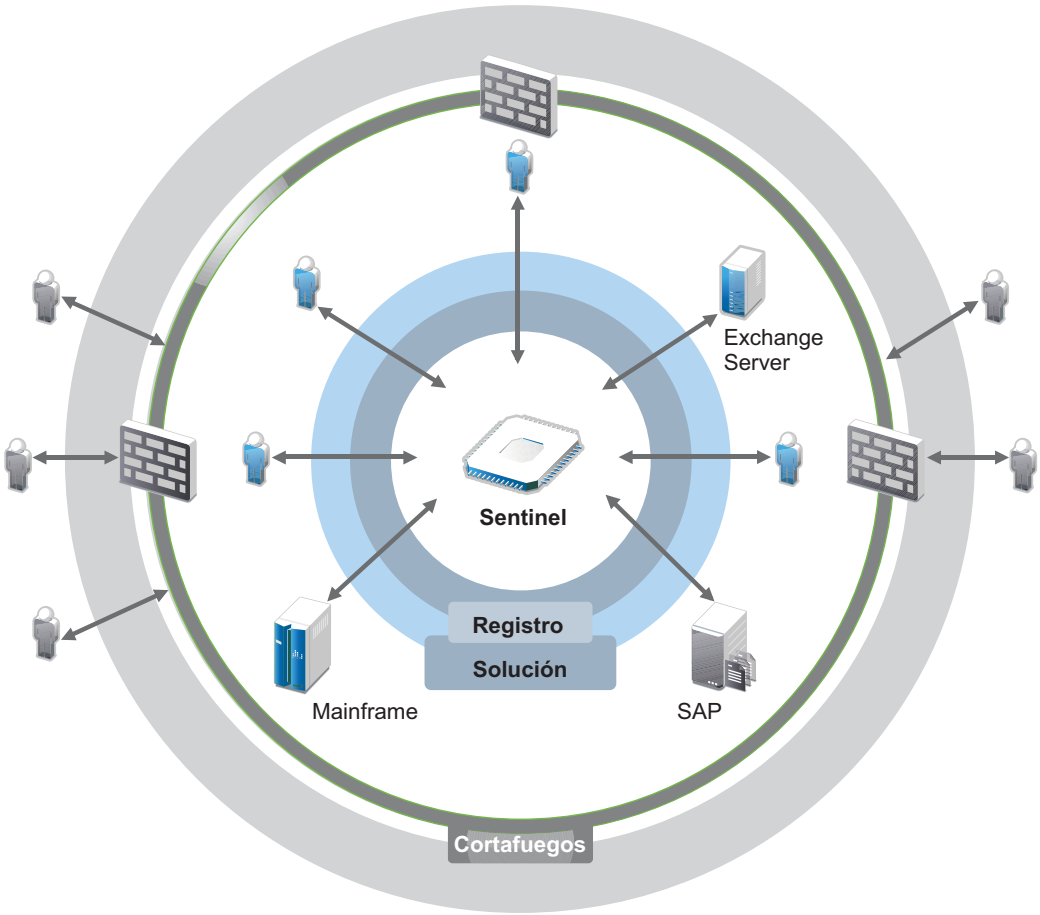
- Recopilar los datos.
- Consolidar los datos.
- Normalizar datos dispares en eventos que se puedan comparar fácilmente.
- Asignar eventos a regulaciones estándar.
- Analizar los datos.
- Comparar los eventos en múltiples sistemas para determinar si existen problemas de seguridad.
- Enviar notificaciones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

Una vez que comprenda los desafíos que conlleva proteger su entorno de TI, debe decidir cómo quiere proteger la empresa para los usuarios y frente a ellos de modo que la experiencia del usuario no se vea afectada. 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*



Con Sentinel, sabe lo que sucede en su entorno de TI en un punto dado y tiene la capacidad de conectar las acciones realizadas en los recursos con las personas que realizan dichas acciones. Esto le permite determinar el comportamiento de los usuarios y supervisar las actividades con eficacia a fin de prevenir las actividades maliciosas.

Sentinel lo consigue de la siguiente manera:

- Ofreciendo una solución única para tratar los controles de TI en múltiples estándares de seguridad.
- Abordando la distancia entre lo que debería ocurrir y lo que está ocurriendo realmente en su entorno de TI.
- Ayudándole a cumplir los estándares de seguridad.
- Ofreciendo programas de información y supervisión del cumplimiento listos para usar.

Sentinel automatiza los procesos de recopilación, análisis y generación de informes de registros con el fin de asegurar que los controles de TI sean eficaces para detectar amenazas y cumplir requisitos de auditoría. Sentinel ofrece supervisión automatizada de los eventos de seguridad, eventos de cumplimiento y controles TI. Le permite actuar de inmediato si se vulnera la seguridad o tiene lugar un evento fuera de conformidad. Sentinel también le permite recopilar información de resumen sobre su entorno, que después puede compartir con los principales participantes.

2 Cómo funciona Sentinel

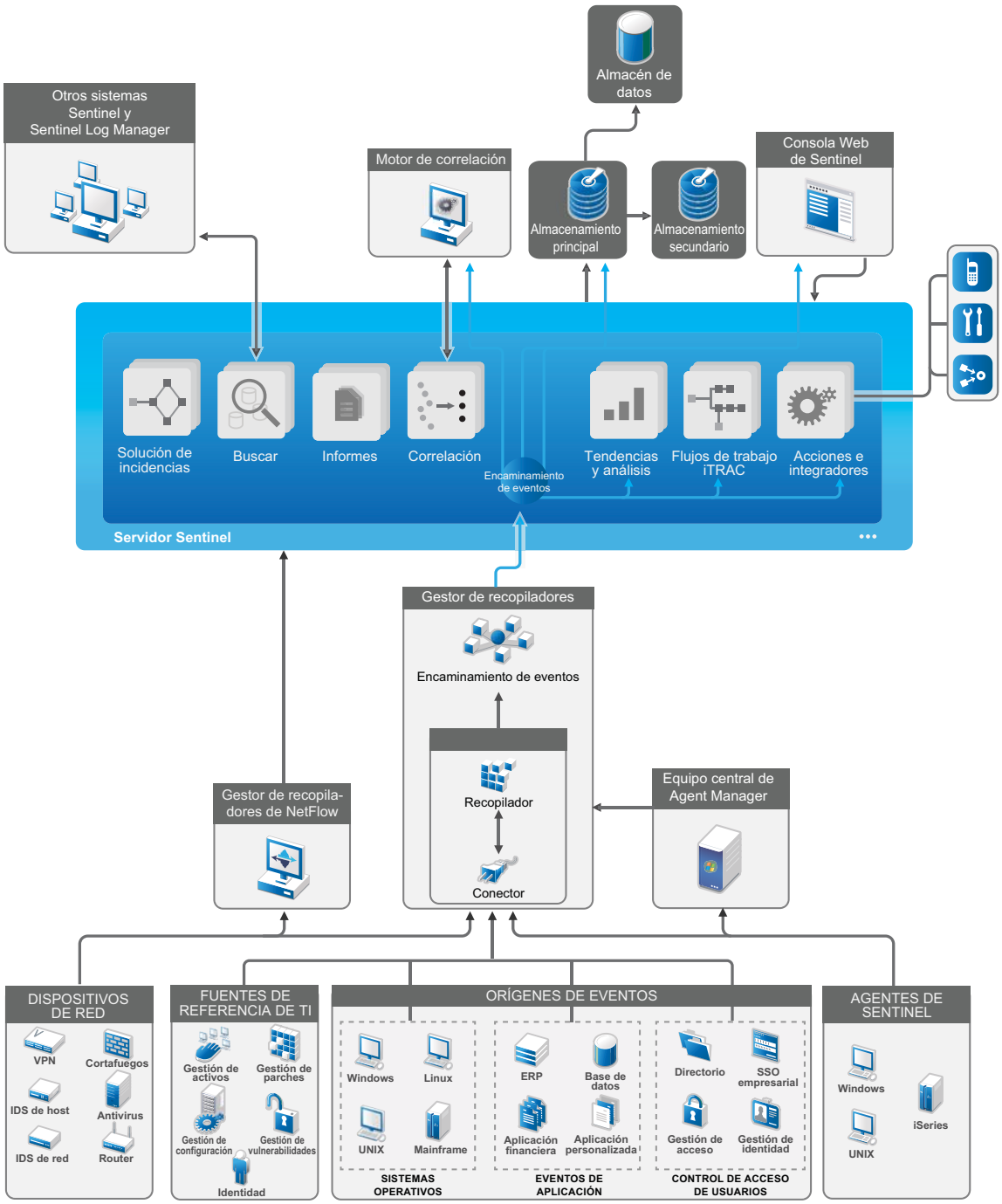
Sentinel gestiona de forma continua la información de seguridad y los eventos en todo el entorno de TI para ofrecer una solución de supervisión completa.

Sentinel hace lo siguiente:

- Reúne registros, eventos e información de seguridad de los diferentes orígenes de su entorno de TI.
- Normaliza los registros, eventos y datos de seguridad recopilados en un formato estándar de Sentinel.
- Almacena eventos en un almacén de datos basado en archivos con directivas de retención de datos personalizables.
- Recopila datos de flujo de la red y ayuda a supervisar de cerca las actividades de la red.
- Proporciona la posibilidad de vincular de forma jerárquica varios sistemas Sentinel, incluido Sentinel Log Manager.
- Le permite buscar eventos en su servidor Sentinel local y en otros servidores Sentinel distribuidos por 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 durante un período específico 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:

2.1 Orígenes de eventos

Sentinel reúne información de seguridad y eventos de diferentes orígenes de su entorno de TI. Estos orígenes se llaman orígenes de eventos. A continuación se indican los orígenes de eventos habituales en su red:

Perímetro de seguridad: Los dispositivos de seguridad —incluido el hardware y el software— utilizados para crear un perímetro de seguridad para su entorno, como cortafuegos, sistemas de detección de intrusos (IDS) y redes privadas virtuales (VPN).

Sistemas operativos: Los diferentes sistemas operativos que se ejecutan en la red.

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

Aplicaciones: Las diferentes aplicaciones instaladas en la red.

Control de acceso de usuarios: Las aplicaciones o dispositivos que permiten a los usuarios acceder a los recursos de la compañía.

Para obtener más información sobre la recopilación de orígenes de eventos, consulte la sección “Collecting and Routing Event Data” (Recopilación y encaminamiento de datos de eventos) de la *NetIQ Sentinel Administration Guide* (Guía de administración de NetIQ Sentinel).

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. Sentinel añade información de categoría (taxonomía) a los eventos, de modo que resulte más fácil comparar eventos entre sistemas que informar de los eventos por separado. Los eventos se procesan mediante visualización en tiempo real, el motor de correlación, consolas y el servidor backend.

Un evento consta de más de 200 campos; los campos de evento son de diferentes tipos y tienen distintas funciones. Existen algunos campos predefinidos, como gravedad, importancia, dirección IP de destino y puerto de destino.

Existen dos conjuntos de campos configurables:

- Campos reservados: para uso interno de Sentinel, permiten ampliar la funcionalidad en el futuro.
- Campos de cliente: los clientes pueden utilizarlos para permitir la personalización.

El origen de un campo puede ser externo o de referencia:

- El valor de un campo externo viene definido de forma explícita por el dispositivo o el recopilador correspondiente. Por ejemplo, puede definirse un campo para que sea el código de generación para la construcción que contiene el activo mencionado como la dirección IP de destino de un evento.
- El valor de un campo referencial se calcula como una función de uno o más campos utilizando el servicio de asignación. Por ejemplo, el servicio de asignación puede calcular un campo utilizando una asignación definida por el cliente mediante una dirección IP de destino desde el evento.

- Sección 2.2.1, “Servicio de asignación”, en la página 24
- Sección 2.2.2, “Asignaciones de emisión continua”, en la página 25
- Sección 2.2.3, “Detección de explotaciones”, en la página 25

2.2.1 Servicio de asignación

El servicio de asignación propaga los datos de relevancia empresarial por todo el sistema. Estos datos pueden enriquecer los eventos con información de referencia.

Puede enriquecer los datos de eventos utilizando asignaciones para añadir información adicional, como datos del host y de identidad, a los eventos entrantes de los dispositivos de origen. Sentinel puede utilizar esta información adicional para las funciones avanzadas de generación de informes y correlación. Sentinel admite varias asignaciones integradas, así como asignaciones personalizadas definidas por el usuario.

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

- Las asignaciones incorporadas se almacenan en la base de datos, se actualizan de forma interna y se exportan automáticamente al servicio de asignación.
- Las asignaciones personalizadas se almacenan como archivos CSV y se pueden actualizar en el sistema de archivos o a través de la interfaz de usuario de Configuración de los datos de la asignación. Después el servicio de asignación se ocupa de cargarlos.

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 acumulación de grandes asignaciones estáticas en la memoria dinámica. Esto es importante en un sistema de misión crítica en tiempo real como Sentinel, que requiere un traslado de datos constante, predictivo y ágil, independiente de cualquier carga transitoria en el sistema.

2.2.3 Detección de explotaciones

Sentinel ofrece la capacidad de contrastar las firmas de datos de eventos con los datos del escáner de vulnerabilidad. Sentinel notifica a los usuarios automáticamente y de forma inmediata cuando se intenta aprovechar un sistema vulnerable. Esto es posible gracias a las funciones siguientes:

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

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. Esto proporciona una referencia cruzada entre firmas de datos de eventos y datos del escáner de vulnerabilidad. Para obtener más información sobre los datos del asesor, visite “Detecting Vulnerabilities and Exploits”(Detección de vulnerabilidades y exploits) en la *NetIQ Sentinel Administration Guide* (Guía de administración de NetIQ Sentinel).

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. Entre las principales funciones del gestor de recopiladores destacan las siguientes:

- Recopilación de datos mediante conectores.
- Análisis y normalización de datos mediante recopiladores.

2.3.1 Recopiladores

Los recopiladores recogen información de los conectores y la normalizan. Realizan las funciones siguientes:

- Recibir datos en bruto de los conectores.
- Analizar y normalizar los datos:
  - Traducir los datos específicos del origen de eventos a los datos específicos de Sentinel.
  - Enriquecer los eventos cambiando el formato de la información que contienen por uno que Sentinel pueda leer.
  - Filtrar los eventos específicos del origen de eventos.
- Añadir relevancia empresarial a los eventos a través del servicio de asignación:
  - Asignar eventos a identidades.
  - Asignar eventos a activos.

- Encaminar eventos.
- Pasar los datos normalizados, analizados y formateados al gestor de recopiladores.
- Enviar mensajes de estado al servidor de Sentinel.

Para obtener más información acerca de los recopiladores, consulte el sitio Web de módulos auxiliares (plug-ins) de Sentinel.

2.3.2 Conectores

Los conectores ofrecen conexiones desde los orígenes de eventos al sistema Sentinel.

Los conectores presentan las siguientes funciones:

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

2.4 Agent Manager

Agent Manager ofrece recopilación de datos basada en host que complementa la recopilación de datos sin agentes, de modo que le permite realizar las tareas siguientes:

- Acceder a registros que no están disponibles a través de 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 y gestionar su configuración, y además actúa 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 Gestor de recopiladores de NetFlow

El gestor de recopiladores de NetFlow recopila datos de flujo de la red (NetFlow, IPFIX, etc.) de dispositivos de red como routers, switches y cortafuegos. Los datos de flujo de la red describen información básica acerca de las conexiones de red entre hosts, incluidos los paquetes y bytes transmitidos. Esto le ayuda a visualizar el comportamiento de hosts individuales o de toda la red.

El gestor de recopiladores de NetFlow realiza las funciones siguientes:

- Recopila datos de flujo de la red en bytes, flujos y paquetes de los dispositivos de red compatibles.
- Agrega y envía los datos recopilados al servidor Sentinel para visualizar y analizar las actividades de la red en su entorno.

Para obtener más información sobre la visualización y análisis de los datos de flujo de la red, consulte “Visualizing and Analyzing Network Flow Data” (Visualización y análisis de los datos de flujo de la red) en la *NetIQ Sentinel User Guide* (Guía del usuario de NetIQ Sentinel).

2.6 Encaminamiento y almacenamiento de datos de Sentinel

Sentinel proporciona numerosas opciones de encaminamiento, almacenamiento y extracción de los datos recopilados. Por defecto, Sentinel recibe los datos de eventos analizados y los datos en bruto que envían los gestores de recopiladores. Sentinel almacena los datos en bruto en particiones protegidas para ofrecer una cadena de evidencia segura, y encamina los datos de eventos analizados de conformidad con las reglas que defina. Puede filtrar los datos de eventos analizados, enviarlos para su almacenamiento o análisis en tiempo real, y encaminarlos a sistemas externos. Sentinel correlaciona todos los datos de eventos que se envían para su almacenamiento con directivas de retención definidas por el usuario que determinan la partición en la que se almacenan los datos, y define la directiva de depuración que utiliza Sentinel para retener los datos de eventos y posteriormente eliminarlos.

La estructura del almacenamiento de datos de Sentinel se compone de tres niveles:

Almacenamiento en línea	Almacenamiento principal, antes llamado almacenamiento local.	Optimizado para escribir y recuperar datos de forma rápida. Almacena los datos de eventos recopilados más recientemente y los datos de eventos buscados con más frecuencia.
	Almacenamiento secundario, antes llamado almacenamiento en red. (optional)	Está optimizado para reducir el uso del espacio en un almacenamiento menos costoso, que aún permite una rápida recuperación. Sentinel migra de forma automática las particiones de datos al almacenamiento secundario.
	Nota: El uso del 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	Almacenamiento de archivado	Cuando las particiones están cerradas, se puede hacer una copia de seguridad de la partición en cualquier servicio de almacenamiento de archivos, como Amazon Glacier. Puede volver a importar las particiones de forma temporal para llevar a cabo análisis forenses a largo plazo siempre que sea necesario.

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 más información, consulte la sección “Configuring Data Synchronization” (Cómo configurar la sincronización de datos) de la *NetIQ Sentinel Administration Guide* (Guía de administración de NetIQ Sentinel).

2.7 Correlación

Un solo evento puede parecer trivial, pero combinado con otros eventos puede indicar un problema potencial. Sentinel le ayuda a correlacionar dichos eventos utilizando las reglas que creó y desplegó en el motor de correlación, y a tomar las medidas oportunas para mitigar 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 obtener más información acerca de la correlación, consulte la sección “Correlating Event Data” (Correlación de datos de eventos) de la *NetIQ Sentinel User Guide* (Guía del usuario de NetIQ Sentinel).

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 cumple 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 User Guide* (Guía del usuario de NetIQ Sentinel).

2.8 Inteligencia de seguridad

La capacidad de correlación de Sentinel le permite buscar patrones de actividad conocidos, que puede analizar por cuestiones de seguridad, conformidad o cualquier otro motivo. 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 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 User Guide (Guía del usuario de NetIQ Sentinel)*.

2.9 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 e infracciones de directivas. Además ofrece integración bidireccional con los sistemas de tickets de 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 User Guide (Guía del usuario de NetIQ Sentinel)*.

2.10 Flujos de trabajo de iTRAC

Los flujos de trabajo de iTRAC ofrecen una solución sencilla y flexible para automatizar y seguir los procesos de respuesta a incidencias de una empresa. iTRAC aprovecha el sistema de incidencias interno de Sentinel para hacer un seguimiento de los problemas de seguridad o del sistemas desde la identificación (mediante reglas de correlación o identificación manual) hasta la resolución.

Puede crea flujos de trabajo mediante pasos manuales o automatizados. Los flujos de trabajo de iTRAC admiten funciones avanzadas como la ramificación, la derivación basada en tiempo y las variables locales. La integración con guiones externos y módulos auxiliares (plug-ins) permite una 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 User Guide (Guía del usuario de NetIQ Sentinel)*.

2.11 Acciones e integradores

Las acciones ejecutan algún tipo de acción de forma manual o automática, como enviar mensajes de correo electrónico. Puede activar las acciones por medio de reglas de encaminamiento, la ejecución manual de una operación de evento o incidencia y 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 Administration Guide* (Guía de administración de NetIQ Sentinel).

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 Administration Guide* (Guía de administración de NetIQ Sentinel).

2.12 Búsqueda

Sentinel ofrece una opción para realizar búsquedas en los eventos. Puede buscar datos en el almacenamiento principal o en el almacenamiento secundario. Con la configuración necesaria, también puede buscar eventos del sistema generados por Sentinel y ver los datos en bruto de cada evento. Para más información, consulte "Performing a Search" (Cómo realizar una búsqueda) en la *NetIQ Sentinel User Guide (Guía del usuario de NetIQ Sentinel)*.

Además, puede buscar servidores Sentinel distribuidos en diversas ubicaciones geográficas. Para más información, consulte "Configuring Data Federation" (Cómo configurar la federación de datos) en la *NetIQ Sentinel Administration Guide* (Guía de administración de NetIQ Sentinel).

2.13 Informes

Sentinel le permite ejecutar informes sobre los datos recopilados. Sentinel se suministra con una variedad de informes personalizables. Algunos informes son configurables, de modo que puede especificar las columnas que se mostrarán en los resultados.

Puede ejecutar, programar y enviar por correo electrónico informes en formato PDF. También puede ejecutar informes como búsquedas y después trabajar con los resultados para, por ejemplo, perfeccionar la búsqueda o 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 User Guide (Guía de usuario de NetIQ Sentinel)*.

2.14 Seguimiento de identidad

Sentinel proporciona un marco de integración para que los sistemas de gestión de identidades puedan realizar un seguimiento de las identidades de cada cuenta de usuario y de los eventos que realiza cada una de esas identidades. Sentinel proporciona información del usuario, como información de contacto, cuentas de usuario, eventos de autenticación recientes, eventos de acceso recientes, cambios en los permisos, etc. Al mostrar información acerca de los usuarios que inician una acción específica o los usuarios que se ven afectados por una acción, Sentinel mejora el tiempo

de respuesta a incidencias y permite el análisis basado en el comportamiento. Para obtener más información, consulte “Leveraging Identity Information”(Cómo aprovechar la información de identidad) en la *NetIQ Sentinel User Guide (Guía del usuario de NetIQ Sentinel)*.

2.15 Análisis de eventos

Sentinel proporciona un potente conjunto de herramientas que le ayudan a buscar y analizar con facilidad datos de eventos fundamentales. Sentinel optimiza el sistema para conseguir la máxima eficiencia en cualquier tipo de análisis, y proporciona métodos para realizar la transición de un tipo de análisis a otro fácilmente y sin problemas.

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 rápido de las tendencias de los eventos y los datos de eventos, así como para la identificación de eventos específicos. Con el tiempo, puede crear filtros mejorados para clases de datos específicas, como resultados de correlación. Puede usar Vistas activas como consola para ver una posición operativa y de seguridad general.

Luego puede usar la búsqueda interactiva para realizar un análisis 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 concentrarse rápidamente en eventos de interés específicos.

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 al permitirle transferir las búsquedas interactivas acumuladas en la interfaz de búsqueda a una plantilla de informe. Al hacerlo se crea inmediatamente un informe que muestra los mismos datos en un formato más adecuado para un mayor número de eventos.

Sentinel incluye muchas plantillas de informe para este fin. Existen dos tipos de plantillas de informe:

- Plantillas optimizadas para mostrar determinados tipos de información, como datos de autenticación o los usuarios creados.
- Plantillas generales que le permiten personalizar grupos y columnas del informe de manera interactiva.

Con el tiempo, desarrollará filtros de uso común e informes que facilitan el flujo de trabajo. Sentinel le permite almacenar esta información y distribuirla a personas de su organización. Para obtener más información, consulte la *NetIQ Sentinel User Guide* (Guía del usuario de NetIQ Sentinel).

II Planificación de su instalación de Sentinel

En los capítulos siguientes se indica cómo planificar la instalación de Sentinel. Si desea instalar una configuración no contemplada en los capítulos siguientes o tiene alguna pregunta, póngase en contacto con el servicio de Asistencia técnica de NetIQ.

3 Lista de verificación de implementación

Utilice la lista de verificación siguiente para planificar, instalar y configurar Sentinel.

Si realiza la actualización desde una versión anterior de Sentinel, no utilice esta lista. Para obtener información sobre la actualización, consulte la Parte V, “Actualización de Sentinel”, en la página 123.

❒	Tareas	Consulte
❒	Revise la información sobre la arquitectura del producto para conocer los componentes de Sentinel.	Parte I, “Conocer Sentinel”, en la página 15.
❒	Revise la información sobre licencias de Sentinel a fin de determinar si necesita usar la licencia de evaluación o la licencia empresarial de Sentinel.	Capítulo 4, “Información sobre licencias”, en la página 35.
❒	Evalúe su entorno para determinar la configuración de hardware. Asegúrese de que los equipos en los que instale Sentinel y sus componentes cumplan los requisitos especificados.	Capítulo 5, “Cumplimiento de los requisitos del sistema”, en la página 39.
❒	Determine el tipo de implantación adecuado para su entorno en función de los eventos por segundo (EPS) del gestor de recopiladores y el motor de correlación, así como de los registros por segundo (RPS) del gestor de recopiladores de NetFlow. Determine el número de gestores de recopiladores, motores de correlación y gestores de recopiladores de NetFlow que necesita instalar para mejorar el rendimiento y el equilibrio de carga.	Sección 6.1, “Ventajas de las implantaciones distribuidas”, en la página 41.
❒	Revise las notas de la versión más recientes de Sentinel para entender la nueva funcionalidad y los problemas conocidos.	Notas de la versión de Sentinel
❒	Instale Sentinel.	Parte III, “Instalación de Sentinel”, en la página 65.
❒	Configure la hora en el servidor Sentinel.	Capítulo 17, “Configuración de la hora”, en la página 99.
❒	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 19, “Configuración de módulos auxiliares (plug-ins) genéricos”, en la página 107.

❒	Tareas	Consulte
❒	Sentinel incluye reglas de correlación listas para usar. Algunas reglas de correlación están configuradas por defecto para ejecutar una acción que envía un correo electrónico cuando se activa la regla. Es el caso, por ejemplo, de la acción Notificar al administrador de seguridad. Por tanto, debe configurar los ajustes del servidor de correo en el servidor Sentinel mediante el integrador SMTP y la acción Enviar correo electrónico.	Encontrará la documentación sobre el integrador SMTP y la acción Enviar correo electrónico en el sitio Web de módulos auxiliares (plug-ins) de Sentinel.
❒	Instale recopiladores y conectores adicionales en su entorno según sea necesario.	Capítulo 15, “Instalación de conectores y recopiladores adicionales”, en la página 93.
❒	Instale gestores de recopiladores y motores de correlación adicionales en su entorno según sea necesario.	Parte III, “Instalación de Sentinel”, en la página 65.

4 Información sobre licencias

Sentinel abarca un amplio espectro de funciones, por lo que cubre diferentes necesidades de muchos de sus clientes. Puede elegir un modelo de licencia acorde con sus necesidades.

La plataforma Sentinel ofrece estos dos modelos de licencia:

- **Sentinel Enterprise:** una solución con toda la gama de funciones que habilita todas las funciones principales de análisis visual en tiempo real y muchas funciones adicionales. Sentinel Enterprise se centra en los casos de uso de SIEM, como la detección de amenazas en tiempo real, las alertas y la corrección.
- **Sentinel for Log Management:** solución para casos de uso de gestión de registros, como las capacidades de recopilación, almacenamiento, búsqueda y notificación de datos.

  Sentinel for Log Management representa una actualización importante con respecto a las funciones incluidas en Sentinel Log Manager 1.2.2, y en algunos casos, se han modificado partes sustanciales de la arquitectura. Para planificar su actualización a Sentinel para la gestión de registros, consulte la página de preguntas frecuentes de Sentinel.

Según la solución y los productos complementarios que compre, NetIQ le proporciona las claves de licencia y los derechos adecuados para un funcionamiento correcto en Sentinel. A pesar de que las claves de licencia y los derechos rigen el acceso básico a las funciones y descargas del producto, debe consultar los términos y condiciones adicionales disponibles en el acuerdo de licencia y el acuerdo de licencia de usuario final.

En la tabla siguiente se esbozan los servicios y funciones específicos habilitados en cada una de las soluciones:

Tabla 4-1 *Servicios y funciones de Sentinel*

Servicios y funciones	Sentinel Enterprise	Sentinel for Log Management
Funciones principales	Sí	Sí
◆ Recopilación de eventos básica ◆ Recopilación de datos no relacionados con eventos (activos, vulnerabilidades, identidades) ◆ Análisis y normalización ◆ Clasificación taxonómica de datos de eventos ◆ Asignación contextual en línea ◆ Recopilación y almacenamiento de NetFlow ◆ Visualización de NetFlow en tiempo real ◆ Visualización de NetFlow basada en eventos ◆ Búsqueda de eventos (local) ◆ Generación de informes de eventos ◆ Filtrado de eventos ◆ Visualización de eventos en tiempo real ◆ Almacenamiento de eventos ◆ Directivas de retención de datos ◆ Sin rechazo de almacenamiento de eventos ◆ Preparación de la publicación 140-2 de los estándares federales de procesamiento de la información (FIPS 140-2) ◆ Acciones activadas manualmente ◆ Creación y gestión manual de incidencias ◆ Acciones y flujos de trabajo de incidencias ◆ Flujos de tareas iTRAC		
Acciones	Sí	Sí
◆ Acciones activadas por correlación (solo si está habilitada la correlación) ◆ Acciones activadas por reglas de encaminamiento (solo si están habilitadas las reglas) ◆ Acciones activadas manualmente		
Reglas de encaminamiento	Sí	Sí
◆ Encaminamiento de eventos (externo) ◆ Acciones activadas por reglas de encaminamiento (solo si están activadas las acciones)		
Sentinel Link	Sí	Sí

Servicios y funciones	Sentinel Enterprise	Sentinel for Log Management
Correlación ◆ Correlación de patrones en tiempo real ◆ Acciones activadas por reglas de correlación (solo si están habilitadas las acciones) ◆ Clasificación de alertas ◆ Consolas de alertas	Sí	No
Sincronización de datos	Sí	Sí
Restauración de datos de eventos desde el archivo de reserva	Sí	Sí
Federación de datos (búsqueda distribuida)	Sí	Sí
Detección de exploits (asesor)	Sí	Sí
Inteligencia de seguridad ◆ Reglas de anomalía ◆ Análisis estadístico en tiempo real	Sí	No

4.1 Licencias de Sentinel

En esta sección se proporciona información sobre los tipos de licencias de Sentinel.

- Sección 4.1.1, “Licencia de evaluación”, en la página 37
- Sección 4.1.2, “Licencia gratuita”, en la página 38
- Sección 4.1.3, “Licencias empresariales”, en la página 38

4.1.1 Licencia de evaluación

La licencia de evaluación por defecto permite usar todas las funciones de Sentinel Enterprise durante un período de evaluación específico con un número ilimitado de EPS en función de la capacidad del hardware. Para obtener información sobre las funciones disponibles en Sentinel Enterprise, consulte la Tabla 4-1, “Servicios y funciones de Sentinel”, en la página 36.

La fecha de caducidad del sistema se basa en los datos más antiguos del sistema. Si restaura eventos antiguos en su sistema, Sentinel actualizará la fecha de caducidad en consonancia.

Cuando caduca la licencia de evaluación, el sistema ejecuta una licencia gratuita básica que habilita un conjunto de funciones limitado y un número de eventos limitado de 25 EPS.

Después de actualizar a una licencia empresarial, Sentinel restaurará todas las funciones. Para prevenir cualquier interrupción de la funcionalidad, debe actualizar el sistema a una licencia empresarial antes de que caduque la licencia de evaluación.

4.1.2 Licencia gratuita

La licencia gratuita permite usar un conjunto limitado de funciones con un número de eventos limitado de 25 EPS.

La licencia gratuita permite recopilar y almacenar eventos. Cuando el número de eventos supere los 25, Sentinel almacenará los eventos recibidos, pero no visualizará la información de dichos eventos en los resultados de búsqueda ni en los informes. Sentinel asigna a estos eventos la etiqueta `OverEPSLimit`.

La licencia gratuita no proporciona funciones en tiempo real. Puede restaurar toda la funcionalidad actualizando la licencia a una de tipo empresarial.

Nota: NetIQ no proporciona asistencia técnica ni actualizaciones de producto para la versión gratuita de Sentinel.

4.1.3 Licencias empresariales

Al adquirir Sentinel, recibe una clave de licencia a través del portal para clientes. Según la licencia que adquiera, la clave de licencia habilitará 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.

Puede añadir la clave de licencia empresarial durante la instalación o en cualquier momento posterior. Para añadir la clave de licencia, consulte la sección “Adding a License Key” (Cómo añadir una clave de licencia) en la *NetIQ Sentinel Administration Guide* (Guía de administración de NetIQ Sentinel).

5 Cumplimiento de los requisitos del sistema

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

Para obtener información sobre el hardware recomendado, sistemas operativos, plataformas de dispositivos y navegadores compatibles, consulte el sitio Web de información técnica de NetIQ Sentinel.

5.1 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 el sitio Web de módulos auxiliares (plug-ins) de Sentinel.

5.2 Entorno virtual

Sentinel es compatible con los servidores VMware ESX. Al configurar un entorno virtual, las máquinas virtuales deben tener dos o más CPU. Para obtener resultados de rendimiento equivalentes 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 los equipos físicos recomendados, consulte el sitio Web de información técnica de NetIQ Sentinel.

6 Consideraciones de implantación

Sentinel tiene una arquitectura adaptable que se puede ampliar para manejar la carga que necesite almacenar en él. En este capítulo se ofrece una descripción general de las consideraciones más importantes a la hora de escalar una implantación de Sentinel. Un profesional de Asistencia técnica de NetIQ o de los servicios para socios de NetIQ puede ayudarle a diseñar un sistema Sentinel adecuado para su entorno de TI.

6.1 Ventajas de las implantaciones distribuidas

De manera predeterminada, el servidor Sentinel incluye los siguientes componentes:

- **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.
- **Gestor de recopiladores de NetFlow:** El gestor de recopiladores de NetFlow recopila datos de flujo de la red (NetFlow, IPFIX, etc.) de dispositivos de red como routers, switches y cortafuegos. Los datos de flujo de la red describen información básica sobre todas las conexiones de red entre hosts, como los paquetes y bytes transmitidos, lo que le ayuda a visualizar el comportamiento de hosts individuales o de toda la red.

Importante: En los entornos de producción, NetIQ recomienda configurar una implantación distribuida porque aísla los componentes de recopilación de datos en un equipo aparte, lo que es importante para manejar aumentos repentinos de procesamiento y otras anomalías con la máxima estabilidad para el sistema.

En esta sección se describen las ventajas de las implantaciones distribuidas.

6.1.1 Ventajas de los gestores de recopiladores adicionales

El servidor Sentinel incluye por defecto un gestor de recopiladores. No obstante, para los entornos de producción, los gestores de recopiladores proporcionan un mejor aislamiento cuando se reciben grandes volúmenes de datos. En esta situación, un gestor de recopiladores distribuido podría verse sobrecargado, pero el servidor Sentinel seguirá respondiendo a las peticiones del usuario.

La instalación de más de un gestor de recopiladores en una red distribuida aporta las siguientes 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.

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 la Parte III, “Instalación de Sentinel”, en la página 65.

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.

6.1.2 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. En los entornos que tienen muchas 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 la Parte III, “Instalación de Sentinel”, en la página 65 .

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.

6.1.3 Ventajas de los gestores de recopiladores de NetFlow adicionales

El gestor de recopiladores de NetFlow recopila datos de flujo de la red de los dispositivos de red. Debe instalar más gestores de recopiladores de NetFlow en vez de usar el gestor de recopiladores de NetFlow del servidor Sentinel a fin de liberar recursos del sistema para funciones importantes como el almacenamiento de eventos y las búsquedas.

Puede instalar más gestores de recopiladores de NetFlow en las siguientes situaciones:

- En los entornos con numerosos dispositivos de red y tasas elevadas de datos de flujo, puede instalar varios gestores de recopiladores de NetFlow para distribuir la carga.
- Si se encuentra en un entorno de múltiples arrendatarios, debe instalar un gestor de recopiladores de NetFlow individual para cada arrendatario a fin de recopilar datos de flujo de la red por arrendatario.

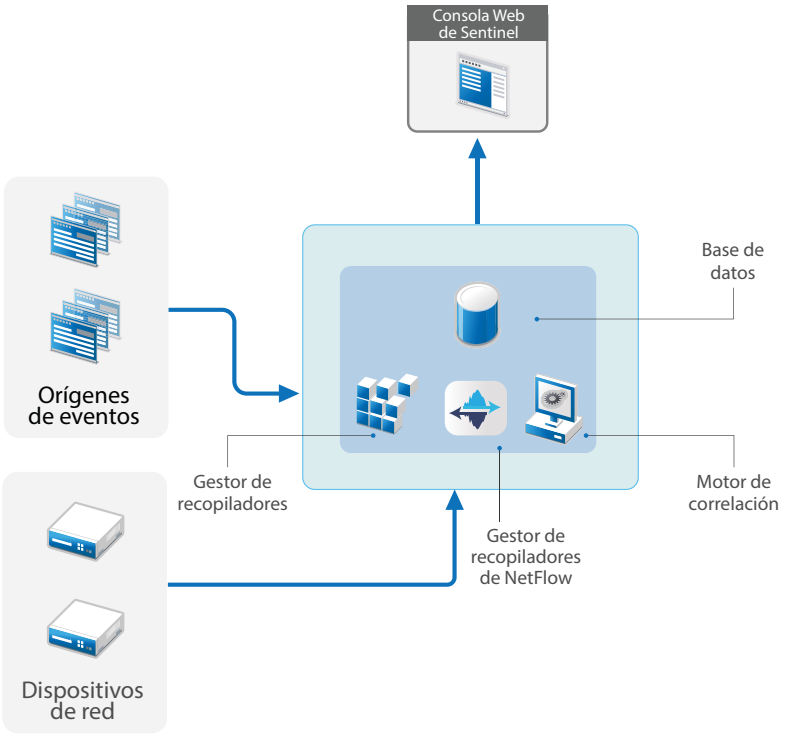
Para obtener más información sobre la instalación de gestores de recopiladores de NetFlow adicionales, consulte el Capítulo 14, “Instalación del gestor de recopiladores de NetFlow”, en la página 91.

6.2 Implantación "todo en uno"

La opción de implantación más básica es un sistema "todo en uno" que incluye todos los componentes en un solo equipo. Una implantación "todo en uno" solo es adecuada si la carga del sistema es pequeña y no es necesario supervisar los equipos Windows. En muchos entornos, las cargas fluctuantes e imprevisibles, así como los conflictos de recursos entre componentes pueden causar problemas de rendimiento.

Importante: Para los entornos de producción, NetIQ recomienda configurar una implantación distribuida porque aísla los componentes de recopilación de datos en un equipo aparte, lo que es importante para manejar aumentos repentinos y otras anomalías con la máxima estabilidad para el sistema.

Figura 6-1 *Implantación "todo en uno"*

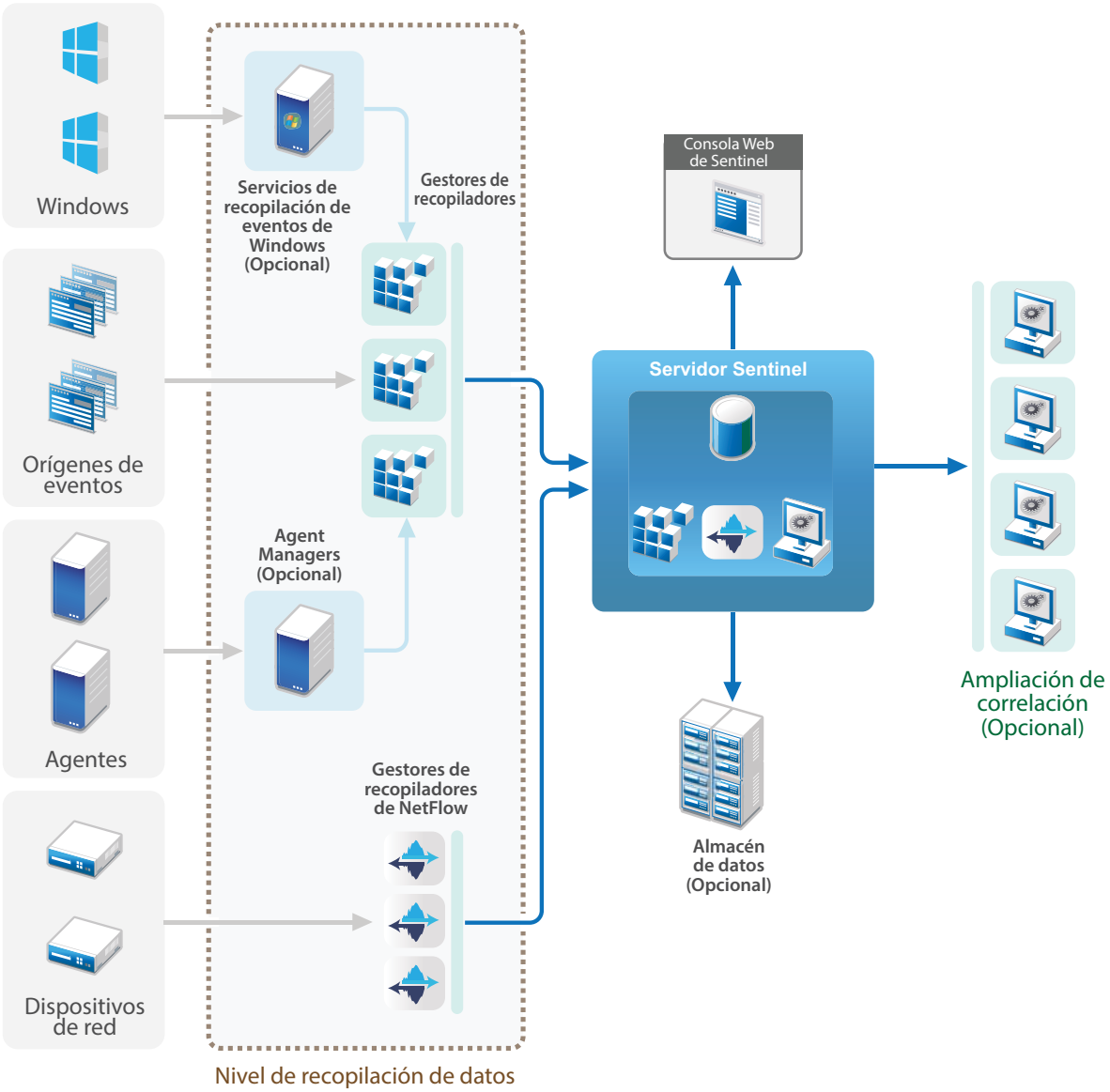


6.3 Implantación distribuida de un nivel

La implantación de un nivel añade la capacidad de supervisar equipos Windows y de manejar una carga mayor que la de la implantación "todo en uno". Puede aumentar la correlación y recopilación de datos añadiendo equipos del gestor de recopiladores, el gestor de recopiladores de NetFlow y el motor de correlación que liberen al servidor Sentinel central de carga de procesamiento. Además de manejar la carga de eventos, las reglas de correlación y los datos de flujo de la red, los gestores de recopiladores remotos, los motores de correlación y los gestores de recopiladores de NetFlow liberan recursos en el servidor central de Sentinel para atender otras peticiones, como almacenamiento y búsqueda de eventos. A medida que aumente la carga del sistema, el servidor central de Sentinel formará un cuello de botella y se necesitará una implantación con más niveles para aumentar más la escala.

Opcionalmente, puede configurar Sentinel para copiar datos de eventos en un almacén de datos, que puede resultar útil para descargar informes personalizados, análisis y otras tareas de procesamiento a otro sistema.

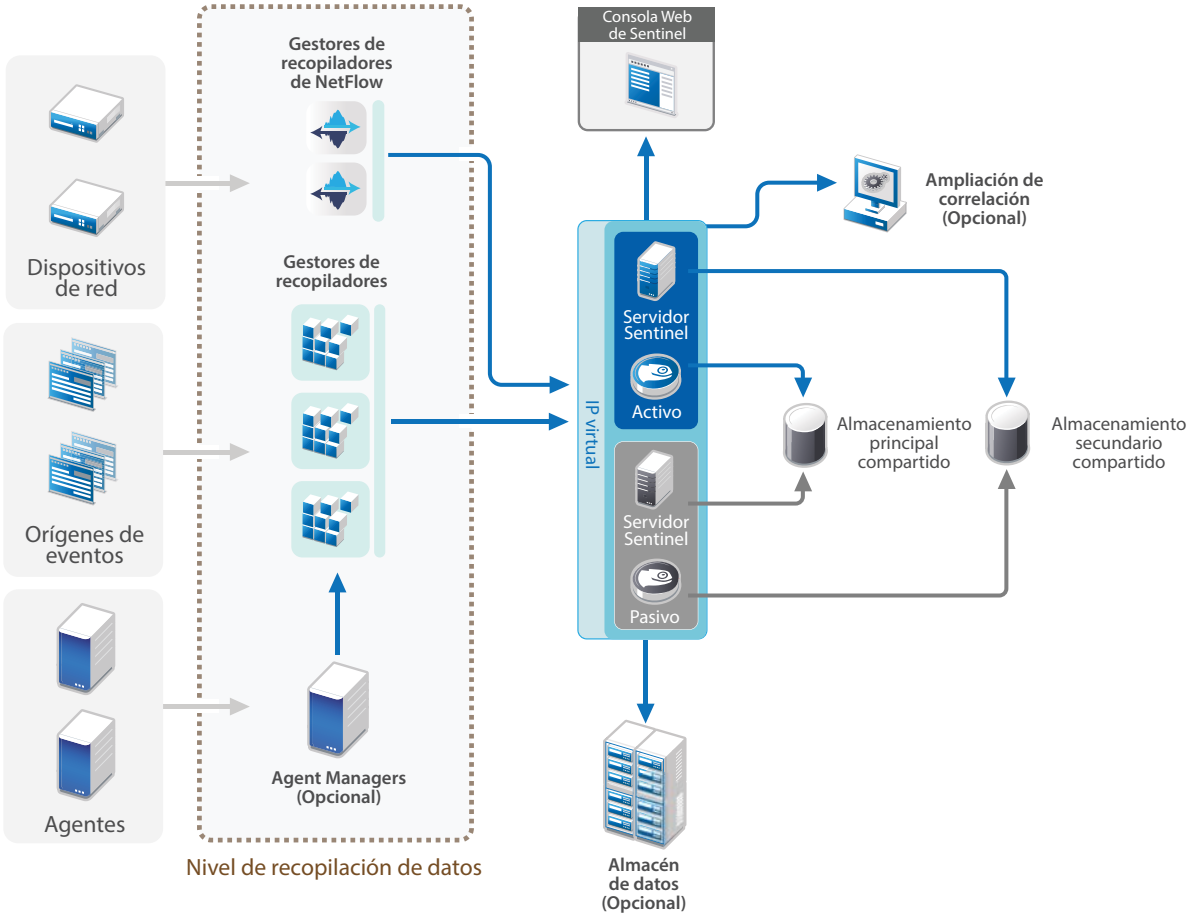
Figura 6-2 *Implantación distribuida de un nivel*



6.4 Implantación distribuida de un nivel con alta disponibilidad

La implantación distribuida de un nivel muestra cómo puede convertirse en un sistema de alta disponibilidad con redundancia de failover. Para obtener más información sobre la implementación de Sentinel con alta disponibilidad, consulte el Parte VI, “Implantación de Sentinel para alta disponibilidad”, en la página 145.

Figura 6-3 *Implantación distribuida de un nivel con alta disponibilidad*

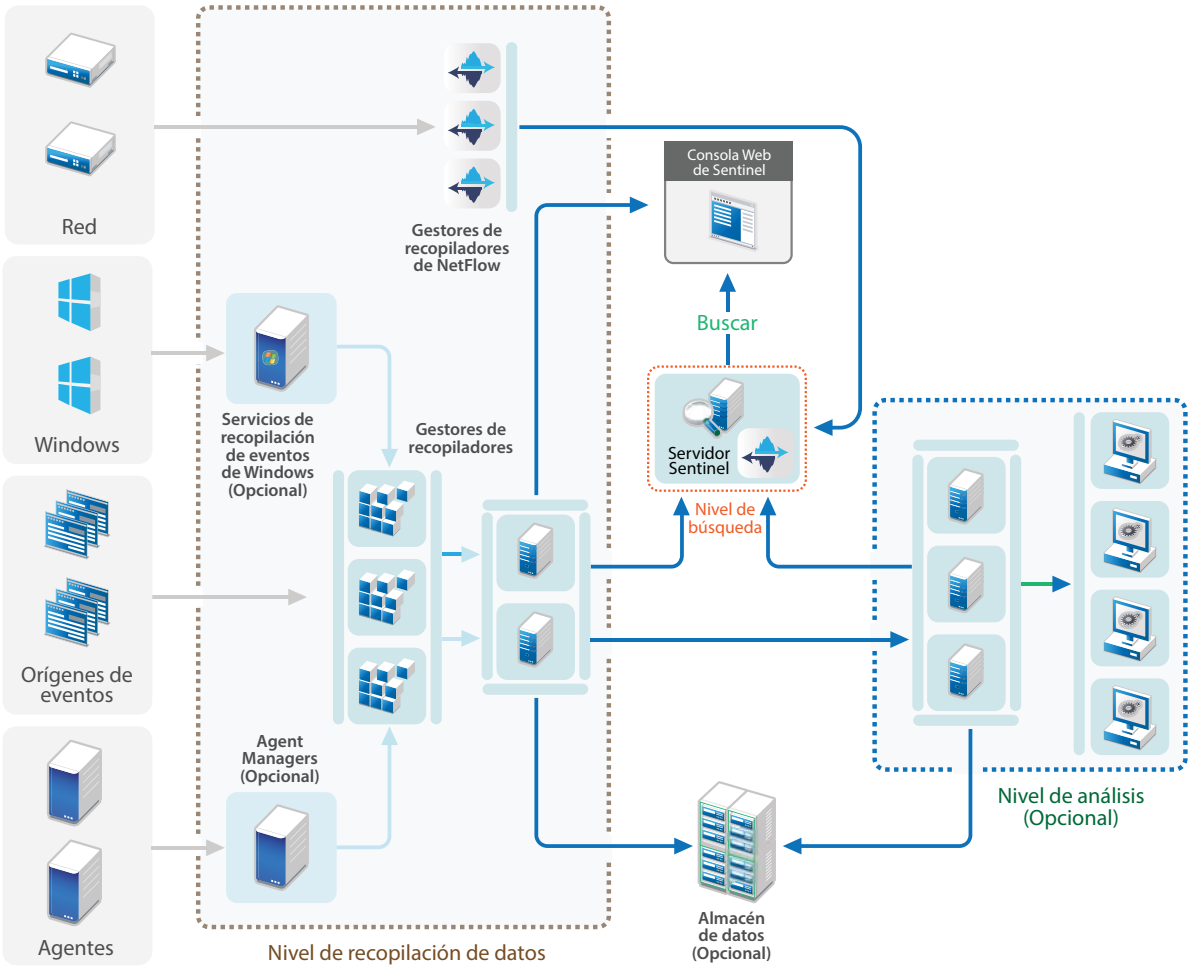


6.5 Implantación distribuida de dos y tres niveles

Estas implantaciones permiten superar las capacidades de manejo de carga de un solo servidor Sentinel central y compartir la carga de procesamiento entre varias instancias de Sentinel al aprovechar Sentinel Link y las funciones de federación de datos de Sentinel. La recopilación de datos se realiza con equilibrio de carga entre varios servidores Sentinel, cada uno de los cuales tiene varios gestores de recopiladores, tal como se muestra en el nivel de recopilación de datos. Si quiere llevar a cabo una correlación de eventos o inteligencia de seguridad, tiene la opción de reenviar datos al Nivel de análisis a través de Sentinel Link. El Nivel de búsqueda proporciona un único punto de acceso práctico para realizar búsquedas en todos los sistemas de todos los demás niveles por medio de la federación de datos de Sentinel. Dado que la petición de búsqueda está federada en varias instancias de Sentinel, esta implementación también tiene propiedades de equilibrio de carga de búsqueda útiles a la hora de escalar y poder manejar una carga de búsqueda intensa.

Los datos de flujo de la red se almacenan en el Nivel de búsqueda para habilitar la navegación fácil a partir de los resultados de búsqueda para el análisis contextual del tráfico de la red.

Figura 6-4 *Implantación distribuida de dos y tres niveles*



6.6 Planificación de particiones para el almacenamiento de datos

Al instalar Sentinel, debe montar la partición del disco para almacenamiento principal en la ubicación en la que se instalará 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 correctos. 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 Sección 6.6.4, “Estructura de directorios de Sentinel”, en la página 49.

Una práctica óptima consiste en asegurarse de que este directorio de datos esté ubicado 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 de los conjuntos de archivos, 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 este artículo sobre la creación de particiones de disco.

Nota: Los sistemas de archivos de ext3 tienen un límite para el almacenamiento de archivos, lo cual impide que un directorio tenga más de 32000 archivos o subdirectorios. NetIQ le recomienda utilizar el sistema de archivos XFS si prevé tener un gran número de directivas de retención o si va a retener los datos durante períodos de tiempo más largos (un año, por ejemplo).

6.6.1 Uso de particiones en instalaciones tradicionales

En las 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 que se describe en la Sección 6.6.4, “Estructura de directorios de Sentinel”, en la página 49. 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`.

6.6.2 Uso de particiones en una instalación de dispositivo

Si utiliza el formato de dispositivo ISO DVD, puede configurar la partición del sistema de archivos del dispositivo durante la instalación siguiendo las instrucciones que se muestran en las pantallas de YaST. 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 13.3.2, “Creación de particiones”, en la página 86.

6.6.3 Mejores prácticas para la disposición de particiones

Muchas organizaciones tienen sus propios esquemas documentados de prácticas óptimas de disposición de particiones para cualquier sistema instalado. La siguiente propuesta de partición tiene como fin orientar a las organizaciones sin directivas definidas y tiene en cuenta el uso específico del sistema de archivos de Sentinel. Por lo general, Sentinel cumple el Estándar de jerarquía del sistema de archivos cuando resulta viable.

Partición	Punto de montaje	Tamaño	Notas
Root	/	100 GB	Contiene archivos del sistema operativo y binarios/configuración de Sentinel.
Boot	/boot	150 MB	Partición de arranque

Partición	Punto de montaje	Tamaño	Notas
Temp	`/tmp`	30 GB	Ubicación de los archivos del SO y los archivos temporales de Sentinel; aislar estos en una partición aparte protege los datos de la aplicación para que no se dañen si un proceso en bucle permanente llena todo el espacio temporal.
Almacenamiento principal	`/var/opt/novell/sentinel`	Calcular utilizando la Información sobre tamaño del sistema.	Esta sección incluirá los datos principales recopilados por Sentinel y otros datos variables, como archivos de registro. Esta partición puede compartirse con otros sistemas.
Almacenamiento secundario	Ubicación basada en el tipo de almacenamiento, NFS, CIFS o SAN.	Calcular utilizando la Información sobre tamaño del sistema.	Área de almacenamiento secundario, que puede montarse a nivel local tal como se indica o de forma remota.
Almacenamiento de archivado	Sistema remoto	Calcular utilizando la Información sobre tamaño del sistema.	Este almacenamiento es para datos archivados.

6.6.4 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 almacenan en el directorio `/opt/novell/sentinel`..
- Los archivos de registro se encuentran en el directorio `/var/opt/novell/log`.
- Los archivos de configuración se encuentran en el directorio `/etc/opt/novell/sentinel`.
- El archivo de ID del 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.

7 Consideraciones sobre implantación para el modo FIPS 140-2

Sentinel también se puede configurar 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.

La habilitación del 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 Web de Sentinel, el Centro de control de Sentinel y el servicio Asesor de Sentinel para usar cifrado validado FIPS 140-2.

7.1 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 6.3 está validado para FIPS 140-2. El módulo de cifrado NSS proporcionado por SLES 11 SP3 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*.

7.1.1 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.

7.1.2 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.

7.2 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
  - Check Point (LEA) 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 114.

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 información sobre cómo usar estos conectores con Sentinel en el modo FIPS 140-2, consulte la sección “Uso de conectores no habilitados para FIPS con Sentinel en el modo FIPS 140-2” en la página 119.

- 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 han actualizado esté disponible con compatibilidad para FIPS, envíe una solicitud mediante Bugzilla.

7.3 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 implantación.	Sección 7.4, “Entornos de implantación”, en la página 54.
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 12.2.2, “Instalación personalizada del servidor Sentinel”, en la página 73. Sección 12.3, “Instalación silenciosa”, en la página 77 Capítulo 20, “Habilitar el modo FIPS 140-2 en una instalación de Sentinel existente”, en la página 109
Configure los módulos auxiliares (plug-ins) de Sentinel para ejecutarse en modo FIPS 140-2.	Sección 21.5, “Configuración de módulos auxiliares (plug-ins) de Sentinel para la ejecución en modo FIPS 140-2”, en la página 114.
Importe certificados en el Almacén de claves de FIPS de Sentinel.	Sección 21.6, “Importación de certificados en la base de datos del almacén de claves de FIPS”, en la página 120

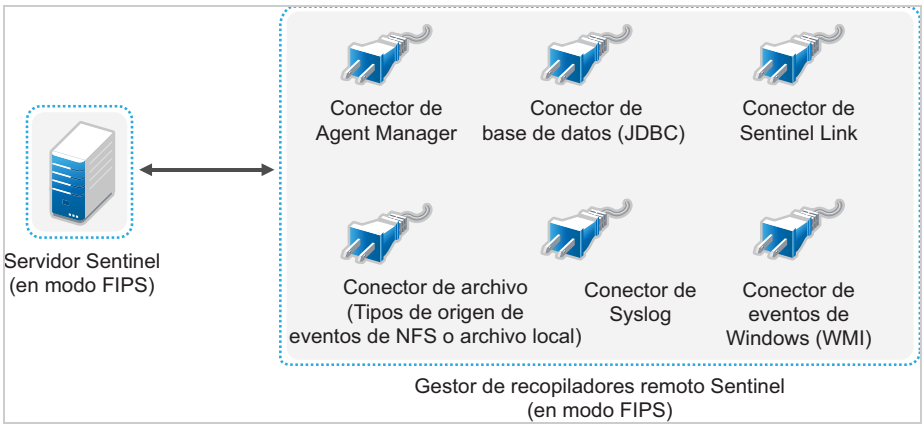
Nota: NetIQ recomienda encarecidamente realizar una copia de seguridad de sus sistemas Sentinel antes de iniciar la conversión al modo FIPS. Si más adelante es necesario revertir el servidor al modo diferente de FIPS, el único método admitido consiste en restaurarlo desde una copia de seguridad. Para obtener más información sobre cómo revertir a un modo diferente de FIPS, consulte “Reversión de Sentinel al modo diferente de FIPS” en la página 120.

7.4 Entornos de implantación

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

7.4.1 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 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 109.

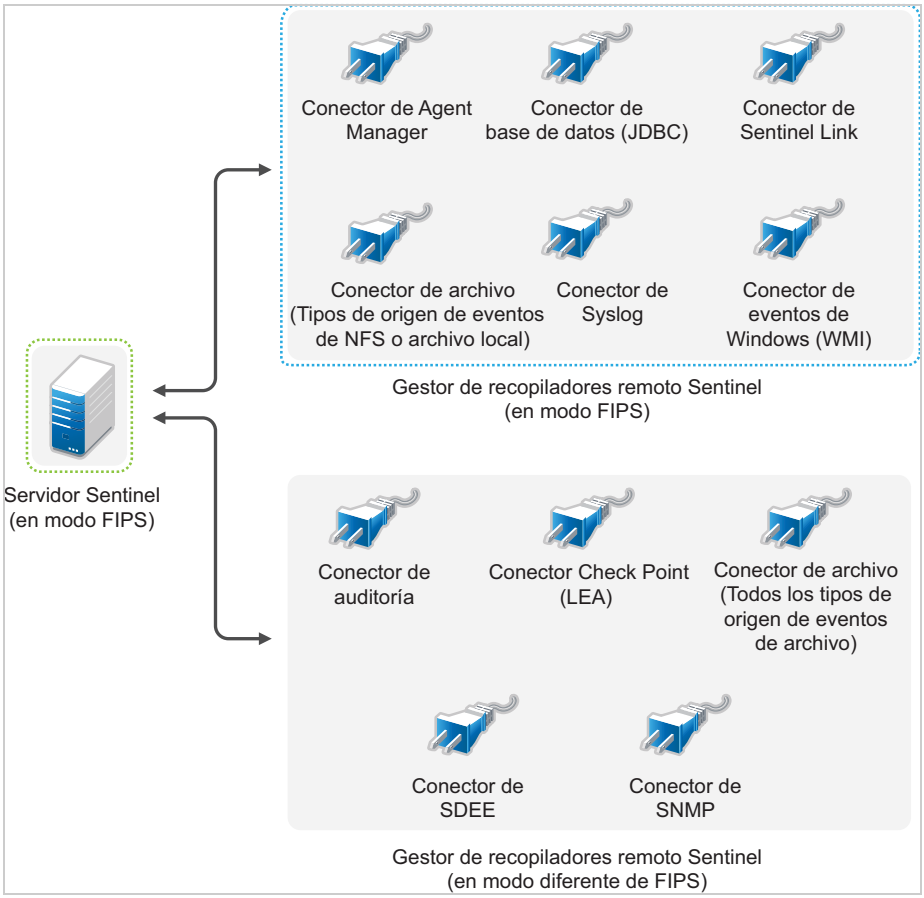
2. Debe tener un gestor de recopiladores remoto Sentinel que se ejecute en modo FIPS 140-2.

   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 109.

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 el “Habilitar el modo FIPS 140-2 en gestores de recopiladores y motores de correlación remotos” en la página 109.
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 114.

7.4.2 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. Suponemos que los datos se recopilan por medio de un gestor de recopiladores. 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, debe 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 requiere la recopilación de datos de orígenes de eventos que utilicen conectores compatibles con el modo FIPS 140-2 y conectores que no son compatibles con dicho modo.

1 Debe tener un servidor Sentinel 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 109.

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

   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 109.

   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 113.

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

4 Configure los motores de correlación remotos, si los hay, para que se ejecuten en modo FIPS 140-2. Para obtener más información, consulte la “Habilitar el modo FIPS 140-2 en gestores de recopiladores y motores de correlación remotos” en la página 109.

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 114.

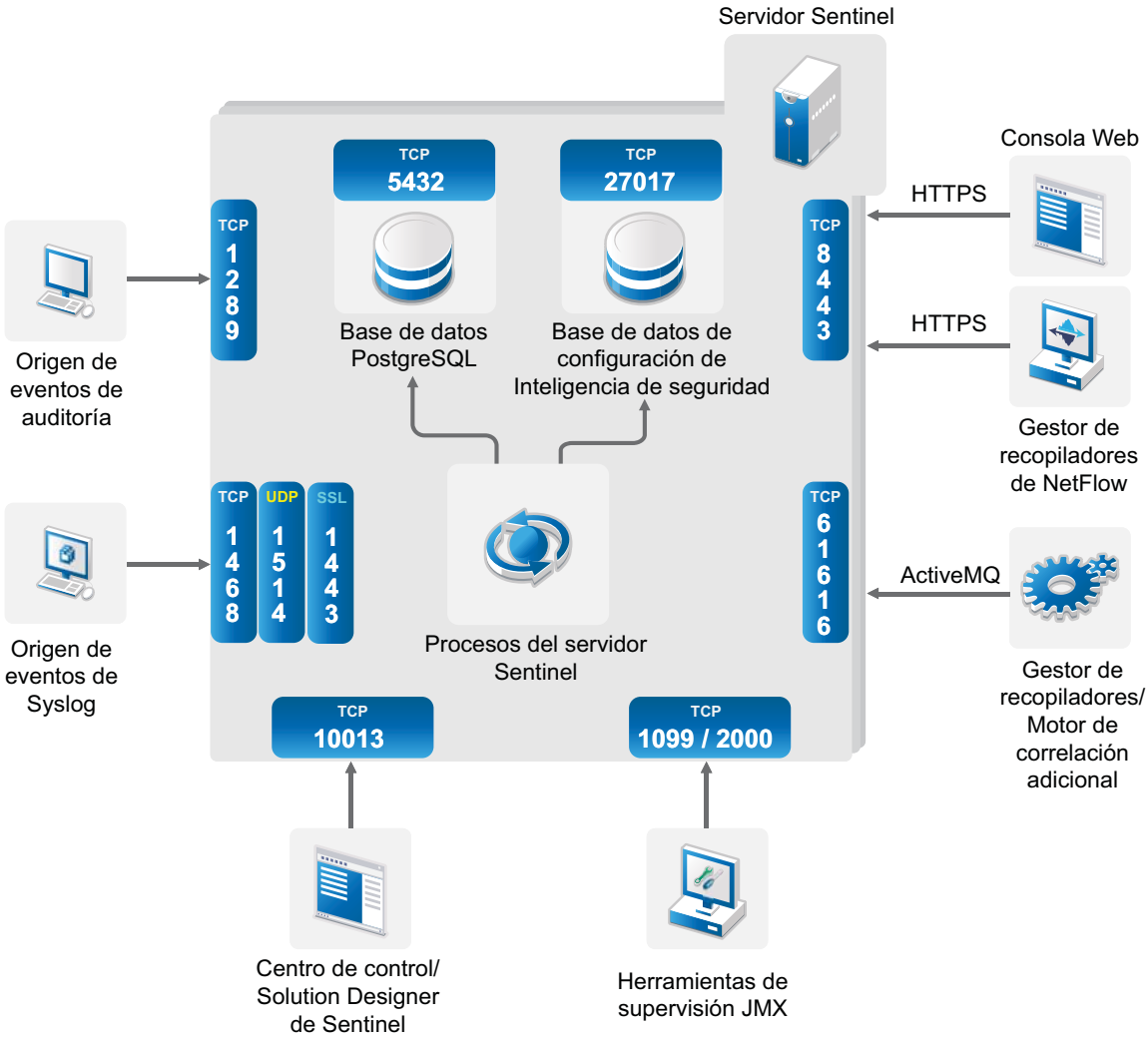
   5a Implemente conectores compatibles con el modo FIPS 140-2 en el gestor de recopiladores remoto que se ejecuta en modo FIPS.

   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.

8 Puertos utilizados

Sentinel utiliza diversos 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 8-1 *Puertos utilizados en Sentinel*



8.1 Puertos del servidor Sentinel

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

8.1.1 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.
TCP 9200	Se utiliza para la comunicación con el servicio de indexado de alertas mediante REST.
TCP 9300	Se utiliza para la comunicación con el servicio de indexado de alertas mediante el protocolo nativo.

8.1.2 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 HTTPS y para las conexiones entrantes de los gestores de recopiladores de NetFlow.
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.

Puertos	Dirección	Necesario/ Opcional	Descripción
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.
TCP 443	Saliente	Opcional	Si se utiliza el Asesor, el puerto inicia una conexión con el servicio del Asesor a través de Internet en la página de actualizaciones del Asesor.
TCP 8443	Saliente	Opcional	Si se utiliza la federación de datos, 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 secundario para usar NFS.
TCP 137, 138, 139, 445	Saliente	Opcional	Si está configurado el almacenamiento secundario 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 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.

8.1.3 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 4984	Entrante	Requerido	Lo utiliza la consola de gestión del dispositivo de Sentinel (WebYaST). También lo utiliza el dispositivo Sentinel para el servicio de actualización.

Puertos	Dirección	Necesario/ Opcional	Descripción
TCP 289	Entrante	Opcional	Se reenvía a 1289 para las conexiones de auditoría.
TCP 443	Entrante	Opcional	Se remite a 8443 para la comunicación HTTPS.
UDP 514	Entrante	Opcional	Se reenvía a 1514 para los mensajes de syslog.
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.

8.2 Puertos del gestor de recopiladores

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

8.2.1 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.

8.2.2 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
TCP 4984	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 auditoría.
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	Se utiliza durante la configuración de 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.

8.3 Puertos del motor de correlación

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

8.3.1 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.

8.3.2 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
TCP 4984	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.

8.4 Puertos del gestor de recopiladores de NetFlow

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

Puertos	Dirección	Necesario/ Opcional	Descripción
HTTPS 8443	Saliente	Requerido	Inicia una conexión con el servidor Sentinel.
3578	Entrante	Requerido	Se utiliza para recibir datos de flujo de la red de los dispositivos de red.

9 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.

9.1 Instalación tradicional

La instalación tradicional instala Sentinel en un sistema operativo 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.	Le permite realizar la instalación con la clave de licencia de evaluación por defecto 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 la Sección 12.2, “Realización de una instalación interactiva”, en la página 72.

- **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 silenciosa. Para obtener más información acerca de una instalación en modo silencioso, consulte la Sección 12.3, “Instalación silenciosa”, en la página 77.

9.2 Instalación del dispositivo

La instalación del dispositivo instala tanto el sistema operativo SLES 11 SP3 de 64 bits como Sentinel.

El dispositivo Sentinel está disponible en los formatos siguientes:

- Una imagen de dispositivo OVF
- 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 13, “Instalación del dispositivo”, en la página 81.

III Instalación de Sentinel

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

10 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.
- **Gestor de recopiladores de NetFlow:** El gestor de recopiladores de NetFlow recopila datos de flujo de la red (NetFlow, IPFIX, etc.) de dispositivos de red como routers, switches y cortafuegos. Los datos de flujo de la red describen información básica sobre todas las conexiones de red entre hosts, como los paquetes y bytes transmitidos, lo que le ayuda a visualizar el comportamiento de hosts individuales o de toda la red.
- **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 “Detecting Vulnerabilities and Exploits” (Detección de vulnerabilidades y exploits) en la *NetIQ Sentinel Administration Guide (Guía de administración de NetIQ Sentinel)*.
- **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. Para los entornos de producción, NetIQ Corporation recomienda configurar una

implantación distribuida porque aísla los componentes de recopilación de datos en un equipo aparte, lo que es importante para manejar aumentos repentinos y otras anomalías con la máxima estabilidad para el sistema. Para obtener más información, consulte la Sección 6.1, “Ventajas de las implantaciones distribuidas”, en la página 41.

11 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 39.
- ❒ 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 B, “Desinstalación”, en la página 179.
- ❒ Si piensa instalar la versión con licencia, obtenga su clave de licencia del Centro de atención al cliente de NetIQ.
- ❒ Asegúrese de que los puertos enumerados en el Capítulo 8, “Puertos utilizados”, en la página 57 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:**

  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

12 Instalación tradicional

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

12.1 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.

12.2 Realización de una instalación interactiva

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

12.2.1 Instalación estándar del servidor Sentinel

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

1. Descargue el archivo de instalación de Sentinel del sitio Web de descargas de NetIQ:
   - **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** .
   - **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 por defecto incluida en el instalador. En cualquier momento durante el período de evaluación 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.

12.2.2 Instalación personalizada del servidor Sentinel

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 del sitio Web de descargas de NetIQ:

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 7.2**.

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

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 21, “Funcionamiento de Sentinel en el modo FIPS 140-2”, en la página 111.

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.

12.2.3 Instalación del gestor de recopiladores y el motor de correlación

Por defecto, Sentinel instala un gestor de recopiladores y un motor de correlación. Para los entornos de producción, NetIQ Corporation recomienda configurar una implantación distribuida porque aísla los componentes de recopilación de datos en un equipo aparte, lo que es importante para manejar aumentos repentinos y otras anomalías con la máxima estabilidad para el sistema. Para obtener información sobre las ventajas de instalar otros componentes, consulte la Sección 6.1, “Ventajas de las implantaciones distribuidas”, en la página 41.

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

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 la Capítulo 5, “Cumplimiento de los requisitos del sistema”, en la página 39.
- 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.

Para instalar el gestor de recopiladores y el motor de correlación, siga estos pasos:

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. Haga clic en **Descargar instalador** en la instalación necesaria.
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 el gestor de recopiladores:

```
./install-cm
```

Para el motor de correlación:

```
./install-ce
```

o bien

Si desea instalar el gestor de recopiladores o el motor de correlación en varios sistemas, puede registrar sus opciones de instalación en un archivo. Puede utilizar este archivo para una instalación de sin supervisión en otros sistemas. Para registrar sus opciones de instalación, especifique el siguiente comando:

Para el gestor de recopiladores:

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

Para el motor de correlación:

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

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

11 Cuando se le solicite, especifique la opción adecuada para proceder con la configuración estándar o personalizada.

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 (Condicional) Si ha elegido la configuración personalizada, especifique lo siguiente:

13a Número de puerto del canal de comunicación del servidor Sentinel.

13b Número de puerto del servidor Web de Sentinel.

14 Cuando se le solicite que acepte el certificado, ejecute el comando siguiente en el servidor Sentinel para verificar el certificado:

Para el modo FIPS:

```
/opt/novell/sentinel/jdk/jre/bin/keytool -list -keystore
/etc/opt/novell/sentinel/config/.activemqkeystore.jks
```

Para el modo diferente de FIPS:

```
/opt/novell/sentinel/jdk/jre/bin/keytool -list -keystore
/etc/opt/novell/sentinel/config/nonfips_backup/.activemqkeystore.jks
```

Compare el certificado generado con el del servidor Sentinel visualizado en el Paso 12.

Nota: Si el certificado no coincide, la instalación se detiene. Vuelva a ejecutar la configuración de instalación y compruebe los certificados.

---

15 Acepte el certificado si el certificado generado coincide con el del servidor Sentinel.

16 Especifique la contraseña del `administrador`.

17 (Condicional) Si ha elegido la configuración personalizada, introduzca `sí` o `s` para habilitar el modo FIPS 140-2 en Sentinel y proceda con la configuración de FIPS.

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

12.3 Instalación silenciosa

La instalación silenciosa o sin supervisión resulta útil si tiene que instalar más de un servidor Sentinel, gestor de recopiladores o motor de correlación 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.

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 12.2.1, “Instalación estándar del servidor Sentinel”, en la página 72 o la Sección 12.2.2, “Instalación personalizada del servidor Sentinel”, en la página 73 y la Sección 12.2.3, “Instalación del gestor de recopiladores y el motor de correlación”, en la página 75.

Para habilitar el 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 del sitio Web de descargas de NetIQ.

2 Entre como usuario `root` al servidor donde desee instalar Sentinel, el gestor de recopiladores o el motor de correlación.

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 realizar la instalación en modo silencioso:

Para el servidor Sentinel:

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

Para el gestor de recopiladores:

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

Para el motor de correlación:

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

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

Si ya ha instalado un servidor Sentinel, puede que el inicio de todos los servicios tarde unos segundos tras la instalación porque el sistema realiza una inicialización única. Espere a que termine la instalación antes de entrar en el servidor.

5 **(Condicional) Si ha elegido habilitar el modo FIPS 140-2 para el servidor Sentinel,** lleve a cabo la configuración del modo FIPS 140-2 realizando las tareas mencionadas en el Capítulo 21, “Funcionamiento de Sentinel en el modo FIPS 140-2”, en la página 111.

12.4 Instalación de Sentinel como usuario diferente de root

Si la directiva de su organización no permite ejecutar la instalación completa de Sentinel como usuario `root`, puede instalar Sentinel como usuario `diferente de root`; es decir, como el usuario `novell`. En esta instalación, algunos pasos se realizan como usuario `root` y luego se continúa la instalación de Sentinel como el usuario `novell` creado por el usuario `root`. Por último, el usuario `root` finaliza la instalación.

Si instala Sentinel como usuario `diferente de root`, deberá hacerlo como usuario novell. NetIQ Corporation no admite instalaciones que no sean realizadas por el usuario root, salvo por el usuario novell, aunque la instalación continúe de manera satisfactoria.

Nota: Cuando instale Sentinel en un directorio existente que no sea el predeterminado, asegúrese de que el usuario novell tiene permisos de propiedad en el directorio. Ejecute el comando siguiente para asignar permisos de propiedad:

```
chown novell:novell <non-default installation directory>
```

---

1. Descargue los archivos de instalación del sitio Web de descargas de NetIQ.
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 comando para cambiar al usuario diferente de root recién creado, es decir, `novell`:

   ```
   su novell
   ```
7. (Condicional) Para realizar una instalación interactiva:

   7a Especifique el comando adecuado dependiendo del componente que vaya a instalar:

Componente	Comando
Servidor de Sentinel	**Ubicación por defecto:** `./install-sentinel`
	Ubicación no predeterminada: `./install-sentinel --location=/foo`
Gestor de recopiladores	**Ubicación por defecto:** `./install-cm`
	Ubicación no predeterminada: `./install-cm --location=/foo`
Motor de correlación	**Ubicación por defecto:** `./install-ce`
	Ubicación no predeterminada: `./install-cm --location=/foo`
Gestor de recopiladores de NetFlow	**Ubicación por defecto:** `./install-netflow`
	Ubicación no predeterminada: `./install-netflow --location=/foo`

7b Continúe con el Paso 9.

8 (Condicional) 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 12.2.1, “Instalación estándar del servidor Sentinel”, en la página 72 o bien la Sección 12.2.2, “Instalación personalizada del servidor Sentinel”, en la página 73.

Para realizar una instalación silenciosa:

8a Especifique el comando adecuado dependiendo del componente que vaya a instalar:

Componente	Comando
Servidor de Sentinel	**Ubicación por defecto:** `./install-sentinel -u <archivo_respuesta>`
	Ubicación no predeterminada: `./install-sentinel --location=/foo -u <archivo_respuesta>`
Gestor de recopiladores	**Ubicación por defecto:** `./install-cm -u <archivo_respuesta>`
	Ubicación no predeterminada: `./install-cm --location=/foo -u <archivo_respuesta>`
Motor de correlación	**Ubicación por defecto:** `./install-ce -u <archivo_respuesta>`
	Ubicación no predeterminada: `./install-ce --location=/foo -u <archivo_respuesta>`
Gestor de recopiladores de NetFlow	**Ubicación por defecto:** `./install-netflow -u <archivo_respuesta>`
	Ubicación no predeterminada: `./install-netflow --location=/foo -u <archivo_respuesta>`

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. Esta instalación puede tardar unos 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 12.2.1, “Instalación estándar del servidor Sentinel”, en la página 72.
   - Si decide continuar con la configuración personalizada, continúe con el Paso 7 al Paso 14 de la Sección 12.2.2, “Instalación personalizada del servidor Sentinel”, en la página 73.

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.

13 Instalación del dispositivo

El dispositivo Sentinel es un dispositivo de software listo para ejecutarse basado en SUSE Studio. El dispositivo combina un sistema operativo SLES 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. Antes de instalar el dispositivo Sentinel, revise la nueva funcionalidad y los problemas conocidos en las notas de la versión del SLES compatible.

La imagen del dispositivo Sentinel viene empaquetada tanto en formato ISO como OVF que pueden implantarse en los entornos virtuales. Para obtener información sobre las plataformas de virtualización compatibles, consulte el sitio Web de información técnica de NetIQ.

13.1 Instalación del dispositivo ISO de Sentinel

En esta sección se proporciona información sobre la instalación de Sentinel, los gestores de recopiladores y los motores de correlación utilizando la imagen del dispositivo ISO. Este formato de imagen permite generar un formato de imagen del disco completa que puede implantarse directamente en el hardware, ya sea físico (bare metal) o virtual (máquina virtual no instalada en un hipervisor) utilizando una imagen DVD de ISO de arranque.

13.1.1 Requisitos previos

Asegúrese de que el entorno en el que va a instalar Sentinel como dispositivo ISO cumpla los siguientes requisitos previos:

- (Condicional) Si va a instalar un dispositivo ISO de Sentinel en un equipo físico (bare metal), descargue la imagen de disco ISO del dispositivo del sitio de asistencia técnica, desempaquete el archivo y cree un DVD.
- Asegúrese de que el sistema en el que desea instalar la imagen de disco ISO tenga como mínimo una memoria de 4,5 GB para que finalice la instalación.
- Asegúrese de que el espacio mínimo en el disco duro sea de 50 GB para que el instalador pueda realizar una propuesta de partición automática.

13.1.2 Instalación de Sentinel

Para instalar el dispositivo ISO de Sentinel:

1. Descargue la imagen del dispositivo virtual ISO del sitio web de descargas de NetIQ.
2. (Condicional) Si va a utilizar un hipervisor:

   Configure la máquina virtual utilizando la imagen de dispositivo virtual ISO y actívela.

   o bien

   Copie la imagen ISO en un DVD, configure la máquina virtual utilizando el DVD y actívela.
3. (Condicional) Si va a instalar el dispositivo Sentinel en un equipo físico (bare metal):
   - **3a** Arranque el equipo físico de la unidad de DVD con el DVD.
   - **3b** Siga las instrucciones del asistente de instalación que se visualizan en pantalla.
   - **3c** 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 configuración del teclado y haga clic en **Siguiente**.
6. Lea y acepte el acuerdo de licencia del software de SUSE Enterprise Server. Haga clic en **Siguiente**
7. Lea y acepte el acuerdo de licencia del usuario final de NetIQ Sentinel. Haga clic en **Siguiente**
8. En la pantalla Hostname (Nombre de host) y Domain Name (Nombre de dominio), especifique los valores correspondientes. Deseleccione la opción **Assign Hostname to Loopback IP** (Asignar nombre de host a IP de retrobucle).
9. Haga clic en **Next** (Siguiente).
10. Seleccione una de las opciones siguientes de ajustes de conexión:
    - 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, haga clic en **Change** (Cambiar) y luego realice los cambios necesarios.
11. Haga clic en **Siguiente**.
12. 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 los valores de configuración de 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
    ```
13. Defina la contraseña `root` y luego haga clic en **Siguiente**.
14. Defina la contraseña del administrador de Sentinel y luego haga clic en **Siguiente**.

Asegúrese de que se haya seleccionado **Instalar la aplicación Sentinel en la unidad de disco duro (solamente para la imagen de Live DVD)** para instalar el dispositivo en el servidor físico. 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; continúe con el Paso 21.

15 En la consola del instalador en tiempo real de YaST2, seleccione **Siguiente**.

La consola del instalador en tiempo real de YaST2 instala el dispositivo en el disco duro. La consola del instalador en tiempo real de YaST2 repite algunos de los pasos anteriores de la instalación.

16 Se muestra la pantalla **Suggested Partitioning** (Partición recomendada) con la configuración de partición recomendada. Revise la configuración de partición, configúrela (si es necesario) y luego seleccione **Next** (Siguiente). Modifique estos ajustes solamente si está familiarizado con la configuración de particiones en SLES.

Puede configurar la configuración de partición utilizando las distintas opciones de partición que se muestran en la pantalla. Para obtener más información sobre cómo configurar particiones, consulte Using the YaST Partitioner (Uso del particionador de YaST) en la *documentación de SLES* y la Sección 6.6, “Planificación de particiones para el almacenamiento de datos”, en la página 47.

17 Introduzca la contraseña de "root" y seleccione **Next** (Siguiente).

18 La pantalla **Live Installation Settings** (Ajustes de instalación en vivo) muestra los ajustes de instalación seleccionados. Revise los ajustes, configúrelos (si es necesario) y luego seleccione**Install** (Instalar).

19 Seleccione **Install** (Instalar) para confirmar la instalación.

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

20 Seleccione **OK** para reiniciar el sistema.

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

22 Introduzca el nombre de usuario y la contraseña "root" en la consola para entrar en el dispositivo.

El valor por defecto del nombre de usuario es `root` y la contraseña es la contraseña que definió en el Paso 17.

23 Pase a la Sección 13.3, “Configuración del dispositivo posterior a la instalación”, en la página 86.

13.1.3 Instalación de gestores de recopiladores y motores de correlación

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

1 Complete los pasos 1 a Paso 13 de la Sección 13.1.2, “Instalación de Sentinel”, en la página 82.

2 Especifique la siguiente configuración para el gestor de recopiladores o el motor de correlación:

- **Nombre de host o dirección IP del servidor Sentinel:** especifique el nombre de host o la dirección IP de servidor Sentinel al que debe conectarse el gestor de recopiladores o el motor de correlación.
- **Puerto del canal de comunicación de Sentinel:** especifique el número de puerto del canal de comunicación del servidor Sentinel. El número de puerto por defecto es `61616`.

- **Puerto del servidor Web de Sentinel:** Especifique el puerto del servidor Web de Sentinel. El puerto por defecto es 8443.
- **Contraseña del usuario administrador del servidor Sentinel:** Especifique la contraseña del usuario `administrador`.
- **Instale la aplicación Sentinel en la unidad de disco duro (solamente para la imagen de Live DVD):** asegúrese de seleccionar esta casilla de verificación para instalar el dispositivo en el servidor físico.

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

3 Haga clic en **Siguiente**.

4 Acepte el certificado cuando se le indique.

5 Realice el Paso 15 al Paso 20 de la Sección 13.1.2, “Instalación de Sentinel”, en la página 82.

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

La consola 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. También muestra la dirección IP de la interfaz del usuario del servidor Sentinel.

7 Realice el Paso 22 al Paso 23 de la Sección 13.1.2, “Instalación de Sentinel”, en la página 82.

13.2 Instalación del dispositivo OVF de Sentinel

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

OVF es un formato de máquina virtual estándar admitido por la mayoría de hipervisores, ya sea directamente o mediante una conversión sencilla. Sentinel admite el dispositivo OVF con dos hipervisores certificados, pero también se puede utilizar con otros hipervisores.

13.2.1 Instalación de Sentinel

Para instalar el dispositivo OVF de Sentinel:

1 Descargue la imagen del dispositivo virtual OVF del sitio de descargas de NetIQ.

2 En la consola de gestión del hipervisor, importe el archivo de imagen OVF como nueva máquina virtual. Deje que el hipervisor convierta la imagen de OVF al formato nativo si se le indica.

3 Revise los recursos de hardware virtual asignados a su máquina virtual para asegurarse de que cumplan los requisitos de Sentinel.

4 Encienda la máquina virtual.

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

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

7 Lea y acepte el acuerdo de licencia de software de SUSE Linux Enterprise Server (SLES) 11 SP3.

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

9 En la página de Hostname (Nombre de host) y Domain Name (Nombre de dominio), especifique dichos datos. Deseleccione la opción **Assign Hostname to Loopback IP** (Asignar nombre de host a IP de retrobucle).

10 Haga clic en **Siguiente**. Se guardará la información configurada de nombre de host.

11 Elija una de las siguientes opciones de conexión de red:

- 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.

12 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
```

13 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.

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

Puede 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.

15 Anote la dirección IP del dispositivo que aparece en la consola. Utilice la misma dirección IP para acceder a la consola Web de Sentinel.

13.2.2 Instalación de gestores de recopiladores y motores de correlación

Para instalar un gestor de recopiladores o un motor de correlación en un servidor VMware ESX como imagen de dispositivo OVF:

1 Realice los pasos 1 a 10 de la Sección 13.2.1, “Instalación de Sentinel”, en la página 84.

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 por defecto es el `61616`.

4 Especifique la contraseña del `administrador`.

5 Haga clic en **Siguiente.**

6 Acepte el certificado.

7 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.

13.3 Configuración del dispositivo posterior a la instalación

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

13.3.1 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 13.3.3, “Registro para recibir actualizaciones”, en la página 87.

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

13.3.2 Creación de particiones

Una buena práctica consiste en asegurarse de que se crean particiones separadas para almacenar datos de Sentinel en una partición diferente 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 de los conjuntos de archivos, 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. Para obtener información sobre cómo planificar sus particiones, consulte la

Sección 6.6, “Planificación de particiones para el almacenamiento de datos”, en la página 47. 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.

   Para obtener información sobre la creación de particiones, consulte Using the YaST Partitioner (Uso del particionador de YaST) en la *documentación de SLES 11*.
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
    ```

13.3.3 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 NetIQ.

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**.

13.3.4 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 proxy de paquetes integrado en el Centro de servicios al cliente de NetIQ que proporciona funciones clave de dicho centro.

Requisitos previos

- Obtenga las credenciales del Centro de servicios al cliente de NetIQ para Sentinel para obtener actualizaciones de NetIQ. Para obtener información sobre la forma de obtener credenciales, comuníquese con Asistencia de NetIQ.
- Asegúrese de que SLES 11 SP3 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 25.3, “Actualización de la aplicación con SMT”, en la página 138.

13.3.5 Instalación de VMware Tools (aplicable únicamente al servidor VMware ESX)

Para que Sentinel funcione de forma eficaz en el servidor VMware ESX, debe instalar VMware Tools. VMware Tools es un conjunto de utilidades que mejora el rendimiento del sistema operativo de la máquina virtual. Además, mejora la gestión del equipo virtual. Para obtener más información sobre la instalación de VMware Tools, consulte VMware Tools for Linux Guests (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.

13.4 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**.

14 Instalación del gestor de recopiladores de NetFlow

Debe instalar el gestor de recopiladores de NetFlow en un equipo diferente y no en el mismo equipo donde está instalado el servidor Sentinel, el gestor de recopiladores o un motor de correlación.

14.1 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 la Capítulo 5, “Cumplimiento de los requisitos del sistema”, en la página 39.
- ❒ Sincronice el tiempo utilizando el protocolo de tiempo de red (NTP).

14.2 Instalación del gestor de recopiladores de NetFlow

Puede instalar gestores de recopiladores de NetFlow utilizando uno de los siguientes métodos:

- **Estándar:** utiliza los valores por defecto para la configuración de NetFlow.
- **Personalizado:** permite personalizar el número de puerto del servidor Sentinel.

Nota

- Para enviar datos de flujo de la red al servidor Sentinel, debe ser administrador, pertenecer a la función de Proveedor de NetFlow, o bien tener permiso para enviar datos de NetFlow.
- Si tiene pensado instalar más de un gestor de recopiladores de NetFlow, debe crear una nueva cuenta de usuario para cada gestor de recopiladores de NetFlow a fin de enviar datos de flujo de la red a Sentinel. Tener diferentes cuentas para cada gestor de recopiladores de NetFlow ofrece un nivel de control adicional con respecto a qué gestores de recopiladores de NetFlow tienen permiso para enviar datos a Sentinel.

Para instalar el gestor de recopiladores de NetFlow:

1. Lance la interfaz Web de Sentinel especificando la siguiente dirección URL en la interfaz 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 de NetFlow, haga clic en **Descargar instalador**.

4 Haga clic en **Guardar archivo** para guardar el instalador en la ubicación deseada.

5 En el indicador de comandos, especifique el siguiente comando para extraer el archivos de instalación.

```
tar zxvf <install_filename>
```

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

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

```
cd <directory_name>
```

7 Especifique el siguiente comando para instalar el gestor de recopiladores de NetFlow:

```
./install-netflow
```

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

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

10 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.

11 Especifique si desea continuar con la instalación Estándar o Personalizada.

12 Especifique el nombre de host o la dirección IP del servidor Sentinel que debe recibir los datos de flujo de la red.

13 (Condicional) Si elige la instalación Personalizada, especifique el número de puerto del servidor Sentinel.

El número de puerto por defecto es 8443.

14 Especifique el nombre de usuario y la contraseña para autenticar en el servidor Sentinel.

Nota: Asegúrese de que las credenciales del usuario que especifique tengan permiso para enviar datos de NetFlow o privilegios administrativos. De lo contrario, la instalación finaliza, pero la autenticación falla cuando el gestor de recopiladores de NetFlow envía datos al servidor Sentinel.

La instalación finaliza. El gestor de recopiladores de NetFlow podría tardar unos minutos en establecer una conexión con el servidor Sentinel.

15 (Opcional) Puede determinar si la instalación del gestor de recopiladores de NetFlow fue satisfactoria realizando una de las siguientes comprobaciones:

- Verificar si los servicios del gestor de recopiladores de NetFlow están en ejecución:

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

- Verificar si el gestor de recopiladores de NetFlow ha establecido una conexión con el servidor Sentinel:

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

- Verificar si el gestor de recopiladores de NetFlow aparece en la consola Web de Sentinel haciendo clic en **Recopilación** > **NetFlow**.

16 Habilite el reenvío del tráfico de flujo de la red en el dispositivo desde el que desea recopilar datos de flujo de la red.

Al habilitar NetFlow en el dispositivo, debe especificar la dirección IP del servidor Sentinel y el puerto en el que el gestor de recopiladores de NetFlow recibe datos del dispositivo habilitado para NetFlow. El número de puerto por defecto es 3578. Para obtener más información, consulte la documentación específica del dispositivo habilitado para NetFlow.

15 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.

15.1 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.

15.2 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.

16 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
  ```

- Compruebe si los servicios de Sentinel están activos y funcionan en modo FIPS o diferente de FIPS:

  ```
  /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.

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.

17 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.

17.1 Comprender el tiempo en Sentinel

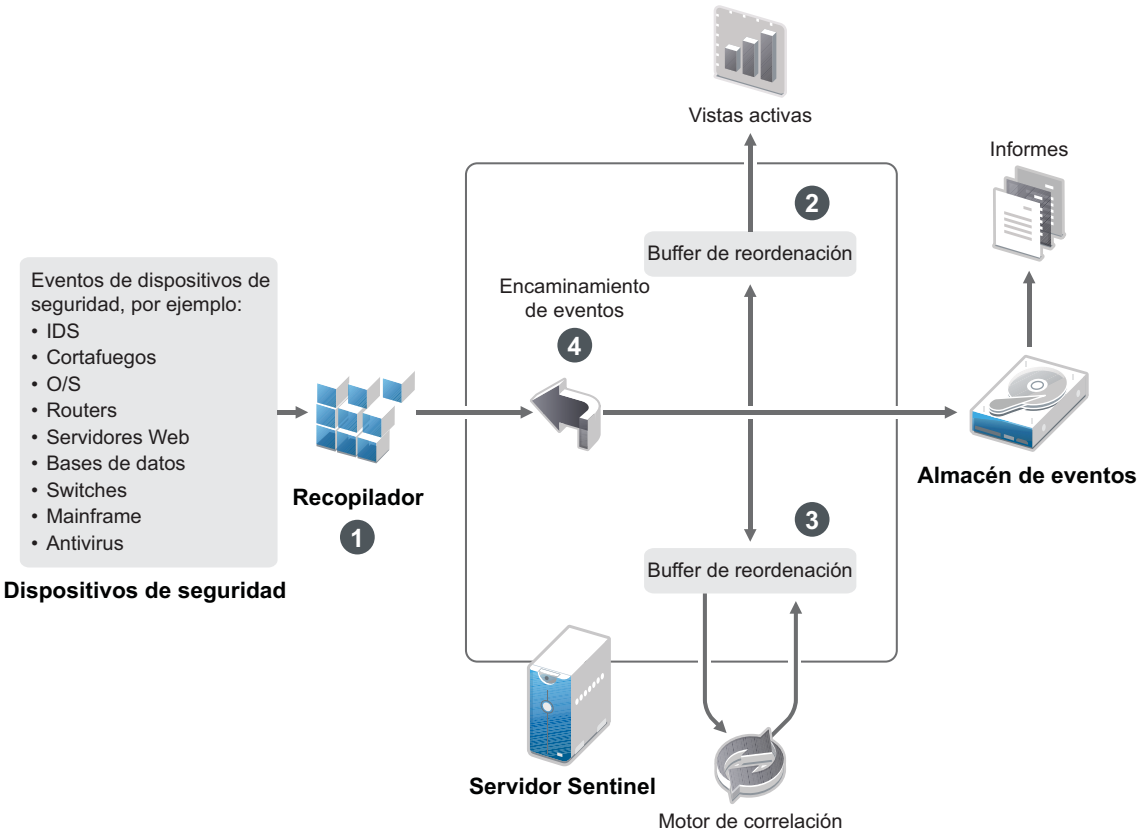
Sentinel es un sistema distribuido compuesto por varios procesos distribuidos a través de la red. Además, puede haber algún retraso introducido por el origen de evento. Para adaptarlo, los procesos de Sentinel reordenan los eventos en un flujo ordenado por tiempo antes de procesarlos.

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 17-1 *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.

17.2 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 Administration Guide* (Guía de administración de NetIQ Sentinel).
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.

17.3 Configuración del límite de tiempo de demora para los eventos

Cuando Sentinel recibe eventos de los orígenes de eventos, puede producirse un retraso entre el tiempo en que se generó el evento y el tiempo que tarda Sentinel en procesarlo. Sentinel almacena los eventos con grandes demoras en particiones separadas. Si muchos eventos sufren una demora por un período de tiempo prolongado, podría indicar que un origen de eventos está configurado incorrectamente. Esto podría perjudicar el rendimiento de Sentinel cuando trate de manejar estos eventos demorados. Puesto que la demora de los eventos puede ser consecuencia de una mala configuración y, en ese caso, quizá no sea aconsejable almacenarlos, Sentinel le permite configurar un tiempo de demora aceptable para los eventos entrantes. El router de eventos abandona los eventos que exceden el límite de demora. Especifique el límite de demora en la siguiente propiedad del archivo`configuration.properties`:

```
esecurity.router.event.delayacceptthreshold = <time in milliseconds>
```

También puede registrar periódicamente una lista en el archivo de registro del servidor Sentinel que muestre los orígenes de eventos de los que se reciben eventos demorados más allá de un umbral específico. Para registrar esta información, especifique el umbral en la siguiente propiedad del archivo `configuration.properties`:

```
sentinel.indexedlog.eventdelay.reportthreshold= <time in milliseconds>
```

17.4 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.

18 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. Apague Sentinel utilizando el siguiente comando:

   ```
   rcsentinel stop
   ```

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

   ```
   ./configure.sh
   ```

3. Especifique `1` para llevar a cabo una configuración estándar o bien `2` para realizar una configuración personalizada de Sentinel.
4. Pulse la barra espaciadora para leer todo el acuerdo de licencia.
5. 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.
6. Introduzca `1` para usar la clave de licencia de evaluación por defecto

   O bien

   Introduzca `2` para especificar una clave de licencia adquirida para Sentinel.
7. 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 8.
   - Si desea cambiar la contraseña existente, introduzca `2`, especifique la nueva contraseña, confírmela y luego continúe con el Paso 8.

     El usuario `admin` es la identidad que se utiliza para realizar tareas administrativas a través de la consola Web de Sentinel, entre otras la creación de otras cuentas de usuario.
8. 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 9.
   - Si desea cambiar la contraseña existente, introduzca `2`, especifique la nueva contraseña, confírmela y luego continúe con el Paso 9.

   La cuenta `dbauser` es la identidad que utiliza 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.
9. 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 10.
   - Si desea cambiar la contraseña existente, introduzca `2`, especifique la nueva contraseña, confírmela y luego continúe con el Paso 10.

     La cuenta `appuser` es una identidad interna, que utiliza el proceso java de Sentinel para establecer conexión e interactuar con la base de datos. La contraseña que introduce aquí sirve para realizar tareas en la base de datos.

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

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

12 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`.

19 Configuración de módulos auxiliares (plug-ins) genéricos

Sentinel viene preinstalado con los módulos auxiliares (plug-ins) por defecto disponibles en el momento del lanzamiento de la versión de Sentinel.

En este capítulo se proporciona información sobre cómo configurar los módulos auxiliares (plug-ins) genéricos.

19.1 Visualización de módulos auxiliares (plug-ins) preinstalados

Puede ver la lista de módulos auxiliares (plug-ins) preinstalados en Sentinel. También puede ver las versiones de los módulos auxiliares (plug-ins) y otros metadatos, que le ayudan a determinar si tiene la versión más reciente de un módulo auxiliar.

Para ver los módulos auxiliares (plug-ins) que tiene instalados en su servidor Sentinel:

1. Entre como administrador en la interfaz Web de Sentinel en la dirección `https://<dirección IP>:8443`, donde 8443 es el puerto por defecto del servidor Sentinel.
2. Haga clic en **Módulos auxiliares (plug-ins)** > **Catálogo**.

19.2 Configuración de la recopilación de datos

Para obtener más información sobre cómo configurar Sentinel para la recopilación de datos, consulte la sección “Collecting and Routing Event Data” (Recopilación y encaminamiento de datos de eventos) de la *NetIQ Sentinel Administration Guide* (Guía de administración de NetIQ Sentinel).

19.3 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 Administration Guide* (Guía de administración de NetIQ Sentinel). .

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 Administration Guide* (Guía de administración de NetIQ Sentinel).

19.4 Configuración de acciones e integradores

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.

20 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`.

20.1 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. Busque 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 21, “Funcionamiento de Sentinel en el modo FIPS 140-2”, en la página 111.

20.2 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 21, “Funcionamiento de Sentinel en el modo FIPS 140-2”, en la página 111.

21 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.

21.1 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 120.

21.2 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 120.
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>/jdk/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 120.
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>/jdk/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 120.

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

21.3 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 120.

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 Administration Guide* (Guía de administración de NetIQ Sentinel).

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`.

21.4 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.

21.5 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`.

21.5.1 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 120.

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.

21.5.2 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 120.

3 Continúe con la configuración del conector.

21.5.3 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 120.

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.

21.5.4 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 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. 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 120.

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.

21.5.5 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 ni autenticación de certificados 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 120.

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 120.

21.5.6 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 "Importación de certificados en la base de datos del almacén de claves de FIPS" en la página 120.

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.

21.5.7 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 120.

3 Continúe con la configuración de la instancia del integrador.

21.5.8 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.

21.5.9 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 en el modo diferente de FIPS para conectar con el servidor Sentinel en el modo FIPS 140-2.

Para obtener más información, consulte la Parte III, “Instalación de Sentinel”, en la página 65.

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 en el modo FIPS 140-2. Para obtener más información sobre estos problemas conocidos, consulte Sentinel 7.1 Release Notes (Notas de la versión de Sentinel 7.1).

21.6 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.

21.7 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 21.7.1, “Reversión del servidor Sentinel al modo diferente de FIPS”, en la página 120
- Sección 21.7.2, “Reversión de gestores de recopiladores o motores de correlación remotos al modo diferente de FIPS”, en la página 121

21.7.1 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.

21.7.2 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.

22 Lista de verificación de implementación

Antes de actualizar Sentinel, revise la siguiente lista de verificación para garantizar una actualización satisfactoria:

Tabla 22-1 *Lista de verificación de implementación*

❒	Tareas	Consulte
❒	Asegúrese de que los equipos en los que instale Sentinel y sus componentes cumplan los requisitos especificados.	Sitio web de información técnica de NetIQ Sentinel
❒	Revise las notas de la versión del sistema operativo compatible para conocer los problemas conocidos.	Notas de la versión de SUSE
❒	Revise las notas de la versión de Sentinel para ver la nueva funcionalidad y conocer los problemas conocidos.	Notas de la versión de Sentinel
❒	Efectúe las tareas que se indica en Requisitos previos.	Capítulo 23, “Requisitos previos”, en la página 127

23 Requisitos previos

23.1 Cómo guardar la información de configuración personalizada

Si ha definido valores de parámetro de configuración personalizados en el archivo `server.conf`, guarde dichos valores en archivos separados antes de proceder con la actualización.

Para guardar la información de configuración personalizada:

1. Entre en el servidor Sentinel como usuario `novell` y vaya al directorio `/etc/opt/novell/sentinel/config/`.
2. Cree un archivo de configuración llamado `server-custom.conf` y añada sus parámetros de configuración personalizada en este archivo.
3. (Opcional) Cree archivos de configuración personalizada similares para otros componentes de Sentinel, como Netflow Collector. Por ejemplo, `netflow-collector-custom.conf`.

Sentinel aplica la configuración personalizada guardada a estos archivos de configuración durante la actualización.

23.2 Integración de Change Guardian

Sentinel es compatible con Change Guardian 4.2 y versiones posteriores. Para recibir eventos de Sentinel, antes debe actualizar el servidor Change Guardian a la versión 4.2 o una posterior para asegurarse de que Sentinel sigue recibiendo eventos de Change Guardian tras la actualización.

23.3 Requisitos previos para versiones anteriores a Sentinel 7.1.1

Sentinel 7.1.1 y las versiones posteriores incluyen MongoDB versión 2.4.1. MongoDB 2.4 requiere eliminar los nombres de usuario duplicados en la base de datos. Si va a actualizar versiones de Sentinel anteriores a 7.1.1, verifique si existen usuarios duplicados y elimínelos si los hay.

Realice los pasos siguientes para identificar usuarios duplicados:

1. Entre en el servidor de Sentinel 7.1 o versión anterior como el usuario novell.
2. Cambie al directorio siguiente:

   ```
   cd opt/novell/sentinel/3rdparty/mongodb/bin
   ```

3. Ejecute los siguientes comandos para verificar si existen usuarios duplicados:

```
./mongo --port 27017 --host "localhost"
use analytics
db.system.users.find().count()
```

Si el `número` es superior a 1, indica que hay usuarios duplicados.

Lleve a cabo los pasos siguientes para eliminar los usuarios duplicados:

1. Ejecute el siguiente comando para mostrar la lista de usuarios:

   ```
   db.system.users.find().pretty()
   ```

   El comando enumera los usuarios junto con las entradas duplicadas. El primer usuario de la lista es el usuario original. Debe mantener el primer usuario y eliminar los demás de la lista.

2. Ejecute el siguiente comando para eliminar los usuarios duplicados:

   ```
   db.system.users.remove({ _id : ObjectId("object_ID") })
   ```

3. Ejecute el siguiente comando para verificar si se han eliminado los usuarios duplicados:

   ```
   db.system.users.find().pretty()
   ```

4. Cambie al usuario administrador de la base de datos:

   ```
   use admin
   ```

5. Repita los pasos Paso 1 a Paso 3 para verificar y eliminar los usuarios `dbausers` duplicados en la base de datos de administración.

24 Actualización de la instalación tradicional de Sentinel

24.1 Actualización de Sentinel

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

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

   Para obtener más información sobre la copia de seguridad de datos, consulte la sección “Backing Up and Restoring Data” (Copia de seguridad y restauración de datos) en la *NetIQ Sentinel Administration Guide (Guía de administración de NetIQ Sentinel 7.1)*.
2. (Condicional) Si ha personalizado los ajustes de configuración en los archivos `server.xml`, `collector_mgr.xml` o `correlation_engine.xml`, asegúrese de que ha creado los archivos de propiedades adecuados con el nombre de obj-component id para estar seguro de que las personalizaciones se mantendrán después de la actualización. Para obtener más información, consulte “Maintaining Custom Settings in XML Files” (Cómo mantener los ajustes personalizados en los archivos XML) en la *NetIQ Sentinel Administration Guide* (Guía de administración de NetIQ Sentinel).
3. Descargue el programa de instalación más reciente del sitio Web de descargas de NetIQ.
4. Entre como usuario `root` en el servidor en el que desea actualizar Sentinel.
5. Especifique el siguiente comando para extraer los archivos de instalación del archivo tar:

   ```
   tar xfz <install_filename>
   ```

   Reemplace *<nombre de archivo_instalación>* por el nombre real del archivo de instalación.
6. Vaya al directorio donde extrajo el archivo de instalación.
7. Especifique el siguiente comando para actualizar Sentinel:

   ```
   ./install-sentinel
   ```
8. 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.
9. Lea el acuerdo de licencia del usuario final e introduzca `sí` o `s` para aceptar la licencia y continuar con la instalación.
10. 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.
11. Borre la memoria caché del navegador Web para ver la versión más reciente de Sentinel.

12 Borre la caché de Java Web Start en los equipos cliente para utilizar la versión más reciente de las aplicaciones Sentinel.

   La caché de Java Web Start se puede borrar con el comando `javaws -clearcache` o desde el Centro de control de Java. Para obtener más información, vaya al sitio http://www.java.com/es/download/help/plugin_cache.xml.

13 (Condicional) Si se ha actualizado la base de datos PostgreSQL a una versión importante (por ejemplo, de 8.0 a 9.0 o de 9.0 a 9.1), elimine los archivos PostgreSQL antiguos de la base de datos PostgreSQL. Para obtener información sobre si se ha actualizado la base de datos PostgreSQL, consulte las notas de la versión de Sentinel.

   13a Cambie al usuario novell.

   ```
   su novell
   ```

   13b Busque en la carpeta `bin`:

   ```
   cd /opt/novell/sentinel/3rdparty/postgresql/bin
   ```

   13c Elimine todos los archivos postgreSQL antiguos mediante el siguiente comando:

   ```
   ./delete_old_cluster.sh
   ```

14 (Condicional) Si va a actualizar desde Sentinel 7.1.1 o una versión anterior, el instalador no migrará por defecto los datos de Inteligencia de seguridad (SI). Para migrar los datos de SI desde Sentinel 7.1.1 o una versión anterior, habilite manualmente la migración de datos de SI de la siguiente manera:

   14a Cambie al usuario novell.

   ```
   su novell
   ```

   14b Abra el archivo `/etc/opt/novell/sentinel/config/server.xml`.

   14c Añada la siguiente propiedad en la sección de componentes `BaseliningRuntime`:

   ```
   <property name="baselining.migration.check">true</property>
   ```

   14d Reinicie el servidor Sentinel.

15 Para actualizar los sistemas de gestor de recopiladores y los sistemas de motor de correlación, consulte la Sección 24.3, “Actualización del gestor de recopiladores o del motor de correlación”, en la página 132.

24.2 Actualización de Sentinel como usuario diferente de root

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

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

   Para obtener más información sobre la copia de seguridad de los datos, consulte “Backing Up and Restoring Data” (Copia de seguridad y restauración de datos) en *NetIQ Sentinel Administration Guide (Guía de administración de NetIQ Sentinel)*.

2 (Condicional) Si ha personalizado los ajustes de configuración en los archivos `server.xml`, `collector_mgr.xml` o `correlation_engine.xml`, asegúrese de que ha creado los archivos de propiedades adecuados con el nombre de obj-component id para estar seguro de que las

personalizaciones se mantendrán después de la actualización. Para obtener más información, consulte “Backing Up and Restoring Data (Copia de seguridad y restauración de datos)” en la*NetIQ Sentinel Administration Guide (Guía de administración de NetIQ Sentinel)*.

3 Descargue los archivos de instalación del sitio Web de descargas de NetIQ.

4 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.

5 Entre como usuario `root` en el servidor en el que desea actualizar Sentinel.

6 Extraiga el RPM `squashfs` de los archivos de instalación de Sentinel.

7 Instale el `squashfs` en el servidor Sentinel.

```
rpm -Uvh <install_filename>
```

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

```
su novell
```

9 (Condicional) Para realizar una actualización interactiva:

9a Especifique el siguiente comando:

```
./install-sentinel
```

Para actualizar Sentinel en una ubicación no predeterminada, especifique la opción --location junto con el comando. Por ejemplo:.

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

9b Continúe con el Paso 11.

10 (Condicional) Para realizar una actualización silenciosa, especifique el siguiente comando:

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

La instalación continúa con los valores almacenados en el archivo de respuesta. La actualización de Sentinel ha finalizado.

11 Especifique el número del idioma que desea usar para la actualización.

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

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

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

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

14 Borre la caché de Java Web Start en los equipos cliente para utilizar la versión más reciente de las aplicaciones Sentinel.

La caché de Java Web Start se puede borrar con el comando `javaws -clearcache` o desde el Centro de control de Java. Para obtener más información, vaya al sitio http://www.java.com/es/download/help/plugin_cache.xml.

15 (Condicional) Si se ha actualizado la base de datos PostgreSQL a una versión importante (por ejemplo, de 8.0 a 9.0 o de 9.0 a 9.1), elimine los archivos PostgreSQL antiguos de la base de datos PostgreSQL. Para obtener información sobre si se ha actualizado la base de datos PostgreSQL, consulte las notas de la versión de Sentinel.

15a Cambie al usuario novell.

```
su novell
```

15b Busque en la carpeta `bin`:

```
cd /opt/novell/sentinel/3rdparty/postgresql/bin
```

15c Elimine todos los archivos postgreSQL antiguos mediante el siguiente comando:

```
./delete_old_cluster.sh
```

16 (Condicional) Si va a actualizar desde Sentinel 7.1.1 o una versión anterior, el instalador no migrará por defecto los datos de Inteligencia de seguridad (SI). Para migrar los datos de SI desde Sentinel 7.1.1 o una versión anterior, habilite manualmente la migración de datos de SI de la siguiente manera:

16a Cambie al usuario novell.

```
su novell
```

16b Abra el archivo `/etc/opt/novell/sentinel/config/server.xml`.

16c Añada la siguiente propiedad en la sección de componentes `BaseliningRuntime`:

```
<property name="baselining.migration.check">true</property>
```

16d Reinicie el servidor Sentinel.

24.3 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 Administration Guide (Guía de administración de NetIQ Sentinel)*.

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.

5 Guarde el archivo del instalador en el servidor del gestor de recopiladores o el motor de correlación correspondientes.

6 Copie el archivo en una ubicación temporal.

7 Extraiga el contenido del archivo.

8 Ejecute el guión siguiente:

Para el gestor de recopiladores:

```
./install-cm
```

Para el motor de correlación:

```
./install-ce
```

9 Siga las instrucciones que aparecen en pantalla para finalizar el procedimiento de instalación.

10 (Condicional) En el caso de instalaciones personalizadas, ejecute el comando siguiente para sincronizar las configuraciones entre el servidor Sentinel, el gestor de recopiladores y el motor de correlación:

```
/opt/novell/sentinel/setup/configure.sh
```

25 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.

25.1 Actualización del dispositivo mediante 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 Administration Guide (Guía de administración de NetIQ Sentinel)*.
2. (Condicional) Si ha personalizado los ajustes de configuración en los archivos `server.xml`, `collector_mgr.xml` o `correlation_engine.xml`, asegúrese de que ha creado los archivos de propiedades adecuados con el nombre de obj-component id para estar seguro de que las personalizaciones se mantendrán después de la actualización. Para obtener más información, consulte “Maintaining Custom Settings in XML Files” (Cómo mantener los ajustes personalizados en los archivos XML) en la *NetIQ Sentinel Administration Guide* (Guía de administración de NetIQ Sentinel).
3. Entre a la consola de la aplicación como usuario `root`.
4. Ejecute el comando siguiente:

   ```
   /usr/bin/zypper patch
   ```
5. (Condicional) Si va a actualizar desde Sentinel 7.0.1 o una versión anterior, introduzca `1` para aceptar el cambio de Novell a NetIQ.
6. (Condicional) Si va a actualizar desde versiones de Sentinel anteriores a 7.2, el instalador muestra un mensaje que indica que se debe resolver una dependencia para ciertos paquetes del dispositivo. Introduzca `1` para desinstalar los paquetes dependientes.
7. (Condicional) Si va a actualizar desde Sentinel 7.2 o una versión posterior, el instalador muestra una opción para indicar el cambio en la arquitectura ncgOverlay. Introduzca la opción adecuada para aceptar el cambio de arquitectura.
8. Pulse `s` para continuar.
9. Pulse `sí` para aceptar el acuerdo de licencia.
10. Reinicie la aplicación Sentinel.
11. (Condicional) Si Sentinel está instalado en un puerto personalizado, o si el gestor de recopiladores o el motor de correlación están en modo FIPS, ejecute el comando siguiente:

    ```
    /opt/novell/sentinel/setup/configure.sh
    ```
12. Borre la memoria caché del navegador Web para ver la versión más reciente de Sentinel.

13 Borre la caché de Java Web Start en los equipos cliente para utilizar la versión más reciente de las aplicaciones Sentinel.

   La caché de Java Web Start se puede borrar con el comando `javaws -clearcache` o desde el Centro de control de Java. Para obtener más información, vaya al sitio http://www.java.com/es/download/help/plugin_cache.xml.

14 (Condicional) Si se ha actualizado la base de datos PostgreSQL a una versión importante (por ejemplo, de 8.0 a 9.0 o de 9.0 a 9.1), elimine los archivos PostgreSQL antiguos de la base de datos PostgreSQL. Para obtener información sobre si se ha actualizado la base de datos PostgreSQL, consulte las notas de la versión de Sentinel.

   14a Cambie al usuario novell.

   ```
   su novell
   ```

   14b Busque en la carpeta `bin`:

   ```
   cd /opt/novell/sentinel/3rdparty/postgresql/bin
   ```

   14c Elimine todos los archivos postgreSQL antiguos mediante el siguiente comando:

   ```
   ./delete_old_cluster.sh
   ```

15 (Condicional) Si va a actualizar desde Sentinel 7.1.1 o una versión anterior, el instalador no migrará por defecto los datos de Inteligencia de seguridad (SI). Para migrar los datos de SI desde Sentinel 7.1.1 o una versión anterior, habilite manualmente la migración de datos de SI de la siguiente manera:

   15a Cambie al usuario novell.

   ```
   su novell
   ```

   15b Abra el archivo `/etc/opt/novell/sentinel/config/server.xml`.

   15c Añada la siguiente propiedad en la sección de componentes `BaseliningRuntime`:

   ```
   <property name="baselining.migration.check">true</property>
   ```

   15d Reinicie el servidor Sentinel.

16 (Condicional) Para actualizar el gestor de recopiladores o el motor de correlación, siga del Paso 3 alPaso 11 .

25.2 Actualización del dispositivo mediante WebYast

La aplicación se puede actualizar utilizando WebYaST solo en Sentinel 7.3.2 y versiones posteriores, y si el archivo RPM de NetIQ Change Guardian se actualizó manualmente tal como se indica en las *Notas de la versión de Sentinel 7.3.2*.

Las actualizaciones del dispositivo desde versiones anteriores a Sentinel 7.3.2 deben realizarse con la utilidad de línea de comandos zypper porque se requiere la interacción del usuario para finalizar la actualización. WebYaST no permite la interacción del usuario necesaria. Para obtener información sobre cómo actualizar la aplicación con zypper, consulte la Sección 25.1, “Actualización del dispositivo mediante zypper”, en la página 135.

1 Entre en el dispositivo Sentinel como usuario con funciones de administrador.

2 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 Administration Guide (Guía de administración de NetIQ Sentinel)*.

3 (Condicional) Si ha personalizado los ajustes de configuración en los archivos `server.xml`, `collector_mgr.xml` o `correlation_engine.xml`, asegúrese de que ha creado los archivos de propiedades adecuados con el nombre de obj-component id para estar seguro de que las personalizaciones se mantendrán después de la actualización. Para obtener más información, consulte "Maintaining Custom Settings in XML Files" (Cómo mantener los ajustes personalizados en los archivos XML) en la *NetIQ Sentinel Administration Guide* (Guía de administración de NetIQ Sentinel).

4 **Si desea actualizar el dispositivo Sentinel**, haga clic en **Dispositivo** para lanzar WebYaST.

5 **Si desea actualizar un dispositivo de gestor de recopiladores o de motor de correlación**, especifique la URL del equipo del gestor de recopiladores o del motor de correlación utilizando el puerto 4984 para lanzar WebYaST como `https://<dirección_IP>:4984`, donde `<dirección_IP>` es la dirección IP del gestor de recopiladores o del motor de correlación. Lleve a cabo del Paso 6 al Paso 10.

6 (Condicional) Si aún no ha registrado el dispositivo para actualizaciones automáticas, hágalo ahora.

Para obtener más información, consulte la Sección 13.3.3, "Registro para recibir actualizaciones", en la página 87.

Si el dispositivo no está registrado, Sentinel muestra una advertencia en amarillo que indica que el dispositivo no está registrado.

7 Para comprobar si existen actualizaciones, haga clic en **Updates** (Actualizaciones).

Se muestran las actualizaciones disponibles.

8 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.

9 Reinicie el servicio Sentinel utilizando la interfaz basada en la Web.

Para obtener más información, consulte la Sección 13.4, "Inicio y detención del servidor mediante WebYaST", en la página 89.

10 (Condicional) Si Sentinel está instalado en un puerto personalizado, o si el gestor de recopiladores o el motor de correlación están en modo FIPS, ejecute el comando siguiente:

```
/opt/novell/sentinel/setup/configure.sh
```

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

12 Borre la caché de Java Web Start en los equipos cliente para utilizar la versión más reciente de las aplicaciones Sentinel.

La caché de Java Web Start se puede borrar con el comando `javaws -clearcache` o desde el Centro de control de Java. Para obtener más información, vaya al sitio http://www.java.com/es/download/help/plugin_cache.xml.

13 (Condicional) Si se ha actualizado la base de datos PostgreSQL a una versión importante (por ejemplo, de 8.0 a 9.0 o de 9.0 a 9.1), elimine los archivos PostgreSQL antiguos de la base de datos PostgreSQL. Para obtener información sobre si se ha actualizado la base de datos PostgreSQL, consulte las notas de la versión de Sentinel.

13a Cambie al usuario novell.

```
su novell
```

13b Busque en la carpeta `bin`:

```
cd /opt/novell/sentinel/3rdparty/postgresql/bin
```

13c Elimine todos los archivos postgreSQL antiguos mediante el siguiente comando:

```
./delete_old_cluster.sh
```

14 (Condicional) Si va a actualizar desde Sentinel 7.1.1 o una versión anterior, el instalador no migrará por defecto los datos de Inteligencia de seguridad (SI). Para migrar los datos de SI desde Sentinel 7.1.1 o una versión anterior, habilite manualmente la migración de datos de SI de la siguiente manera:

14a Cambie al usuario novell:

```
su novell
```

14b Abra el archivo `/etc/opt/novell/sentinel/config/server.xml`.

14c Añada la siguiente propiedad en la sección de componentes `BaseliningRuntime`:

```
<property name="baselining.migration.check">true</property>
```

14d Reinicie el servidor Sentinel.

25.3 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 la Sección 13.3.4, “Configuración del dispositivo con SMT”, en la página 88.

2. 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 Administration Guide (Guía de administración de NetIQ Sentinel)*.

3. (Condicional) Si ha personalizado los ajustes de configuración en los archivos `server.xml`, `collector_mgr.xml` o `correlation_engine.xml`, asegúrese de que ha creado los archivos de propiedades adecuados con el nombre de obj-component id para estar seguro de que las personalizaciones se mantendrán después de la actualización. Para obtener más información, consulte “Maintaining Custom Settings in XML Files” (Cómo mantener los ajustes personalizados en los archivos XML) en la *NetIQ Sentinel Administration Guide* (Guía de administración de NetIQ Sentinel).

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

5. Actualice el repositorio para la actualización:

   ```
   zypper ref -s
   ```

6. Compruebe si la aplicación está habilitada para la actualización:

   ```
   zypper lr
   ```

7. (Opcional) Compruebe las actualizaciones disponibles para la aplicación:

   ```
   zypper lu
   ```

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

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

9 Actualice la aplicación:

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

10 Reinicie el dispositivo.

```
rcsentinel restart
```

11 (Condicional) Si Sentinel está instalado en un puerto personalizado, o si el gestor de recopiladores o el motor de correlación están en modo FIPS, ejecute el comando siguiente:

```
/opt/novell/sentinel/setup/configure.sh
```

12 (Condicional) Para actualizar el gestor de recopiladores o el motor de correlación, siga del Paso 4 alPaso 11 .

26 Configuraciones posteriores a la actualización

En este capítulo se especifican las configuraciones que se deben realizar tras la actualización.

26.1 Adición del controlador JDBC DB2

Después de actualizar a Sentinel, añada el controlador JDBC correcto y configúrelo para la recopilación y sincronización de datos. Siga estos pasos para hacerlo:

1. Copie la versión correcta del controlador IBM DB2 JDBC (`db2jcc-*.jar`) para su versión de base de datos DB2 en la carpeta `/opt/novell/sentinel/lib`.
2. Asegúrese de definir la propiedad y los permisos necesarios para el archivo de controlador.
3. Configure este controlador para la recopilación de datos. Para obtener más información, consulte la documentación del conector de base de datos.

26.2 Configuración de las propiedades de federación de datos en la aplicación Sentinel

Siga este procedimiento tras actualizar la aplicación Sentinel, de modo que la federación de datos no muestre ningún error en el entorno si hay dos o más tarjetas NIC configuradas:

1. En el servidor del solicitante autorizado, añada la siguiente propiedad al archivo `/etc/opt/novell/sentinel/config/configuration.properties` de este modo:

   ```
   sentinel.distsearch.console.ip=<una de las direcciones IP del solicitante autorizado>
   ```

2. En el servidor de origen de datos, añada la siguiente propiedad al archivo `/etc/opt/novell/sentinel/config/configuration.properties` de este modo:

   ```
   sentinel.distsearch.target.ip=<una de las direcciones IP del origen de datos>
   ```

3. Reinicie Sentinel:

   ```
   rcsentinel restart
   ```

4. Entre en el servidor del solicitante autorizado y haga clic en Integración. Si el origen de datos que desea añadir ya existe, suprímalo y añádalo de nuevo con una de las direcciones IP que especificó en el paso 2.

   Del mismo modo, añada solicitantes autorizados utilizando las direcciones IP especificadas en el paso 1.

27 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, incluidos los paquetes de soluciones, se cargan con frecuencia en el sitio Web de módulos auxiliares (plug-ins) 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 Implantación de Sentinel para alta disponibilidad

Puede usar este apéndice para instalar NetIQ Sentinel 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. Para obtener más información sobre cómo implementar la alta disponibilidad y la recuperación tras fallos en el entorno Sentinel, póngase en contacto con el servicio de Asistencia técnica de NetIQ.

Nota: La configuración de alta disponibilidad (HA) solo se admite en el servidor Sentinel. Sin embargo, los gestores de recopiladores y los motores de correlación aún pueden comunicarse con el servidor Sentinel de alta disponibilidad.

28 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.

Para obtener más información acerca de la alta disponibilidad, consulte la SUSE High Availability Guide (Guía de alta disponibilidad de SUSE).

28.1 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 (HA) permiten a los encargados de implementarlas declarar dependencias entre los servicios que deben estar altamente disponibles, 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 o 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).

28.2 Almacenamiento compartido

Todos los clústeres de alta disponibilidad (HA) 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 y 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.

28.3 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.

28.4 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.

29 Requisitos del sistema

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

- ❒ **(Condicional) Para instalaciones de dispositivos de alta disponibilidad (HA)**, asegúrese de que el dispositivo HA de Sentinel tenga disponible una licencia válida. El dispositivo HA de Sentinel es un dispositivo ISO que incluye los siguientes paquetes:
  - Sistema operativo SUSE Linux Enterprise Server (SLES) 11 SP3
  - Paquete SUSE Linux Enterprise Server High Availability Extension (SLES HAE)
  - Software de Sentinel (incluido HA rpm)
- ❒ **(Condicional) Para las instalaciones tradicionales de HA**, asegúrese de que estén disponibles el instalador de Sentinel (archivo TAR) y la imagen ISO de SUSE Linux High Availability Extension (SLE HAE) con licencias válidas.
- ❒ **(Condicional) Si utiliza el sistema operativo SLES con kernel versión 3.0.101 o posterior**, debe cargar manualmente el controlador de vigilancia en el equipo. Para buscar el controlador de vigilancia adecuado para el hardware de su equipo, póngase en contacto con su proveedor de hardware. Para cargar el controlador de vigilancia, realice lo siguiente:
  1. En el indicador de comandos, ejecute el siguiente comando para cargar el controlador de vigilancia en la sesión actual:

     ```
     /sbin/modprobe -v --ignore-install <watchdog driver name>
     ```

  2. En el archivo `/etc/init.d/boot.local`, añada la siguiente línea para garantizar que el equipo cargue automáticamente el controlador de vigilancia cada vez que se arranque:

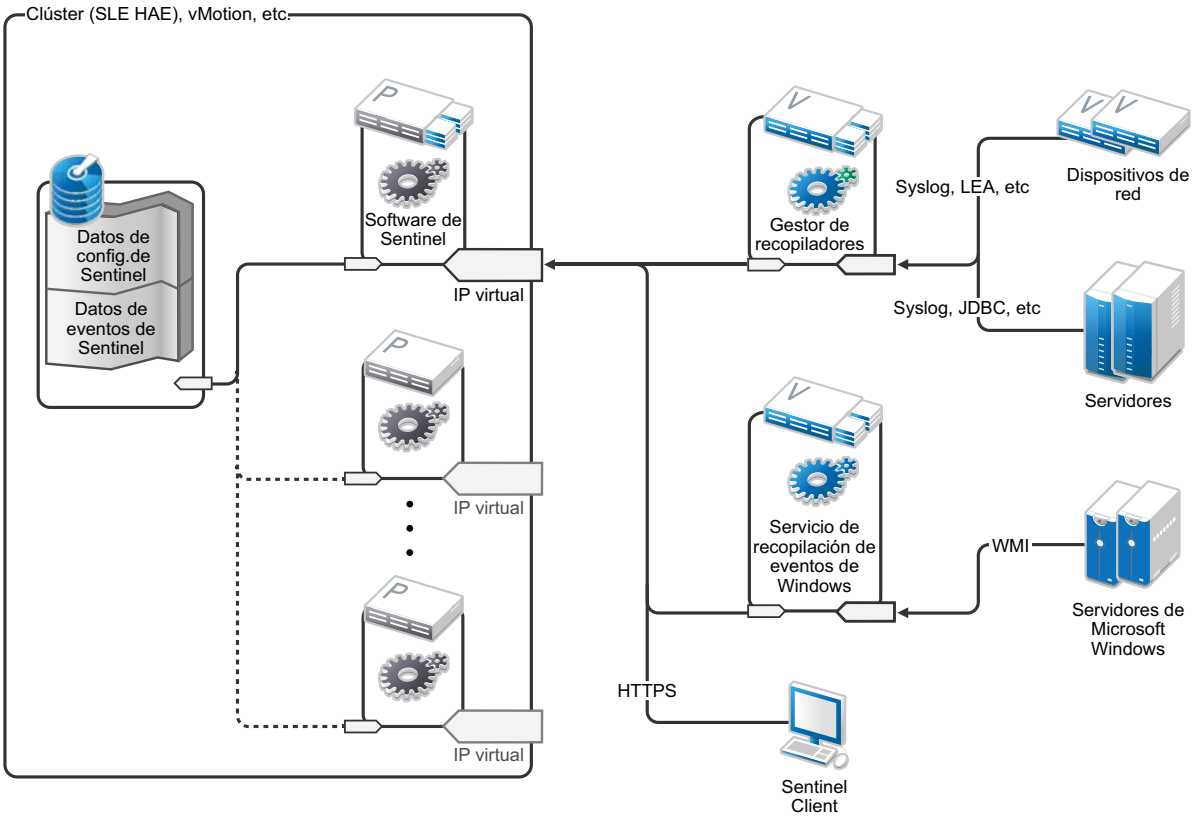
     ```
     /sbin/modprobe -v --ignore-install <watchdog driver name>
     ```
- ❒ Asegúrese de que cada nodo de clúster que alberga servicios de Sentinel cumpla los requisitos especificados en el Capítulo 5, “Cumplimiento de los requisitos del sistema”, en la página 39.
- ❒ Asegúrese de que haya espacio de almacenamiento compartido suficiente para los datos y la aplicación Sentinel.
- ❒ Asegúrese de utilizar una dirección IP virtual para los servicios que se pueda migrar de un nodo a otro al producirse el failover.
- ❒ Asegúrese de que el dispositivo de almacenamiento compartido cumpla los requisitos de características de tamaño y rendimiento especificados en el Capítulo 5, “Cumplimiento de los requisitos del sistema”, en la página 39. NetIQ recomienda una máquina virtual de SUSE Linux estándar configurada con destinos iSCSI como almacenamiento compartido.
- ❒ Asegúrese de tener como mínimo dos nodos de clúster que cumplan los requisitos de recursos para ejecutar Sentinel en el entorno del cliente. NetIQ recomienda dos máquinas virtuales de SUSE Linux.
- ❒ Asegúrese de crear un método de comunicación de los nodos del clúster con el almacenamiento compartido, como FibreChannel para una SAN. NetIQ recomienda una dirección IP dedicada para conectarse con el destino iSCSI.

- ❒ Asegúrese de tener una dirección IP virtual que se pueda migrar desde un nodo del clúster a otro para que sirva como dirección IP externa de Sentinel.
- ❒ Asegúrese de tener al menos una dirección IP por nodo del clúster para las comunicaciones internas del clúster. NetIQ recomienda una simple dirección IP de unidifusión, pero se prefiere multidifusión para los entornos de producción.

30 Instalación y configuración

En esta sección se proporcionan los pasos de instalación y configuración de Sentinel en un entorno de alta disponibilidad (HA).

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



30.1 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 Sentinel y los requisitos locales del cliente. Pruebe los sistemas para garantizar su funcionamiento y estabilidad adecuados.

Utilice la siguiente lista de verificación como guía para realizar la instalación y configuración inicial.

	Elementos de la lista de verificación
?	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 39 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 39 en función del número de eventos esperado y de las directivas de retención de datos del almacenamiento principal y secundario.
?	Si desea configurar cortafuegos en el sistema operativo para limitar el acceso a Sentinel y al clúster, consulte el Capítulo 8, “Puertos utilizados”, en la página 57 para obtener detalles sobre qué puertos deben estar disponibles dependiendo de la configuración local y de los orígenes que enviarán los datos de eventos.
?	Asegúrese de que todos los nodos del clúster tengan sincronizada la hora. Puede usar NTP o una tecnología similar para este propósito.
?	◆ El clúster requiere una resolución de nombre de host fiable. Introduzca todos los nombres de host del clúster interno en el archivo `/etc/hosts` a fin de garantizar la continuidad del clúster en caso de fallo del DNS. ◆ Asegúrese de no asignar un nombre de host a una dirección IP de retrobucle. ◆ Al configurar el nombre de host y el nombre de dominio durante la instalación del sistema operativo, deseleccione la opción**Assign Hostname to Loopback IP** (Asignar nombre de host a IP de retrobucle).

NetIQ recomienda la siguiente configuración:

- **(Condicional) Para instalaciones tradicionales de HA:**
  - Dos VM de nodo de clúster SUSE Linux 11 SP3.
  - (Condicional) Puede instalar X Windows si requiere configurar la interfaz gráfica de usuario. Defina los guiones de arranque para iniciarse sin X (nivel de ejecución 3), de manera que pueda iniciarlos solo cuando sea necesario.
- **(Condicional) Para instalaciones de dispositivos HA:** Dos máquinas virtuales de nodo en clúster basada en dispositivo ISO HA. Para obtener información sobre la instalación del dispositivo ISO HA, consulte la Sección 13.1.2, “Instalación de Sentinel”, en la página 82.
- Los nodos tendrán una NIC 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 SP3 VM configurada con destinos iSCSI Targets para almacenamiento compartido
  - (Condicional) Puede instalar X Windows si requiere configurar la interfaz gráfica de usuario. Defina los guiones de arranque para iniciarse sin X (nivel de ejecución 3), de manera que pueda iniciarlos solo 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. Por ejemplo, 172.16.0.3 (almacenamiento03).
  - 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.

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.

30.2 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, quizá necesite proporcionar conexiones físicas además de una configuración adicional. Sentinel utiliza este almacenamiento compartido para almacenar las bases de datos y los datos de eventos. Asegúrese de que el almacenamiento compartido tenga un tamaño adecuado en función del número de eventos previsto y de las directivas de retención de datos

Ejemplo de configuración de almacenamiento compartido

Una implementación típica podría usar una SAN rápida conectada mediante FibreChannel a todos los nodos del clúster, con una matriz RAID de gran tamaño para almacenar datos de eventos locales. Se podría utilizar una NAS independiente o un nodo iSCSI para el almacenamiento secundario más lento. Siempre que el nodo del clúster pueda montar el almacenamiento principal como dispositivo de bloques normal, podrá ser utilizado por la solución. El almacenamiento secundario también puede montarse como dispositivo de bloques, o bien podría ser un NFS o volumen CIFS.

Nota: NetIQ recomienda configurar el almacenamiento compartido y probar a montarlo en cada nodo del clúster. Sin embargo, la configuración del clúster manejará el montaje real del almacenamiento.

NetIQ recomienda usar el siguiente procedimiento para crear destinos de iSCSI alojados por una máquina virtual de SUSE Linux:

1. Conéctese a `storage03`, la máquina virtual que creó durante la Config inicial e inicie una sesión en la consola.
2. Utilice el comando `dd` para crear un archivo en blanco de cualquier tamaño para el almacenamiento principal de Sentinel:

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

3. Cree un archivo de 10 GB lleno de ceros copiados del archivo /`dev/zero pseudo-device`. Consulte la información o la página principal del comando `dd` para obtener información detallada de las opciones de la línea de comandos.

4 Repita los pasos 1 a 3 para crear un archivo para el almacenamiento secundario:

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

Nota: Para este ejemplo creó dos archivos con las mismas características de tamaño y rendimiento para representar los dos discos. Para una implementación de producción, puede crear el almacenamiento principal en una red SAN rápida y el almacenamiento secundario en un volumen iSCSI, NFS o CIFS más lento.

30.2.1 Configuración de destinos iSCSI

Configure los archivos `localdata` y `networkdata` como destinos iSCSI:

1 Ejecute YaST desde la línea de comandos (o 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 SP3.

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.

Nota: Este procedimiento 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.

30.2.2 Configuración de iniciadores iSCSI

Use el siguiente procedimiento para dar formato a los dispositivos:

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 de 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 SP3.
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 del destino iSCSI (10.0.0.3), seleccione **No Authentication** (Sin autenticación) y luego haga clic en **Next** (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 principal), 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 secundario. Esto debe dar lugar a una partición `/dev/sdc1` o disco formateado similar (denominado `/dev/<NETWORK1>` a continuación).
21. Salga de YaST.

22 **(Condicional) Si realiza una instalación tradicional de HA**, 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
```

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

23 (Condicional) Si realiza una instalación tradicional de HA, para desmontarla:

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

24 (Condicional) Para las instalaciones de dispositivos de alta disponibilidad, repita los pasos 1 a 15 para asegurarse de que cada nodo del clúster se pueda montar en el almacenamiento compartido local. Reemplace la IP del nodo del paso 5 por una IP diferente para cada nodo del clúster.

25 (Condicional) Para las instalaciones de dispositivos de alta disponibilidad, repita los pasos 1 a 15, 22 y 23 para asegurarse de que cada nodo del clúster se pueda montar en el almacenamiento compartido local. Reemplace la IP del nodo del paso 5 por una IP diferente para cada nodo del clúster.

30.3 Instalación de Sentinel

Hay dos opciones para instalar Sentinel: instalar cada uno de los componentes de Sentinel en el almacenamiento compartido usando la opción `--location` 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.

NetIQ recomienda instalar Sentinel en cada nodo del clúster que pueda alojarlo. Después de instalar Sentinel por primera vez, debe llevar a cabo una instalación completa, incluidos los archivos binarios de la aplicación, la configuración y todos los almacenes de datos. Para las instalaciones posteriores en otros nodos del clúster, solo instalará la aplicación. Los datos de Sentinel estarán disponibles una vez que haya montado el almacenamiento compartido.

30.3.1 Instalación del primer nodo

- “Instalación tradicional de HA” en la página 158
- “Instalación de un dispositivo HA de Sentinel” en la página 159

Instalación tradicional de HA

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
```

4 Ejecute la instalación estándar, configurando el producto como corresponda. El programa de instalación instala los binarios, las bases de datos y los archivos de configuración. El programa de instalación también configura las credenciales de entrada, los ajustes de configuración y los puertos de red.

5 Inicie Sentinel y pruebe las funciones básicas. Puede usar la dirección IP de nodo de clúster externa estándar para acceder al producto.

6 Apague Sentinel y desmonte el almacenamiento compartido mediante los siguientes comandos:

```
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 un dispositivo HA de Sentinel

El dispositivo HA de Sentinel incluye el software de Sentinel ya instalado y configurado. Para configurar el software Sentinel para HA, realice los siguientes pasos:

1 Conéctese a uno de los nodos de clúster (node01) y abra la ventana de la consola.

2 Acceda al directorio siguiente:

```
cd /opt/novell/sentinel/setup
```

3 Registre la configuración:

3a Ejecute el comando siguiente:

```
./configure.sh --record-unattended=/tmp/install.props --no-start
```

En este paso se registra la configuración en el archivo`install.props`, que se requiere para configurar los recursos del clúster mediante el guión `install-resources.sh`.

3b Especifique la opción para seleccionar el tipo Configuración de Sentinel.

3c Especifique `2` para introducir una nueva contraseña.

Si especifica `1`, el archivo `install.props` no almacena la contraseña.

4 Apague Sentinel utilizando el siguiente comando:

```
rcsentinel stop
```

Este paso eliminará los guiones de inicio automático de manera que el clúster pueda gestionar el producto.

```
insserv -r sentinel
```

5 Mueva la carpeta de datos de Sentinel al almacenamiento compartido utilizando los siguientes comandos. Este movimiento permite que los nodos utilicen la carpeta de datos de Sentinel a través del almacenamiento compartido.

```
mkdir -p /tmp/new
mount /dev/<SHARED1> /tmp/new
mv /var/opt/novell/sentinel /tmp/new
umount /tmp/new/
```

6 Verifique el desplazamiento de la carpeta de datos de Sentinel al almacenamiento compartido utilizando los siguientes comandos:

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

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

30.3.2 Instalación de nodos posteriores

- “Instalación tradicional de HA” en la página 160
- “Instalación de un dispositivo HA de Sentinel” en la página 160

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.

Instalación tradicional de HA

1 Conéctese a cada nodo del clúster adicional (node02) y abra una ventana de consola.

2 Ejecute los comandos siguientes:

```
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
```

```
insserv -r sentinel
```

Instalación de un dispositivo HA de Sentinel

1 Conéctese a cada nodo del clúster adicional (node02) y abra una ventana de consola.

2 Ejecute el comando siguiente:

```
insserv -r sentinel
```

3 Detenga los servicios de Sentinel.

```
rcsentinel stop
```

4 Elimine el directorio de Sentinel.

```
rm -rf /var/opt/novell/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.

30.4 Instalación del clúster

Debe instalar el software del clúster solo para instalaciones tradicionales de alta disponibilidad (HA). El dispositivo HA de Sentinel incluye el software de clúster y no requiere instalación manual.

NetIQ recomienda el siguiente procedimiento para configurar la extensión de alta disponibilidad de SUSE Linux con una superposición de Resource Agent específica de Sentinel:

1. Instale el software de clúster en cada nodo.
2. Registre cada nodo del clúster con el gestor de clústeres.
3. Verifique que cada nodo del clúster aparezca en la consola de gestión de clústeres.

   Nota: El OCF Resource Agent para Sentinel es un guión shell sencillo que ejecuta una variedad de comprobaciones para verificar si Sentinel es funcional. Si no utiliza el OCF Resource Agent para supervisar Sentinel, debe desarrollar una solución de supervisión similar para el entorno de clúster local. Para desarrollar una propia, revise el Resource Agent existente, almacenado en el archivo `Sentinelha.rpm` en el paquete de descarga de Sentinel.

4. Instale el software central SLE HAE de acuerdo con la Documentación de SLE HAE.Para obtener información sobre la instalación de productos complementarios de SLES, consulte la Guía de implantación.
5. Repita el paso 4 en todos los nodos del clúster. 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.
6. Instale un RPM adicional para proporcionar los Resource Agent de clúster adicionales específicos de Sentinel. El RPM puede encontrarse en el archivo `novell-Sentinelha-<versión_Sentinel>*.rpm` incluido en el paquete de descarga por defecto de Sentinel, que desempaquetó para instalar el producto.
7. En cada nodo del clúster, copie el archivo `novell-Sentinelha-<versión_Sentinel>*.rpm` en el directorio `/tmp` y luego ejecute los siguientes comandos:

```
cd /tmp
rpm -i novell-Sentinelha-<Sentinel_version>*.rpm
```

30.5 Configuración del clúster

Debe configurar el software del clúster para registrar cada nodo del clúster como miembro del clúster. Dentro del proceso de configuración, también puede configurar recursos de fencing y STONITH (Shoot The Other Node In The Head) a fin de garantizar la uniformidad en el clúster.

NetIQ recomienda el siguiente procedimiento para la configuración de clústeres:

Para esta solución, debe utilizar 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. Debe utilizar además un destino iSCSI configurado en la misma máquina virtual de SUSE Linux que alberga el almacenamiento compartido para que sirva como dispositivo SBD (Split Brain Detection) para fines de fencing.

Configuración de SBD

1. 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
   ```

2. Cree un archivo de 1 MB lleno de ceros copiado de`/dev/zero` pseudo-device.
3. Ejecute YaST desde la línea de comandos o la interfaz gráfica del usuario: `/sbin/yast`
4. Seleccione **Servicios de red** > **Destino iSCSI**.
5. Haga clic en **Destinos** y seleccione el destino existente.
6. Seleccione**Editar**. La interfaz del usuario presentará una lista de LUN (unidades) que están disponibles.
7. Seleccione **Añadir** para añadir un LUN nuevo.
8. Deje el número LUN 2. Busque en el cuadro de diálogo **Vía** y seleccione el archivo `/sbd` que ha creado.
9. 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.
10. 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). Asegúrese además de no asignar un nombre de host a una dirección IP de retrobucle.

Realice los siguientes pasos para 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), 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 **OK** 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 restart` 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 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), 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 **OK** (Aceptar) para salir de la herramienta del Iniciador de iSCSI.

7 Ejecute el comando siguiente: `sleha-join`

8 Introduzca la dirección IP del primer nodo del clúster.

(Condicional) Si el clúster no se inicia correctamente, realice los siguientes pasos:

1 Copie manualmente `/etc/corosync/corosync.conf` de `node01` a `node02`, o ejecute `csync2 -x -v`en el `nodo 01`, o bien configure manualmente el clúster en `node02` a través de YaST.

2 Ejecute `/etc/rc.d/openais start` en `node02`

(Condicional) Si el servicio `xinetd` no añade correctamente el nuevo servicio `csync2`, el guión no funcionará correctamente. El servicio `xinetd` 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 el comando`kill -HUP `cat /var/run/xinetd.init.pid` y luego vuelva a ejecutar el guión `sleha-join`.

3 Ejecute `crm_mon` en cada nodo del clúster para verificar que el clúster funcione correctamente. También puede usar "hawk", la consola Web, para verificar el clúster. El nombre de usuario por defecto es `hacluster` y la contraseña `linux`.

(Condicional) Dependiendo de su entorno, realice las siguientes tareas para modificar otros parámetros:

1 Para asegurarse de que un fallo en un nodo de un clúster formado por dos nodos no detenga inesperadamente todo el clúster, defina la opción global de clúster `no-quorum-policy` en `ignore`:

```
crm configure property no-quorum-policy=ignore
```

Nota: Si el clúster tiene más de dos nodos, no defina esta opción.

2 Para asegurarse de que el gestor de recursos permita a los recursos ejecutarse en su lugar y desplazarse, defina la opción global de clúster `default-resource-stickiness` en 1:

```
crm configure property default-resource-stickiness=1.
```

30.6 Configuración de recursos

Resource Agents se suministra 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 la base de datos PostgreSQL que almacena la configuración y los metadatos de eventos.

NetIQ recomienda la siguiente configuración de recursos:

NetIQ 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 usar el siguiente procedimiento de configuración para editar el guión según corresponda.

1 Conéctese al nodo original en el que se instaló Sentinel.

Nota: Debe ser el nodo en el que ejecutó la instalación completa de Sentinel.

2 Edite el guión para que aparezca de la siguiente manera, donde `<SHARED1>` es el volumen compartido que creó anteriormente:

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

cd /usr/lib/ocf/resource.d/novell

./install-resources.sh
```

3 (Condicional) Podría tener problemas con los nuevos recursos que aparecen en el clúster; ejecute `/etc/rc.d/openais restart` en node02 si experimenta este problema.

4 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.

5 Si su entorno varía con respecto a esta solución recomendada por NetIQ, puede editar el archivo `resources.cli` (en el mismo directorio) y modificar las definiciones primitivas desde aquí. Por ejemplo, la solución recomendada utiliza un simple recurso de Sistema de archivos; quizá desee usar un recurso cLVM que emplee más funciones de clúster.

6 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
```

7 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.

30.7 Configuración de almacenamiento secundario

Realice los siguientes pasos para configurar el almacenamiento secundario de manera que Sentinel pueda migrar particiones de eventos a otro almacenamiento menos costoso:

Nota: Este proceso es opcional y el almacenamiento secundario no necesita ser de alta disponibilidad de la misma forma que configuró el resto del sistema. Puede usar cualquier directorio, montado a partir de una SAN o no, un volumen NFS o CIFS.

1 En la consola Web de Sentinel, en la barra de menú de la parte superior, haga clic en **Almacenamiento**.

2 Seleccione **Configuración**.

3 Seleccione uno de los botones circulares de almacenamiento secundario no configurados.

NetIQ recomienda usar un destino iSCSI simple como ubicación de almacenamiento compartido en red, con prácticamente la misma configuración que el almacenamiento principal. En su entorno de producción, sus tecnologías de almacenamiento podrían ser diferentes.

Utilice el siguiente procedimiento para configurar el almacenamiento secundario para su uso en Sentinel:

Nota: Puesto que NetIQ recomienda usar un destino iSCSI para esta solución, el destino se montará como directorio para su uso como almacenamiento secundario. Debe configurar el montaje como recurso del sistema de archivos de forma similar a como se configuró el sistema de archivos de almacenamiento principal. Esto no se configuró automáticamente dentro del guión de instalación de recursos, ya que había otras variaciones posibles.

---

1. Revise los pasos anteriores para determinar qué partición se creó para su uso como almacenamiento secundario (`/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 consola o ejecute el comando:

   ```
   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` o `Hawk`) y asegúrese de que el almacenamiento secundario esté montado correctamente (utilice el comando `mount`).
5. Entre en la interfaz Web de Sentinel.
6. Seleccione **Storage** (Almacenamiento) y después **Configuration** (Configuración) y, a continuación, seleccione la **SAN (montada localmente**) en Almacenamiento secundario no configurado.
7. Introduzca la vía en la que se ha montado el almacenamiento secundario, por ejemplo `/var/opt/netdata`.

NetIQ recomienda usar 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.

31 Actualización de Sentinel con alta disponibilidad (HA)

Al actualizar Sentinel en un entorno HA, debe actualizar primero los nodos pasivos del clúster y luego actualizar el nodo de clúster activo.

31.1 Requisitos previos

- Descargue el programa de instalación más reciente del sitio Web de descargas de NetIQ.
- Si utiliza el sistema operativo SLES con kernel versión 3.0.101 o posterior, debe cargar manualmente el controlador de vigilancia en el equipo. Para buscar el controlador de vigilancia adecuado para el hardware de su equipo, póngase en contacto con su proveedor de hardware. Para cargar el controlador de vigilancia, realice lo siguiente:
  1. En el indicador de comandos, ejecute el siguiente comando para cargar el controlador de vigilancia en la sesión actual:

     ```
     /sbin/modprobe -v --ignore-install <watchdog driver name>
     ```

  2. Añada la siguiente línea al archivo `/etc/init.d/boot.local` para asegurarse de que el equipo cargue automáticamente el controlador de vigilancia durante cada inicio:

     ```
     /sbin/modprobe -v --ignore-install <watchdog driver name>
     ```

31.2 Actualización de una instalación tradicional de HA de Sentinel

1 Habilite el modo de mantenimiento en el clúster:

```
crm configure property maintenance-mode=true
```

El modo de mantenimiento le ayuda a evitar interrupciones en los recursos del clúster en ejecución durante la actualización de Sentinel. Este comando se puede ejecutar desde cualquier nodo del clúster.

2 Compruebe si el modo de mantenimiento está activo:

```
crm status
```

El estado de los recursos del clúster debería ser sin gestionar.

3 Actualice el nodo del clúster pasivo:

3a Detenga la pila del clúster:

```
rcopenais stop
```

Al detener la pila del clúster, se garantiza que los recursos del clúster sigan estando accesibles y se evitan las barreras de nodos.

3b Entre como usuario `root` en el servidor en el que desea actualizar Sentinel.

3c Extraiga los archivos de instalación del archivo tar:

```
tar xfz <install_filename>
```

3d Ejecute el comando siguiente en el directorio donde extrajo los archivos de instalación:

```
./install-sentinel --cluster-node
```

3e Cuando finalice la actualización, reinicie la pila del clúster:

```
rcopenais start
```

Repita el paso 3 para todos los nodos del clúster pasivos.

3f Elimine los guiones de inicio automático de manera que el clúster pueda gestionar el producto.

```
cd /
```

```
insserv -r sentinel
```

4 Actualice el nodo del clúster activo:

4a Realice una copia de seguridad de su configuración y luego cree una exportación de ESM.

Para obtener más información sobre la copia de seguridad de datos, consulte la sección "Backing Up and Restoring Data" (Copia de seguridad y restauración de datos) en la *NetIQ Sentinel Administration Guide (Guía de administración de NetIQ Sentinel 7.1)*.

4b Detenga la pila del clúster:

```
rcopenais stop
```

Al detener la pila del clúster, se garantiza que los recursos del clúster sigan estando accesibles y se evitan las barreras de nodos.

4c Entre como usuario `root` en el servidor en el que desea actualizar Sentinel.

4d Ejecute el siguiente comando para extraer los archivos de instalación del archivo tar:

```
tar xfz <install_filename>
```

4e Ejecute el comando siguiente en el directorio donde extrajo los archivos de instalación:

```
./install-sentinel
```

4f Cuando finalice la actualización, inicie la pila del clúster:

```
rcopenais start
```

4g Elimine los guiones de inicio automático de manera que el clúster pueda gestionar el producto.

```
cd /
```

```
insserv -r sentinel
```

4h Ejecute el siguiente comando para sincronizar cualquier cambio que se haya hecho en los archivos de configuración:

```
run csync2 -x -v
```

5 Inhabilite el modo de mantenimiento en el clúster:

```
crm configure property maintenance-mode=false
```

Este comando se puede ejecutar desde cualquier nodo del clúster.

6 Compruebe si el modo de mantenimiento está inactivo:

```
crm status
```

El estado de los recursos del clúster debería ser iniciado.

7 (Opcional) Compruebe si Sentinel se actualizó correctamente:

```
rcsentinel version
```

31.3 Actualización de una instalación de dispositivo HA de Sentinel

Puede actualizar una instalación de dispositivo de alta disponibilidad de Sentinel mediante el parche Zypper y también a través de WebYast.

- Sección 31.3.1, “Actualización del dispositivo de alta disponibilidad de Sentinel mediante Zypper”, en la página 169
- Sección 31.3.2, “Actualización del dispositivo de alta disponibilidad de Sentinel mediante WebYast”, en la página 171

31.3.1 Actualización del dispositivo de alta disponibilidad de Sentinel mediante Zypper

Debe registrar todos los nodos de dispositivo a través de WebYast antes de realizar la actualización. Para obtener más información, consulte la Sección 13.3.3, “Registro para recibir actualizaciones”, en la página 87. Si no registra el dispositivo, Sentinel mostrará una advertencia en amarillo.

1 Habilite el modo de mantenimiento en el clúster.

```
crm configure property maintenance-mode=true
```

El modo de mantenimiento le ayuda a evitar interrupciones en los recursos del clúster en ejecución durante la actualización del software de Sentinel. Este comando se puede ejecutar desde cualquier nodo del clúster.

2 Compruebe si el modo de mantenimiento está activo.

```
crm status
```

El estado de los recursos del clúster debería ser sin gestionar.

3 Actualice el nodo del clúster pasivo:

3a Descargue las actualizaciones del dispositivo HA de Sentinel.

```
zypper -v patch -d
```

Este comando descarga actualizaciones para los paquetes instalados en el dispositivo, incluido Sentinel a `/var/cache/zypp/packages`.

3b Detenga la pila del clúster.

```
rcopenais stop
```

Al detener la pila del clúster, se garantiza que los recursos del clúster sigan estando accesibles y se evitan las barreras de nodos.

3c Una vez descargadas las actualizaciones, instálelas utilizando el siguiente comando:

```
rpm -Uvh /var/cache/zypp/packages/sentinel_server_7000_x86_64-Updates/rpm/
noarch/*.rpm /var/cache/zypp/packages/sentinel_server_7000_x86_64-Updates/
rpm/x86_64/*.rpm /var/cache/zypp/packages/sentinel_server_7000_x86_64-
Updates/rpm/i586/*.rpm --excludepath=/var/opt/novell/
```

3d Ejecute el siguiente guión para llevar a cabo el proceso de actualización:

```
/var/adm/update-scripts/sentinel_server_ha_x86_64-update-<version>-
overlay_files.sh
```

3e Cuando finalice la actualización, reinicie la pila del clúster.

```
rcopenais start
```

Repita el paso 3 para todos los nodos pasivos del clúster.

4 Actualice el nodo del clúster activo:

4a Realice una copia de seguridad de su configuración y luego cree una exportación de ESM.

Para obtener más información sobre la copia de seguridad de los datos, consulte "Backing Up and Restoring Data" (Copia de seguridad y restauración de datos) en *NetIQ Sentinel Administration Guide (Guía de administración de NetIQ Sentinel)*.

4b Detenga la pila del clúster.

```
rcopenais stop
```

Al detener la pila del clúster, se garantiza que los recursos del clúster sigan estando accesibles y se evitan las barreras de nodos.

4c Entre en el dispositivo de Sentinel como administrador.

4d Para actualizar el dispositivo Sentinel, haga clic en **Dispositivo** para lanzar WebYaST.

4e Para comprobar si existen actualizaciones, haga clic en **Updates** (Actualizaciones).

4f Seleccione y aplique las actualizaciones.

Las actualizaciones pueden tardar unos minutos en finalizar. Una vez finalizada de forma satisfactoria la actualización, aparecerá 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.

4g Borre la memoria caché del navegador Web para ver la versión más reciente de Sentinel.

4h Cuando finalice la actualización, reinicie la pila del clúster.

```
rcopenais start
```

4i Ejecute el siguiente comando para sincronizar cualquier cambio que se haya hecho en los archivos de configuración:

```
run csync2 -x -v
```

5 Inhabilite el modo de mantenimiento en el clúster.

```
crm configure property maintenance-mode=false
```

Este comando se puede ejecutar desde cualquier nodo del clúster.

6 Compruebe si el modo de mantenimiento está inactivo.

```
crm status
```

El estado de los recursos del clúster debería ser iniciado.

7 (Opcional) Compruebe si Sentinel se actualizó correctamente:

```
rcsentinel version
```

31.3.2 Actualización del dispositivo de alta disponibilidad de Sentinel mediante WebYast

Debe registrar todos los nodos de dispositivo a través de WebYast antes de realizar la actualización. Para obtener más información, consulte la Sección 13.3.3, “Registro para recibir actualizaciones”, en la página 87. Si no registra el dispositivo, Sentinel mostrará una advertencia en amarillo.

1 Habilite el modo de mantenimiento en el clúster.

```
crm configure property maintenance-mode=true
```

El modo de mantenimiento le ayuda a evitar interrupciones en los recursos del clúster en ejecución durante la actualización del software de Sentinel. Este comando se puede ejecutar desde cualquier nodo del clúster.

2 Compruebe si el modo de mantenimiento está activo.

```
crm status
```

El estado de los recursos del clúster debería ser sin gestionar.

3 Actualice los nodos del clúster pasivos:

3a Detenga la pila del clúster.

```
rcopenais stop
```

Al detener la pila del clúster, se garantiza que los recursos del clúster sigan estando accesibles y se evitan las barreras de nodos.

3b Especifique la URL del nodo del clúster pasivo mediante el puerto 4984 para lanzar WebYaST como `https://<dirección_IP>:4984`, donde `<dirección_IP>` es la dirección IP del nodo del clúster pasivo. Entre en el dispositivo de Sentinel como administrador.

3c Para comprobar si existen actualizaciones, haga clic en **Updates** (Actualizaciones).

3d Seleccione y aplique las actualizaciones.

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

3e Cuando finalice la actualización, reinicie la pila del clúster.

```
rcopenais start
```

Repita el Paso 4 para todos los nodos del clúster pasivos.

4 Actualice el nodo del clúster activo:

4a Realice una copia de seguridad de su configuración y luego cree una exportación de ESM.

Para obtener más información sobre la copia de seguridad de los datos, consulte “Backing Up and Restoring Data” (Copia de seguridad y restauración de datos) en *NetIQ Sentinel Administration Guide (Guía de administración de NetIQ Sentinel)*.

4b Detenga la pila del clúster.

```
rcopenais stop
```

Al detener la pila del clúster, se garantiza que los recursos del clúster sigan estando accesibles y se evitan las barreras de nodos.

4c Entre en el dispositivo de Sentinel como administrador.

4d Para actualizar el dispositivo Sentinel, haga clic en **Dispositivo** para lanzar WebYaST.

4e Para comprobar si existen actualizaciones, haga clic en **Updates** (Actualizaciones).

4f Seleccione y aplique las actualizaciones.

Las actualizaciones pueden tardar unos minutos en finalizar. Una vez finalizada de forma satisfactoria la actualización, aparecerá 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.

4g Borre la memoria caché del navegador Web para ver la versión más reciente de Sentinel.

4h Cuando finalice la actualización, reinicie la pila del clúster.

```
rcopenais start
```

4i Ejecute el siguiente comando para sincronizar cualquier cambio que se haya hecho en los archivos de configuración:

```
run csync2 -x -v
```

5 Inhabilite el modo de mantenimiento en el clúster.

```
crm configure property maintenance-mode=false
```

Este comando se puede ejecutar desde cualquier nodo del clúster.

6 Compruebe si el modo de mantenimiento está inactivo.

```
crm status
```

El estado de los recursos del clúster debería ser iniciado.

7 (Opcional) Compruebe si Sentinel se actualizó correctamente:

```
rcsentinel version
```

32 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.

32.1 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 Administration Guide* (Guía de administración de NetIQ Sentinel) 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.

32.2 Recuperación

32.2.1 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.

32.2.2 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.

32.2.3 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 Administration Guide* (Guía de administración de NetIQ Sentinel) 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.

VII Apéndices

A Solución de problemas

En esta sección se enumeran los problemas que podrían ocurrir durante la instalación y las medidas para solucionar dichos problemas.

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

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

A.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.

A.3 La interfaz Web está en blanco en Internet Explorer después de entrar a la sesión

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 > 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**.

B Desinstalación

En este apéndice se proporciona información sobre la desinstalación de Sentinel y otras tareas posteriores a la desinstalación.

B.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.

B.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.

B.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.

B.2.2 Desinstalación del gestor de recopiladores y del motor de correlación

Siga los pasos indicados a continuación para desinstalar el gestor de recopiladores y el motor de correlación:

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

B.2.3 Desinstalación del gestor de recopiladores de NetFlow

Siga los pasos indicados a continuación para desinstalar el gestor de recopiladores de NetFlow:

1 Entre en el equipo del gestor de recopiladores de NetFlow.

Nota: Debe acceder con el mismo permiso de usuario que utilizó para instalar el gestor de recopiladores de NetFlow.

2 Cambie al directorio siguiente:

```
/opt/novell/sentinel/setup
```

3 Ejecute el comando siguiente:

```
./uninstall-sentinel
```

4 Introduzca `s` para desinstalar el gestor de recopiladores.

El guión detiene primero el servicio y luego lo desinstala por completo.

B.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.